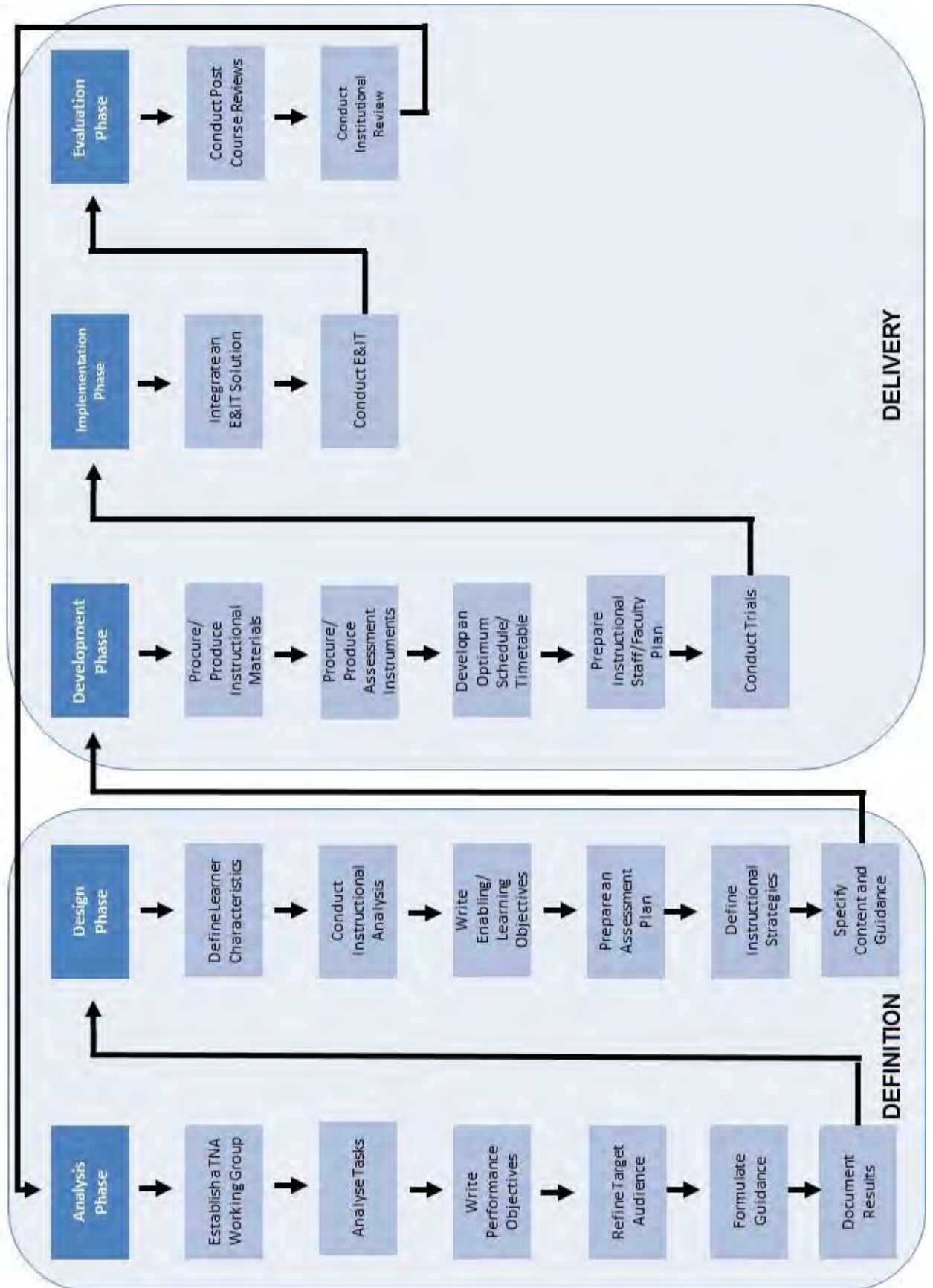


NATO Systems Approach to Training



**PERFORMANCE PROFICIENCY LEVELS AND KEY WORDS**

1. **Basic through to Master.** Proficiency levels provide a scale which defines a degree of competence (“expertise”) required in order to perform principle duties and tasks on the job within NATO. The duties and tasks are used to capture the performance gap while the proficiency level scale determines the depth of knowledge and skill that an E&IT solution is intended to target in order to resolve the performance gap<sup>73</sup>. Key action words are used to describe job performance and the action words are categorized based on broad functional areas. The levels of proficiency are based on a modified version of the generic skill descriptions used to augment NATO Occupation Codes. The levels of proficiency and related generic skill descriptors are as follows:

- a. Basic Level – Follow.
- b. Intermediate Level – Assist.
- c. Advance Level – Apply.
- d. Expert Level – Enable/Advisor.
- e. Master Level – Initiate/Shape/Influence.

2. **Institutional Leaders.** Enterprise level descriptors, that are indicative of institutional leadership, are not included in the proficiency levels listed above. Institutional leadership positions within NATO are responsible for setting the vision and strategy as well as inspiring and providing overall leadership. Institutional leaders have significant experience and substantial professional military education which prepares them for work within a complex global environment. Institutional leaders will make the critical decisions which shape and position the organization for future success and this will also integrate a long-term view. Key Leader Engagement events, conferences, seminars and related senior level planning forums are frequently conducted within NATO in large part to keep a broad audience aware of evolving issues and their implications. These forums, combined with expert and master level briefs, provide institutional leaders with the essential foundation to make informed decisions and achieve institutional leadership. An exception to this comes in the form of formalized foundation training which is provided to a specific a Training Audience supporting an operational mission and/or exercise.

---

<sup>73</sup> The generic eight skill levels outlined in NATO Occupation Codes – Generic Skill Descriptions have been modified given five levels of proficiency are adequate to identify and define NATO E&T requirements. The eight levels are outlined in Appendix C to NATO Occupational Area Codes, Version 4.0, published 14 December 2007 by NATO C3 Agency.

<b>Job Performance Proficiency Levels</b>	
<b>100</b>	<p><b>Basic Level (Follow)</b> <b>Skill &amp; Knowledge</b></p> <p>The level of proficiency required to successfully perform a routine task or series of task elements (e.g, a step in a sequence of actions) in a structured environment with supervision. Is expected to seek guidance in unexpected conditions. This requires remembering information including facts, terms, concepts, principles as well as the processes and procedures defining job requirements.</p> <p><b>Functional Area:</b> Support.</p>
<b>200</b>	<p><b>Intermediate Level (Assist)</b> <b>Skill &amp; Knowledge</b></p> <p>The level of proficiency required to become functional and successfully perform a series of tasks independently with minimal oversight. Uses discretion in resolving problems and may plan and schedule work within short timeframes. This requires interpreting information, constructing meaning and the comprehension of facts, terms, concepts, and principles as well as the processes and procedures essential to enable understanding and accomplishing job requirements.</p> <p><b>Functional Area:</b> Communication, Administrative, Technical and Finance.</p>
<b>300</b>	<p><b>Advance Level (Apply)</b> <b>Skill &amp; Knowledge</b></p> <p>The level of proficiency required to interpret direction and guidance and successfully plan and complete tasks independently as well as potentially monitoring the work of others. Uses discretion to resolve increasingly more complex problems. This requires the application of concepts, principles processes and procedures in both non-routine (new) and concrete situations as well as executing, implementing and carrying out processes and procedures to satisfy job requirements.</p> <p><b>Functional Area:</b> Communication, Administrative, Technical, Finance, Teaching, Creating and Leadership/ Management.</p>
<b>400</b>	<p><b>Expert Level (Enable/Advisor)</b> <b>Skill &amp; Knowledge</b></p> <p>The level of proficiency required to execute a broad range of complex professional and/or technical work activities leveraging prior education, training and practical experience; this includes maintaining an awareness of developing trends within the wider occupational field, analytical thinking and providing institutional leaders discipline and/or inter-disciplinary related advice. This level requires setting work objectives and assigning task and the ability to deconstruct and integrate concepts, principles and procedures to support reasoning and as well as the application of a systematic approach to solving non-routine and ill-defined problems.</p> <p><b>Functional Area:</b> Communication, Administrative, Technical, Finance, Teaching, Creating, Research and Leadership/ Management.</p>
<b>500</b>	<p><b>Master Level (Initiate, Shape and Influence)</b> <b>Skills &amp; Knowledge</b></p> <p>The level of proficiency required to execute highly complex work activities covering, technical, financial and quality aspects for a functional area. Leverages considerable education, training and extensive practical experience to advise commanders as well as exert significant influence over policy development and contribute to the formulation of strategy and organizational objectives. Decisions made impact the functional area of the enterprise. Able to assess and evaluate risks and understand the implications of new concepts, technologies and trends. This requires adapting concepts and principles as well as processes and procedures to support critical, asymmetric thinking and reasoning potentially leading research efforts and building knowledge, theory and alternative approaches within a recognized body of knowledge.</p> <p><b>Functional Area:</b> Communication, Administrative, Technical, Finance, Teaching, Creating, Research and Leadership/ Management.</p>

**Job Performance - Key Word Areas & Indicators**

The following key action words are used to describe job task performance. Key word indicators are categorized into nine broad functional areas. Additional functional areas may be created as deemed necessary. Most of the key words provided below are common across multiple proficiency levels; however, some of the functional areas are more applicable to specific proficiency levels. Example: "Support" key words are applicable to the Basic Proficiency Level while other functional areas (e.g., Research) are more applicable to higher levels.

Support	Administrative	Communication	Creating	Finance	Teaching	Technical	Leadership / Management	Research
aid assist contribute help out observe support	approve arrange catalogue classify collect compile contract dispatch distribute execute file generate implement operate organize prepare process purchase record retrieve screen specify staff systematize tabulate transcribe validate	address advise arbitrate arrange articulate author clarify collaborate compose condense confer consult contact convey convince correspond counsel debate develop direct display draft edit enlist formulate incorporate influence inform interpret judge lecture market mediate moderate negotiate persuade promote propose publicize reconcile recruit staff suggest translate synthesize write	adapt assemble build combine compose conceptualize create customize design develop devise direct establish fabricate fashion illustrate improve initiate institute integrate introduce invent originate pioneer plan prepare revitalize select shape solve	administer adjust allocate analyse appraise assess audit balance budget calculate classify compile compute commit conserve contract correct determine develop estimate forecast inspect manage market measure monitor plan predict project purchase quantify reconcile reduce research verify	adapt advise clarify coach convey coordinate demystify develop enable encourage evaluate facilitate familiarize guide inform instruct mentor persuade stimulate train	activate administer advise aim calculate calibrate construct debug design devise diagnose dismantle dispose dissect dissemble engineer engage estimate extract fasten inspect install maintain manipulate manufacture map measure mend mix monitor move navigate operate overhaul plot predict programme propose rehabilitate remodel repair replace restore sight solve survey target test verify	activate administer advise allocate analyse approve appraise assign authorize chair control coordinate delegate develop direct enforce enhance establish estimate evaluate execute formulate guide improve implement initiate inspire judge lead mentor modernize motivate organize oversee plan preside prioritize produce recommend resolve review schedule select spearhead structure supervise transform	analyse assess attain clarify collect conduct critique diagnose detect determine evaluate examine experiment extract formulate identify inspect interpret interview invent investigate locate measure organize research review select solve study summarize survey systematize test verify

**TASK STATEMENT – TRACKING MATRIX**

1. **The Task Statement.** Tracking Matrix is a locally generated form used to provide an audit trail confirming the source of performance statements used in the development of Performance Objectives. The matrix ensures performance statements remain linked, and accounted for, relative to the E&IT solutions that are created. Documenting the performance statements provides a DH with an audit trail to the TRA Report and it is helpful in maintaining discipline alignment. NEW performance statements generated by the TNA WG would become a subject for discussion during an Annual Discipline Conference. The matrix is also useful for capturing TRA performance statements which the TNA WG determines do NOT require training.

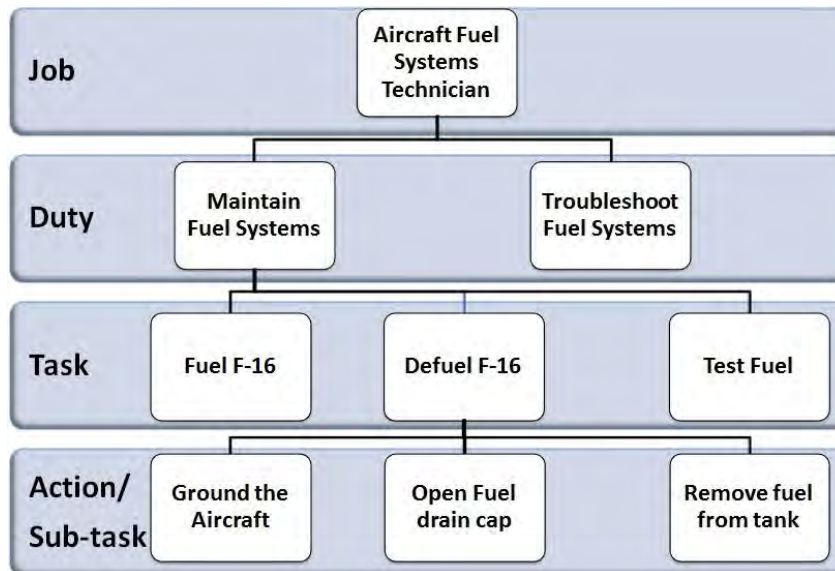
2. The following is an example how the Performance Statements may be tracked. This example uses sample statements and is NOT complete.

<p align="center"><b>TRA Report</b> <b>Performance/Task Statement Tracking Matrix</b></p> <p><b>Instructions.</b> Assign a Tacking Number to each performance statement in the TRA Report that is intended to be part of the E&amp;IT solution. The Tracking Number is generated by the TNA WG. Associate the Tracking Number to the Source Details for this statement from within the TRA Report (meaning identify the line number or paragraph in the TRA Report). Performance statement proficiency is indicated in the TRA Report or otherwise assigned by the TNA WG.</p>						
#	Source	Source Details (para #)	Assigned Tracking Number	Performance (Task) Statement	Proficiency	No Train *
1	TRA	3	T001	<i>Insert TRA Report statement here</i>		
2						
..						
10	TRA	3.1	T010	<b>Deliver preventive health services</b>	3	
..						
21	NEW	WG	T210	<b>Interpret communicable disease directives and policy</b>	3	
..						
25	TRA	3.2	T220	<b>Implement communicable disease protocols</b>	3	
..						
31	TRA	3.3	-	<b>Inject Immunizations</b>	3	*
32	TRA	3.4	-	<b>Decode syringe sizes</b>	2	*

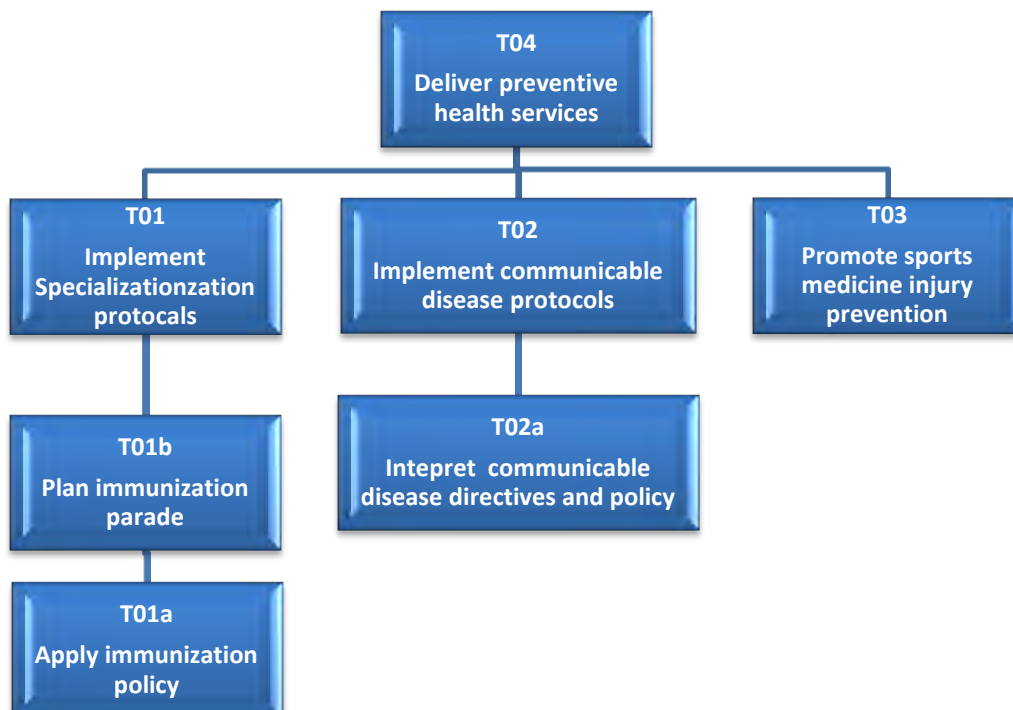
**TASK ANALYSIS**

The following are example task analysis dependency diagrams. These highlight hierarchical and procedural relationships. Tasks stem from a specific job and duty areas.

**Example 1: Maintain Fuels Systems**



**Example 2: Preventative Medicine**



## PERFORMANCE OBJECTIVES

### INTRODUCTION

1. POs specify, in precise terms, what an individual must be able to do in terms of job performance and how well. The following will:
  - a. Describe the three parts to a Performance Objective (PO).
  - b. Provide guidance to support the development of POs.
  - c. Include example POs. The example POs provide additional considerations to include in a final product.
2. A PO includes:
  - a. A performance statement which is a clear, concise and precise statement representing a logical and complete part of the job function (a duty area) which is observable and measurable.
  - b. Conditions statement which describe the situation, context, in which the performance is accomplished.
  - c. Standards describe how, and how well, performance must be completed. Standards specify a definite level of achievement and provide the clear and specific criterion defining the required degree of proficiency.

### PERFORMANCE STATEMENTS

3. Performance statements can eliminate the subjective interpretations and ambiguity of what is to be accomplished. The **performance statement** is the first element of a PO and represents a balance of clarity and brevity while capturing multiple tasks often associated with a duty area. The performance statement is ideally a single sentence with one key (action) word, an object for the action word and any necessary qualifiers. The following conventions apply:
  - a. **Clarity.** Represent actual and specific job performance. Also, avoid the use of technical and/or occupational jargon.
  - b. **Brevity.** Limit verbosity by not exceeding what is sufficient for follow-on activities.
  - c. **Flexibility.** The task should be adaptable enough to meet minor and evolving work criteria.

d. **Limit the Task Statement to One Key (Action) Word or Verb.** At times, two action words may seem necessary; however, one of the two action words is often a supporting action. The superior action should be used in the task statement because it signifies the “end”. The additional supporting elements will get defined during the development of E&IT solutions. At this point the focus is job performance:

(1) **Example 1: Analyse and Identify = Identify.** One must first “Analyse” in order to “Identify,” therefore “Analyse” is the supporting action. “Identify” is the superior task.

(2) **Example 2: “Assemble and Disassemble”.** These action words are frequently together in the same task statement. In most cases, the first step in assembling is disassembling. Therefore, the job task is to assemble. Occasionally disassembly is performed independently of assembly and task procedure is inherently separate. In this situation “assemble and disassemble” are two separate and discrete job tasks.

e. **Avoid Expressing Ambiguity and Value Judgements.** The key is to express what tasks are accomplished on-the-job, not how and/or how well tasks must be completed (e.g., effectively Identify Tactical Intelligence Factors) or degree (e.g., thoroughly Identify Tactical Intelligence Factors). The proficiency of a task completion is stated in operational policy/doctrine manuals and associated training publications.

f. **Avoid Expressing how Job Tasks are Achieved.** Focus on the outcome of work.

(1) **Example.** An Intelligence Operator must first “Analyse Tactical Intelligence Data” in order to “Identify Tactical Intelligence Factors.” The act of “identification” demonstrates that analysis has occurred. In this situation, “analysis” is the most prominent skill based supporting activity that enables the identification of tactical intelligence factors. The most significant means to the outcome of a task (such as analysis) are almost always skill and/or applied knowledge based supporting activities (e.g. operating machines and tools, analysing sources of information, methods employed, steps of a procedure, and cognitive and/or psychomotor skills). These activities support and/or enable the completion of a genuine job task.

4. Constructing performance statements involves the application of principles described previously. Table J-1 reviews examples and provides further guidance to consider when developing performance statements.

Performance Statements	
Example	Comment
<b>Obtain a venepuncture blood specimen</b>	Good example: <ul style="list-style-type: none"> <li>• Identifies the task being done with one action word – <b><i>Obtain.</i></b></li> <li>• Identifies the object (what) is being acted upon – <b><i>a blood specimen.</i></b></li> </ul>



Performance Statements	
Example	Comment
	<ul style="list-style-type: none"> <li>Qualifies the action. When necessary, uses a qualifier to distinguish a means, methodology or approach - <b>venepuncture</b>.</li> </ul> <p><b>Note:</b> qualifiers are only necessary when there are alternative means, method or approach for conducting the action.</p>
<p><b>Plan, organize and control travel expenses</b></p>	<p>More than one key (action) word – a performance statement is not intended to be a list of sub-tasks.</p> <p><b>Revision:</b> Control travel expenses</p>
<p><b>Understand the laws of armed conflict</b></p>	<p>Focus on job performance action words <b>not</b> the enabling supporting elements (knowledge). Knowledge requirements <b>may</b> be reflected in the <i>Standard</i>; however, knowledge elements are often better left to defining/writing the Enabling/Learning Objectives during the Design Phase.</p> <p><b>Suggestion:</b> When constructing performance statements focus on the outcome - “Why” is the knowledge required; <b>understanding the laws of armed conflict</b> is required in order to?</p> <p><b>Revised:</b> <i>Advise Commanders on the laws of armed conflict*</i>.</p> <p>* <b>Note:</b> Context is important and in some situations a performance statement which is “knowledge based” maybe better reflected in the standard. Example: “<i>Apply the laws of armed conflict</i>” is not an ideal performance statement given “Why” is the knowledge required is still not clear. A clear understanding of the Target Audience is also essential in order to correctly describe desire performance</p>
<p><b>The student will learn forklift operations by studying the operator's manual</b></p>	<p>This is not a performance statement. This refers to a learning activity not a performance outcome to be achieved as a result of E&amp;IT. Observing the student reading provides no measure of whether learning has occurred and there is no clear result or product from the specified action.</p> <p><b>Revised:</b></p> <ul style="list-style-type: none"> <li><i>Load trailers (given a forklift)</i></li> <li><i>Operate a forklift (move pallets and cargo, maintain situational awareness, adhere to safety procedure outlines in reference X)</i></li> </ul> <p>* <b>Note:</b> Desired performance must be placed into the proper context hence the conditions and standard statements become important and in many situations provide qualifiers for the performance statement.</p>

Table J-1 Performance Statement - Guidance

**CONDITION STATEMENTS**

5. Conditions reflect the work situation as accurately as possible, but include only those factors that influence job performance. Conditions address what is normally provided as well as what might otherwise not be unavailable. An example is as follows:

- a. Tools and equipment.
- b. Job aids, reference manual and specific material.
- c. Supervision.
- d. Assistance.
- e. Environment (day, night, temperature extremes).
- f. Special physical, psychological demands (confined work space, noise).

**STANDARDS STATEMENTS**

6. Standards reflect the product, process or combination of both which describe how and how well the task(s) must be satisfied. Standards are based on actual job requirements and included specific criterion which are either based in doctrine or references and reflect the performance outcome to be judged. The measure generally addresses as following:

a. **Speed.** The speed of performing a task can have a critical effect on the outcome of a mission: a rapid response can contribute to the success of a mission but too slow a response may spell disaster. In other settings, work must be done quickly in order to avoid backlogs and to promote overall unit effectiveness. Standards of speed must reflect operational requirements as in the following examples:

- (1) Rescue hitch must be tied within 3 minutes or.
- (2) Rate of typing is 45 words per minute.

b. **Soundness of Judgement.** If the judgement or decision required in performing a task is such that successful performance will be seriously affected by a wrong decision, it must be shown as a measure in the standard. For example, "patient is referred to medical officer when seriousness of ailment is beyond the medical assistant's own authorized scope of care". If the end product is the decision itself, then the standard must directly measure the adequacy of the member's analytical or decision-making ability.

c. **Measures of Accuracy.** Accuracy measures are often used as a means for describing a desired level of proficiency (tunes a radio to achieve a signal strength within 5% of maximum range) or physical dimensions of a finished product as well as a maximum error rate.

d. **Completeness.** This can describe the steps to be followed in a process as well as their specific sequence.

**EXAMPLE - PERFORMANCE OBJECTIVES**

7. **The following are Example POs.** POs are included within Part 2 of the Course Control Document II - Course Proposal. Additional paragraphs may be included to further amplify the requirements described within the first three paragraphs of the PO. Note: Each PO should include the proficiency level indicator.

**PERFORMANCE OBJECTIVE - EXAMPLE 1: CBRN WARNING AND REPORTING SPECIALIST**

<b>Performance Objective 001</b>	
1.	<b>Performance Statement:</b> Predict nuclear hazard fallout.
2.	<b>Conditions:</b>
a.	Given:
	(1) Map scale 1:250,000
	(2) ATP-45(E) - Warning and Reporting Hazard Prediction CBRN Incident Operators Manual
	(3) Weather information including a wind message and forecast
3.	<b>Standard:</b> Interpret the intelligence provided and select an appropriate course of action in order to produce a simplified estimate of the yield within an accuracy of 10% by interpreting the Basic Wind Message and constructing a wind vector plot.
4.	<b>Proficiency Level:</b> 400

**PERFORMANCE OBJECTIVE - EXAMPLE 2: COOK**

<b>Performance Objective 002</b>	
1.	<b>Performance Statement:</b> Prepare Breakfast Meal Items
2.	<b>Conditions:</b>
	a. Given:
	(1) References, recipes and written instructions;
	(2) Food supplies;
	(3) Equipped cooking establishment and materials;
	(4) Portion Size standards;
	(5) Personal protective equipment;
	(6) Food Services clothing;
	(7) Cooking establishment; and
	(8) Minimal supervision.
3.	<b>Standard:</b> Adhering to the principles of teamwork, cost awareness, economy of resources, hygiene, sanitation, safety and security procedures and environmental regulations, the Cook shall prepare the breakfast meal items by:
	a. Adhering to food safety regulations in accordance with (IAW) Reference P 269 chap 7 (Hygiene and Sanitation);
	b. Preparing Breakfast IAW P 269 with specific attention to:
	(1) recipe fundamentals;
	(2) ten principles of cooking; and
	(3) proper weights, measures and conversion within an accuracy of 5%.
	c. Preparing food and beverage breakfast items from raw ingredients IAW Reference P 269 or commercial mixes as per instructions, to include;
	(1) hot and cold cereals;
	(2) eggs (any style);
	(3) pancakes;
	(4) French toast;
	(5) Preparing Crepes and Cooking Crepes;
	(6) starches (beans, potatoes);
	(7) vegetables;
	(8) fruits; and
	(9) Breakfast meat product.
4.	<b>Proficiency Level:</b> 300
5.	<b>Reference.</b> Publication (P) 269 - Food Preparation and the Professional Chef, (2011) Culinary Institute of America

**PERFORMANCE OBJECTIVE - EXAMPLE 3: EMERGENCY FIRST AID****Performance Objective 003**

1. **Performance Statement.** Administer First Aid.
2. **Conditions:**
  - a. **Given:**
    - (1) casualty, and
    - (2) emergency first aid kit.
  - b. **Denied:** references; and
  - c. **Environment:** Under any condition.
3. **Standard.** In accordance with casualty directive, administer First Aid to include:
  - a. Initiating emergency scene management within five seconds of discovering a casualty and applying first aid protocols as the situation dictates and as determined through the conduct of
    - (1) a scene survey,
    - (2) a primary survey,
    - (3) a secondary survey; and
    - (4) ongoing casualty care;
  - b. treating shock, unconsciousness and fainting;
  - c. applying direct and indirect methods of adult artificial respiration;
  - d. initiating adult choking procedures;
  - e. treating severe bleeding;
  - f. applying single rescuer adult CPR;
  - g. conducting child and infant resuscitation;
  - h. applying proper care for injuries to:
    - (1) bones,
    - (2) joints and muscles,
    - (3) the head and eyes,
    - (4) spinal and pelvic areas, and
    - (5) chest area;
  - i. Dressing wounds, to include:
    - (1) penetrating injuries, and
    - (2) burns; and
  - j. stabilising diabetic emergencies, seizures and convulsions, asthmatic attack and allergic reactions.

4. **Proficiency Level:** 300
5. **References.** *A list of publications and manuals applicable to this PO.*
6. **TRA Cross Reference.** *A list of the TRA performance statement numbers which were captured during the task analysis and which are used here to provide an audit trail to the TRA statements.*
7. **Limitations.** *Additional considerations which may affect the development of the E&IT solution, including student assessment considerations. Example: The ETF providing this training does not have the resources to test the “any condition” requirement stated in para 2c. Actual performance will be in a classroom setting with full light and low light to simulate different degrees of difficulty.*
8. **Other Remarks.** *Additional considerations.*

## **COURSE CONTROL DOCUMENT I – CONTROL FORM**

The Control Form is a coversheet to a Course Proposal. This is the basis of agreement for moving forward and formalizing an E&IT solution within a specific ETF. The coversheet is specific to a course and along with the Course Proposal initiates a course within the NATO Education Training Opportunities Catalogue (ETOC). The Control Form identifies the specific stakeholders concerned with managing a discipline and the definition and delivery of E&IT solutions. When applicable the supporting area (a sub-category within a discipline) is identified. Areas are captured within the ETOC. The sign offs may include an External Course OPR, should the ETF require expert support which is external to the ETF. The Control Form may also include various sign offs internal to the ETF. The Control Form may be adapted to meet the needs of the originator (the ETF) with additional sign offs. All NATO selected and approved E&IT solutions, including those which are already developed and in place, require a Control Form. An example Control Form is enclosed. Technical support is available at: [eitephelp@act.nato.int](mailto:eitephelp@act.nato.int).

COURSE CONTROL DOCUMENT I – CONTROL FORM				
<input type="checkbox"/> <i>New Course</i> <input type="checkbox"/> <i>Revision</i> → <i>Brief Description</i>		<i>COURSE TITLE</i>		
<i>Discipline</i>		<i>Area (if applicable)</i>		<i>ETOC Course Code (if applicable)</i>
#	Activity	Unit Name	Acknowledgement	Date
1	<i>ETF Officer of Primary Responsibility (OPR): Responsible for the E&amp;IT solution within the ETF.</i>  <i>Enclose:                      CCD II – Course Proposal (or an equivalent).</i>	ETF	<i>Signature:</i>  <i>Name:</i>  <i>Rank:</i>  <i>Position:</i>	DD/MM/YY
2	<i>ETF Command - Endorsement. ETF leadership intent to support NATO and implement a proposed or modified E&amp;IT solution.</i>	ETF	<i>Signature:</i>  <i>Name:</i>  <i>Rank:</i>  <i>Position:</i>	DD/MM/YY
3	<i>External Course OPR. This endorsement is ONLY included when the ETF responsible for the SAT Delivery Stage requires support from the NCS during the Implementation Phase.</i>  <input type="checkbox"/> <i>Not Required(NR)*</i>  <i>* NR return requires ETF Command acknowledgement</i>	RA Representative	<i>Signature:</i>  <i>Name:</i>  <i>Rank:</i>  <i>Position:</i>	DD/MM/YY
4	<i>Department Head. Acknowledges the proposed E&amp;IT solution is in alignment with the discipline TRA Report. The new E&amp;IT solution will be activated as "Listed" within the ETOC until CCD III is uploaded.</i>  <i>Note: The DH is responsible and accountable for ensuring CCD I is produced; however, this is completed in close coordination with an ETF.</i>	DH	<i>Signature:</i>  <i>Name:</i>  <i>Rank:</i>  <i>Position:</i>	DD/MM/YY



**COURSE CONTROL DOCUMENT – II: COURSE PROPOSAL**

The Course Proposal provides the foundation for an E&IT solution and includes enough detail to identify where and how the solution fits within the discipline landscape. The Course Proposal, along with the coversheet (Course Control Document – I) is entered into the NATO Education Training Opportunities Catalogue (ETOC) by the responsible Education and Training Facility (ETF) to initiate a course.

<b>COURSE CONTROL DOCUMENT II - COURSE PROPOSAL</b>	
<b>COURSE TITLE:</b>	<b>CODE:</b>
<p><b>1. <u>PART- 1</u>: COURSE REQUIREMENT</b></p> <p><b>a. Requirement:</b> <i>The rationale (need) for the creation or otherwise modification of a course. This addresses the initial tasking to address a performance gap along with the background and history which served as the basis for creating a course.</i></p> <p><b>b. Aim:</b> <i>Provides the overall intent of the E&amp;IT.</i></p> <p><b>c. Security Classification:</b> <i>Identifies the security clearance required for the course.</i></p> <p><b>d. Target Audience:</b> <i>A brief description confirming the intended audience specifying who is eligible to enrol on the course. The details further identify the rank level, language proficiency and other assumed prerequisites.</i></p> <p style="padding-left: 40px;">(1) <b>Rank Level.</b></p> <p style="padding-left: 40px;">(2) <b>Language Proficiency.</b></p> <p><b>e. Training Strategy:</b> <i>A brief description concerning how the E&amp;IT requirement will likely be resolved including an estimate of the duration for a course or other alternative intervention.</i></p> <p><b>f. Estimated Number of Students per year:</b> <i>An estimate of the demand from the NCS, NFS, NATO Nations, Partners and others that may potentially require this course on an annual basis. The RA is expected to capture the potential NCS/NFS demand while MPD should capture partner nation demand.</i></p> <p><b>g. Depth of Knowledge:</b> <i>An estimate of the depth of knowledge to be achieved through the course. This is the extrapolated from the highest proficiency level assigned to the Performance Objectives.</i></p>	

<b>COURSE CONTROL DOCUMENT II - COURSE PROPOSAL</b>	
<b>COURSE TITLE:</b>	<b>CODE:</b>
<p><b>2. <u>PART- 2</u>: PERFORMANCE OBJECTIVES (POs)</b></p> <p><i>Details each of the intended outcomes to be addressed through an E&amp;IT solution, includes a performance statement (essential task), the conditions and prescribed standard to be achieved.</i></p> <p><b>PO 1:</b></p> <ol style="list-style-type: none"> <li>1. <b>Performance Statement.</b> <i>A clear, concise and precise statement representing a logical and complete part of the job function, which is observable and measurable.</i></li> <li>2. <b>Conditions:</b> <i>Conditions provide context and describe the situation, under which the performance must be completed.</i></li> <li>3. <b>Standards.</b> <i>The Standards describe how and how well performance must be completed.</i></li> <li>4. <b>Proficiency Level.</b> <i>Specifies a level (100-500) which broadly defines and captures the degree of competence or "expertise" to be achieved on the job.</i></li> </ol> <p><b>PO 2:</b></p> <ol style="list-style-type: none"> <li>1. <b>Performance Statement.</b> <i>A clear, concise and precise statement representing a logical and complete part of the job function, which is observable and measurable.</i></li> <li>2. <b>Conditions:</b> <i>Conditions provide context and describe the situation, under which the performance must be completed.</i></li> <li>3. <b>Standards.</b> <i>The Standards describe how and how well performance must be completed.</i></li> <li>4. <b>Proficiency Level.</b> <i>Specifies a level (100-500) which broadly defines and captures the degree of competence or "expertise" to be achieved on the job.</i></li> </ol>	

## LEARNING DOMAINS

### LEVELS OF LEARNING

1. Learning domains are classification schemes developed by educational theorists to support the development of instruction and guide student evaluation<sup>74</sup>. The initial work in this area was published in the 1950's and has continued to evolve<sup>75</sup>. There are three specific domains and within each there is a hierarchy, commonly referred to as a taxonomy, which reflects the progressive levels of learning. The learning of the lower levels enables progress into the higher levels of the taxonomy. The learning domains are aligned with the knowledge, skill and attitudinal elements that define a performance gap. The three domains are as follows:

a. **Cognitive Domain (the Knowledge Elements).** The cognitive domain addresses mental skills and intellectual abilities that progress from remembering and the recall or recognition of specific facts through to evaluating and creating new knowledge. The cognitive domain involves the processing of information (storing, recalling and interpreting) and its subsequent application or use. The cognitive domain aligns with the knowledge elements supporting tasks. The knowledge elements include the theoretical and practical understanding of subject matter required to effectively accomplish a step, task, or series of tasks.

b. **Psychomotor Domain (the skills elements).** The psychomotor domain addresses coordination, dexterity, manipulation, strength, speed as well as actions which demonstrate fine motor skills, including the use of precision instruments or tools. The levels within the psychomotor domain reflect a progression from observation and imitation through to mastery and adapting of learned skills. The psychomotor domain is aligned with physical skills and addresses the performance of tasks. Skills-based learning consists of an organized and coordinated pattern of mental and/or physical activity that becomes more precise through repetition and practice.

c. **Affective Domain (the attitude elements).** The affective domain addresses emotions and in particular beliefs, feelings and convictions which underlie behaviour and motivates action. The affective domain is aligned with attitude and, in general, relates to a pre-disposition to behave in certain ways. Attitude is believed to be developed over time and is shaped by an environment and experiences. Outcomes within the affective domain tend to be the most difficult to articulate. The learning within the affective domain is often integrated with events which support the cognitive and psychomotor domain.

---

<sup>74</sup> A complete list of references which are the basis for the learning domains are provided at the end of this section.

<sup>75</sup> More recent research has resulted in the development of alternative versions of the Psychomotor Domain as well as subtle adjustments to the classification levels within the Cognitive Domain.

Cognitive Domain	
Levels	Examples and Key Words
<p><b>1</b></p> <p><b>Knowledge/Remember:</b> The ability to recall of facts, terms, concepts, principles and the procedures previously learned material.</p>	<p><b>Examples:</b></p> <ul style="list-style-type: none"> <li>Recite a policy,</li> <li>List safety rules.</li> </ul> <p><b>Key Words:</b> arrange, define, duplicate, identify, label, list, mark, match, name, order, recall, recite, reproduce, recognize, reproduce, select, state.</p>
<p><b>2</b></p> <p><b>Comprehension/Understand:</b> The ability to interpret information, construct meaning and understand facts, terms, concepts, principles and procedures.</p>	<p><b>Examples:</b></p> <ul style="list-style-type: none"> <li>Summarize the principles of war.</li> <li>Explain debugging a computer system.</li> </ul> <p><b>Key Words:</b> allocate, arrange, categorize, classify, convert, , distinguish, estimate, extend, explain, extrapolate, group, illustrate, infer, interpret, label, match, paraphrase, predict, reiterate, report, restate, review, reword, rewrite, select, separate, summarize, theorize, translate.</p>
<p><b>3</b></p> <p><b>Application:</b> The ability to use concepts, principles and procedures in both new and concrete situations</p>	<p><b>Examples:</b></p> <ul style="list-style-type: none"> <li>Calculate the sonar range.</li> <li>Construct a job interview guide.</li> </ul> <p><b>Key Words:</b> apply, associate, administer, apply, calculate, change, classify, compute, compare, conduct, contrast, control, construct, discover, examine, execute, employ, establish, examine, illustrate, identify, implement, initiate, interpret, manipulate, modify, operate, perform, predict, prepare, produce, relate, respond, show, solve.</p>
<p><b>4</b></p> <p><b>Analysis:</b> The ability to deconstruct concepts, principles and procedures to support analytical thinking and reasoning skills; includes the examination of information, making inferences and finding evidence to support generalizations.</p>	<p><b>Examples:</b></p> <ul style="list-style-type: none"> <li>Breakdown a financial balance sheet</li> <li>Troubleshoot a piece of equipment</li> </ul> <p><b>Key Words:</b> analyse, breakdown, catalogue, compare, condense, contrast, deconstruct, derive, design, determine, diagram, differentiate, discriminate, distinguish, divide, examine, experiment, explain, extrapolate, graph, infer, interpret, modify, measure, outline, plan, plot, predict, produce, project, quantify, resolve, revise, relate, separate, summarize, search, solve, test, troubleshoot.</p>
<p><b>5</b></p> <p><b>Synthesis/Build:</b> The ability to rearrange, adapt and integrate ideas. Putting elements/ parts together to form new patterns or structures. The emphasis is creating and building knowledge based on new ideas and creative thinking, including developing new/unique structures, systems, models and approaches and creating new meaning,</p>	<p><b>Examples:</b></p> <ul style="list-style-type: none"> <li>Formulate an Op Order</li> <li>Compile a business plan</li> </ul> <p><b>Key Words:</b> analyse, appraise, arrange, assemble, build, calculate, categorize, collect, combine, compare, compile, compose, construct, create, design derive, develop, devise, encrypt, estimate, evaluate, format, formulate generate, measure, modify, originate, outline, organize, plan, produce, propose, rearrange, reconstruct, reframe, relate, reorganize, revise, rewrite, route, summarize, write.</p>
<p><b>6</b></p> <p><b>Evaluation/Assess:</b> The ability to make judgements about the value of ideas or materials this includes critical thinking and assessing viability</p>	<p><b>Examples:</b></p> <ul style="list-style-type: none"> <li>Select the most effective solution</li> <li>Defend a proposal</li> </ul> <p><b>Key Words:</b> appraise, assess, compare, conclude, contrast, criticise, critique, decide, defend, describe, diagnose, discriminate, evaluates, explain, interpret, judge, justify, rank, recommend, relate, summarize, support, validate.</p>

<b>Psychomotor Domain<sup>76</sup></b>	
<b>Domain Level</b>	<b>Examples and Key Words</b>
<p><b>1</b></p> <p><b>Perception:</b> The ability to use sensory cues to guide motor activity.</p>	<p><b>Key Words:</b> describe, detect differentiate, distinguish, identify, isolate, recognize, relate, select, sketch</p>
<p><b>2</b></p> <p><b>Set/ Readiness:</b> Readiness to act includes mental, physical, and emotional pre-requisites. These three sets are dispositions that predetermine a person's response to different situations (sometimes called mindsets)</p>	<p><b>Key Words:</b> adhere, display, explain, state.</p>
<p><b>3</b></p> <p><b>Guided Response/Imitation</b> The early stages in learning a skill that includes imitation and potentially trial and error. Adequacy of performance is achieved by practicing.</p>	<p><b>Key Words:</b> adhere, arrange, assemble, build, construct, copy, dismantle, display, dissect, fasten, fix, follow, grind, heat, imitate, manipulate, measure, mend, prepare, react, repeat, replicate reproduce, responds, trace, try.</p>
<p><b>4</b></p> <p><b>Mechanism/Manipulation:</b> This is the intermediate stage in learning a complex physical or mental skill. Learned responses have become habitual and the movements can be performed with some confidence and proficiency</p>	<p><b>Key Words:</b> assemble, build, calibrate, construct, dismantle, fasten, grind, heat, manipulate, measure, mend, mix, organize, shape, sketch.</p>
<p><b>5</b></p> <p><b>Complex Overt Response/Precision:</b> Performing a skill with a high degree of precision Performance involves complex action.</p>	<p><b>Key Words:</b> assemble, build, calibrate, complete, construct, control, demonstrate, dismantle, display, dissect, execute fasten, fix, grind, heat, manipulate, measure, mend, mix, organize, perfect, sketch, show.</p> <p><b>NOTE:</b> The Key Words are the same as Mechanism, but will have qualifying adverbs or adjectives that indicate that the performance is quicker, better, more accurate,</p>
<p><b>6</b></p> <p><b>Adaptation/Articulation:</b> Skills are well developed and can be modified and combined to adapt and integrate to satisfy a non-standard tasks and situations.</p>	<p><b>Key Words:</b> Adapt, adjust, alter, arrange, assault, combine, composes, construct, coordinate, create, design, develop, estimate, formulate, integrate, invent, modify, rearrange, reorganize, revises, solve, troubleshoot,</p>
<p><b>7</b></p> <p><b>Origination/Naturalization:</b> Creating new approaches to fit a particular situation or specific problem. Learning outcomes emphasize creativity based upon highly developed skills which are second-nature and natural, without needing to think much about it.</p>	<p><b>Key Words:</b> arrange, build, combine, compose, construct, create, design, initiate, make, originate.</p>

<sup>76</sup> The Psychomotor Domain, as presented here, is a hybrid of the models proposed by Simpson (1972) and Dave (1970). Details are provided in the reference list at the end of this section,

<b>Affective Domain</b>	
<b>Domain Level</b>	<b>Examples and Key Words</b>
<p><b>1</b></p> <p><b>Receiving (Perception):</b>                      Aware of an attitude, behaviour, or value but not yet ready to act on the situation.</p>	<p><b>Examples:</b> Listen to others opinions</p> <p><b>Key Words:</b> Accept, ask, choose, describe, follow, give, hold, identify, locate, name, point to, select, sit, erects, reply, use.</p>
<p><b>2</b></p> <p><b>Responding (Interpreting):</b>                      Active participation on the part of the learners. Attends and reacts to a particular phenomenon. Learning outcomes may emphasize compliance in responding, willingness to respond, or satisfaction in responding (motivation).</p>	<p><b>Examples:</b> Participates in discussions.</p> <p><b>Key Words:</b> Answer, assist, aid, complete, comply, conform, cooperate, discuss, examine, greet, help, label, obey, perform, practice, present, read, recite, report, respond, select, tell, write</p>
<p><b>3</b></p> <p><b>Valuing:</b>                      The worth or value a person attaches to a particular object, phenomenon, or behaviour. This ranges from simple acceptance to the more complex state of commitment. Valuing is based on the internalisation of a set of specified values, while clues to these values are expressed in the learner's overt behaviour and are often identifiable.</p>	<p><b>Examples:</b> Propose plans to social improvement and follows through with commitment. Informs management on matters that one feels strongly about.</p> <p><b>Key Words:</b> Accept, complete, defend, demonstrate, devote, differentiate, explain, follow, form, initiate, invite, join, justify, propose, pursue, read, report, seek, select, share, study, work.</p>
<p><b>4</b></p> <p><b>Organization:</b>                      Internalisation of values and beliefs. Organizes values into priorities by contrasting different values, resolving conflicts between them, and creating a unique value system. The emphasis is on comparing, relating, and synthesising values.</p>	<p><b>Examples:</b> Recognizes the need for balance between freedom and responsible behaviour.</p> <p><b>Key Words:</b> Adhere, alter, arrange, codify, combine, compare, complete, defend, discriminate, display, explain, formulate, generalize, identify, integrate, modify, order, organize, prepare, relate.</p>
<p><b>5</b></p> <p><b>Internalising Values:</b>                      Has a value system that controls their behaviour. The behaviour is pervasive, consistent, predictable, and most importantly, characteristic of the learner. Instructional objectives are concerned with the student's general patterns of adjustment (personal, social, emotional).</p>	<p><b>Examples:</b>                      Cooperates in group activities (displays teamwork). Displays a professional commitment to ethical practice on a daily basis.</p> <p><b>Key Words:</b> Act, discriminate, display, influence, internalize, listen, modify, perform, practice, propose, qualifies, question, revise, serve, solve, verify.</p>

## References

2. The following references were used and adapted in order to produce the learning domain taxonomies.

a. **Cognitive Domain**

Bloom, B.S. (Ed.). Engelhart, M.D., Furst, E.J., Hill, W.H., Krathwohl, D.R. (1956). *Taxonomy of Educational Objectives, Handbook I: The Cognitive Domain*. New York: David McKay Co Inc.

Anderson, L.W., & Krathwohl (Eds.). (2001). *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives*. New York: Longman.

b. **Psychomotor Domain**

Simpson E.J. (1972). *The Classification of Educational Objectives in the Psychomotor Domain*. Washington, DC: Gryphon House.

Dave, R.H. (1970). Psychomotor levels in *Developing and Writing Behavioural Objectives*, pp.20-21. R.J. Armstrong, ed. Tucson, Arizona: Educational Innovators Press.

c. **Affective Domain**

Krathwohl, D.R., Bloom, B.S., Masia, B.B. (1973). *Taxonomy of Educational Objectives, the Classification of Educational Goals. Handbook II: Affective Domain*. New York: David McKay Co., Inc

**ENABLING/LEARNING OBJECTIVES - EXAMPLE****COURSE CONTROL DOCUMENT III - PROGRAMME OF CLASSES****Code:****Title: Geo-Spatial Intelligence Analyst****PO 12:** Interpret Object-Oriented GPS data files.**ELO 012.01:**

1. **Performance:** Describe general geodesy principles
2. **Conditions:** Given:
  - a. Orders;
  - b. ADP and ancillary equipment;
  - c. Current software and GIS extensions; and
  - d. GPS data sets.
3. **Standards:** Explain general geodesy by:
  - a. Identifying the basic terms and concepts for geodesy;
  - b. Explaining the earth's dimensions;
  - c. Describing positioning techniques; and
  - d. Explaining projections.
4. **Assessment:** 30 question multiple choice theory test.
5. **Instructional Strategy:**

<b>Content</b>	<b>Method &amp; Time</b>		<b>References</b>
<b>Identify geodesy terms and concepts</b>	Lecture	50 min	A: Chap 1, Page 5-7
TP1 Introduce the concept of geodesy			
TP2 Define of Geodesy;			
TP3 Explain Pythagoras theory and the use to measure the circumference of the earth			
TP4 Eratosthenes theory used to measure the circumference of the earth.			
<b>Explain the earth's dimensions</b>	Lecture	100 min	A: Chap 2, Page 29-35
TP1 Explain the shape of the earth;			
TP2 Explain Measurement Parameters			
TP3 Define Ellipsoids, Geoids and Spheroids.			
<b>Describe horizontal positioning techniques</b>	Lecture	100 min	A: Chap 4, Page 49-71
TP 1 Outline horizontal and vertical Positioning on the Earth's surface;			
TP2 2D and 3D Cartesian Coordinate System			
TP3 Types of Horizontal Positioning;			



Content	Method & Time		References
TP4 Polar coordinates, Azimuth, and Bearing Direction Coordinates;			
TP5 True, Grid, and Magnetic North;			
TP6 Curvilinear Coordinate System			
TP7 Time (hours-min-sec)			
TP8 Triangulation, Trilateration, and Traversing; and.			
TP9 Explain the earth's dimensions			
<b>Describe vertical positioning</b>	Lecture	100 min	A: Chap 5, Page 36-45
TP1 Explain Vertical Positioning on the earth's surface			
TP2 Identify 4 Types of Vertical Positioning			
TP3 Describe precise levelling, trigonometric measurement, barometric and echo sounding			
TP4 Outline Trigonometric Height Measurement			
TP5 2D and 3D Cartesian Coordinate System			
<b>Explain projections</b>	Lecture	100 min	A: Chap 4, Page 49-71
TP1 Identify projection characteristics: area, shape, direction, scale;			
TP2 Differentiate projection characteristics: area, shape, direction, scale;			
TP3 Identify types of projections azimuthal, conic, cylindrical;			
TP4 Differentiate projection characteristics: azimuthal, conic, cylindrical;			
TP5 Explain Point of Light Origin (orthographic, stereographic, sinusoidal, mercator, globular).			
<b>Geodesy Test</b>	Test	70 min	
<b>Geodesy Debrief</b>	Debrief	30 min	
<b>Total Time:</b>		550 min	

**6. Depth of Knowledge: 200**

**7. References:** A. Kaula, M. (2000). Theory of Satellite Geodesy: Applications of Satellites To Geodesy.

**8. Limitations:**

**9. Resources:**

- a. White board;
- b. Globe; and
- c. Projection System
- d. Student Handout – Geodesy Backgrounder - Handout

## **DEPTH OF KNOWLEDGE – PERFORMANCE PROFICIENCY MATRIX**

1. Depth of Knowledge (DoK) refers to the level of learning to be achieved as a result of an E&IT solution. DoK is an inclusive term addressing both the Cognitive Domain (Knowledge elements) and the Psychomotor Domain (skill elements)<sup>77</sup>. The DoK - level of learning is based on job proficiency skill and knowledge requirements and the enclosed matrix aligns job performance proficiency levels with DoK levels of learning.

2. The matrix is a tool that supports the design and development of E&IT solutions. The matrix is also useful for providing a preliminary assessment of the fit between an existing E&IT solution and a NATO E&IT requirement. During the design and development of E&IT solutions the DoK matrix is used to:

- a. Develop Enabling/Learning Objectives (ELOs) at the appropriate level of learning and in alignment with Performance Objectives (POs).
- b. Identify and select instructional methods.
- c. Guide student assessment and preparing an assessment plan.

---

<sup>77</sup> Affective Domain – attitudinal elements are integrated with cognitive and psychomotor learning and as result are part of the criteria and behavioural traits captured within the standards of the applicable ELOs.

Job Performance Outcomes		Enabling/Learning Outcomes	
Job/Function Proficiency Level		Levels of Learning - Depth of Knowledge(and skill) Descriptors-	Learning Key Word Indicators
100	<b>Basic Level - (Follow)</b> <b>Skill &amp; Knowledge</b> The level of proficiency required to successfully perform a routine task or series of task elements (e.g, a step in a sequence of actions) in a structured environment with supervision. Is expected to seek guidance in unexpected conditions. This requires remembering information including facts, terms, concepts, principles as well as the processes and procedures defining job requirements.	<b>100</b> <b>Psychomotor:</b> <b>Perceptions, Readiness &amp; Guided Response</b> This involves the readiness to act, observing and imitating prescribed and defined actions and processes. Includes the use of sensory cues and establishing the mental, physical, and emotional prerequisites to skills development.	adhere adhere, arrange, assemble, dismantle, detect, display, fasten, follow, grind, heat, identify, imitate, measure, mend, prepare, recognize, repeat, replicate, reproduce, responds, select, sketch, trace,
		<b>Cognitive:</b> <b>Remembering explicit knowledge</b> Enable an individual to recall elements and details of structure or process and recognize or identify specific information.	arrange, define, duplicate, identify, label, list, mark, match, name, order, recall, recite, reproduce, recognize, reproduce, select, state.
200	<b>Intermediate Level (Assist)</b> <b>Skill &amp; Knowledge</b> The level of proficiency required to become functional and successfully perform a series of tasks independently with minimal oversight. Uses discretion in resolving problems and may plan and schedule work within short timeframes. This requires interpreting information, constructing meaning and the comprehension of facts, terms, concepts, and principles as well as the processes and procedures essential to enable understanding and accomplishing job requirements.	<b>200</b> <b>Psychomotor:</b> <b>Mechanism/Manipulation</b> The intermediate stage in learning a complex skill. Learned responses achieve functional proficiency and become habitual and can be performed with some confidence and proficiency.	assemble, build, calibrate, construct, dismantle, fasten, grind, heat, manipulate, measure, mend, mix, organize, shape, sketch.
		<b>Cognitive:</b> <b>Comprehending/Understanding:</b> Enable an individual to interpret information; construct meaning and comprehend facts, terms, concepts, principles and procedures.	arrange, categorize, classify, convert, distinguish, estimate, explain, extrapolate, group, illustrate, label, match, paraphrase, predict, reiterate, restate, reword, rewrite, report, select, separate, summarize, translate.

Job Performance Outcomes		Enabling/Learning Outcomes	
Job/Function Proficiency Level		Levels of Learning - Depth of Knowledge(and skill) Descriptors-	Learning Key Word Indicators
300	<b>Advance Level (Apply)</b> <b>Skill &amp; Knowledge</b> The level of proficiency required to interpret direction and guidance and successfully plan and complete tasks independently as well as potentially monitoring the work of others. Uses discretion to resolve increasingly complex problems. This requires the application of concepts, principles processes and procedures in both non-routine, new, and concrete situations as well as executing, implementing and carrying out processes and procedures to satisfy job requirements.	<b>300 Psychomotor:</b> <b>Complex response/Precision</b> Performing skills with a high degree of precision. Performance involves complex action.	assemble, build, calibrate, construct, control, dismantle, display, dissect, execute fasten, fix, grind, heat, manipulate, measure, mend, mix, organize, perfect, sketch.
		<b>300 Cognitive:</b> <b>Applying</b> Enable an individual to use concepts, principles and procedures in both new and concrete situations – put theory into practice.	administer, apply, calculate, change, compute, construct, examine, execute, employ, identify, implement, manipulate, modify, operate, perform, predict, prepare, produce, relate, respond, show, solve.
400	<b>Expert Level (Enable/Advisor)</b> <b>Skill &amp; Knowledge</b> The level of proficiency required executing a broad range of complex professional and/or technical work activities leveraging prior education, training and practical experience; this includes maintaining an awareness of developing trends within the wider occupational field, analytical thinking and providing institutional leaders discipline and/or inter-disciplinary related advice. This level requires setting work objectives and assigning task and the ability to deconstruct and integrate concepts, principles and procedures to support reasoning and as well as the application of a systematic approach to solving non-routine and ill-defined problems.	<b>400 Psychomotor:</b> <b>Adaptation</b> Skills are well developed and can be modified and combined to adapt and integrate to satisfy a non-standard tasks and situations.	adapt, adjust, alter, arrange, assault, assess, combine, composes, construct, coordinate, create, create, design, develop, estimate, formulate, integrate, invent, modify, master, manage, rearrange, reorganize, revises, specify, solve, troubleshoot, varies.
		<b>400 Cognitive:</b> <b>Analysing</b> Enable an individual to deconstruct concepts, principles and procedures to support analytical thinking and reasoning; includes the examination of information, making inferences and finding evidence to support generalizations.	analyse, break down, compare, condense, contrast, deconstruct, design, diagram, differentiate, discriminate, distinguish, divide, experiment, extrapolate, graph, infer, interpret, modify, measure, plan, plot, predict, produce, project, quantify, resolve, revise, search, solve, test, troubleshoot.

Job Performance Outcomes		Enabling/Learning Outcomes	
Job/Function Proficiency Level		Levels of Learning - Depth of Knowledge(and skill) Descriptors-	Learning Key Word Indicators
500	<p><b>Master Level (Initiate, Shape and Influence) Skills &amp; Knowledge</b></p> <p>The level of proficiency required to execute highly complex work activities covering, technical, financial and quality aspects for a functional area. Leverages considerable education, training and extensive practical experience to advise commanders as well as exert significant influence over policy development and contribute to the formulation of strategy and organizational objectives. Decisions made impact the functional area of the enterprise. Able to assess and evaluate risks and understand the implications of new concepts, technologies and trends. This requires adapting concepts and principles as well as processes and procedures to support critical, asymmetric thinking and reasoning potentially leading research efforts and building knowledge, theory and alternative approaches within a recognized body of knowledge.</p>	<p><b>Psychomotor: Originate</b></p> <p>Creating new approaches to resolve problems and challenging situations. Learning outcomes emphasize creativity based upon highly developed skills which are second-nature and natural, without needing to think much about it.</p>	<p>arrange, build, combine, compose, construct, create, design, initiate, make, originate.</p>
		<p><b>500 Cognitive: Assessing/Building/Creating</b></p> <p>Adapting and integrating concepts, principles and procedures to create and build knowledge, theory and alternative approaches. Enables higher order thinking and reasoning and includes the examination of information, making inferences and formulating solutions.</p>	<p>appraise, assemble, assess, build, categorize, combine, compile, compose, conclude, construct, contrast, create, critique, defend, design, derive develop, devise, diagnose, discriminate, encrypt, estimate, evaluate, formulate generate, hypothesize, integrate, interpret, invent, investigate, judge, justify, measure, modify, outline, originate, organize, plan, predict, propose, rank, rearrange, recommend, reconstruct, reframe, revise, rewrite, summarize, validate, war game, write.</p>

**METHODS OF INSTRUCTION**

1. The following tables describe suggested methods of instruction in terms of their definition, application and suggested techniques for instructors. A summary concerning the use of coaching is also provided at the conclusion of the Annex. The methods of instruction are as follows:

- a. Behaviour Modelling.
- b. Case Study.
- c. Demonstration and Performance.
- d. Field Trip.
- e. Gaming.
- f. Guided Discussion.
- g. Interactive Lecture.
- h. Panel Discussion.
- i. Peer Learning.
- j. Problem-based Learning (Small Group – Syndicate Work).
- k. Role Play.
- l. Self-Study.
- m. Simulation (including In-basket Exercise, Serious Gaming).
- n. Study Assignment.
- o. Tutorial.

<b>Behaviour Modelling</b>	
<b>Definition</b>	Behaviour modelling is a form of demonstration and it generally captured as part of the Demonstration/Performance method. Behaviour modelling is used during a demonstration to achieve attitudinal elements including the development of interpersonal skills. This method allows the learner to see the desired behaviours or skills first hand. Learners acquire new behaviours by observing live or video models and then rehearsing (practicing) the behaviours. Behaviour modelling is usually employed with smaller groups, as each learner must rehearse the behaviour as part of the learning process.
<b>Application</b>	<p>The instructor introduces the lesson by describing the what, why, when and where of the topic. The instructor describes the skill in question and then models both effective and ineffective behaviours verifying that learners have clearly understood the procedures, before moving on. Next, the instructor provides learners with a video or live presentation that sets the job context and models effective and ineffective behaviour in that setting.</p> <p>Following the modelling session, the instructor discusses the behaviour and what learners should do during their practice session. Learners discuss and practice modelling effective behaviour on their own or with a partner. Then each learner demonstrates the behaviour while the instructor and the remainder of the class observes. The instructor provides feedback to the learners and coaches them on their performance.</p> <p>Learners reflect on the feedback and repeat the exercise. This process continues until learners master the behaviour. Ideally, learners should be videotaped so that they can observe their behaviour and reflect on their performance and the instructor feedback. Instructors should have learners try the behaviour as soon as possible in the lesson. Learners must be provided adequate time to practice to allow them to master the behaviour.</p>
<b>Techniques</b>	<p>Instructors must be able to demonstrate effective and ineffective behaviours to employ this method even when a supporting video is used. It is critical that the correct behaviours are accurately modelled; otherwise learners may become confused and discouraged.</p> <p>Instructors employing the behaviour modelling method should be able to provide detailed feedback to the learner on his or her performance. Correct behaviours should be positively reinforced, and areas requiring improvement identified.</p>

<b>Case Study</b>	
<b>Definition</b>	In the case study method the instructor provides learners with the opportunity to deal with a simulated, real life situation in the classroom. Learners respond to the scenario related to the target performance, by examining the facts and incidents of the case, to critically analyse data and develop solutions.
<b>Application</b>	<p>The case study method is used to challenge learners to apply what they know to a realistic situation. It allows learners to actively participate with the instructor in applying the concepts or principles under study and to foster problem solving, higher-level learning and respect of other opinions.</p> <p>This method of instruction should be employed with smaller groups of relatively mature learners. The primary objective is not to find a correct solution to the problem posed, but to understand the principles involved.</p> <p>To employ the case study method, prior to the lesson, the instructor should verify that the case matches the experience level of the learners and select a logical sequence in which to analyse the case. Adequate time must be allowed to ensure that learners fully understand the case problem and scenario. Learners can read the case in class or ahead of time.</p> <p>To begin the lesson, the instructor should introduce the case and relate it to the learners' past experiences. The instructor should indicate how the lesson fits into the course overall and how it will proceed. Learners should be advised of the lesson objective and the approach that they are expected to use to analyse the case. Learners should clearly understand whether there is a specific view that they are expected to adopt when examining the case.</p> <p>During the lesson, the instructor elaborates on each main point through well-formed, pre-planned questions. For example, what are the facts, assumptions, and problems of the case, what is the cause of the problem, what are the consequences? The instructor guides the class from issue to issue and leads them to discuss critical points. When required, the class can be split into smaller groups for discussion. In this situation the instructor must rotate from group to group to verify that they understand the issues and to answer learner questions.</p> <p>To debrief the case, the instructor addresses the facts of the case. Where small groups were formed the instructor asks each group to provide one or two points relevant to the course. The instructor asks learners to provide the points learned from the case. The instructor concludes by summarizing the case, relating it to the principle to be illustrated and suggesting how the principle applies in other situations.</p>
<b>Techniques</b>	<p>There are a number of techniques the instructor can use to facilitate analysis of the case study. They include:</p> <ul style="list-style-type: none"> <li>• monitor learners who are not participating and try to draw them into the discussion, starting with closed questions and then asking for an opinion or comment on an issue.</li> <li>• ask stimulating questions when needed to promote thinking or guide the discussion, e.g., What is the importance of that fact? Do we need to look at additional facts or information? Is there another way of looking at it?</li> <li>• ask learners to respond to a question instead of responding yourself, when possible.</li> <li>• record learners' points on a chalk board (also give each group a flipchart for group work).</li> <li>• summarize the discussion to assist learners to refocus and progress when necessary.</li> </ul>



<b>Demonstration and Performance</b>	
<b>Definition</b>	<p>Demonstration is a method of instruction where the instructor, performs a sequence of actions (steps) to complete a specific task or tasks. The demonstration shows the learner what to do, how to do it and through explanations brings out the why, where and when it is done. This method incorporates behaviour modelling. Learners acquire new behaviours by observing models and then applying in practice. The method is used to:</p> <ul style="list-style-type: none"> <li>• teach manipulative operations or procedures.</li> <li>• teach trouble-shooting.</li> <li>• illustrate principles.</li> <li>• teach operation or function of equipment or tools.</li> <li>• teach teamwork.</li> <li>• set standards of quality.</li> <li>• Teach safety procedures.</li> </ul> <p>Performance. Performance is a method in which the course member learns by doing, i.e., is required to perform under controlled conditions the operation, skill or movement being taught. An instructor assumes the role of coach. It is used to:</p> <ul style="list-style-type: none"> <li>• teach manipulative operations or procedures.</li> <li>• teach operation or function of equipment.</li> <li>• teach team skills.</li> <li>• Teach safety procedures.</li> </ul>
<b>Application</b>	<p>In practice, the Demonstration and Performance methods are used together when teaching skills. Learners observe the performance of the target task and rehearse it under controlled conditions.</p>
<b>Techniques</b>	<p><b>Techniques.</b> Instructors using the demonstration and performance method must be highly skilled in the procedures to be demonstrated. Learners must be shown the correct procedures. Providing an effective demonstration requires careful planning. Prior to the lesson, the instructor ensures that the task has been broken down into small sequential steps. If necessary, the instructor should rehearse the lesson prior to delivery to ensure the procedures are accurate and clear. The instructor also prepares all materials in advance and organizes the class so all can see.</p> <p>The instructor begins by introducing the lesson, identifying what learners will be able to do at the end, where this skill can be applied and why it is important to learn. During the lesson, the instructor explains each step and then demonstrates each step reiterating the critical components. In larger groups it may be helpful to provide a hand-out outlining the steps for learners to follow. Learners practice the task step by step under supervision. The instructor provides assistance or re-demonstrates as necessary. The instructor may also pose questions to the learners throughout the demonstration to ensure they understand the steps. Practice under supervision continues until the learner masters the skill. Mastery may require practice beyond class time depending on the complexity of the task and the level of the learner.</p> <p>Allowing learners to practice as early as possible and positively reinforcing everything learners do correctly enhances learning. The Demonstration and Performance method can also be used to support an explanation of a theory or concept (e.g., physics — heavier objects fall faster than lighter objects).</p>

<b>Field Trip</b>	
<b>Definition</b>	<p>The field trip is a planned learning experience in which learners observe “real life” operations that illustrate what was discussed or learned in the classroom. It is realistic and brings relevance to instruction. The field trip is used to:</p> <ul style="list-style-type: none"> <li>• reinforce and clarify classroom learning.</li> <li>• inject variety into the training situation.</li> <li>• permit learners to view operations or equipment which cannot easily be shown in the classroom.</li> <li>• Set a realistic context for learning.</li> </ul>
<b>Application</b>	<p>The field trip requires careful planning to ensure it enhances classroom learning. Prior to the trip, the exact operation or equipment that learners will observe must be specified. Details such as transportation, safety or security considerations and whether members of the field unit will be available to demonstrate the use of equipment should be pre-arranged.</p>
<b>Techniques</b>	<p>If learners will be allowed to manipulate equipment, appropriate procedures should be pre-arranged and presented to the learners. During the presentation, learners can rotate through the demonstration, while others observe or look at other materials. Learners may be grouped and given access to equipment if careful supervision is not warranted or if additional personnel are available to supervise them on the job site. Planning the field trip will ensure instructional goals are achieved and that control of the learning situation are maintained.</p> <p>The Field Trip can be valuable to enhance motivation, demonstrate the relevance of material being taught and facilitate transfer to the workplace.</p>

<b>Gaming</b>	
<b>Definition</b>	<p>Gaming is a method employed to allow learners to practice behaviours under the conditions of the game. Games include conflict, rules and in some cases teams and this leads to competition: “winners” and “losers”. Games are motivating for learners and can transfer well to the job but can have negative implications.</p> <p>Games are used with one or more individuals to practice skills associated with a social system or human interaction. The game must instruct some type of skill such as applying strategies or principles. Normally steps or procedures are repeated allowing learners to develop skills.</p>
<b>Application</b>	<p>Before employing this method the instructor must explain the game and rules. During the game instructors should ensure that the game is played in the manner expected.</p>
<b>Techniques</b>	<p>Games can inject variety into the classroom but it is critical that the game support learning of course material, for example, games allowing learners to practice language, recall terms, recognize equipment parts, and use strategies in games of tactics.</p>

<b>Guided Discussion</b>	
<b>Definition</b>	<p>Guided Discussion is a method in which learners are guided in steps to reach instructional objectives by drawing out their opinions, knowledge, experience and capabilities and by building on these to explore and develop new material. Learners discuss issues to expand their knowledge of the subject. It is used to:</p> <ul style="list-style-type: none"> <li>• develop imaginative solutions to problems (e.g., through brainstorming).</li> <li>• stimulate thinking and interest and secure learner participation.</li> <li>• encourage reflection.</li> <li>• supplement lectures, reading or laboratory exercises.</li> <li>• determine how well learners understand concepts and principles.</li> <li>• prepare learners to apply theory or procedure.</li> <li>• clarify or review points.</li> <li>• determine learner progress and the effectiveness of prior instruction.</li> <li>• Foster attitudinal change.</li> </ul>
<b>Application</b>	<p>This method of instruction is employed with a small group of 4 -12 persons normally seated in a circular or horseshoe fashion to facilitate discussion. Reading material should be provided to learners in advance so that learners are familiar with the concepts that will be discussed.</p>
<b>Techniques</b>	<p>To conduct a guided discussion, an instructor should introduce the topic and scenario, outline the main discussion points, state the what, where and why of the lesson and create an open environment.</p> <p>During the body of the lesson the instructor poses open lead-off questions to guide the discussion towards the aim. Conducting a guided discussion requires skills in order to recognize digression and tactfully redirect discussion using rephrased questions, comments or summaries. Encouragement of learner discussion is essential by inviting members to talk, using follow-on questions and resolving conflict.</p> <p>The instructor concludes the lesson by reviewing all the main points contributed by both the learner and instructor and relating points back to the lesson aim.</p> <p>The guided discussion is relevant and meaningful to the learner if it is designed to meet their needs. It stimulates thinking and can result in higher levels of retention due to extensive learner participation.</p>

<b>Interactive Lecture</b>	
<b>Definition</b>	<p>The interactive lecture is a formal or semi-formal presentation in which the instructor presents a series of events, facts, principles, etc. and learners listen and participate by asking or responding to questions and commenting. It is efficient and standardized. It is used to:</p> <ul style="list-style-type: none"> <li>• orient learners and generate interest.</li> <li>• introduce a subject or give an overview.</li> <li>• give direction on procedures.</li> <li>• present basic or background material.</li> <li>• introduce a demonstration, discussion or performance.</li> <li>• illustrate application of rules, principles, or concepts.</li> <li>• Review, clarify, emphasize or summarize.</li> </ul>
<b>Application</b>	<p>The interactive lecture can be employed with groups as large as forty. However, the larger the group the more difficult to build in lecture interactivity. Prior to the lesson, the instructor considers issues that could arise and prepares examples and explanations to deal with them. The instructor practices lecture delivery and prepares material.</p>
<b>Techniques</b>	<p>During the lecture, the instructor pays attention to learner feedback such as facial expressions, body language and alertness. If learners appear unsure it is best to deal with the problem before moving forward by asking if anyone has questions or posing questions to the class. Learner involvement can be promoted by: providing an outline of the lecture's main points; citing relevant comparisons, reasons, examples, statistics and testimonials (CREST); mixing surprising or interesting points with dryer material to stimulate learners; identifying problems the material is relevant to; and incorporating other methods after 20 minutes of lecture such as a video. Discussion or hand-out completion can improve learner attention during the second part of the lecture. The instructor concludes by summarizing key points and re-motivating learners.</p>
<b>Panel Discussion</b>	
<b>Definition</b>	<p>A panel discussion is designed to provide an opportunity for a group to hear several (3-5) people knowledgeable about a specific issue or topic, present information and discuss their views. A panel discussion may help the audience further clarify and evaluate their positions regarding the specific issues or topics being discussed and increase their understanding of the positions of others. Panel discussions offer insight and potential lessons learned and may also be used to provide differing perspectives on a topic or issue.</p>
<b>Application</b>	<p>The moderator introduces a topic/issue which stems from specific desired learning outcomes and the members of the panel present their views and opinions regarding the issue or topic for a set amount of time. The panel should be aware of the intent of the session in order to provide time to prepare.</p> <p>The panel discusses the issue or topic with each other by asking questions or reacting to the views and opinions of other panel members. A specific amount of time should be established. As necessary the moderator directs the discussion and presents questions.</p> <p>The moderator closes the discussion and provides a summary of main points discussed.</p> <p>The moderator opens for questions from observers before moving on to the next topic or issue.</p> <p>Panel discussions are well suited to online forums, video-teleconferences and teleconferences. Often this is the best way to attract leading experts.</p>
<b>Techniques</b>	<p>The moderator is critical to the success of the panel. The moderator controls the discussions, ensuring the objectives are being achieved:</p> <ul style="list-style-type: none"> <li>• Clearly state the objective at the outset as part of the introduction. It reminds</li> </ul>

	<p>the panellists why they are there and informs participants of the intended outcome.</p> <ul style="list-style-type: none"> <li>• The moderator introduces the panellists. Keep it focused on the background relevant to the issue. The intent is to inform the audience so they can form appropriate questions.</li> <li>• Moderators are not panellists, the answers and discussions should flow among the participants and include opportunities for engagement with the audience.</li> <li>• Let the panellists talk to each other; however, ensure the discussion and debate is addressing the intended outcomes.</li> <li>• Ideally the discussions can move online forums at a later date providing the opportunity for participants to interact further with the members of the panel.</li> </ul>
--	---

<b>Peer Learning</b>	
<b>Definition</b>	<p>During peer learning, structured materials are provided to learners who then teach their peers. This method is motivational and is used to facilitate:</p> <ul style="list-style-type: none"> <li>• team building.</li> <li>• recall of facts.</li> <li>• comprehension of concepts.</li> </ul>
<b>Application</b>	<p>Peer learning results in increased learning and retention rates for both learners receiving and providing instruction. Those acting as learners benefit from the individual instruction and those acting as instructors benefit from preparing and developing instruction.</p>
<b>Techniques</b>	<p>Peer learning can consist of advanced learners assisting individual learners, learners leading group discussions and learners having the opportunity to play both the learner and the instructor. It is most valuable to have learners play both roles if possible. Instructors should pair stronger and slower learners allowing the stronger learner to instruct or coach skills first. Then they can switch allowing both to have the benefit of extra practice and providing instruction. Peer learning increases learner participation and motivation. The quality of instruction must be assured.</p>

<b>Problem-based Learning (Small Group - Syndicate)</b>	
<b>Definition</b>	<p>Problem-based learning is a method that facilitates the learning of principles and concepts by having learners work on solving a problem drawn from the work environment. It is often used to develop critical thinking skills and problem solving.</p>
<b>Application</b>	<p>This method is usually conducted with small groups of 5 to 7 learners or with pre-established teams. Instructors prepare carefully constructed problems that will serve as the learning stimulus. Problems must be as realistic as possible so that learners can relate it to their work.</p>
<b>Techniques</b>	<p>During the lesson, learners analyse the problem and work towards solving it. Instructors facilitate learning by posing questions to get learners thinking and talking (e.g., What are the clues, facts and any guesses about the problem and the causes? What other information is needed?). The instructor should ensure that all learners participate, because discussion is key to learning, but they should try not to influence decisions. Instructors may also challenge learners thinking by questioning learners without leading them to the correct answer (e.g., What does this mean? What are the implications?).</p> <p>Instructors using this method must be experienced in facilitating learning and coaching learners. Instructors should refer to the coaching section in this manual for detailed information on the coaching process.</p>

<b>Role Play</b>	
<b>Definition</b>	<p>In this method, learners play defined roles in a scenario designed to reflect the conditions of the target performance. It allows learners to:</p> <ul style="list-style-type: none"> <li>• learn through practicing what they will have to do on the job.</li> <li>• learn by imitating others' behaviour.</li> <li>• learn from the feedback of others.</li> <li>• Learn through practice and reflection on each role play they participate in.</li> </ul> <p>Role-playing exercises are methods of interaction in which learners play out and practice realistic behaviours by assuming specific roles and circumstances. They are used to represent a social system or interpersonal process in miniature so that the learner can practice making the responses to various situations that are similar to those he or she will encounter on the job. Role play is often used for language training, attitudinal objectives and to develop human interaction skills. It is realistic and promotes cooperative learning.</p> <p>The instructor begins the lesson by clearly explaining the objective of the lesson (what, where, when and why). It is critical to explain that role-playing is a learning process and learners are not expected to play their roles perfectly from the start. This will help to put learners at ease.</p> <p>The instructor must clearly explain each role the learners will play. This is followed by a demonstration of the role-play either on video or through a live performance by instructional staff. Learners are paired or grouped together and the role-plays are cycled through. The instructor does not interfere during the role-play unless learners require cues or assistance, or a safety issue arises.</p>
<b>Application</b>	<p>Following each role-play, the instructor debriefs the learner on his or her performance. Correct behaviours should be positively reinforced, and areas requiring improvement identified. Ideally, the role-play will have been videotaped so that learners can watch their performance and reflect on it and the constructive feedback provided by the instructor to improve performance.</p>
<b>Techniques</b>	<p>Instructors should be able to accurately demonstrate the skills being acquired during the role-play to assist learners if necessary. Instructors employing role-play should be able to coach learners and provide them with detailed feedback on their performance.</p>

<b>Self-Study</b>	
<b>Definition</b>	<p>Self-study is a method of self-instruction using printed and/or audio-visual or computer-based media, often presented through Advanced Distributed Learning (ADL)/e-Learning or programmed instructional packages (PIPs) to be completed prior to, during, or following a course. Learners receive instructional materials containing built in feedback and work through them independently. It is used to:</p> <ul style="list-style-type: none"> <li>• provide remedial or make-up instruction for late arrivals, absentees or transients.</li> <li>• maintain previously learned skills which are not performed frequently enough.</li> <li>• accelerate or enrich learning of advanced learners.</li> <li>• provide common knowledge and skill background for learners prior to onset of course.</li> <li>• provide review and practice of knowledge and skills.</li> <li>• permit learning by those who cannot attend a course.</li> </ul> <p>Self-study can provide staff with needed time to prepare for instruction while learners complete individual activities. However, this method does require considerable lead-time to prepare material especially if they are technology-based.</p>
<b>Application</b>	<p>Prior to the self-study session, the instructor should confirm that required materials and resources are available and prepare any additional hand-outs or instructions.</p>

<b>Techniques</b>	The instructor must provide clear direction to the learner on what they have to do and allow them the opportunity to pose questions or raise concerns. Depending on the complexity of the activities and the maturity of the learners, an instructor should check in with learners to ensure they are progressing and provide assistance as necessary. Some self-study materials enable learners to skip material they already know and progress at their own pace.
-------------------	---

<b>Simulation (including In-basket Exercise, Serious Gaming)</b>	
<b>Definition</b>	<p>Simulations are used to provide instruction of complex skills using a dynamic representation of a system or the actual equipment and the job environment. A simulator is an apparatus built to run the simulation. Simulations are context specific and realistic and facilitate transfer of learning to the job and do not necessarily require simulators to create the environment. Role players are often used in parallel as part of the method to create the require context.</p> <p>Simulation provides learners with situated learning and practice. The simulation may not exactly duplicate actual physical skills but should effectively duplicate conceptual tasks. Instructors should employ simulations so that learners learn how a system or device works while avoiding danger or other limitations of the real environment (e.g., access to equipment, weather, and operations).</p>
	Complex skills must be progressively developed. Instructors should provide learners with simple scenarios or problems at the beginning and gradually build up to more complex situations as the learners' skills advance. Instructors may be able to stop simulations to provide direction or explanations and slow down or speed up the process to facilitate learning. It is through specific, constructive feedback and coaching from instructors that learners' skill will develop.
<b>Application</b>	Simulations can be developed in a variety of forms. For example, the in-basket exercise is a type of simulation in which learners respond to a variety of memorandums, directives, and messages that recreate a job specific scenario. Interruptions, emergencies, and random events are usually factored into the exercise. The in-basket method is effective for developing decision-making and prioritizing skills. War gamming is an example of serious games. Serious games are not a simulation alone. It may be a simulation combined with elements of game-play. Serious games have evolved significantly as a means of computer generated environments, micro-worlds and role plays.
<b>Techniques</b>	Instructors must provide coaching, guidance and constructive feedback to learners on their performance during simulation. Instructors are referred to the section titled Coaching in this manual for detailed guidance on the coaching process that should be employed to enhance learning during a simulation.

<b>Study Assignment</b>	
<b>Definition</b>	<p>Study assignment entails the assignment of the study of books, periodicals, manuals or hand-outs, and/or the review of audio-visual materials; the completion of a project or research paper, or prescribes problems and exercises for the practice of a skill. It can:</p> <ul style="list-style-type: none"> <li>• orient learners to a topic prior to classroom or laboratory work.</li> <li>• set the stage for a lecture, demonstration or discussion.</li> <li>• provide for or capitalize on individual differences in ability, background or experience through differentiated assignments.</li> <li>• provide for the review of material covered in class or to give practice.</li> <li>• provide enriching material.</li> </ul>
<b>Application</b>	Providing learners with study assignments facilitates learning by covering concepts in greater detail and by allowing instructors to assess individual learner progress. Study assignments are helpful to all learners and especially those experiencing difficulty.
<b>Techniques</b>	Study assignments require instructor preparation time in advance for development of materials and instructions. To ensure out of class assignments are effective the instructor must provide clear direction, verify that work is completed and provide detailed feedback to the learner.

<b>Tutorial</b>	
<b>Definition</b>	<p>Tutorial is a method of instruction in which an instructor works directly with an individual to ensure the successful completion of activities. It may be customized to meet the learner's needs. It is used to:</p> <ul style="list-style-type: none"> <li>• teach highly complex skills and operations, or operations involving danger or expensive equipment – within this context this is closely aligned with coaching.</li> <li>• provide individualized often remedial assistance/instruction.</li> </ul> <p>The tutorial is a highly motivating method of instruction as it provides one on one individualized instruction. There is much more time for one-on-one interaction as the learner absorbs the material.</p> <p>During the tutorial the instructor is able to adapt to the learner and use instructional strategies that will meet the learner's needs. For example, some learners respond more quickly to visual representation and diagrams than written text. Others may catch on quicker by discussing how something works to fully understand it. Often a tutorial will involve several strategies depending on the complexity of the topic and the needs of the learner and will focus on the areas of difficulty.</p>
<b>Application</b>	<p>Tutorials are ideal for providing remedial help or instructing complicated or dangerous procedures and techniques are described as part of coaching. This method of instruction does require extensive time to conduct depending on the number of learners.</p>
<b>Techniques</b>	<p>To effectively use the tutorial method instructors should be able to determine any difficulties that the learner is experiencing and respond to them. Instructors should be able to recognize whether the learner responds better to hands on experiences, discussions, visual or text materials and use this to provide them with the appropriate learning experience if they are experiencing difficulty. Knowledge of a variety of instructional methods and strategies will assist the instructor using the tutorial method.</p> <ul style="list-style-type: none"> <li>• <b>Note:</b> OJT is an instructional method; however, it is addressed separately because it is implemented in the unit versus the training establishment or learning centre.</li> </ul>

<b>Coaching</b>	
<b>Definition</b>	<p>Coaching consists of aspects of the performance and demonstration method of instruction but is more learner centred and developmental. The instructor's role as a coach is to draw the learner's attention to critical elements of the task execution. The instructor, based on his or her knowledge of the individual learner, asks the learner questions which will lead them to take the next appropriate step in the procedure or take a different direction altogether. This is especially important when learners lose their train of thought or focus. The instructor must assist the learner to get back on track and continue with the task. Questions to the learner to assess his or her thinking and situational awareness under these conditions should be clear, concise and require short responses so that the flow of the task or operation is not disrupted. Instructors must be constantly monitoring the learners' performance to determine what they are doing correctly, as well as areas requiring improvement and how to correct them. The coaching sessions require a thorough debrief to complete the experiential learning cycle.</p>
<b>Application</b>	<p><b>Simulators.</b> Simulators are employed for the development of complex skills such as piloting aircraft, ships, submarines and operating combat vehicles. The coaching method is employed to assist learners to develop skills in simulators. Coaching in this context is situated in the environment and is normally one to one or one to small group.</p>
<b>Techniques</b>	<p>Coaching is typically one-on-one or small group and the instructor role can be conducted in three stages consisting of briefing, monitoring and debriefing.</p> <p><b>BRIEFING</b></p>



	<ul style="list-style-type: none"><li>• The learner should initially be put at ease and advised of the aim of the simulation session and any relevant background. This step serves to engage the appropriate mental model of the task under development.</li><li>• The instructor should then explain and demonstrate each component of the task emphasizing the critical elements. Large tasks should be broken down into smaller tasks so that it can be taught in smaller chunks. Exactly what is being done at each component of the task should be demonstrated and described as well as why it is performed that way. Questions from the learner are encouraged to ensure they understand what to do.</li><li>• Immediately prior to the simulation session the instructor reviews the main points of the task and confirms that the learner is ready.</li></ul> <p><b>MONITORING</b></p> <ul style="list-style-type: none"><li>• This stage consists of performance and observation, preferably using a standard checklist. The learner performs the task while the instructor closely monitors to see that it is carried out correctly and to note corrections the learner must make. The learner should be allowed to carry out the task. The instructor must keep track of what the learner is doing and use brief questions to assess his or her thinking or keywords to cue or help the learner to proceed to the next component.</li></ul> <p><b>DEBRIEFING</b></p> <ul style="list-style-type: none"><li>• Before providing feedback, the instructor examines the learner's performance to determine what was done properly and what areas are weak, and to determine why the problem is occurring. Then the instructor can provide precise constructive feedback on strengths and the weaknesses, and also advise the learner how to correct the problems using explanation and demonstration. It is preferable to focus on correcting two to three major problems in each run rather than every minor error because too much feedback will overwhelm and de-motivate the learner.</li><li>• The debrief must be a positive learning experience, so the instructor should put the learner at ease and present a positive, supportive attitude. The instructor should begin by summarizing the learner's overall performance.</li><li>• Instructors should take the time to address the components of the task that were performed well in order to reinforce the correct behaviour, instil confidence and motivate the learner. As the session continues the instructor identifies and analyses two to three problem areas providing clear explanations of what was done incorrectly. The instructor should encourage the learner to participate in analysing his or her performance of the task by posing guiding questions. The instructor provides guidance on how to correct deficiencies and suggestions to improve performance.</li><li>• The instructor concludes by summarizing strong points, reconfirming what will be done to correct the two to three major problems addressed and by re-motivating the learner.</li></ul>
--	---

## **METHOD SELECTION MATRIX**

1. The following method selection matrix identifies methods based on the classification of an ELO (Cognitive versus Psychomotor) and the intended level of learning to be achieved, as indicated by Depth of Knowledge (DoK) and skill key word indicators. The following considerations should also be factored into method selection:

- a. What will interest, engage and motivate students?
- b. Does the target audience have prior learning (knowledge, skill and/or experiences) which could be leveraged?
- c. Are there operational scenarios, lessons learned, incident reports or stories which could be leveraged and used to promote higher levels of learning through more active engagement? This, in turn, could influence decisions to use specific imagery and video.

Method Selection			
	Type of Learning	Depth of Knowledge (and skill) Key Word Indicators	Method of Instruction
100	<b>Psychomotor Perceptions, Readiness &amp; Guided Response</b>	adhere, arrange, assemble, dismantle, detect, display, fasten, follow, grind, heat, identify, imitate, measure, mend, prepare, recognize, repeat, replicate, reproduce, responds, select, sketch, trace,	<ul style="list-style-type: none"> <li>• Demonstration / performance</li> <li>• Role play</li> </ul>
	<b>Cognitive Remembering explicit knowledge</b>	arrange, define, duplicate, identify, label, list, mark, match, name, order, recall, recite, reproduce, recognize, reproduce, select, state.	<ul style="list-style-type: none"> <li>• Lecture</li> <li>• Self-Study</li> <li>• Tutorial</li> </ul>
200	<b>Psychomotor Mechanism/Manipulation</b>	assemble, build, calibrate, construct, dismantle, fasten, grind, heat, manipulate, measure, mend, mix, organize, shape, sketch.	<ul style="list-style-type: none"> <li>• Demonstration / performance</li> <li>• Role play</li> <li>• Simulation</li> <li>• OJT</li> </ul>
	<b>Cognitive Comprehending/ Understanding</b>	arrange, categorize, classify, convert, distinguish, estimate, explain, extrapolate, group, illustrate, label, match, paraphrase, predict, reiterate, restate, reword, rewrite, report, select, separate, summarize, translate.	<ul style="list-style-type: none"> <li>• Lecture</li> <li>• Self-Study</li> <li>• Tutorial</li> <li>• Field trip</li> <li>• Small Group</li> <li>• Gaming</li> </ul>
300	<b>Psychomotor Complex response/Precision</b>	assemble, build, calibrate, construct, control, dismantle, display, dissect, execute fasten, fix, grind, heat, manipulate, measure, mend, mix, organize, perfect, sketch.	<ul style="list-style-type: none"> <li>• Demonstration/ Performance</li> <li>• Gaming</li> <li>• Simulation</li> <li>• Role play</li> <li>• OJT</li> </ul>
	<b>Cognitive Applying</b>	administer, apply, calculate, change, compute, construct, examine, execute, employ, identify, implement, manipulate, modify, operate, perform, predict, prepare, produce, relate, respond, show, solve.	<ul style="list-style-type: none"> <li>• Lecture</li> <li>• Guided Discussion</li> <li>• Study assignment</li> <li>• Self-study</li> <li>• Gaming</li> <li>• Simulation</li> <li>• Panel Discussion</li> <li>• Peer learning</li> <li>• Small Group</li> <li>• Role play</li> <li>• Case study</li> </ul>
400	<b>Psychomotor Adaptation</b>	adapt, adjust, alter, arrange, assault, combine, composes, construct, coordinate, create, design, develop, estimate, formulate, integrate, invent, modify, rearrange, reorganize, revises, solve, troubleshoot,	<ul style="list-style-type: none"> <li>• Performance</li> <li>• Gaming</li> <li>• Role play</li> <li>• Simulation</li> <li>• OJT</li> </ul>
	<b>Cognitive Analysing</b>	analyse, break down, compare, condense, contrast, deconstruct, design, diagram, differentiate, discriminate, distinguish, divide, experiment, extrapolate, graph, infer, interpret, modify, measure, plan, plot, predict, produce, project, quantify, resolve, revise, search, solve, test, troubleshoot.	<ul style="list-style-type: none"> <li>• Lecture</li> <li>• Guided Discussion</li> <li>• Self-study</li> <li>• Gaming</li> <li>• Peer learning</li> <li>• Panel Discussion</li> <li>• Small Group</li> <li>• Simulation</li> <li>• Role play</li> <li>• Case study</li> </ul>
500	<b>Psychomotor Originate</b>	arrange, build, combine, compose, construct, create, design, initiate, make, originate.	<ul style="list-style-type: none"> <li>• Performance</li> <li>• Gaming</li> <li>• Simulation</li> <li>• Role play</li> </ul>
	<b>Cognitive Assessing/Building/ Creating:</b>	appraise, assemble, assess, build, categorize, combine, compile, compose, conclude, construct, contrast, create, critique, defend, design, derive develop, devise, diagnose, discriminate, encrypt, estimate, evaluate, formulate generate, hypothesize, integrate, interpret, invent, investigate, judge, justify, measure, modify, outline, originate, organize, plan, predict, propose, rank, rearrange, recommend, reconstruct, reframe, revise, rewrite, summarize, validate, war game, write.	<ul style="list-style-type: none"> <li>• Self-Study</li> <li>• Gaming</li> <li>• Simulation</li> <li>• Role play</li> <li>• Case study</li> <li>• Peer learning</li> <li>• Panel Discussion</li> <li>• Small Group</li> <li>• Field Trip</li> </ul>

**COURSE CONTROL DOCUMENT (CCD) III – PROGRAMME OF CLASSES**

1. The Programme of Classes is the final course control document developed to define an NATO E&IT solution<sup>78</sup>. The ETF generates the Programme of Classes. This CCD includes the ELO and provides the details supporting the overall instructional strategy including the final structure of the content, the instructional method as well as the time allocated to complete the ELO. CCD III also includes student assessment details.

2. The CCD III - Programme of Classes is uploaded to the ETOC by the ETF and subsequently verified with the DH as an appropriate solution to meet the previously identified POs in CCD II. Example formats for CCD III are enclosed. The format for CCD III may be adapted by ETFs as required. ETOC technical support is available at: [eitephelp@act.nato.int](mailto:eitephelp@act.nato.int).

---

<sup>78</sup> Course Control Documents (CCD) are the output products for the NATO SAT Definition Stage. The CCD define a NATO E&IT solution. ETFs may use other forms and formats to describe their respective plan to satisfy an E&IT requirement. The alternative formats include: Training Plan, Programme of Learning, Course Curriculum, Programme of Instruction as well as Course Syllabus. The essential elements to be addressed are outlined in Chapters 5 and 6.

**Course Control Document – III: Programme of Classes**

COURSE CODE	COURSE TITLE					
ETOC assigned number	Insert Title					DoK:
	<b>Performance Objective</b> Insert the performance statement describing what a learner will be able to do upon completion of a specified Performance Objective (PO).					
Serial	Enabling/Learning Objective Performance statement	Conditions	Standards	Teaching Points (TP)		
				Lesson Title	Method & Time	References
ELO 1.1	The statement clear, concise and precise statement representing a logical and complete segment of what is to be learned in order to achieve a PO.	A list of the conditions which describe the situation in which learning will occur.	Defines the level of proficiency that determines if the required level of learning is achieved.	A label assigned to a grouping of TPs TP 1- TP 2- TP3-	An estimate of the time required to satisfy each of the ELOs based on the methods and media.	The reference for each teaching point
ELO 1.2				A label assigned to a grouping of TPs TP 1- TP 2- TP3-	An estimate of the time required to satisfy each of the ELOs based on the methods and media.	The reference for each teaching point
<b>Resources:</b> Identifies the materials used during lesson (example: Handout 20 x 1)						
<b>References:</b> The complete list of the references which is abbreviated in the TP section						
<b>Assessment:</b> The content is captured within the Assessment Plan and a summary is provided here. Practical or Written. Group or Individual. On own or combined with other EOs. Also indicates how the results be used to determine disposition?						
<b>Limitations:</b> A description of limitations which prevent the completion of an Enabling Objective.						
<b>Remarks:</b> Comments that further clarify the design intent captured within the ELO.						

**Control Document – III: Programme of Classes**

COURSE CODE	COURSE TITLE					
<b>Performance Objective</b>						
Serial	Enabling/Learning Objective Performance statement	Conditions	Standards	Teaching Points (TP)		
				Lesson Title	Method & Time	References
ELO 1.1						
ELO 1.2						
ELO 1.3						
ELO 1.4						
<b>Resources:</b>						
<b>References:</b>						
<b>Assessment:</b>						
<b>Limitations:</b>						
<b>Remarks:</b>						

COURSE CONTROL DOCUMENT III - PROGRAMME OF CLASSES																																																															
<b>Code:</b>	<b>Title:</b>																																																														
<p><b>PO 1:</b> <i>Insert the performance statement describing what a learner will be able to do upon completion of a specified Performance Objective (PO).</i></p> <p><b>ELO 1.1:</b></p> <ol style="list-style-type: none"> <li>1. <b>Performance:</b> <i>The statement clear, concise and precise statement representing a logical and complete segment of what is to be learned in order to achieve a PO.</i></li> <li>2. <b>Conditions:</b> <i>A list of the conditions which describe the situation in which learning will occur.</i></li> <li>3. <b>Standards:</b> <i>Defines the level of proficiency that determines if the required level of learning is achieved.</i></li> <li>4. <b>Assessment:</b> <i>The content is captured within the Assessment Plan and a summary is provided here. Practical or Written. Group or Individual. On own or combined with other EOs. Also indicates how the results be used to determine disposition?</i></li> <li>5. <b>Instructional Strategy:</b></li> </ol> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr> <th style="width: 55%; text-align: center;">Content</th> <th colspan="2" style="width: 20%; text-align: center;">Method &amp; Time</th> <th style="width: 25%; text-align: center;">References</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">a. <b>Lesson Title:</b> <i>A label assigned the 1st grouping of teaching points (TPs)</i></td> <td style="text-align: center; vertical-align: top;"><i>Identify methods</i></td> <td style="text-align: center; vertical-align: top;"><i>An estimate of the time</i></td> <td style="text-align: center; vertical-align: top;"><i>Links content to a source</i></td> </tr> <tr><td style="padding: 5px;">TP 1</td><td></td><td></td><td></td></tr> <tr><td style="padding: 5px;">TP2</td><td></td><td></td><td></td></tr> <tr><td style="padding: 5px;">TP3</td><td></td><td></td><td></td></tr> <tr><td style="padding: 5px;">TP4</td><td></td><td></td><td></td></tr> <tr><td style="padding: 5px;">TP5</td><td></td><td></td><td></td></tr> <tr> <td style="padding: 5px;">b. <b>Lesson Title:</b> <i>A label assigned to a 2<sup>nd</sup> grouping of TPs</i></td> <td></td> <td></td> <td></td> </tr> <tr><td style="padding: 5px;">TP 1</td><td></td><td></td><td></td></tr> <tr><td style="padding: 5px;">TP2</td><td></td><td></td><td></td></tr> <tr><td style="padding: 5px;">TP3</td><td></td><td></td><td></td></tr> <tr> <td style="padding: 5px;">c. <b>Lesson Title:</b> <i>A label assigned to a 3rd grouping of TPs</i></td> <td></td> <td></td> <td></td> </tr> <tr><td style="padding: 5px;">TP 1</td><td></td><td></td><td></td></tr> <tr><td style="padding: 5px;">TP2</td><td></td><td></td><td></td></tr> <tr> <td style="padding: 5px;"><b>Total Time:</b></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <ol style="list-style-type: none"> <li>6. <b>Depth of Knowledge:</b> <i>Specifies a level (100-500) which identifies the level of learning.</i></li> <li>7. <b>Limitations:</b> <i>A description of limitations which prevent the completion of Enabling/Learning Objective.</i></li> <li>8. <b>Resources:</b> <i>Comments that further clarify the design intent captured within the Enabling/Learning Objective.</i></li> </ol>				Content	Method & Time		References	a. <b>Lesson Title:</b> <i>A label assigned the 1st grouping of teaching points (TPs)</i>	<i>Identify methods</i>	<i>An estimate of the time</i>	<i>Links content to a source</i>	TP 1				TP2				TP3				TP4				TP5				b. <b>Lesson Title:</b> <i>A label assigned to a 2<sup>nd</sup> grouping of TPs</i>				TP 1				TP2				TP3				c. <b>Lesson Title:</b> <i>A label assigned to a 3rd grouping of TPs</i>				TP 1				TP2				<b>Total Time:</b>			
Content	Method & Time		References																																																												
a. <b>Lesson Title:</b> <i>A label assigned the 1st grouping of teaching points (TPs)</i>	<i>Identify methods</i>	<i>An estimate of the time</i>	<i>Links content to a source</i>																																																												
TP 1																																																															
TP2																																																															
TP3																																																															
TP4																																																															
TP5																																																															
b. <b>Lesson Title:</b> <i>A label assigned to a 2<sup>nd</sup> grouping of TPs</i>																																																															
TP 1																																																															
TP2																																																															
TP3																																																															
c. <b>Lesson Title:</b> <i>A label assigned to a 3rd grouping of TPs</i>																																																															
TP 1																																																															
TP2																																																															
<b>Total Time:</b>																																																															

**COURSE MONITORING**

Course Monitoring is an additional element supporting the Post Course Review - Internal Evaluation. Course Monitoring concentrates on the delivery of instruction and gathers observation data. The focus is on the performance of individual instructors (Instructional Effectiveness) and assesses many elements that may affect course quality including a confirmation of the alignment of the objectives with what is delivered, appropriateness of the instructional methods, quality of instructional materials, time allocation. Observations for improving student evaluation may also be included. Course Monitoring also provides an opportunity to verify that instructors have the prerequisite qualifications and training is satisfied. An example observation sheet to support Course Monitoring is provided below.

**Lesson Observation Checklist**

<b>Monitor Name</b>		<b>Start Time:</b>	
<b>Date of Audit:</b>		<b>End Time:</b>	
<b>Course Number:</b>		<b>Instructor/Facilitator:</b>	
<b>Lesson Title:</b>			

<b>Supporting Documentation</b>	<b>Yes</b>	<b>Some</b>	<b>No</b>	<b>N/A</b>
<b>Lesson Plan for the period of instruction was available.</b>				
<b>Written guidance to students for syndicate work was provided.</b>				
<b>The lesson title is clearly identified in Course Critique.</b>				
<b>The Lesson is clearly identified in the Course Schedule.</b>				

<b>Lesson Alignment</b>	<b>Yes</b>	<b>Some</b>	<b>No</b>	<b>N/A</b>
<b>The aim of the Lesson is clearly stated.</b>				
<b>The teaching points presented align with the LO stated in the CCD III.</b>				
<b>The references for the lesson are stated and are consistent with the CCD III.</b>				
<b>The timing for the lesson is consistent with the CCD III and the Course Schedule.</b>				
<b>The syndicate work was aligned with the objectives outlined in the CCD III.</b>				
<b>The instructional strategy used was aligned with the instructional strategy listed in the CCD III.</b>				
<b>The DOK was consistent with the level identified in the CCD III.</b>				
<b>The assessment strategy is consistent with the CCD III.</b>				



<b>Instructional Effectiveness</b>	<b>Yes</b>	<b>Some</b>	<b>No</b>	<b>N/A</b>
The training facility was adequately prepared to deliver instruction.				
Supporting materials were readily available.				
The facilitator gained and maintained the attention of the class.				
The facilitator established the relevance of what was being presented to the students.				
The teaching points were presented in a logical sequence.				
The facilitator provided relative verbal support (examples / explanations / statistics).				
The visual aids used were clear and supported the teaching points.				
Media used during the lesson were of appropriate number, duration and quality.				
The facilitator engaged the students during the lesson using effective questioning techniques.				
The facilitator emphasized important points / issues.				
The facilitator periodically checked for student understanding.				
The facilitator provided a summary of the main teaching points at the end of the lesson.				

<b>Student Assessment</b>	<b>Yes</b>	<b>Some</b>	<b>No</b>	<b>N/A</b>
Assessment details / test instructions provided to the student.				
The assessment is at the proper DOK for the course.				
An answer key or assessment checklist for syndicate presentations is available.				
The assessment is aligned with the course lesson objectives and CCD III.				
The DOK being assessed is consistent with the LO(s) in the CCD III.				
The content assessed aligns with the content presented during the course.				
Students are provided with the results of the assessment as well as facilitator feedback.				

**Other Comments and Best Practice Observations**

## TEST ITEM ANALYSIS

1. Through the quantifying of data (systematically assigning numbers to data) statistical analysis can be performed so that relationships and trends can be identified and interpreted. A trend is a pattern or prevailing theme. Trends can reveal strengths and weaknesses within a course. For test items, item analysis is used to quantify data so that test items of questionable quality can be identified as well as indicate areas where individuals have not mastered objective(s). In the case of surveys, observations and other forms feedback the data is quantified and interpreted through descriptive statistics. The use of statistical software applications can make the process of data interpretation an easier task. Data must be interpreted to identify the problems so that recommendations can be made and solutions generated. Item analysis provides information about the reliability and validity of test items. Item analysis can be performed in terms of the following:

- a. Test Item Difficulty.
- b. Test Item Discrimination.

## TEST ITEM DIFFICULTY

2. The frequency of students answering a test item correctly determines the level of difficulty. For example, if 45 of 50 students answer an item correctly, then the level of difficulty is low (.90) since 90 percent were able to answer correctly. However, if 10 out of 50 students answer correctly, then the level of difficulty is high (.20). The possible range for the Difficulty Index is 0 to 1; the closer to 0 the more difficult the item. The difficulty index is the proportion of students who answer a test item correctly and is calculated in the example below.

**Example:**

**Difficulty Index (p).** The proportion of students who answer a test item correctly.

$$p = \frac{\text{Number of students selecting correct answer}}{\text{Total number of students attempting the test item}}$$

$$p = \frac{45}{50} = .90$$

3. When Difficulty Index or “p” level is less than about .25, the item is considered relatively difficult. When the Difficulty Index is above .75 the item is considered relatively easy. A Difficulty Index above .75 on its own does not indicate a result of 1. Tests should appear to have a low level of difficulty given the intent this indicates higher levels of proficiency. Item difficulty should be considered along with test item discrimination when assessing the effectiveness of a test item.

**TEST ITEM DISCRIMINATION**

4. Test item discrimination is an index of an item's effectiveness at discriminating those who appear to have learned content better from those who have not. It is the degree to which students with high overall scores on a particular test get a test item correct. The item discrimination index is referred to as a point bi-serial correlation coefficient. Its possible range is -1.00 to 1.00. A strong positive correlation (.3) suggests that students who get any one question correct also have a relatively high score on the overall test. Any positive value is an indication of a positive correlation and this is generally acceptable.

**Example:**

**Discrimination Index (D).** The Measure of the extent to which a test item discriminates or differentiates between students who perform well on the overall test and those who do not perform well on the overall test.

$$D = \frac{\text{Number who got item correct in an upper group} - \text{Number with item correct in lower group}}{\text{Total number of students in both groups}}$$

$$D = \frac{7-3}{20} = .2$$

**Note:** D does not require the total population completing a test to be included in the calculation. Depending on the size of the group a representative sample is satisfactory. Example: Use 50% of the total population comprised of the top 25% and the bottom 25%.

**INTERPRETING RESULTS**

5. Test items which consistently result with a higher level of difficulty (e.g.,  $p=.25$ ) and a corresponding positive discrimination index (e.g.,  $D = .25$ ) indicate a quality test item. It is also acceptable to have a low level of difficulty (e.g.,  $p= .90$ ) and discrimination near zero (meaning no discrimination) and still have a desirable and quality test item. The intent is to determine if the test item itself is measuring what it should. When the level of difficulty is higher (e.g.,  $p = .25$ ) and there is any negative discrimination (e.g.,  $p = -.25$ ) the item should be reviewed if there is a trend. If this result is an outlier and occurs during a single application (one course of several), this is an indication there may have been issue with course execution and monitoring of the next event is recommended.



NATO Communications and Information Agency  
Agence OTAN d'information et de communication

**AGENCY DIRECTIVE**  
**AD 06.00.16 INTERIM**  
**CONFIGURATION MANAGEMENT**

Effective date: 2/25/2020 (*Precise date as per Approver's e-signature date*)

Revision No: Original

Issued by: COO SMC Branch Chief \_\_\_\_\_

Approved by: COO \_\_\_\_\_

Table of Amendments

Amendment No	Date issued	Remarks

Author Details

Organization	Name	Contact Email
COO SMC	Julian Davis	<a href="mailto:Julian.davis@nr.ncia.nato.int">Julian.davis@nr.ncia.nato.int</a>
COO NSII	Andreas Hutzenlaub	<a href="mailto:Andreas.Hutzenlaub@nr.ncia.nato.int">Andreas.Hutzenlaub@nr.ncia.nato.int</a>

Document/Process Owner

Organization	Name	Contact Email
COO SMC	Angelo Talarico	<a href="mailto:Angelo.talarico@nr.ncia.nato.int">Angelo.talarico@nr.ncia.nato.int</a>

## Table of Contents

<b>1</b>	<b>REFERENCES.....</b>	<b>4</b>
<b>2</b>	<b>PURPOSE.....</b>	<b>4</b>
<b>3</b>	<b>APPLICABILITY.....</b>	<b>5</b>
<b>4</b>	<b>SCOPE.....</b>	<b>6</b>
<b>5</b>	<b>DISTRIBUTED AUTHORITY.....</b>	<b>6</b>
5.1	Enterprise CM versus Domain CM-----	6
<b>6</b>	<b>BASELINE TYPES.....</b>	<b>7</b>
6.1	Configuration Baseline -----	7
6.2	The Functional Baseline -----	7
6.3	The Allocated Baseline -----	7
6.4	The Product Baseline-----	8
6.5	The Service Baseline -----	8
<b>7</b>	<b>CONFIGURATION MANAGEMENT PROCESS.....</b>	<b>9</b>
7.1	Management and Planning-----	9
7.2	Configuration Identification-----	9
7.3	Configuration Control-----	10
7.4	Configuration Status Accounting-----	10
7.5	Configuration Audit -----	10
<b>8</b>	<b>PROCESS INTERFACES.....</b>	<b>11</b>
<b>9</b>	<b>ROLES AND RESPONSIBILITIES.....</b>	<b>11</b>
9.1	CM Business Process Owner (COO SMC)-----	11
9.2	Enterprise Configuration Manager (COO SMC)-----	11
9.3	Domain Configuration Manager (Service Enabling Service Line, Project Office) -----	12
9.4	Configuration Administrator (COO SMC, Service Enabling Service Line, Project Office) -----	12
	<b>ANNEX A CONFIGURATION ITEM TYPES.....</b>	<b>13</b>
	<b>ANNEX B DEFINITIONS.....</b>	<b>22</b>
	<b>ANNEX C ABBREVIATIONS.....</b>	<b>24</b>

## List of Figures

Figure 1 - NCI Agency Configuration Management Context.....	5
Figure 2 – Enterprise versus Domain CM.....	6
Figure 3 - Configuration Management Processes.....	9
Figure 4 - Process Interfaces.....	11

## AD 06.00.16

### CONFIGURATION MANAGEMENT

#### 1 REFERENCES

- A. STANAG 2290 - Unique Identification of Items;
- B. STANAG 4427 - Configuration Management in System Life Cycle Management, Edition 3, dated 18 Dec. 141;
- C. AAP-48 NATO System Life Cycle Processes Edition B Version 1, dated Mar 2017;
- D. NCI Agency AD 01.01 - Agency Policy on Management and Control of Directives, Notices, Processes, Procedures and Instructions, dated 20 May 2014;
- E. NCI Agency AD 06.00.13 Service Change Management dated Dec 2016;
- F. NCI Agency Visual Identity Guidelines – Version 1.3 (2013);
- G. ITIL Service Transition, edition 2011, Axelos;
- H. NCI Agency Enterprise Information and Communication Technology Service Delivery Model (ESDM), Dated Nov 2016;
- I. NCI Agency 2020 Service Rates and Costed Customer Services Catalogue version 4.0, dated 14 Mar 2019;
- J. NCI Agency CSSC SOP 09.02 V2 - NCIARECCEN-4-136529;
- K. NCI Agency AI TECH 06.03.01 Identification of Software Assets dated Jun 2016;
- L. BMC CMDB Common Data Model Document.

#### 2 PURPOSE

The NCI Agency's mission is to deliver secure, coherent, cost effective and interoperable communications and information systems and services. The purpose of this Directive is to define the principles, process, roles and responsibilities required to successfully execute the function of Configuration Management (CM).

The NCI Agency CM falls under the governance of the NCI Agency Chief Operating Officer (COO). It is based on NATO Policies and Standards, Military Standards and Industry best practice; aggregated and adapted into the NCI Agency Policies and Directives that are established by the NCI Agency Chief Information/Technology Officer (SStrat) and COO. The NCI Agency CM operational foundations as detailed within this AD mandate that all Agency entities shall adhere to this document.

With this document in hand, the Service Lines (SL) will be enabled to develop their own CM Plans<sup>2</sup> that trigger specific Standard Operating Procedures (SOPs) to support the lifecycle of Configuration Items (CIs); this approach is called "distributed authority" and is explained further in Section 5.

CM is closely linked to Service Change Management (Ref E), which controls the changes to CIs<sup>3</sup>. Under no circumstance will a CI be allowed to change its current version/state without an approved Change Request. CI Types are listed in Annex A with an example of attributes.

---

<sup>1</sup> This reference includes the NATO standards defined in ACMP-2000, ACMP-2009, ACMP-2100 and subordinates Standard Related Documents (SRD).

<sup>2</sup> Lifecycle Configuration Management Plans are detailed in STANAG 4427

<sup>3</sup> For Domain CM, it is recognized that other documents i.e. Standardisation Agreements (STANAGs) will also control changes to CIs, depending upon the operating environment i.e. AMDC2.

Under the accountability of the service enabling SL Chief (SLC), the CM Plan will be implemented into one or more Service areas supported by specific CM SOPs and Agency Instructions (AIs). Figure 1 below depicts the CM documentation context that this document formalises.

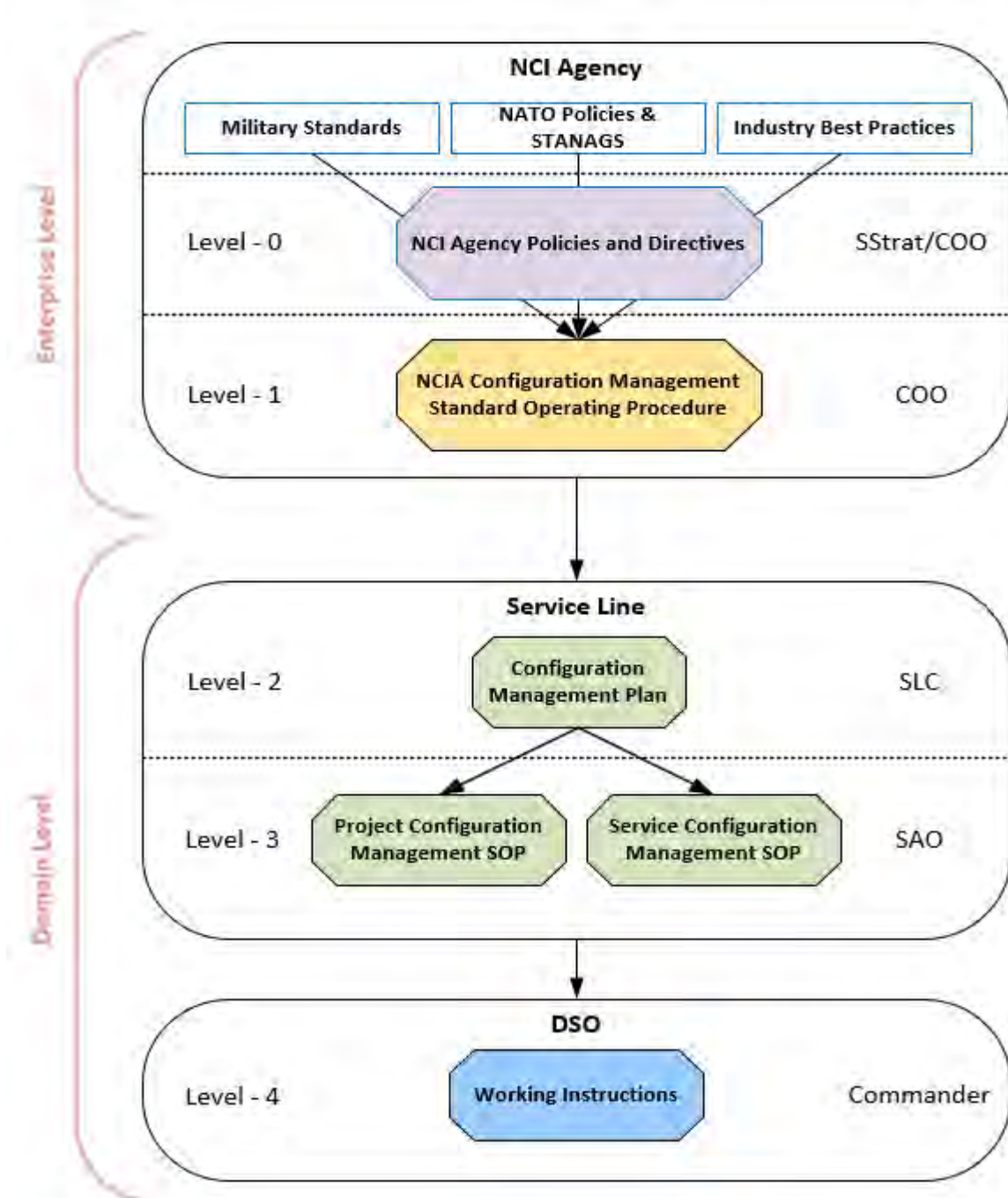


Figure 1 - NCI Agency Configuration Management Context

### 3 APPLICABILITY

This Directive applies to all elements of the Agency, in particular to all NCI Agency staff involved in developing, implementing and maintaining IT systems services or software products. It is the responsibility of all NCI Agency Programme, Service Delivery, Product and Project Managers to ensure they support its implementation and to incorporate the content of this AD into relevant organisational structures, as well as, ensure the contractual documentation from external suppliers is acquired.



#### 4 SCOPE

This document establishes the foundation of CM across the NCI Agency Enterprise. It constitutes the initial standard of CM baselines and process across the service lifecycle. It is expected that this “standard” grows in iterations over a period of time adapting to the Agency P3M (Project, Programme & Portfolio Management) and Service (Enterprise Service Delivery Model) methodologies and standards.

#### 5 DISTRIBUTED AUTHORITY

##### 5.1 Enterprise CM versus Domain CM

SMC Branch under COO is accountable for the Enterprise CM process, across all security domains including mission networks. It distributes CM authority to the Organisational Elements (OE) i.e. SLs and CSUs, allowing them configuration planning and control whilst remaining under SMC governance.

Throughout the Agency, CM process, procedures and tools are not standardized and different OEs have implemented the process at different levels of maturity. Distributed authority allows OEs to pursue their own CM plans and make decisions within the specified boundaries of rigor and quality in fulfilling them. However, the ultimate goal is to achieve a standardised CM approach across the Enterprise.

OEs are mandated to create their own Configuration Control Board’s (CCB) for their own “Domain” to control the service configuration baselines in terms of core and support services i.e. platforms, infrastructure and software.

To conceptualise this distributed authority, this document makes a distinction between “Domain CM” and “Enterprise CM” as depicted in Figure 2 – Enterprise versus Domain CM below.

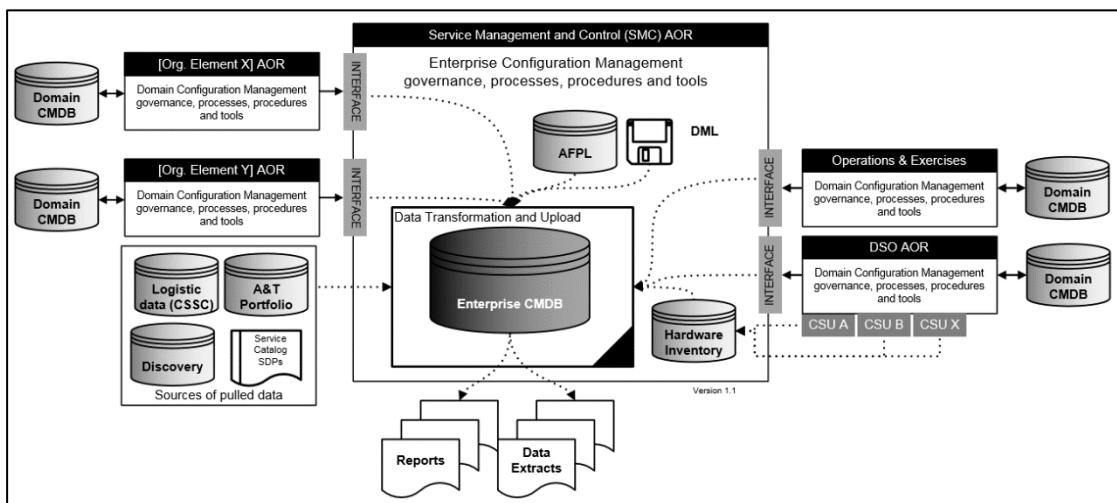


Figure 2 – Enterprise versus Domain CM

The “Domain CM” processes are the ones implemented in the different OEs e.g. NSII, AMDC2 etc. for a specific purpose, with specific governance rules, procedures and tools. Each SL, or, more generally, each Agency OE is responsible for its own Domain CM; they must ensure coherency across/with the other OE/SLs to sustain their capabilities. Likewise, Enterprise CM data may be cascaded to the Domain under agreed conditions.

The “Enterprise CM” process is the process defined by SMC Branch, whose goal is to establish an Enterprise Configuration Management System (CMS), with its own governance, procedures and tools. It defines data interface requirements with the different OEs, when Domain CM data must be pulled from or pushed in the Enterprise CMDB.

The interfaces between each domain CM and Enterprise CM is a set of requirements (data and structure) defined by SMC Branch to integrate information coming from the domains into the Enterprise CMDB. Minimum interface requirements will be agreed and documented, as CI attributes within the domain may be far more specific and detailed, which the Enterprise cannot consume or support.

A number of CMDBs and data sources are used for the population of the Enterprise CMDB. For example, data discovery (System Centre Configuration Manager (SCCM)) and the hardware inventory (Cormant CS, formerly known as Cablesolve).

The complete collection of CMDBs and data sources, form, on a conceptual perspective, the Agency CMS. To provide users the ability to discover CIs within the various localized CMS through a centralized search engine, each Agency OE is responsible to implement an interface for its CMS that is conformant with: OpenSearch 1.1 (Draft 6), RFC 7303, RFC 4287, RSS 2.0W3C - XML 1.0 (Recommended).

## 6 BASELINE TYPES

### 6.1 Configuration Baseline

A Configuration Baseline is a snapshot at a particular moment in time or an event of a set of CIs with its attributes and relationships to each other.

Configuration Baselines are under version control and can be only modified into the next baseline by the Change Management Process.

Within NATO there are many Configuration Baselines defined depending on stakeholder requirements and domain. For the NCI Agency that focusses on P3M and Service Delivery, the Allied Configuration Management Publications (ACMPs) within the governance of STANAG 4427 (Ref B) and the adaptation of the ITIL V3 Framework are the most suitable and are applied to NCI Agency CM. The CIs assigned to a Baseline are not limited to the ones mentioned below. The list of mandatory CIs for each baseline is maintained by SMC Branch.

### 6.2 The Functional Baseline

The Functional Baseline constitutes the functional and non-functional requirements for a Product or Service with its assigned test specification and relevant architectural artefacts.

Typical Configuration Items for the Functional Baseline are:

- Product/System Requirements Specification
  - System Test Specification
  - Architecture artefacts
- Service (Level) Requirements Specification
  - Service (Level) Test Specification
- Interface Documentation
  - Service Interoperability Points
  - Interoperability Test Specification

### 6.3 The Allocated Baseline

The Allocated Baseline constitutes the design of a Product or Service and its conformity to the related Functional Baseline.

Typical Configuration Items for the Allocated Baseline are:

- Product/System Design Specification
  - Product/System Design Acceptance Report
- Service Design Package

- Architecture Model
- Service Design Specification

### 6.4 The Product Baseline

The Product Baseline constitutes all CIs that build the final Product and its corresponding approved Functional and Allocated Baseline.

Typical CIs of the Product Baseline are but not exclusive to

- All Project deliverables, e.g. Product Breakdown Structure (C MDB), Product Operating and Maintenance Manuals, Product Training Manuals, Product Acceptance Test Reports, other
- Architectural Models and Engineering drawings
- COTS documentation i.e. datasheets etc.

### 6.5 The Service Baseline

The Service Baseline is the collection of Product Baselines, Resources, and Enabling Services that constitute the Customer facing Business Service as defined in the NCIA Service Catalogue. It furthermore contains key Service Management documents. An example of the Service Baseline is depicted at Figure 3 below.

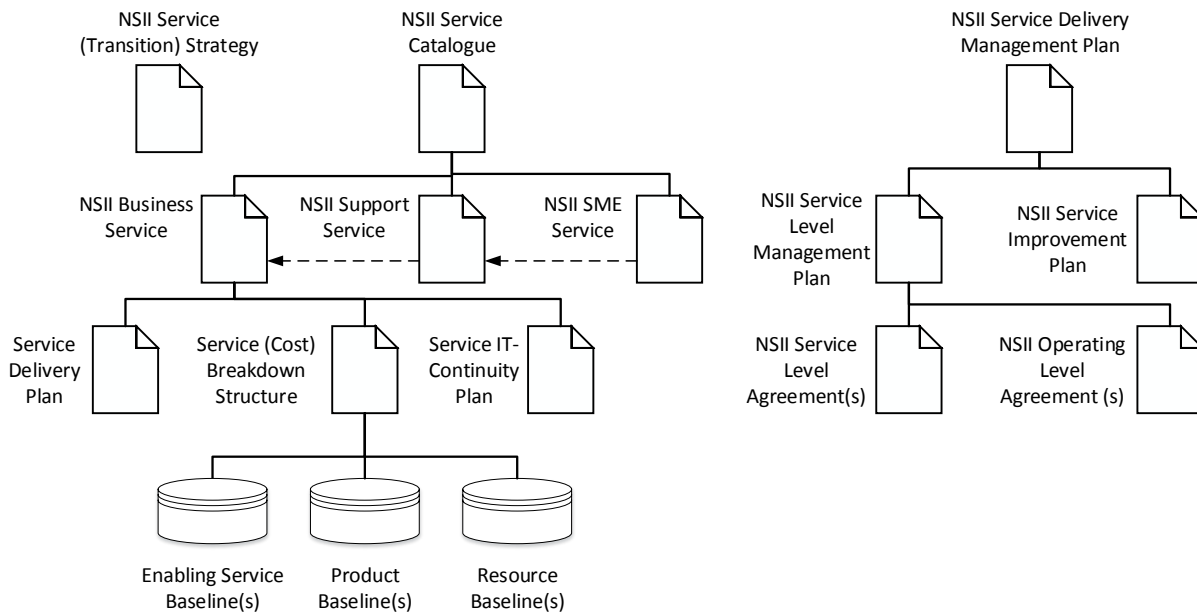


Figure 3 - Example Service Baseline from NSII

## 7 CONFIGURATION MANAGEMENT PROCESS

The CM Process is defined in the Allied Configuration Management Publications (ACMPs), Ref B. It is responsible for ensuring that information (identification, attributes and relationships) about CIs that are required to deliver a Service or Asset (e.g. Software Products, System Documentation, Training Material) are defined and maintained, in all phases of its lifecycle, as defined in Ref C.

There shall be no modification to or creation of a CI without an approved Request for Change (RFC). This principle ensures that changes are recorded, evaluated, planned, tested, implemented, and reviewed in accordance with a defined process.

The CM process is depicted in Figure 4 - Configuration Management Processes below and is decomposed in five sub-processes:

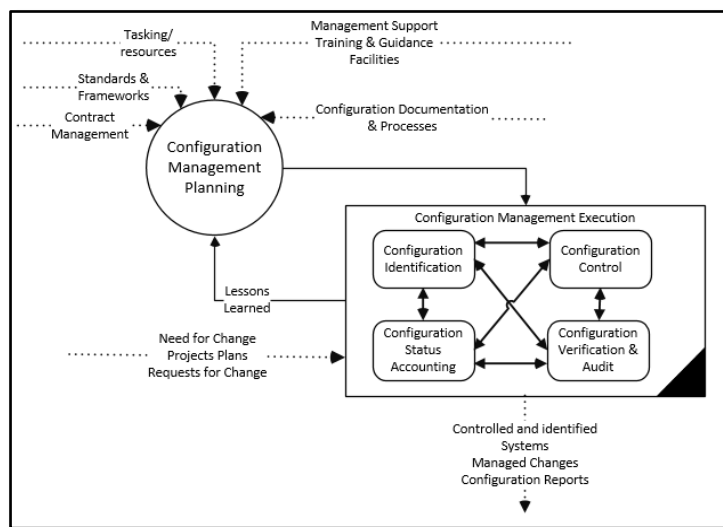


Figure 4 - Configuration Management Processes

### 7.1 Management and Planning

CM Planning is the process of identifying the resources and documenting the activities required for CM execution, with regard to the Organization policies. The sub-process typically produces the CM Plan.

- **Inputs:** Projects and Services
- **Outputs:** CM Plan<sup>4</sup>

### 7.2 Configuration Identification

Configuration Identification consists of defining the framework for unique identification of CIs and maintaining baselines, which document the system or subsystem architecture (product structure), components and any developments at any point in time.

It is the basis by which changes to any part of a system are identified, documented, and later tracked through design, development, testing, and final delivery.

<sup>4</sup> STANAG 4427 Ed3. Mandates basic principles of CM for SLCM. NATO shall use a Life-Cycle Configuration Management Plan (LCCMP) as the basis for all contractual CM requirements that are placed on Suppliers through the life of the system. The document provides guidance for the build-up of the complete set of contractual CM requirements.

Configuration Identification incrementally establishes and maintains the definitive current basis for Configuration Status Accounting (CSA) of a system and its CIs throughout their life cycle.

- **Inputs:** Discoverable CI types<sup>5</sup>
- **Outputs:** Populated CMDB with relationships

### 7.3 Configuration Control

Configuration Control is the systematic evaluation, coordination, approval or disapproval and dissemination of all proposed changes to a CI and/or its configuration documentation; after formal establishment of its configuration baseline and verifying the implementation of all approved changes. In ITIL the Configuration Control, process is called “Change Management”.

- **Inputs:** Change request, Service Request, CMDB
- **Outputs:** Modified CI, Triggers, alarms, notification and report

### 7.4 Configuration Status Accounting

Configuration Status Accounting is an element of CM, consisting of the recording and reporting of information needed to manage a configuration effectively.

- **Inputs:** CMDB, incident record, service request, change request
- **Outputs:** Status report, baseline configuration report, unauthorized usage report

### 7.5 Configuration Audit

Checking a CI for compliance with its configuration documentation. There are two types of configuration audits:

- Functional Configuration Audit
  - **Inputs:** Product Baseline, Functional Baseline & Allocated baselines
  - **Outputs:** Audit Conformity report
- Physical Configuration Audit
  - **Inputs:** Product Baseline, Service Baseline
  - **Outputs:** Audit Conformity report

---

<sup>5</sup> Non-discoverable CI Types are those data types that cannot be discovered by automated software tools e.g. applications, products and services.

## 8 PROCESS INTERFACES

As depicted in Figure 5 - Process Interfaces below, the Enterprise CM process interfaces with a number of other processes and consumes data from different data sources in order to maintain the Enterprise CMDB.

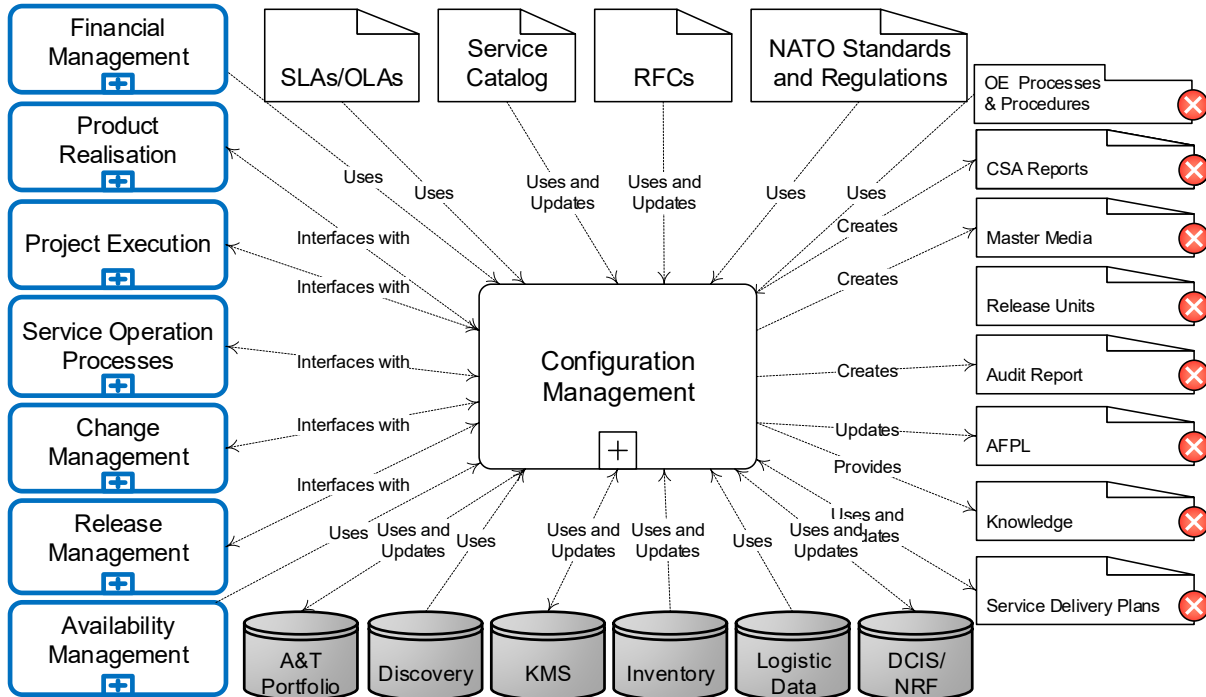


Figure 5 - Process Interfaces

## 9 ROLES AND RESPONSIBILITIES

### 9.1 CM Business Process Owner (COO SMC)

Develops CM strategies, policies, standards, and guidelines. Champions the importance and value of CM and develops new methods and organisational capabilities (including automation) for CM. Provides resources to drive adoption of, and adherence to, policies and standards. Measures and monitors adherence to standards and ensures consistent execution of the process across the Agency.

### 9.2 Enterprise Configuration Manager (COO SMC)

Ensures that operational processes are in place to maintain secure configuration, consistent classification and management of CIs, and for the verification and audit of configuration records. Develops, configures and maintains tools (including automation) to identify, track, log and maintain accurate, complete and current information. Reports on the status of CM. Identifies problems and issues and recommends corrective actions.

Agrees scope of CM processes and the configuration items (CIs) and related information to be controlled. Identifies, evaluates and manages the adoption of appropriate tools, techniques and processes (including automation) for CM to ensure information is complete, current and accurate. Plans the capture and management of CIs and related information. Contributes to development of CM strategies, policies, standards, and guidelines with Service Strategy.

### 9.3 Domain Configuration Manager (Service Enabling Service Line/Branch, Project Office)<sup>6</sup>

The Domain Configuration Manager shares the same responsibilities as the Enterprise Configuration Manager but their primary focus is on their Domain. Further responsibilities include:

- The Domain Configuration Manager is responsible for normalizing<sup>7</sup> all its Domain CIs before being consumed by the Enterprise CMDB. This will increase data integrity and reduce duplication.
- Reports on the status of the Domain CM. Identifies problems and issues and recommend corrective actions.

### 9.4 Configuration Administrator (COO SMC, Service Enabling Service Line/Branch, Project Office)

This assistant role can be carried out at both the Enterprise and Domain levels. The Configuration Administrator applies tools, techniques and processes to track, log and correct information related to configuration items. Verifies and approves changes ensuring protection of assets and components from unauthorised change, diversion and inappropriate use. Ensures that users comply with identification standards for object types, environments, processes, lifecycles, documentation, versions, formats, baselines, releases and templates. Performs internal audits to check the accuracy of information and undertakes any necessary corrective action under direction.

---

<sup>6</sup> NATO Joint AirC2 Configuration Items are currently managed in the AMDC2 Domain CMDB. The requirement of CI normalization for the data exchange between the Domain and the Enterprise CMDB are waived for those CIs until a more detailed analysis of the data exchange requirements between the CMDBs are performed.

<sup>7</sup> Automated normalisation, searches for variations of the same field value and converts them into a single preferred value. It works best for descriptive values such as names or standard units of measurement.

## ANNEX A CONFIGURATION ITEM TYPES

A Configuration Item (CI) is a physical, logical or conceptual entity that is part of the IT environment and has configurable attributes. See Annex B for a more detailed description of a CI.

Enterprise Configuration Management as detailed in this AD uses the Commercial of the Shelf (COTS) product BMC Atrium Configuration Management Database (CMDB) for the purpose of recording CIs, their attributes and their relationships.

BMC deploys an “out the box” Common Data Model (CDM), which is a set of CIs and relationship classes. These classes represent the physical, logical and conceptual items of all IT environments, including IT Federation that the Enterprise will want to track in the CMDB. The CDM is scaleable and the functionality exists to create a new class of CI or extend an existing one with additional attributes. The CI types are detailed in Table 1 - CI Types below.

Attributes for each CI type can be a related standard or inherited. As an example, Software standard and inherited attributes are listed in Table 2 - Software Summary Attributes and Table 3 - Software Inherited Attributes below. These tables show the fidelity of information associated to a CI.

A full description of each type and associated attributes can be found on BMC CMDB Common Data Model Document, Ref L.



**Table 1 - CI Types**

AccessPoint	FinancialElement	ProtocolEndpoint
Account	HarwarePackage	Rack
Activity	HardwareSystemComponent	RemoteFileSystem
AdminDomian	IPConnectivitySubnet	RequestableOffering
Application	IPEndPoint	ResourceAllocationSettingData
ApplicationInfrastructure	IPXConnectivityNetwork	ResourcePool
ApplicationService	Keyboard	Role
ApplicationSystem	LAN	ServiceLevelTarget
BaseElement	LANEndpoint	ServiceOffering
BiosElement	LNConnection	ServiceOfferingInstance
BusinessProcess	LocalFileSystem	Settings
BusinessService	LogicalDisk	Share
Cabling	LogicalEntity	Software
Card	LogicalSystemComponent	SoftwareServer
CDROMDrive	MainFrame	StorageExtent
Chassis	Media	StorageVolume
CloudInstance	Memory	System
Cluster	Monitor	SystemComponent
Collection	NetworkPort	SystemResource
CommunicationEndpoint	NTDomain	SystemService
ComputerSystem	Offering	SystemSoftware
ConcreteCollection	OperatingSystem	Tag
ConnectivityCollection	Option	TapeDrive
ConnectivitySegment	OptionChoice	Transaction
Contract	Organisation	UPS
ContraLine	Package	UserCommnity
Cost	Patch	VirtualSystemEnabler
DataBase	Person	VirtualSystemSettingData
DataBaseStorage	PhysicalLocation	WAN
DiskDrive	PointingDevice	
DiskPartition	Price	
Document	Printer	
Equipment <sup>8</sup>	Processor	
FileSystem	Product	

<sup>8</sup> Equipment includes DCIS Systems

**Table 2 - Software Summary Attributes**

Data type	Name	Description
character	<b>BuildNumber</b>	Attribute that specifies the internal identifier for a compilation of the software element.
character	<b>BuildType</b>	Attribute that specifies the type of build used for the operating system. Examples are retail build and checked build.
character	<b>ConfigurationBasicNumber</b>	Attribute that specifies the internal identifier of the basic configuration of the software element.
character	<b>ContractID</b>	Attribute that identifies of the contract governing the software element.
character	<b>InstallLocation</b>	Attribute that specifies the location where the software is installed.
integer	<b>LicensesAvailable</b>	Attribute that specifies the number of licenses available for the software element.
enumeration	<b>LicenseType</b>	<p>Attribute that specifies the type of license available for the software element.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> <li>• 0 - (Group)</li> <li>• 1 - (Site)</li> <li>• 2 - (Global)</li> <li>• 3 - (Server)</li> </ul> <p>There is no default value.</p>
character	<b>PatchNumber</b>	Attribute that specifies the internal identifier for the latest patch applied to the software element.
character	<b>ServicePack</b>	Attribute that specifies the internal identifier for the latest service pack applied to the software element. For mainframe software elements, this attribute stores the FMID (function modification identifier) with System Modification Program/Extended (SMP/E), a code that identifies the release levels of the element.

**Table 3 - Software Inherited Attributes**

Data type	Name	Description
character	<b>AccountID</b>	Attribute that specifies the account to which the instance belongs. This value is used to set permissions for the instance and is intended for implementing multitenancy. Accounts can represent customers, organizations, departments, or other parties to which you want to give access to a limited set of configuration items (CIs) and relationships.
character	<b>ADDMIntegrationId</b>	ADDM integration Id - attribute used to store the ADDM Foreign key
character	<b>AssignedTo</b>	Attribute that specifies the person to whom the instance is assigned;
character	<b>AttributeDataSourceList</b>	Attribute that specifies a list of all other attributes in the class, each with the source dataset that supplied the attribute's value the last time the instance was merged. This enables each attribute to participate in Merge activities by using the precedence value of the dataset that populated it. Used by the Reconciliation Engine.
enumeration	<b>Availability</b>	<p>Attribute that specifies the adverse effects that a loss of availability of the instance has on organizational operations, assets, or individuals. Ensures that your organization has timely and reliable access to information in the instance (44 U.S.C., SEC. 3542).</p> <p>Possible values are:</p> <ul style="list-style-type: none"> <li>• 10 - (N/A) Indicates no effect</li> <li>• 20 - (Low) Indicates limited adverse effects</li> <li>• 30 - (Moderate) Indicates serious adverse effects</li> <li>• 40 - (High) Indicates severe or catastrophic adverse effects</li> </ul> <p>There is no default value.</p>

Data type	Name	Description
character	<b>Category</b>	Attribute that specifies user-defined categorization of the instance. Used with the Type and Item attributes.
character	<b>CITag</b>	Specifies the unique identifier of the VM represented by this CI.
character	<b>ClassId</b>	Attribute that specifies the unique identifier of the class to which the instance belongs.
character	<b>CMDBRowLevelSecurity</b>	Attribute that specifies the permission groups that have read-only access to the instance data.
character	<b>CMDBWriteSecurity</b>	Attribute that specifies the permission groups that have read/write access to the instance data.
enumeration	<b>Confidentiality</b>	<p>Attribute that specifies the adverse effects that a loss of confidentiality of the data in the instance has on organizational operations, assets, or individuals. Preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information (44 U.S.C., SEC. 3542).</p> <p>Possible values are:</p> <ul style="list-style-type: none"> <li>• 10 - (N/A) Indicates no effect</li> <li>• 20 - (Low) Indicates limited adverse effects</li> <li>• 30 - (Moderate) Indicates serious adverse effects</li> <li>• 40 - (High) Indicates severe or catastrophic adverse effects</li> </ul> <p>There is no default value.</p>
dateTime	<b>CreateDate</b>	Attribute that specifies the date and time the instance was created; Value supplied by: AR System.
character	<b>DatasetId</b>	Attribute that specifies the unique identifier of the dataset to which the instance belongs. This can be the ID of the BMC Remedy Asset Management dataset (BMC.ASSET) or the ID of a discovery application dataset (for example, BMC.ADDM or BMC.IMPORT.CONFIG).
character	<b>Description</b>	Attribute that contains a textual description of the instance.
enumeration	<b>FailedAutomaticIdentification</b>	<p>Attribute that specifies whether manual identification is required. Used by the Reconciliation Engine.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> <li>• 0 - (False)</li> </ul>

Data type	Name	Description
		<ul style="list-style-type: none"> <li>1 - (True)</li> </ul> <p>The default value is "0".</p>
diary	<b>History</b>	Attribute that specifies the history of the instance in diary format. Syntax: Diary.
character	<b>ImpactComputationModel</b>	Attribute that specifies the status of this CI based on statuses propagated from provider CIs. This attribute was formerly named StatusModel in the SIM extension.
character	<b>InstanceId</b>	Attribute that specifies the internal unique identifier of the instance. Instances that share the same reconciliation identity do not share the same InstanceId.
enumeration	<b>Integrity</b>	<p>Attribute that specifies the level of adverse effects that a loss of integrity of the instance has on organizational operations, assets, or individuals. Guards against improper information modification or destruction, and includes information ensuring nonrepudiation and authenticity (44 U.S.C., SEC. 3542).</p> <p>Possible values are:</p> <ul style="list-style-type: none"> <li>10 - (N/A) Indicates no effect</li> <li>20 - (Low) Indicates limited adverse effects</li> <li>30 - (Moderate) Indicates serious adverse effects</li> <li>40 - (High) Indicates severe or catastrophic adverse effects</li> </ul> <p>There is no default value.</p>
enumeration	<b>isVirtual</b>	<p>Attribute that specifies whether the instance is virtual or physical. To ensure correct reconciliation with data created by BMC Software products, use NULL instead of No for an instance that is not virtual.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> <li>0 - (No)</li> <li>1 - (Yes)</li> </ul> <p>There is no default value.</p>
character	<b>Item</b>	Attribute that specifies the user-defined categorization of the instance. This attribute is used with the Category and Type attributes.

Data type	Name	Description
character	<b>LastModifiedBy</b>	Attribute that specifies the user that last modified the instance; Value supplied by: AR System.
dateTime	<b>LastScanDate</b>	Attribute that specifies the last date and time the instance was scanned. Used by discovery applications.
character	<b>ManufacturerName</b>	Attribute that specifies the organization that produced the entity represented by the instance. For example, if the instance represents a Pro Widget 2000, the ManufacturerName might be Acme Widget Company.
enumeration	<b>MarkAsDeleted</b>	<p>Attribute that specifies whether the instance is soft deleted. To ensure correct reconciliation with data created by BMC Software products, use NULL instead of No for an instance that is not soft deleted;</p> <p>Possible values are:</p> <ul style="list-style-type: none"> <li>• 0 - (No)</li> <li>• 1 - (Yes)</li> </ul> <p>There is no default value.</p>
character	<b>MarketVersion</b>	Attribute that specifies the publicised version number of the entity represented by the instance.
character	<b>Model</b>	Attribute that specifies the name by which the kind of entity represented by the instance is generally known. For example, the Model of a laptop computer might be "Latitude E4300" or "MacBook Pro".
dateTime	<b>ModifiedDate</b>	Attribute that specifies the date and time the instance was last modified; Value supplied by: AR System.
character	<b>Name</b>	Attribute that specifies the name of the instance. Some discovery applications and other data sources populate this attribute with values that are unique but not human readable. In this case, they should also populate the NameFormat attribute with a value specifying the format of the Name value and the ShortDescription attribute with the human-readable name of the instance.
character	<b>NameFormat</b>	Attribute that specifies the heuristic used to generate the Name value. For example, a computer system might be identified by an external DNS name or by a static IP address. The heuristic will likely not be the same for each subclass of this class. This attribute should be populated by any data source that provides a Name value that is not human readable.

Data type	Name	Description
diary	<b>Notes</b>	Attribute that specifies the general notes in diary format about the item represented. Syntax: Diary; by the instance.
character	<b>OwnerContact</b>	Attribute that specifies information about how to contact the primary system owner (for example, a phone number, an email address, or both).
character	<b>OwnerName</b>	Attribute that specifies the name of the primary system owner.
character	<b>ParentCITag</b>	Specifies the unique identifier of the parent virtual machine (VM).
enumeration	<b>Priority</b>	<p>Attribute that specifies the customer-assigned instance priority.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> <li>• 0 - (PRIORITY_5)</li> <li>• 1 - (PRIORITY_4)</li> <li>• 2 - (PRIORITY_3)</li> <li>• 3 - (PRIORITY_2)</li> <li>• 4 - (PRIORITY_1)</li> </ul> <p>The default value is "0".</p>
character	<b>ReconciliationIdentity</b>	Attribute that specifies the identifier assigned either manually or by an Identification activity. It is unique to all instances in any dataset that represent the same real-life CI or relationship. The value for ReconciliationIdentity stays the same when the instance is copied or moved to other datasets.
enumeration	<b>ReferenceInstance</b>	<p>Reserved for use in a future version of BMC Atrium CMDB.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> <li>• 0 - (ReferenceInstance)</li> </ul> <p>There is no default value.</p>
character	<b>RequestId</b>	Internal system field used for permissions to AR System form entries; Value supplied by: AR System.
character	<b>SerialNumber</b>	Attribute that specifies the manufacturer-allocated identifier used to identify the physical entity represented by the instance.
character	<b>ShortDescription</b>	Attribute that specifies a short textual description used to provide a human-readable name for the instance.
character	<b>Submitter</b>	Attribute that specifies a unique account identifier of the user that created the instance.

Data type	Name	Description
enumeration	<b>Supported</b>	<p>Attribute that specifies whether technical support is provided for this class. If the value set to No, the class is deprecated and support might not be provided for it in the future;</p> <p>Possible values are:</p> <ul style="list-style-type: none"> <li>• 0 - (Yes)</li> <li>• 1 - (No)</li> <li>• 2 - (N/A)</li> </ul> <p>The default value is "0".</p>
character	<b>SystemClassId</b>	<p>Unique identifier of the class of the system to which the component belongs. This attribute value is automatically propagated from the related configuration item (CI).</p>
character	<b>SystemName</b>	<p>Name of the system to which the component belongs. This attribute value is automatically propagated from the related configuration item (CI).</p>
character	<b>TokenFormat</b>	<p>Attribute that specifies the heuristic used to generate the value of the TokenId attribute. The heuristic is defined in a subclass of this class;</p>
character	<b>TokenId</b>	<p>Attribute that specifies the unique identifier populated by some discovery applications and used by the Reconciliation Engine to identify instances.</p>
character	<b>Type</b>	<p>Attribute that specifies the user-defined categorization of the instance used with the Category and Item attributes</p>
character	<b>VersionNumber</b>	<p>Attribute that specifies the internal, full resolution, version number of the entity represented by the instance.</p>



**ANNEX B DEFINITIONS**

Term	Definition
Approved Fielded Product List (AFPL)	AFPLs are maintained to provide NATO, its Agencies and the Nations with a managed list of authorized systems configuration baselines in order to assure interoperability between all entities. All items listed in the AFPL are approved by the SMC Software Change Advisory Board (CAB). The AFPL is the only authoritative data source for software versions/systems approved for deployment on a specific network.
Baseline	A baseline is a set of one or more CIs items whose content and status have been verified and accepted at a particular stage in their life cycle. It identifies a description of a system at a distinct point in time and at a distinct level of maturity. Baselines can be composed of various CIs (e.g. Request for Changes, documentation, software and hardware items) and provide the foundation for change control of individual or grouped CIs.
Change Request	Also called Request for Change (RFC). A generic name applied to a change, regardless of the change type, when the context requires this level of abstraction.
Configuration Item (CI)	A Configuration Item (CI) is any component that needs to be managed in order to deliver an IT Service or a System. Information about each CI is recorded in a CMDB and is maintained throughout its Life cycle by CM. CIs are under the Configuration Control (i.e. Change Management). CIs typically include hardware, software, IT Assets or formal documentation such as process documentation and documents associated to the supported system(s).
Configuration Management Database (CMDB)	A database used to store Records about CIs throughout their lifecycles, together with their attributes and inter-relationships <sup>9</sup> .
Configuration Management System (CMS)	The Configuration Management System is an overarching entity logically grouping multiple CMDBs.
Definitive Media Library (DML)	The DML is a secure location where master media of authorized versions of all systems are stored and protected.
Product	A product is a CI type that is produced at the end of a development process execution, and that serves a particular and defined objective.

<sup>9</sup> In the context of this document, the abbreviation “CMDB” is used for the concept of configuration management database. It is not meant to be used as a brand name of any specific software vendor.



Release Unit	A Release Unit (RU) is a set of CIs that will be built, tested and deployed together as a single entity.
Release Package	A Release Package (RP) is one or more CIs which are normally deployed as a single entity. The Release Package contains the Release Unit and the documentation produced during the RFC evaluation (System Admin Notes, Test report...)
Service Asset	A Service Asset is any resource or capability that contributes to the delivery of a service (e.g.: server, router, system, software, license, document...).
System	A system is a set of interacting and/or interdependent components, with observable inter-components communication, forming an integrated whole with a defined objective.
Version Description Document (VDD) <sup>10</sup>	A document delivered in the Release Unit, describing the content of the system version. Its main purpose is to list all the dependencies of the system it describes.

---

<sup>10</sup> This document is sometimes called Software Version Description, or Release notes. In the context of this AD, the term VDD will be used.

**ANNEX C ABBREVIATIONS**

Abbreviation	Meaning
AD	Agency Directive
AFPL	Approved Fielded Product List
AKA	Also Known As
CCB	Configuration Control Board
CMDB	Configuration Management Database
CM	Configuration Management
CMP	Configuration Management Plan
CMS	Configuration Management System
COTS	Commercial off-the-shelf software
CSF	Critical Success Factor
CSI	Continuous Service Improvement
ESDM	Enterprise Service Delivery Model
OE	Organisational Element
QA	Quality Assurance
RACI	Responsible, Accountable, Consulted, Informed
RFC	Request for Change
SACM	Service Asset Configuration Management
SAO	Service Area Owner
SCCM	Microsoft System Center Configuration Manager
SDP	Service Delivery Plan
SLC	SL Chief
SMC	Service Management and Control
SOP	Standard Operating Procedures
SSRM	System Submission Requirements Matrix
STANAG	Standardisation Agreement



NATO Communications and Information Agency  
Agence OTAN d'information et de communication

**AGENCY INSTRUCTION**

**AI 23.02**

**DEPLOYMENT MANAGEMENT PLANNING**

Effective date: 14 October 2019 (*Precise date as per Approver's e-signature date*)

Revision No: Original

Issued by: Service Line Chief (SMC) \_\_\_\_\_

Approved by: COO \_\_\_\_\_

Table of Amendments

Amendment No	Date issued	Remarks

Author Details

Organization	Name	Contact Email
COO SMC	Julian	<a href="mailto:Julian.davis@ncia.nato.int">Julian.davis@ncia.nato.int</a>

Document/Process Owner

Organization	Name	Contact Email
COO SMC	Angelo Talarico	<a href="mailto:Angelo.talarico@nr.ncia.nato.int">Angelo.talarico@nr.ncia.nato.int</a>

## Table of Contents

<b>1</b>	<b>REFERENCES .....</b>	<b>4</b>
<b>2</b>	<b>PURPOSE .....</b>	<b>4</b>
<b>3</b>	<b>APPLICABILITY .....</b>	<b>4</b>
<b>4</b>	<b>SCOPE .....</b>	<b>4</b>
<b>5</b>	<b>BACKGROUND .....</b>	<b>4</b>
5.1	DEPLOYMENT MANAGEMENT PLANNING .....	4
<b>6</b>	<b>PROCESS DEPLOYMENT MANAGEMENT PLANNING – PREPARE RELEASE .....</b>	<b>4</b>
	<b>ANNEX A PREPARE RELEASE FLOWCHART &amp; INSTRUCTIONS.....</b>	<b>5</b>
	<b>APPENDIX 1 TO ANNEX A DEPLOYMENT PLAN TEMPLATE .....</b>	<b>8</b>
	DOCUMENT PURPOSE .....	8
	NOTE .....	8
	SCOPE .....	8
	RELEASE UNIT (S):.....	10
	DEPLOYMENT SCHEDULE: .....	10
	OUT-OF-SCOPE .....	10
	CONSTRAINTS AND EXTERNAL DEPENDENCIES.....	11
	SUPPORT ROLES AND RESPONSIBILITIES DETAIL.....	12
	DETAILED DEPLOYMENT ACTIVITIES.....	13
	EARLY LIFE SUPPORT (ELS) .....	13
	RISK MANAGEMENT .....	14
	MITIGATION/CONTINGENCY STRATEGY .....	15
	RESPONSIBLE PERSONNEL.....	16
	CRITICAL EVENTS .....	17
	BACK-OUT PLAN (ROLLBACK PLAN) .....	17
	BUSINESS INTERRUPTION EVENT LOG.....	18
	IDENTITY AND ACCESS MANAGEMENT CREDENTIALS .....	19
	SITE SERVICE ACCEPTANCE CHECKLIST .....	20
	COMMUNICATION PLAN .....	21
	TRAINING PLAN.....	22
	INSTRUCTOR.....	22
	USER TRAINING 1 .....	22
	TECH TRAINING 1.....	22
	USER TRAINING 2 .....	22
	DOCUMENTATION.....	23
	ACCREDITATION.....	24
	AFPL AUTHORISATIONS .....	24
	ISSUE MANAGEMENT.....	25
	DECISION LOG.....	25
	DISTRIBUTION LIST .....	26
	<b>APPENDIX 2 TO ANNEX A SITE SERVICE ACCEPTANCE CHECKLIST .....</b>	<b>27</b>
	<b>APPENDIX 3 TO ANNEX A ENTERPRISE CAB – DOTMLPPF PROCESS .....</b>	<b>32</b>
	<b>APPENDIX 4 TO ANNEX A DECISION MAKING AUTHORITY.....</b>	<b>33</b>
	<b>APPENDIX 5 TO ANNEX A PRIVILEGED USER ACCESS REQUEST FORM.....</b>	<b>33</b>

### DEPLOYMENT MANGAEMENT PLANNING

## 1 REFERENCES

- A. AD 06.03.01 Deployment Management dated Sep. 2014
- B. AI 06.00.04 Approved Service Interruption dated Oct. 2019

## 2 PURPOSE

The purpose of this Agency Instruction (AI) is to instruct the Release Manager<sup>1</sup> in preparing a deployment plan in support of a change to an existing service or new service.

## 3 APPLICABILITY

This AI applies to all elements of the Agency, in particular to all NCI Agency staff involved in developing, implementing and maintaining IT services or software products. It is the responsibility of all NCI Agency Programme, Service Delivery, Product and Project Managers to ensure they follow the instructions contained within this document.

## 4 SCOPE

All services being deployed under P3M (Project, Programme & Portfolio Management) and all Services supported and deployed by the NCI Agency Service Lines (SLs) i.e. Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Software as a Service (SaaS) across all security domains/networks operated and maintained locally or centrally by the NCI Agency

## 5 BACKGROUND

### 5.1 Deployment Management Planning

*Deployment Management Planning* shall begin during Project Initiation and shall not only be executed for the initial rollout of new services, but also for all types of releases; i.e. maintenance, emergency and technology refresh

The *Deployment Management Plan* is intended to provide customers, final users, stakeholders and support personnel with a smooth transition to the new service or product being deployed. It describes in detail each step of the deployment process at each deployment location. It further define all of the work steps for complete deployment, and who does them.

Responsibility for *Deployment Management Planning* lies with the SLs or Programme that runs the project, but requires close collaboration with the Release & Deployment Management office within the Chief Operating Office Service Management & Control, Change & Configuration Authority (COO SMC CCA).

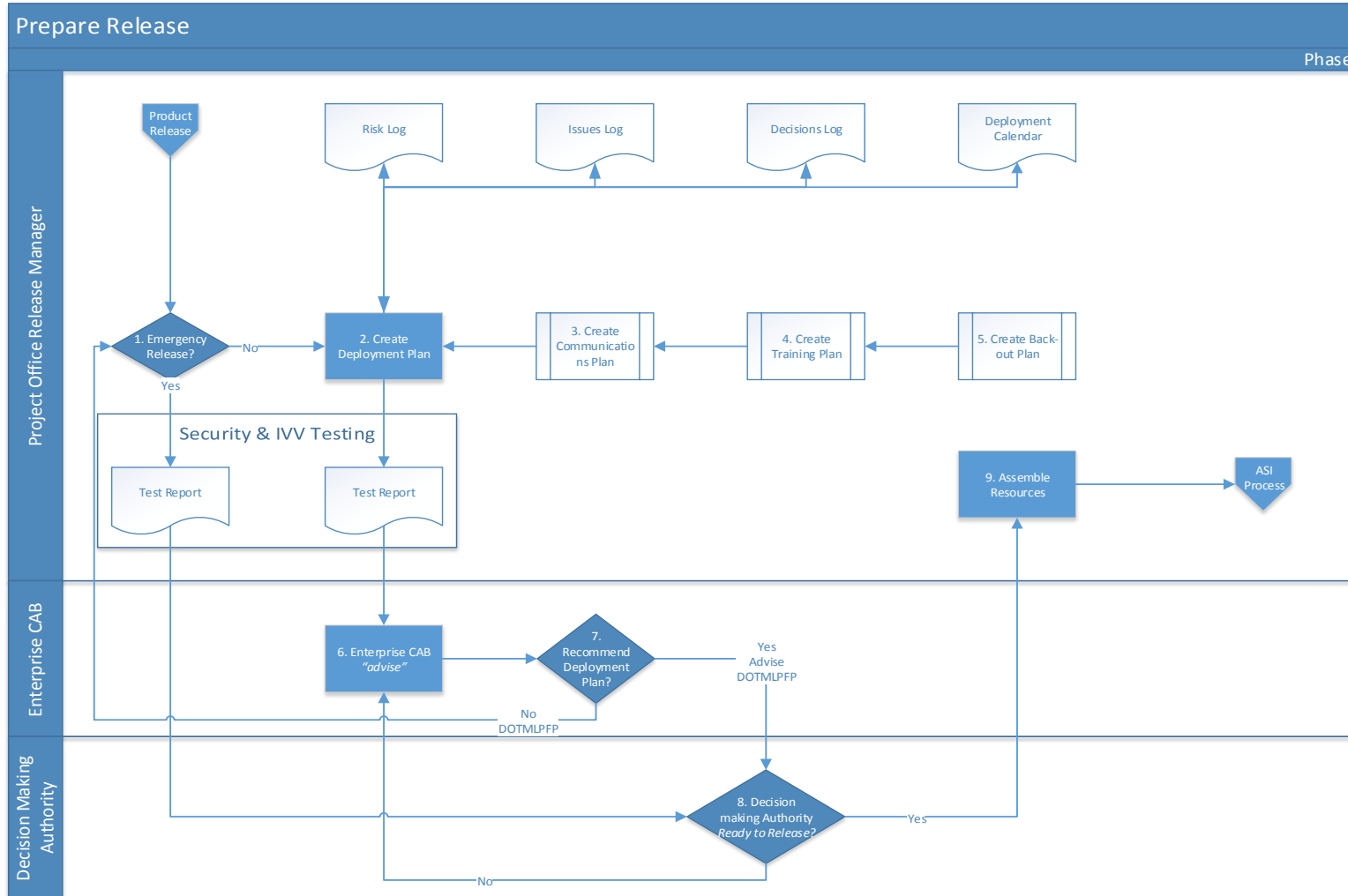
## 6 PROCESS DEPLOYMENT MANAGEMENT PLANNING – PREPARE RELEASE

For this AI it is assumed that the Planning, Building and Testing phases of release management have taken place. Diagram 1 and Table 1 in Annex A below depict and describe the instructions taken to develop and authorise a deployment management plan before actual deployment.

---

<sup>1</sup> The Release Manager is a role and can be carried out by the Project Manager (PM) or the Service delivery Manager (SDM).

**PREPARE RELEASE FLOWCHART & INSTRUCTIONS**



**Figure 1 - Prepare Release Flowchart**



**Table 1 - Prepare Release Instructions**

Step	Instructions
1	<ul style="list-style-type: none"> <li>• Is the release an emergency?               <ul style="list-style-type: none"> <li>○ Go to Step 8 “Decision Masking Authority” with “Test Report<sup>2</sup>”</li> <li>○ If not, proceed to Create Deployment Plan</li> </ul> </li> </ul>
2	<ul style="list-style-type: none"> <li>• Create Deployment Plan – See Template at Appendix A</li> </ul>
3	<ul style="list-style-type: none"> <li>• Create <b>Communications Plan</b> (included as Annex to the Deployment Plan)               <ul style="list-style-type: none"> <li>○ Communicate release plans and dates, details of where to find and sign up for training courses (if appropriate), and where to obtain more detailed information about the release</li> <li>○ Provide a list of actions the users need to carry out to prepare themselves and their work places for the release</li> <li>○ Release Manager and others involved in the release process should check and confirm that users have actually performed these tasks</li> </ul> </li> </ul>
4	<ul style="list-style-type: none"> <li>• Create <b>Training Plan</b> (included as Annex to the Deployment Plan)               <ul style="list-style-type: none"> <li>○ Release Manager identifies the skills and abilities required to support and maintain the release</li> <li>○ Release Manager arranges for a skills gap analysis to be performed on those responsible for carrying out those tasks</li> <li>○ Release Manager or members of the training department (where available) can determine the best way to develop the required skills</li> </ul> </li> </ul>
5	<ul style="list-style-type: none"> <li>• Create <b>Back-out Plan</b> (included as Annex to the Deployment Plan)               <ul style="list-style-type: none"> <li>○ Release Manager prepares a plan detailing how a specific change or release can be undone during rollout or after being applied, if deemed necessary due to NATO operational requirements</li> </ul> </li> </ul>
6	<ul style="list-style-type: none"> <li>• <b>Enterprise CAB</b> <ul style="list-style-type: none"> <li>○ Reviews the Deployment Plan and associated change paperwork, including Test Report from IVV &amp; Security</li> <li>○ Compiles DOTMLPFP<sup>3</sup> (Refer Appendix 3)</li> <li>○ Advises Yes or No (Step 7)</li> <li>○ <b>Determine the level of Decision Making Authority (Refer Appendix 4)</b></li> </ul> </li> </ul>
7	<ul style="list-style-type: none"> <li>• The <b>Enterprise CAB</b> will make an “advise” to deploy statement to Decision Making Authority:               <ul style="list-style-type: none"> <li>○ Advise NO, go back to Step 1, with full DOTMLPFP justification</li> <li>○ Advice YES, go to Step 8, with full DOTMLPFP justification, including risks even if mitigated</li> </ul> </li> </ul>
8	<ul style="list-style-type: none"> <li>• <b>Decision Making Authority</b> (s/he will be nominated based on the impact of the “change”; see Appendix 4). <b>Involved only on a Yes recommendation from Enterprise CAB.</b> <ul style="list-style-type: none"> <li>○ NO, go to Step 6 “Enterprise CAB”</li> <li>○ If YES, go to Step 9 “Assemble Resources”</li> </ul> <p><b>NOTE: if the Decision making authority decides for “Yes” , it Requires Approved Service Interruption (ASI) Process to be invoked</b></p> </li> </ul>
9	<ul style="list-style-type: none"> <li>• <b>Assemble resources:</b></li> </ul>

<sup>2</sup> If “Battle Short” procedure is declared, test report is not required.

<sup>3</sup> Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities and Policy process (Appendix 3)



Step	Instructions
	<ul style="list-style-type: none"> <li>○ Release Manager confirms that all of the necessary resources can be accessed to successfully deploy the release into production</li> <li>○ Release Manager confirms that all of the materials and equipment needed for the release have been transported to the site or location where it is to be installed</li> <li>○ Release Manager, shall confirm that the people and process side of the production environment are ready for the release</li> <li>○ Release Manager creates ASI ticket</li> </ul>

## DEPLOYMENT PLAN TEMPLATE

### Document Purpose

This document is intended to provide key stakeholders with a solid understanding of the scope, approach and execution planned for the <Service/Product> Deployment. It will provide important facts on the end-user support to be provided during the Pre-Deployment, Deployment and Post Deployment phases. In particular, this document includes detailed information regarding the approach, issue tracking and escalation process, project communication, contact and conference call numbers, roles and responsibilities, resource allocation, and scheduling during the Post-Deployment Support period. Also included/referenced in the document are Contingency plans, Entrance and Exit Criteria for the Post-Deployment Support period.

### Note

If not otherwise specified by an explicit time-zone-designator all times within this document are stated in ZULU/UTC.

### Scope

In Scope: In scope is the deployment and support of the new <Service/Product> at < CSU, Service Line, other>.

<Make reference to the Project Implementation Plan and fill in anything else that may be in scope on this project>

## Deployment Plan Template

**Document Date:** <date>

**Document Reference Number:** <number>

Service Line:			
Service Name:			
NCI Agency RFC Number:		NCI Agency Project ID:	
ASI Number:		Deployment Activity:	

**Table of Amendments**

Amendment Number	Date Issued	Remarks

**Author (s) Details**

Name	Org/Unit	Contact Email/Phone

**Key Stakeholder Approval**

Approver Name	Org/Unit Role	Signature	Date

**Release Unit (s):**

*Project / Programme team  
Manager or Delegated*

*<Reference change management requirements and Release Units and Release Records from Definitive Media Library (DML)>*

Release Unit / Product Version / CIs

*<Identify the distribution processes for delivering the configuration items / release units to the respective deployment sites>*

**Deployment Schedule:**

*Project / Programme team  
Manager or Delegated*

*<Provide evidence of deployment authorization and RFC acceptance.>*

CSU/Service Line/Site	Start Date	End Date

**Out-of-Scope**

*<Fill in anything that may be out of scope on this deployment activity/project>*

## Constraints and external dependencies

*Project / Programme team*

*Configuration Manager*

- *List of Configuration Items (including the serial numbers, asset tag numbers, locations, etc.) on which the deployment should be implemented;*
- *Related changes, problems and known errors;*
- *A system or service which does not completely conform to its specified requirements should be identified and recorded through configuration management and required change requests submit IAW change management procedures;*
- *Information on known errors should be communicated to incident management;*
- *Identification of any required changes to business processes, procedures or instructions;*

### Support Roles and Responsibilities Detail

*Project / Programme team in cooperation with the prospective Service Owner*

This section describes the support that will be required for the successful deployment of <service/product>, including 2<sup>nd</sup> and 3<sup>rd</sup> level service support that will be available to this <service/product>. The following table describes the roles and responsibilities of the various parties involved in the deployment process.

Role / Responsible Party	Responsibilities
<b>End User</b>	<ul style="list-style-type: none"> <li>Identify &lt;Service/Product&gt; related issues/errors and report the issues to &lt;Responsible Party&gt; for help</li> <li>Attend user training for &lt;Service/Product&gt;</li> <li>Report issues and errors using &lt;Name of incident management tool available to end-user&gt;</li> <li>.....</li> </ul>
<b>Customer</b>	<ul style="list-style-type: none"> <li>Identify &lt;Service/Product&gt; related negative business impacts and report the issues to &lt;Responsible Party&gt; for help</li> <li>.....</li> </ul>
<b>OPSCEN</b>	<ul style="list-style-type: none"> <li>Prepare personnel of all affected Service Desks (central/local) to respond to known issues and frequently asked questions.</li> <li>.....</li> </ul>
<b>CSU</b>	<ul style="list-style-type: none"> <li>Prepare technical infrastructure for the deployment of &lt;Service/Product&gt; as specified by &lt;Responsible Party&gt;</li> <li>.....</li> </ul>
<b>Service Line</b>	<ul style="list-style-type: none"> <li>Ensure 3<sup>RD</sup> level support is in place</li> <li>Ensure escalation process from 2<sup>nd</sup> to 3<sup>rd</sup> level is establish and communicated to all stakeholders (mailbox/POC)</li> <li>.....</li> </ul>
<b>&lt;list other roles and responsibilities&gt;</b>	<ul style="list-style-type: none"> <li>.....</li> </ul>

**Detailed Deployment Activities**

*Project / Programme team*

*Implementation Manager*

#	Date	Start Time (Zulu)	Expected Duration	Cis Affected	Activity Name & Reference to Scripted Instruction	Responsible Resource	Dependent Activities
1	<i>dd-mm-yy or D+0</i>	<i>hh-mm or h +</i>	<i>1 Day</i>				
2							

**Early Life Support (ELS)**

*Project / Programme team*

*Implementation Manager*

The ELS management section contains details about the planned early life support for <service/product>



## Risk Management

*Project / Programme team*

*Risk Manager*

The risk management section contains an analysis of likely risks with both high and low impact, as well as strategies to help the deployment project avoid being derailed should problems arise. The project team to avoid having the analysis become stale and not reflective of actual potential deployment risks periodically reviews the risk management section.

*<Identify risks to the overall deployment plan and address this in your risk log.>*

- *common project pitfalls: lack of resources, unrealistic schedules*
- *deployment success criterion*
- *quality of software during development*
- *legal issues*
- *security issues*
- *quality of training and support*
- *business disruptions*

*<Create a risk matrix for the <service/product> deployment project>*

Severity choices: negligible/marginal/critical/catastrophic

Probability choices: certain/likely/possible/unlikely/rare

Risk strategy choices: avoid/mitigate/accept/share

Risk	Probability	Severity	Risk Strategy	Comments
Site access denied to deployment team members.	Rare	Critical	Avoid	Confirm access procedures with local security authorities before

### Mitigation/Contingency Strategy

<Identify every single possible thing that can go wrong during service deployment activities and address this in your Contingency Strategy.>

- *quality and compatibility of hardware,*
- *quality of infrastructure and underlying services,*
- *quality of data migration procedures and tools,*
- *backups, restorations and other disaster recovery.*

Reduce the risk of disrupting end users by establishing contingency plans. In general, it is possible to isolate and resolve any problems that occur during each phase of the deployment. However, it is important to analyse potential risks and identify the levels of user impact and downtime that might necessitate rolling back the entire deployment and continue to operate in the pre-deployment environment.

## Responsible Personnel

*Project / Programme team*

*Implementation Manager*

*<Define who has overall responsibility for all resources of the service in the event of failure>*

*<Define who will be directing the response and recovery>*

*<Identify who will ensure that all required actions are performed>*

**Critical Events**

*Project / Programme team*

*Implementation Manager and/or Risk Manager*

If a critical risk occurs, it is expected that it will be raised via the service desk to the leader of the onsite deployment team.

Event	Reasons For Failure	Risk Assessment	Options/Backup Resources	Recommendation
<b>Failure of</b> <b>&lt;Resource&gt;</b>	<i>&lt;Identify the possible reasons for failure in priority order&gt;</i> <i>&lt;Identify warning signs or indicators of failure&gt;</i>	<i>Probability</i> <i>&lt;assess chances of event occurring&gt;</i> <i>Impact:</i> <i>&lt;Identify areas that are affected&gt;</i> <i>&lt;List areas that may be affected&gt;</i>	<i>&lt;List any documentation, or backup resources available&gt;</i>	<i>&lt;Outline the steps that should be taken in the event of the loss of a particular resource or service&gt;</i>
<b>Data Corruption</b>				
....				

**Back-out Plan (Rollback Plan)**

*Project / Programme team*

*Implementation Manager and/or Risk Manager*

**Recovery Time Objective (RTO):**

*<State the recovery time objective (this is the time up to which the system is monitored and after which the plan is implemented in order to prevent serious business impact)>*

**Recovery Activities:**

*Example:*

*As part of the Deployment Plan, snapshots of the Virtual Machines of the affected servers will be taken at D 09:30 ZULU with a retention period of 1 week (Activity X, Activity Y ...). This will allow us to roll back to the point in time when the snapshot was taken. Sub-sequent to D + 7, it will not be possible to back out any changes and other workarounds will be required. In the event of a requirement to back out the deployment we will restore the VMs. Estimated restore time is approximately 5 minutes.*

**Notification:**

*<Provide Contact Lists and any other resources that need to be notified, including internal and external contacts (including suppliers and external service providers)>*

### Business Interruption Event Log

*Project / Programme team*

*Implementation Manager and/or Risk Manager*

The leader of the on-site deployment team is responsible to maintain a log of what transpires during the business interruption:

Incident Description	Incident #	Site	Date/Time	Handled by	Description of Resolution

### Identity and Access Management Credentials

The purpose of access management is to manage the rights of users and privileged users to use a service (resource) or groups of services (resources). Access authorisation is accomplished through the execution of both Access and Security Management, which enables the organization to manage the confidentiality and integrity of the organization's data and information.

Access will be initiated by a service request through the Request Fulfilment process or the Change Management process through a Request for Change (RFC), and will rely on Identity Access Management (IDAM) and Security Management to create, update, restrict and remove access rights.

Appendix 5 – the Privilege User Access Request Form shall be submitted to ensure all levels of support can manage the Infrastructure, Platform and Software to deliver the agreed level of support to the Customer.



### Site Service Acceptance Checklist

*Project / Programme team*

*Implementation Manager in collaboration with the  
prospective Service Owner*

The criteria in the **Site Service Acceptance Checklist** for <service/product> (see template in Appendix 2) must be met prior to the end of the Post-Deployment Period (four weeks after end of ELS). NOTE that any exceptions to the exit criteria should be noted and accepted by all key stakeholders (IT and Customer/Business).

**Communication Plan**

*Project / Programme team*

*Implementation Manager*

*<Identify why we need to communicate, what are our communication objectives>*

*<Identify communication channels such as websites, documents, meetings, blogs>*

*<Identify collaterals/material: electronic, paper, multimedia>*

*<Allocate resources: budget, roles, and responsibilities>*

Task or Audience	Channel	Who Drafts	Implementer or Presenter	Draft Due	Final Due	Materials Needed	Complete	Notes



## Training Plan

*Project / Programme team*

*ILS Officer*

The Training Plan describes the approach, activities and tasks required by the deployment team to ensure the necessary skills are attained to achieve the successful deployment of the *service/product*. It also outlines the timeline by which training will be delivered to end-user and technical support staff.

### Training tools and techniques

*<Describe the training techniques that will be used, e.g. instructor-led, online, etc.>*

*<Identify tools needed such as computers, training manuals, facilities etc.>*

### Curriculum

*<Course descriptions and instructors>*

### Training Materials

*<Define what training materials are required (e.g. hand-outs, workbooks, demos, etc.) and who is responsible to prepare training materials by when>*

### Training Environment

*<Identify facilities, equipment, conditions required>*

*<Ensure timely sending of invitations to trainees.>*

### Training Evaluation

*<Describe how feedback will be obtained, e.g. evaluation forms, surveys, questionnaires, etc.>*

*<Describe how feedback obtained will be analysed to ensure the training objectives were met>*

### Detailed training schedule/location

Course	Planned Date/Time	Venue/Location	Instructor
User Training 1			
Tech Training 1			
User Training 2			
.....			

### User Training

*< Define training subjects, training goals per functionality and training per functionality>*

*Instructor: <Identify name of instructor >*

*Training audience: <List staff to be trained>*

### Technical Support Training

*< Define training subjects, training goals per functionality and training per functionality>*

*Instructor: <Identify name of instructor >*

*Training audience: <List staff to be trained>*

## Documentation

*Project / Programme team*

*ILS Officer*

*Perspective Service Owner / CSU Commander*

Appropriate documentation should be available prior to deployment, made available to CSUs and SLs and stored under configuration management against the released configuration item. This documentation should include:

- Support documentation, e.g. SLAs, OLAs and underpinning contracts.
- Mandatory training requirements for service operations staff;
- Support documentation, e.g. system overview, installation and support procedures, diagnostic aids, operating and administration instructions;
- RU/Software distribution processes;
- Installation procedures/scripts;
- Interface for escalation of problems to the 3<sup>rd</sup> level and points of contact at the service lines for the respective service and service assets.
- Configuration baseline for the Release Unit including associated configuration items such as system documentation, test environments, test documentation;
- Service Design Package section related to the Release Unit
- Testing: fit for purpose, fit for use
- Integrated Logistic Plan, including warranty information



## Accreditation

*Project / Programme team*

*Security Officer*

Appropriate documentation about accreditation duration, and renewal plan should be available prior to deployment, made available to CSUs and SLs and stored under configuration management against the released configuration item. This documentation should include:

- Any TEMPEST documentation
- Any current and future documentation released by the accreditation Authorities
- Any proof of security risks accepted by the operational authority for operational reasons.

## AFPL authorisations

*Project / Programme team*

*Security Officer*

Appropriate documentation about the authorisation to operate

## Issue Management

*Project / Programme team*

*Implementation Manager*

During deployment, planning the Issue-Action-Decision Log is used to record deployment issues and their associated actions and owners as well as decisions taken.

### Issues & Actions Log

#	Issue	Status	Owner	Priority	Due Date	Action Item(s) and Comments
1	Engineering Resource availability is limited	Open	PM	High		Acquire funding for contract engineering support
2	.....					
3	.....					

### Decision Log

Decision choices: Approved, Declined, Pending, Cancelled

#	Description	Decision	Decision Date	Related Items	Comments (How and why the decision was made)
1	Will CSU/SL be involved in training end users?	Declined	dd-mm-yy	Training Development	Although more training is needed, it is not cost efficient to establish the required skill base to provide end-user training within local CSUs

Distribution List

*Project / Programme team*

*Implementation Manager*

*<List all stakeholders that are either accountable or responsible for activities identified in this deployment plan as well as those stakeholders that must be consulted or informed about deployment activities>*

**SITE SERVICE ACCEPTANCE CHECKLIST**

<b>Site Service Acceptance Checklist</b>			
The scope of this checklist covers the deployment of new or modified services into live production environments or the retirement of services			
Customer Support Unit / Site			
Service Name:			
NCI Agency RFC Number:		CSU/SL tracking number:	
Change Type: <sup>4</sup>	<input type="checkbox"/> Normal		<input type="checkbox"/> Emergency
Deployment Activity	<input type="checkbox"/> New	<input type="checkbox"/> Modified	<input type="checkbox"/> Retired
<b>Part I: Points of Contact</b> This part identifies all relevant staff (contact details need to include: name, telephone number, unclassified email) that need to be aware of the change.			
Role / POC	primary	(alternate POC)	Notes
Deployment Management	name: tel: email:		
local user/customer representative	rank/name: tel: email:	rank/name: tel: email:	
local Customer Support Unit	name: tel: email:	name: tel: email:	
Service Manager	name: tel: email:	name: tel: email:	
Service Line	name: tel: email:	name: tel: email:	

<sup>4</sup>Changes that are not standard require that all of the Change process steps be completed. These changes require a full range of assessments and authorizations to ensure completeness, accuracy, and the least possible service disruption. In addition, these changes must be scheduled to ensure that blackout periods are not violated, that CI modifications occur during defined Change Windows, that Change owners are available to perform the needed tasks, and so on.

An emergency change is one that must be done immediately. It is of such a high priority that scheduling is not required. An example of an emergency Change might be the installation of new antivirus software during a period of severe viral infestation across the data center.

Standard changes are those that are relatively low-risk and well understood. These changes are often expedited and do not require explicit authorization. It may also be called a pre-approved change. Standard Changes are ones that are processed frequently, such as installing a standard desktop application or a request to add a user to a security group.

Site Service Acceptance Checklist			
Change Management	<i>name:</i> <i>tel:</i> <i>email:</i>		
Quality Assurance	<i>name:</i> <i>tel:</i> <i>email:</i>		
Service Asset and Configuration Mgmt.	<i>name:</i> <i>tel:</i> <i>email:</i>		
<b><i>Part II: Pre-deployment Checks</i></b> This part identifies items/activities that need to be completed before deployment can start, if an item/activity is not required please provide justification under comments (e.g. emergency change)			
<i>Item</i>	<i>Status (pass/ongoing/fail)</i>	<i>Details/Notes/Comments</i>	<i>Initials</i>
notification provided to local CSU & SL 15 working days in advance	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
local CSU & SL provided with Deployment Plan	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
Agency Deployment Authorization Exists	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
Resources and procedures for ELS in place	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
Documentation Availability	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
DML Provided Media Availability	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
DP Identified Hardware Availability	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
All risks, constraints and exclusion are identified and managed	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
SLAs, OLAs and UP Contracts in place	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
Roll-back/contingency plan exists	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
Assign privileged user access credentials	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail	<i>addition check</i>	

<b>Site Service Acceptance Checklist</b>			
	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail	<i>addition check</i>	
<b><u>Part III: Deployment Checks</u></b>			
This part identifies items/activities that need to be conducted during on-site deployment if an item/activity is not required please provide justification under comments (e.g. emergency change)			
<i>Actual deployment</i>	<i>Start:</i>		<i>End:</i>
<i>Item</i>	<i>Status (pass/ongoing/fail)</i>	<i>Details/Notes/Comments</i>	<i>Initials</i>
Service Operations training provided to CSU & SL	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
User training provided to user community	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
Service Line/deployment team has installed and verified service locally	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
individual risks have been mitigated if they occurred	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
Documentation identified in plan provided to CSU & SL	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
Early life support (ELS) is available	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
Known issues and workarounds documented	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
Affected CSUs prepared for Level 1 support	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
OPSCEN prepared for Level 1 Support	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
Verify privileged user access	<input type="checkbox"/> pass <input type="checkbox"/> ongoing <input type="checkbox"/> fail		
<b><u>Part IV: Post-Deployment Exit Criteria</u></b>			
This part identifies items/activities that need to be checked during the Post Implementation Review (PIR) typically taking part after the modified service has been in operations for 6 six weeks			
<i>Item</i>	<i>Completed (yes/partial/no)</i>	<i>Details/Notes/Comments</i>	
Business Objectives of the Change achieved?	<input type="checkbox"/> yes <input type="checkbox"/> partial <input type="checkbox"/> no		
Were customer and user surveys conducted and are statistics on customer/user satisfaction available?	<input type="checkbox"/> yes <input type="checkbox"/> partial <input type="checkbox"/> no		



Site Service Acceptance Checklist		
Stakeholders have agreed to the condition of the service stability and support can be transition to normal production support operations (Service Desk)	<input type="checkbox"/> yes <input type="checkbox"/> partial <input type="checkbox"/> no	
All Very High and High issues pertaining to the changed service have been resolved or are being address in a manner agreed upon with all key stakeholders	<input type="checkbox"/> yes <input type="checkbox"/> partial <input type="checkbox"/> no	
Are the agreed KPIs (e.g. service availability) established and maintained?	<input type="checkbox"/> yes <input type="checkbox"/> partial <input type="checkbox"/> no	
There are no unexpected or undesirable side effects to functionality and service levels.	<input type="checkbox"/> yes <input type="checkbox"/> partial <input type="checkbox"/> no	
Are OLAs, SLA and UP Contracts effective?	<input type="checkbox"/> yes <input type="checkbox"/> partial <input type="checkbox"/> no	
Did the deployment plan work correctly?	<input type="checkbox"/> yes <input type="checkbox"/> partial <input type="checkbox"/> no	
The remediation plan functioned correctly, if needed.	<input type="checkbox"/> yes <input type="checkbox"/> partial <input type="checkbox"/> no	
Service Desk/Integrations Hand-off meeting is held and they agree to officially support the service	<input type="checkbox"/> yes <input type="checkbox"/> partial <input type="checkbox"/> no	
Has Problem Management been notified about all remaining residual risks and all deferred/open issues?	<input type="checkbox"/> yes <input type="checkbox"/> partial <input type="checkbox"/> no	
Service Line (Production team) has assumed responsibility for all deferred/open issues and is ready to resume normal production processes.	<input type="checkbox"/> yes <input type="checkbox"/> partial <input type="checkbox"/> no	
Is the first, second and third level support effective?	<input type="checkbox"/> yes <input type="checkbox"/> partial <input type="checkbox"/> no	
Are issue log and known issues database in place and up-to-date?	<input type="checkbox"/> yes <input type="checkbox"/> partial <input type="checkbox"/> no	

Site Service Acceptance Checklist			
Are user change management procedures in place?	<input type="checkbox"/> yes	<input type="checkbox"/> partial	<input type="checkbox"/> no
Is monitoring and resolutions of incidents and problems conducted?	<input type="checkbox"/> yes	<input type="checkbox"/> partial	<input type="checkbox"/> no
Cost, time and effort adhered to for the deployment?	<input type="checkbox"/> yes	<input type="checkbox"/> partial	<input type="checkbox"/> no
Service catalogue(s) adapted to reflect new release deployment?	<input type="checkbox"/> yes	<input type="checkbox"/> partial	<input type="checkbox"/> no
	<input type="checkbox"/> yes	<input type="checkbox"/> partial	<input type="checkbox"/> no
Findings arising from the implementation and lessons to improve the deployment process or to avoid mistakes in future			
<i>Part V: Final clearance information / Sign-off</i>			
Site Service Acceptance	Signature	Date	Comments
Local CSU			
Service Line Manager			
Quality Assurance			

### ENTERPRISE CAB – DOTMLPFP PROCESS

**Doctrine:** To examine the way the Operational and Technical authorities perform the Operations with emphasizes on the Operational Community that will pay the consequences of the transitional gap. Is there existing doctrine that addresses or relates to the business need covered by the new benefit / deliverables / outcome? Is it NATO or Agency only? Are there operating procedures in place that will be followed during the Operations stage? (**Chief Technology Office Rep**)

- **Organization:** The organization analysis examines how the Agency and the User community are organized to run the Operations stage. It looks to see if there is the right organizational structure in place, or capability that is elsewhere developed addressing the capability gap from another perspective. Where is the transition occurring? What organization(s) are impacted by the Transition? Is the organization properly staffed and funded to deal with the Transition? (**Service Owner/Business Change Manager Rep**)
- **Training:** The training analysis examines how we prepare our workforces to address tactically from basic training, advanced individual training, various types of unit training, joint exercises, and other ways to see if improvement can be made to offset transitional gaps. Is the transition covered, at least in part, by a complete Training plan? Does training exist which addresses the new Operations? (**Education & Training rep**)
- **Materiel:** The materiel analysis examines all the necessary equipment and systems that are needed by our workforces to conduct and operate effectively the new outcome / deliverables or to profit from the new benefit, and if the Logistic plan are presenting any critical gaps. Does the transition-plan address, at least in part, adequate material or equipment? (**Integration Logistics Support rep**)
- **Leadership and Education:** The leadership and education analysis examines how we prepare our leaders to lead the new Operations from OR/B grades to top level leaderships (flagged Officers) and their overall professional development. Does the transition plan ensure that the operational leadership understand the scope of the transition? Does leadership have the resources at their disposal to afford the transition efforts? (**Directorate Service Operation / Customer rep**)
- **Personnel:** The personnel analysis examines availability of qualified people for peacetime, exercise, and wartime operations to support the transition. Is the transition plan addressing the ability or increased ability to place qualified and trained personnel in the correct occupational specialties? Are the right personnel in the right positions (skill set match)? (**Programme / Project rep**)
- **Facilities:** The facilities analysis examines Agency and User property, installations and industrial facilities that support our workforces to afford the transition. Does the transition plan have adequate level of operations and maintenance? Is the infrastructure adequate? (**General Services / Customer rep**)
- **Policy:** The Policy examines any NATO, Agency, or international policy issues that may prevent effective implementation of changes in the other seven DOTMLPFP-P elemental areas. (**Legal / Human Resource rep**)

**DECISION MAKING AUTHORITY**

The main driver to escalate the authorization of change (deployment) is driven by the risk assessment. Dependent upon the level of risk and the category of change, a higher change authority (decision making body) will be consulted. Every IT Change has a risk associated, which is unavoidable. It is up to the Enterprise CAB to assess the risk as best as possible based on the information presented.

Figure 2 below assists in identifying the correct Change Authority.

Change Authority Escalation		Change Category			
		1	2	3	4
Risk Level	5	3	4	5	5
	4	3	4	4	4
	3	3	3	3	3
	2	2	2	3	3
	1	1	2	3	3

Figure 2 -Change Authority Escalation

Depending on the number selected from Figure 2 above, the Change Escalation Authority point of entry can be selected from Figure 3 below.

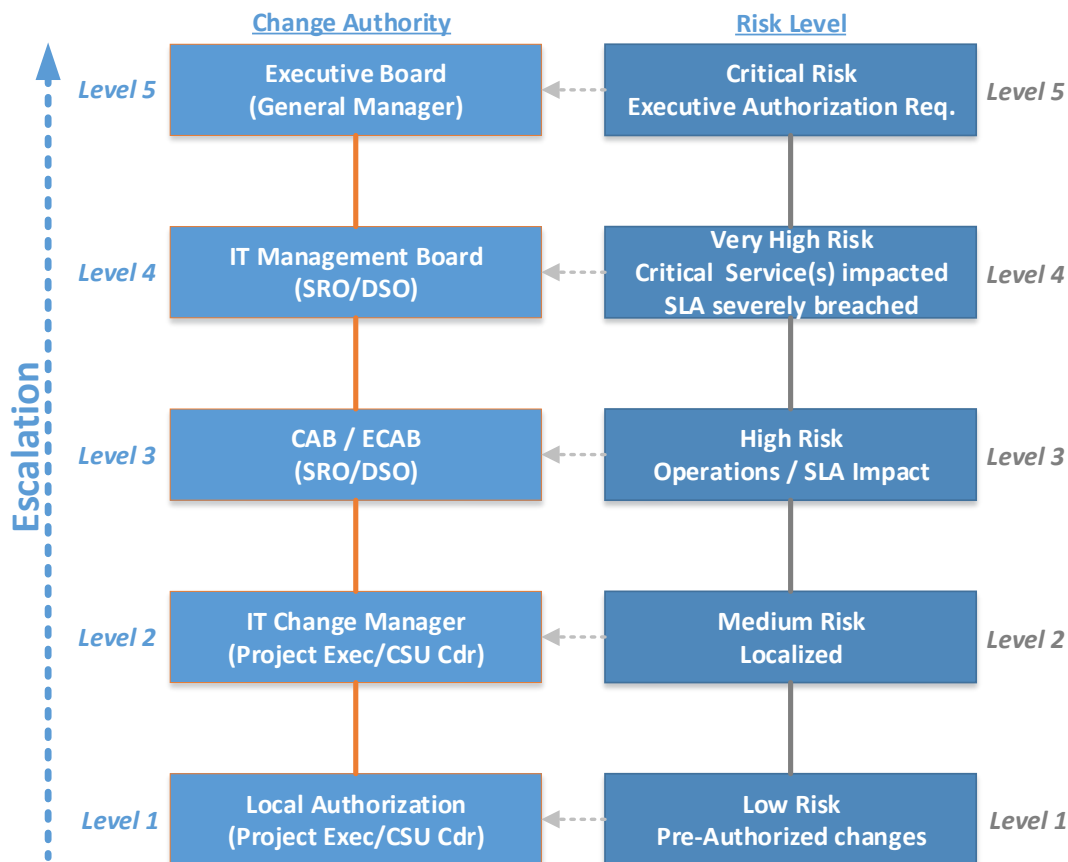


Figure 3: Change Authority Escalation Flow

**PRIVILEGED USER ACCESS REQUEST FORM**

<b>GENERAL INFORMATION</b>				
1.	<u>Request date (dd/mm/yyyy):</u>			
2.	<u>Rank of the Requestor:</u>			
	<u>First and Last Name of the Requestor:</u>			
3.	<u>PE Post / Job title:</u>			
4.	<u>Current Security Clearance</u>			
5.	<u>Current Security Clearance Expiry Date</u>			
Please complete the appropriate fields; for an Access Provision request complete fields 6 to 11, for Change Requests complete fields 12 and 13. <b>The Authorization block is required for ALL Requests.</b>				
<b>ACCESS REQUEST</b>				
6.	<u>Requested Permission System:</u> (Enter the requested System; i.e. Core IS, Network, Functional Services, Cyber Defence, Voice or Boundary Protection Devices).	<u>Access Level:</u> (Level 1, Level 2, Level 3)	<u>Local/Domain/Enterprise Access</u>	<u>Domains:</u> (State which Domain/s – NU, NS, MS access is required)
7.	<u>Location:</u>			
8.	<u>Description:</u>			
9.	<u>Justification:</u> (Please provide a justification/reason for the requested level of permissions)			
10.	<u>Completed training:</u> (Please list the completed training related to the request permission level)			
11.	<u>Experience in:</u> (Please list the experience (examples to include exercises and in the CIS Discipline for which permissions are requested)			
12.	<u>Starting Date:</u> Provide the starting date when the requested permissions need to be delegated			
13.	<u>End Date:</u> Provide the date when the requested permissions need to be revoked (End of NRF/Exercise/Operation). Note:			

	cannot be <u>after</u> Security Clearance expires (5).	
<b>CHANGE REQUEST</b>		
10.	<u>Request for Change type:</u> (Specify whether it is a baseline or membership criteria change)	
11.	<u>Description:</u> (Please provide a detailed explanation of the change)	
<b>AUTHORIZATION</b>		
12.	<u>Section Chief Signature / Date:</u>	
13.	<u>CSU, Service Line</u> <u>Signature / Date:</u>	
14.	<u>Configuration Control Board</u> <u>Signature / Date:</u>	
<b>Change &amp; Configuration Board Decision</b>		
15.	<input type="checkbox"/> Approved <input type="checkbox"/> Rejected Date of Decision/Board Meeting:	
16.	<u>Comments (required for Rejection):</u>	
17.	<u>Board Member Name/Role:</u> <u>Signature / Date:</u>	



NATO Communications and Information Agency  
Agence OTAN d'information et de communication

## **AGENCY INSTRUCTION**

### **AI TECH 06.03.01**

#### **Identification of Software Assets**

Effective date: 21 June 2016 [*precise date as per Approver's e-signature date*]

Revision No: 1

Issued by: Chief, Service Life-Cycle Management Branch \_\_\_\_\_

Approved by: Director Service Strategy \_\_\_\_\_

Table of Amendments

Amendment No	Date issued	Remarks
Rev. 1	21 Jun 2016	Added Naming convention for source code namespaces and assemblies
Amendment 1	27 Oct 2016	Changes made in Annex A, page 15: sub 7, 8, and 9 (marked in red)

Author Details

Organization	Name	Contact Email/Phone
SStrat	Dr Gernot FRIEDRICH	<a href="mailto:gernot.friedrich@ncia.nato.int">gernot.friedrich@ncia.nato.int</a> ; +31 70 374 - 3613



## Table of Contents

1	References .....	4
2	Purpose .....	4
3	Applicability.....	4
4	Scope.....	4
5	NATO Software Versioning and release item Identification .....	5
5.1	Identification of Configuration Items .....	5
5.2	Naming convention for source code namespaces and assemblies .....	5
5.3	Software Versioning .....	7
5.4	Naming Convention .....	9
5.5	Release to Production .....	10
6	Labelling and Marking .....	10
6.1	Software Identification (SWID) Tags .....	10
6.1.1	SWID tags in Contracts .....	10
6.1.2	Generating Tag files .....	11
6.1.3	Installing Tag Files.....	11
6.1.4	Tag Archiving.....	12
6.2	Software Product Documentation.....	13
6.3	Marking of Software Distribution Media.....	13
7	Change Management .....	14
8	Review .....	14
	Annex A: Versioning Specification .....	15
	Annex B: Versioning Pattern for Web Services.....	17
	Annex C: SWID Tag Usage.....	19
	Annex D: Sample SWID Tag Files .....	23
	Annex E: Definitions of Terms .....	26
	Annex F: Classification of Software.....	28
	Annex G: Request for deviation/waiver .....	33

## AGENCY INSTRUCTION (TECH) 06.03.01

### Identification of Software Assets

#### 1 REFERENCES

- A. Directive 1 Rev 1 NCI Agency Executive and Supporting Structures, dated 3 May 2013 ([NCIARECCEN-4-10487](#))
- B. Directive 01.01 Rev 1 Agency Policy on Management and Control of Directives, Notices, Processes, Procedures and Instructions, dated 20 May 2014 ([NCIARECCEN-4-22852](#))
- C. Directive 06.00.01 Management and Control of Directives, Processes, Procedures and Instructions on Service Management, dated 3 Jun 2014 ([NCIARECCEN-4-23297](#))
- D. Directive 06.02.01 Release Management, dated 8 Sep 2014 ([NCIARECCEN-4-26092](#))
- E. ISO/IEC 19770-2 - Software identification (SWID) tag
- F. ISO/IEC 19770-2 - Software identification (SWID) tag, XML Schema, 2009, <http://standards.iso.org/iso/19770/-2/2009/schema.xsd>
- G. RFC 4122, A Universally Unique Identifier (UUID) URN Namespace, July 2005, <http://www.ietf.org/rfc/rfc4122>
- H. Directive 06.01.02 Data Management, dated 7 Feb 2016 ([NCIARECCEN-4-119681](#))

#### 2 PURPOSE

The purpose of this Instruction is to establish – based on best practices – standard conventions to automatically identify NATO Software and software products from third parties that are deployed on NCI Agency managed infrastructure. This identification is a critical enabler for Vulnerability and Configuration Management in general and Endpoint and Software Asset Management (SAM) in particular.

#### 3 APPLICABILITY

This Instruction supports the implementation of AD 06.02.01 (Ref D) and applies to all elements of the Agency, in particular to all NCI Agency staff involved in developing, implementing and maintaining software or software based services. It is the responsibility of all NCI Agency Programme, Service Owners, Service Delivery Managers and Project Managers, Integrated Logist Support Officers to ensure its implementation and to incorporate the content of this technical Instruction into relevant contractual documentation for external suppliers.

#### 4 SCOPE

This document covers all software, specifically developed by NATO or acquired for NATO where the software is either the property of NATO or NATO has unlimited rights to use and distribute. Such software is referred to as NATO Software<sup>1</sup>.

Whilst Release Version Identification for Commercial Off-The-Shelf (COTS) and for Government Off-The-Shelf (GOTS) software are determined by the respective vendors or producers of those products;

---

<sup>1</sup> This excludes specific hardware dependent software, such as firmware.

labelling and marking specification must also be applied to those third party software to be approved for use on NCI Agency managed infrastructure.

Software Identification tags must be created for each and every software configuration item (CI) including purchased Software that is not owned by NATO (e.g. for which we only procure a licence to use).

## 5 NATO SOFTWARE VERSIONING AND RELEASE ITEM IDENTIFICATION

Software versioning is the process of assigning either unique version names or unique version numbers to unique states of computer software. This identification across the entire life-cycle is a critical enabler for Software Development, Configuration Management in general and Software Asset Management in particular with the goals to limit operational and legal risks related to the ownership and use of software. Software Asset Management involves managing and optimizing the acquisition, deployment, maintenance, utilization, and disposal of software assets within an organization. Software assets must be recorded at a level of detail justified by the business need, typically to the level of "independent change".

### 5.1 Identification of Configuration Items

The relationships among a Software Product and its enabling, systems, components and services are defined by boundaries. Such a boundary establishes which items are under direct control of a project. Configuration Items (CI) inside a boundary are under direct project control and are typically part of the NATO Software Product delivered by the project.

- CIs that are provided by parties outside the boundary shall retain their original identification even if this does not comply with the conventions specified by this document. Within the NCI Agency Internal Architecture the relationship "depends on" is to be used to model this relationship.
- If an individual software CI within the boundary of the project is changed – this includes re-generation or recompilation as part of an automated build process - it shall inherit the build number of its parent. Within the NCI Agency Internal Architecture the relationship "is composed of" is to be used to model this relationship.

Reference data<sup>2</sup> sets that are required for the functioning of the software must be put under configuration control as well. Typically reference data sets are used by multiple NATO Software Products and should be managed as a common resource. Configuration management of these reference data sets is the responsibility of the designated data stewards (see Ref H).

### 5.2 Naming convention for source code namespaces and assemblies

Namespaces organize source code objects defined in an assembly. A namespace is a declarative region that provides a scope to the identifiers (the names of types, functions, variables, etc.) inside it. Namespaces are used to organize source code into logical groups and to prevent name collisions and ambiguity that can occur especially when the respective code base includes multiple libraries or when software components are being re-used in different projects. All identifiers at namespace scope are visible to one another without qualification. Identifiers outside the namespace can access the members by using the fully qualified name for each identifier.

---

<sup>2</sup> Reference data is any kind of data that is used solely to categorize other data found in a database, or solely for relating data in a database to information beyond the boundaries of the project. Applications typically implement reference data as tables/arrays that have just a couple of columns — a code and a description — and change slowly over time.

For NATO Software, developers shall use the following naming conventions for namespaces (C# or VB.NET, C++) and packages (Java) of managed source code:

**Nato\_(<productline>\_<product>|<product>|Commons)[\_<component>][\_<subcomponent>]<class>**

**Nato** The root of namespaces for software that is owned by NATO

**"\_"** Separating character(s)

- for C#, VB.NET and Java, single period (Unicode U+002E) “.”
- for C++; double colon (Unicode U+003A) “:.”

**Commons** Software components accessible to all NATO Software projects; these resources are held in common, and are not owned by a single product or productline.

**productline** The name of a set of software-intensive systems that share a common, managed set of features satisfying the specific needs of a particular market segment or mission and that are developed from a common set of core assets in a prescribed way (see also Annex C to AD 06.02.01).

**product** The name of software for which releases will be built. Releases typically result in new product versions (see also Annex C to AD 06.02.01).

**component** The name of a software component or module. The term component is generally used for a re-usable set of source code with discrete structure that can interact with other components within the same parent namespace. Components and modules are an integral piece of any robust application's architecture and typically help in keeping the units of code for a project both cleanly separated and organized.

Examples:

- `Nato.LogFS.MNT.MyClass1`
- `Nato.LogFS.MNT.Scheduling.MyClass2`
- `Nato.Commons.C4ISRViz.MyClass3`

The concept of namespaces does not exist in JavaScript, everything created in JavaScript is by default global. For more information on namespacing patterns for JavaScript to avoid “polluting” the global namespace please see Osmani 2015<sup>3</sup>. Whatever namespacing pattern is used, the naming for those namespaces should follow the naming conventions for Java packages above.

In addition the following guidelines apply:

- a) The level of subcomponents may be arbitrarily deep, but as a recommendation the entire namespace together with the classname should not include more than 5 “periods” in total.
- b) A nested namespace/package should have a dependency on types and classes in the containing namespace/package. For example, the classes in the `Nato.LogFS.MNT.Scheduling` depend on the classes in `Nato.LogFS.MNT`. However, the classes in `Nato.LogFS.MNT` must not depend on the classes in `Nato.LogFS.MNT.Scheduling`.

---

<sup>3</sup> Addy Osmani, *Learning JavaScript Design Patterns*, O'Reilly Media, 2015

- c) Do not use the same name for a namespace/package and a class.
- d) Use plural names for a namespace/package if it is semantically appropriate.
- e) Names of productline, product, (sub-) component shall be composed of a minimum of 2 and a maximum of 128 alphanumeric characters (A-Za-z0-9).
- f) When the package contains multiple sibling namespaces, recommendation is to:
  - a. consider two packages;
  - b. refactoring into single namespace;
  - c. eventually, refactor with appropriate group name.
- g) Use pascal-case notation (case-sensitive), and use it consistently.

**Note:** “Java compiler and interpreter are case-sensitive, so you must capitalize consistently. This case sensitivity reflects Java’s heritage as an outgrowth of C and C++.”

Within high-level programming languages, assemblies are collections of types and resources that form a logical unit of functionality and contain all or part of a reusable library. For example a .NET assembly is either contained in a single dynamic-link library (DLL) or executable (EXE). Where assemblies are the physical organization of a code library, namespaces are a logical organization and should be factored independent of the assembly's organization. Assembly and DLL names do not have to correspond to namespace names but it is reasonable to follow the namespace name when naming assemblies, such as: `Nato.LogFS.MNT.Scheduling.dll`

Source code, classes or libraries which are used from other product lines as dependencies (*depends\_on*) within a product line, both internal to NATO and external (e.g.) will be clearly identified by their own namespaces (e.g. Google Map Class uses `google.maps.Map`)

### 5.3 Software Versioning

As a software evolves, whether by the addition of new functionality, or via changes to the implementation of existing functionality, there is the need to indicate the kind of change. This is important, because applications and services have been constructed which depend upon this functionality. Since changes to the software's interfaces can affect other applications and services, version numbers shall indicate the significance of changes between different releases. Version numbering for NATO Software must conform with the Versioning Specification in Annex A.

At the outset it is important to define the kinds of change that can be introduced to a software product (and which also apply at a finer granularity to individual components of a software product and interfaces to other software products). The following three terms define a simple taxonomy of change:

- A *major release* is an incompatible change to the software, and implies that [some] applications dependent on the earlier major release (specifically those that relied upon the specific features that have changed incompatibly) will need to be changed in order to work on the new major release.
- A *minor release* of the system software is an upward-compatible change - one which adds some new features and interfaces, but maintains compatibility for all existing external interfaces. Applications (or other software products) dependent on an earlier minor release will not need to be changed in order to work on the new minor release: Since the later release contains all the earlier external interfaces, the change(s) imparted to the system does not affect those applications.

- A *revision or patch release* is a compatible change which does not add any new interfaces: A change is made to the implementation (such as to improve performance, scalability or some other qualitative property) but provides an interface equivalent to all other revisions at the same minor level. Again, dependent applications (or other software products) will not need to be changed in order to work on that release as the change imparted to the system (or library) does not undermine their dependencies.

Fixes to software deficiencies not affecting external interfaces increment the patch version, backwards compatible feature or interface additions/changes increment the minor version, and backwards incompatible interface changes increment the major version.

At a fine-grained level, revision control mechanisms such as individual *build numbers* shall be used for identifying incremental development baselines during software development, whether or not this results in an actual release of software.

The correct handling of interface versioning in distributed systems is non-trivial, unfortunately versioning has not been built into the Web services architecture. Developers of NATO web services should use the pattern defined in Annex B.

For mid-to-long term planning purpose such as the maintenance of the Agency's Internal Architecture and Service Portfolio, planned software products may be referenced by a truncated or wildcard notation such as iGeoSIT 2.0 or JOCWatch 2.\*.

Examples:

- JOCWatch 2.0.2.1367-b1
- LOGFAS 6.1.1.1271
- iGeoSIT 2.0.0.2821-rc1 (is composed of):
  - iGeoSIT Client 2.0.0.2821-rc1
  - iGeoSIT Server 2.0.0.2821-rc1
    - is composed of:
      - iGeoSIT Web Map Services 2.0.0.2821-rc1
      - iGeoSIT Databroker Service 2.0.0.2821-rc1
      - iGeoSIT Databroker NVG Service 2.0.0.2821-rc1
      - iGeoSIT NSR Service 2.0.0.2821-rc1
      - iGeoSIT WMS Configuration Tool 2.0.0.2821-rc1
      - iGeoSIT Databroker Configuration Tool 2.0.0.2821-rc1
    - depends on:
      - Symbology Service 1.5.1
      - Java Runtime Environment 1.7.0\_21-b11
      - Apache Tomcat 7.0.39

## 5.4 Naming Convention

All files containing NATO Software Products and configuration items for distribution or deployment shall be identified using the following convention:

**<date>\_<classification>\_<title>\_<version number>[\_<platform>][\_<processor>][\_<local>][.<extension>]**

<b>date</b>	The date should be entered in YYYYMMDD format <sup>4</sup> . The date should be the date the file was created or amended.
<b>classification</b>	Abbreviated classification markings should reflect the highest classification of the content of the file and should use one of the 5 options defined in the Guidance for NATO File Naming [Annex 1 to AC/322-N(2010)0025].
<b>title</b>	Name of the Software Product or Configuration Item in free text, using only characters from the set A-Z, a-z, 0-9, hyphen (U+002D) and brackets (U+0028, U+0029, U+005B, U+005D, U+007B, U+007D).
<b>version number</b>	Must contain at least the major, minor, review parts of the NATO Software version number separated by a dot (".", Unicode U+002E); it may also contain the build part NATO Software version number (see Annex A).
<b>platform</b>	Indicates the operating system type or Application Binary Interface (ABI) for which the software was compiled.  Examples: win32, win64, unix, HPUX, solaris10, osx10.8, linux2.6, glibc23, sles10, el5, debian6.0, freebsd8.0, Android, iOS
<b>processor</b>	Indicates the instruction set of the processor for which the software was compiled. Examples: i386, i586, i686, x86, x86_64, POWER, ARM, ARMv8_A, sparc, IA_64, MIPS, OpenRISC
<b>local</b>	Indicates the language for which the software was localized. The identifier is composed from a language subtag (shortest ISO 639 code) and an optional region two-letter sub-tag according to the assignments found in [ISO3166-1] distinguished and separated from the other subtag by a hyphen ("- ", Unicode U+002D). Examples: fr, en, en-GB
<b>extension</b>	A filename extension is a suffix, separated from the base filename by a dot (".", Unicode U+002E) to the name of a computer file applied to indicate the encoding (file format) of its contents or usage.  Examples : .msi (Microsoft Windows Installer installation package), .pkg.gz (Compressed Solaris Software Package) .iso (disc ISO binary image file), .zip (compressed ZIP archive file), .rpm (Linux package manager file)
<b>"_ "</b>	Separator ("_ ", Unicode U+005F).

### Examples:

- 20140403\_NU\_iGeoSIT\_Server\_2.0.0\_win32\_en.msi
- 20140303\_NU\_NIRIS\_3.6.0\_solaris10\_sparc\_en.pkg.gz

---

<sup>4</sup> This convention follows the basic format as defined in ISO standard 8601

## 5.5 Release to Production

At the end of the release process, the Service/System Manager is accountable for delivering all release units to the Agency's Change Management Authority as a single release package along with Requests For Change (RFC) to initiate the process of deploying the release to a live-environment and/or to add the product as a product offering to the NCI Agency Service Catalogue.

Pre-release type designation must only be used for the software media and accompanying documentation in order to ensure that no further builds have to be produced when a software version designated as RC gets approved. Change Management spearheads the evaluation of the RFCs and approves all RUs of the release package. Any required changes to correct minor defects (e.g. source code or data files) encountered during the software release approval shall result in a new software build (for the same software version). When a RC passes all relevant tests and gets approved for use the pre-release type designator and sequence number shall be removed.

## 6 LABELLING AND MARKING

### 6.1 Software Identification (SWID) Tags

Software identification (SWID) tags shall be used to support security, logistics and compliance by enabling the accurate discovery and inventory of software products. SWID tags support software inventory and asset management initiatives record unique and normalized information about software application, including its name, edition, version, whether it is part of a bundle and more. In support of Cyber Defence activities, service delivery managers must actively manage (inventory, track, and correct) all software on their networks so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

SWID tags are mandatory for NATO Software and media tags shall be added to each software installation media. The SMC Service Line is responsible for maintaining the Definitive Media Library will be accountable for distributing and maintaining the SWID tags for all NATO Software.

Furthermore when the software is installed on NCI Agency controlled infrastructure the SWID information shall be accessible to external agents monitoring the software installed on a target platform, e.g. stored on the hard disk of the server where the software is installed.

#### 6.1.1 SWID tags in Contracts

Software purchasing organizations within NCI Agency must include requirements for appropriate SWID tag support in all contracts for all software configuration items including those that NATO does not own. Practical guidance including sample contractual wording and negotiation points to ensure the Agency receives and can manage required information to accurately identify software, can be found at:

[http://taqvault.org/wp-content/uploads/2013/05/iss-n005-v11\\_how\\_to\\_get\\_vendors\\_to\\_make\\_software\\_more\\_manageablepdf-1.pdf](http://taqvault.org/wp-content/uploads/2013/05/iss-n005-v11_how_to_get_vendors_to_make_software_more_manageablepdf-1.pdf)

For off-the-shelf software that does not have swid tags assigned by the software creator, the contracting officer is responsible to obtain appropriate swid tags from the Release Manager.



### 6.1.2 Generating Tag files

A SWID tag is an XML file containing authoritative identification and management information about a software product; its structure is specified in Reference E. The schema definition (XSD) for XML documents used as software identification tags is available at Reference F. The standard defines 7 mandatory elements and 30 optional elements. The standard also allows for extensions to the structure of SWID tags to ensure the tags can provide additional data required by NATO.

- All software installed on NCI Agency controlled infrastructure shall have a software identification tags (swidtag) in standard conform format.
- Annex C provides more detail on the contents of swidtags for NATO Software.
- Projects are responsible for the creation of swidtags for NATO Software and for third party software acquired for use in NCI Agency managed infrastructure.
- Swidtags for NATO Software shall be extended with STANAG 4774 conformant Confidentiality Labels.
- Swidtags for NATO Software shall be extended with the tag\_type element (xmlns=http://www.tagvault.org/tv\_extensions.xsd).
- Each software asset (including different versions) shall have a unique swidtag assigned.
- Products that are installed as part of a suite a sSWID tag shall be used to identify the suite, and individual products within the suite are assigned their own SWID tags that reference the suite. Those swidtags must maintain the otherwise optional <component\_of> element.
- Software installers used by software developers for NATO Software (i.e. InstallShield, AdvancedInstaller, InstallAnywhere) must support SWID tags.
- For third party software not containing an original swidtag assigned by the software creator, an install package that contains only the software identification tag shall be created.
- In case SWID tags cannot be automatically installed by software installers (e.g. legacy or third party software) the installation documentation shall describe the process to manually install the SWID tags.
- For inspection and preparation for long-term preservation the individual SWID tags shall also be included in the the software installation media as external files.
- All SWID tags created shall be validated that they are well-formed and valid XML and meet the standards defined data restrictions; validated SWID tags may be digitally signed.

Tag file names for NATO Software are to be formatted like:

**<regid>\_<product\_title>-<unique\_software\_identifier>.swidtag**

<b>regid</b>	The regid is a unique and consistent identifier for an organization at a specific point in time. For NATO Software the regid shall be regid.1997-08.int.nato
<b>product_title</b>	The product name, which is the same as the value of <product> in the tag file.
<b>unique_software_identifier</b>	The same as the value of <software_id/unique_id> in the tag file.
<b>"_"</b>	Separator (Unicode U+005F).

### 6.1.3 Installing Tag Files

Two copies of the SWID tag file must be installed on each system that the software is installed on. The first copy of the tag file should be accessible in the top level directory of the installed software package

itself and the second copy of the tag file must be installed in a platform dependent file system location as:

**<file system location>\regid.1997-08.int.nato<tagfilename>**

The file system location is the platform dependant standard location where the software discovery tools expect to find tag files; if the directory "regid.1997-08.int.nato" does not exist it must be created.

Typical values for file system locations are shown in the following table:

<b>platform</b>	<b>file system location / environment variable</b>
Apple® Mac OS X (Leopard and later)	<root>/Library/Application Support/regid.1997-08.int.nato
UNIX and LINUX	usr/share/regid.1997-08.int.nato
Microsoft® Windows 2000 (V5.0), Windows XP (V5.1) and Server 2003+ Server 2003 R2 (V5.2)	%ALLUSERSPROFILE%\Application Data\regid.1997-08.int.nato
Microsoft® Windows Vista (V6.0), Windows Server 2008 (V6.0), Windows Server 2008 R2 (V6.1), Windows 7 (V6.1), Windows Server 2012 (V6.2), Windows 8 (V6.2), Windows Server 2012 R2 (V6.3), and Windows 8.1 (V6.3)	%PROGRAMDATA%\regid.1997-08.int.nato

#### 6.1.4 Tag Archiving

Tag archiving should occur when the software is no longer in use and has been removed from production, development, testing and back up environments. Once this end-of-life status has been reached swidtag files shall be archived for at least 5 years<sup>5</sup>. Change Managers are responsible to submit swidtag files for retired software to NCI Agency Registry for long term preservation. A service at any time can be 'retired', especially when it is progressing as a 'project' in the pipeline phase, in case a software was never deployed on a NCI Agency maintained infrastructure as part of a service the respective project manager is responsible to submit SWID tag files for long term preservation.

Software Identification on User Interfaces Titles and version numbers of the application itself and all of its components together with required copyright notices and disclaimers shall be accessible via the applications' 'About' user control; Figure 1 shows the implementation of this concept in Microsoft Excel 2013. Product Name and/or title of the respective configuration item together with the version number shall also be reflected in the properties of executables or other libraries (i.e. exe, dll file(s)) so that it is displayed by operating systems that supports this.

NATO Software for other environments shall similarly display the installed release version according to the convention for the platform in question (i.e. a command-line application should implement an option or switch /v or -v that displays software identification information or an iOS app should provide version information in the build-in Settings App).

<sup>5</sup> For example, in the US the retention period is 7 year for tax purposes and the EU guidance is a period of 3 years.

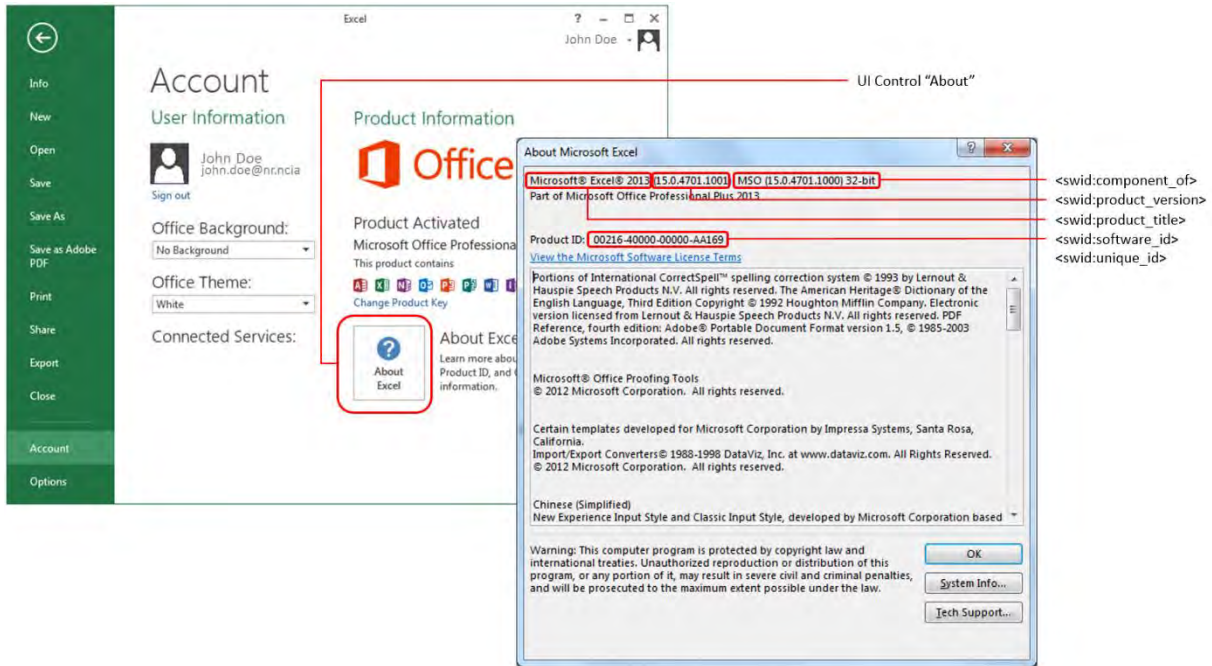


Figure 1: Sample implementation of the "About" concept in MS-Excel 2013

## 6.2 Software Product Documentation

Software product documentation is concerned with describing the delivered software product. It must evolve in step with the product which it describes. Product documentation includes user documentation which tells users how to use the software product and system documentation which is principally intended for maintenance engineers.

A common system maintenance problem is ensuring that all documentation entities are kept in step when underlying CIs change. To help with this, the relationships and dependencies between documents and parts of documents should be recorded. All documents, however short, shall identify the complete name and version identifier of the software they refer to, originator, date of production, the type of document, and configuration management information of the document itself, which might deviate from the Identification Convention defined above. The document shall also contain a list of those CIs (title and version identifier) that the document or parts thereof refers to.

## 6.3 Marking of Software Distribution Media

All media holding NATO Software shall be marked with the complete name and version identifier of the software they contain in accordance with the Software Identification Convention defined above. Media containing only an updated subset of a software system shall be labelled differently, reflecting the fact that such media does not contain a fully installable system (i.e. Service Pack for instance). The media shall also identify the baselined and fielded software release that it applies to.

All media shall carry the required copyright notices and disclaimers for those embedded CIs that are NATO owned or provided by a third party. All CIs that are NATO owned shall be marked as follows:

**NATO PROPERTY/RELEASING AUTHORITY: [name of releasing authority]**

whereby the string "name of releasing authority" may only contain official names of NATO civil or military bodies; CIs developed or acquired by NCI Agency and owned by NATO shall carry the following label: NATO PROPERTY/RELEASING AUTHORITY: NATO Communications and Information Agency.

## **7 CHANGE MANAGEMENT**

Staff across all elements of the Agency may identify the need for changes to this Agency Technical Instruction. Requests for changes (RFCs) to this Technical Instruction shall be made in writing to the Service Strategy Management Support office ([general.sstrat@ncia.nato.int](mailto:general.sstrat@ncia.nato.int)). The Service Strategy Management Support office is responsible for logging all RFCs and to notify the respective custodian.

## **8 REVIEW**

This Instruction will stay in effect until superseded by a further revision or decision of the Director Service Strategy<sup>6</sup> or General Manager NCI Agency. In exceptional circumstances, deviations from the procedures and formats defined in this Instruction can be requested with the request form in Annex G and are subject to approval by the Chairperson of the SLMB<sup>7</sup>.

---

<sup>6</sup> Reference A assigns the responsibility for Design Authority, technical coherence, technical standards, independent testing and validation, architectural control and technical innovation within the Agency to Director Service Strategy (Dir SStrat).

<sup>7</sup> Normally the SLMB is chaired by DSStrat, however, the CONOPS identifies special programmes and projects that are managed directly by GM (SLMB at GM).

## ANNEX A: VERSIONING SPECIFICATION

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

1. Software using NATO Versioning MUST declare a public interface definition. It is RECOMMENDED to declare these interface definitions in the code itself or they MAY exist strictly in documentation. However it is done, interface definitions SHOULD be precise and comprehensive.
2. A normal version number MUST have four parts separated by a period (decimal ASCII Code 46) and take the form X.Y.Z.B where X, Y, Z and B are non-negative integers, and MUST NOT contain leading zeroes. X is the major version, Y is the minor version, Z is the patch version and B is the build number. Each element MUST increase numerically. For instance: 1.9.0.230 -> 1.10.0.267 -> 1.11.0.311
3. Once a versioned release package has been released, the contents of that version MUST NOT be modified. Any modifications MUST be released as a new version.
4. Major version zero (0.y.z.b) is for initial development. Anything may change at any time. The public interface SHOULD NOT be considered stable.
5. Version 1.0.0 defines the first public interface definition. The way in which the version number is incremented after this release is dependent on this public interface definition and how it changes.
6. Build number B (x.y.z.B) MUST be incremented if the source is recompiled or if the processor, platform, or compiler changes. Identifiers MUST NOT be empty and MUST NOT be reset, even across major releases.
7. Patch version Z (x.y.Z.b |  $Z \geq 0$ ) MUST be incremented if only backwards compatible bug fixes are introduced. A bug fix is defined as an internal change that fixes incorrect behavior or a security vulnerability.
8. Minor version Y (x.Y.z.b |  $Y \geq 0$ ) MUST be incremented if new, backwards compatible functionality is introduced to the public interfaces. It MUST be incremented if any public interface functionality is marked as deprecated. It MAY be incremented if substantial new functionality or improvements are introduced within the private code. It MAY include patch level changes. Patch version MUST be reset to 0 when minor version is incremented.
9. Major version X (X.y.z.b |  $X \geq 0$ ) MUST be incremented if any backwards incompatible changes are introduced to the public interfaces. It MAY include minor and patch level changes. Patch and minor version MUST be reset to 0 when major version is incremented.
10. A pre-release version MAY be denoted by appending a hyphen (decimal ASCII Code 45) and one of the following identifiers: *a*, *b*, *te*, *rc* which MAY be followed by a numeric identifier. Numeric identifiers MUST NOT include leading zeroes. A pre-release version indicates that the version is unstable and might not satisfy the intended compatibility requirements as denoted by its associated normal version. Examples: 1.10.0.267-b3, 1.10.0.270-rc1.

- a) Pre-release identifier “a” (for alpha) SHOULD be used if more features are being added to the software.
  - b) Pre-release identifier “b” (for beta) SHOULD be used once the software version is *feature complete*.
  - c) Pre-release identifier “rc” (for release candidate) SHOULD be used for beta version which is *code complete* and with potential to be a final product, which is ready to release unless significant deficiencies emerge.
  - d) Software versions intended to be released externally for test and evaluation purposes MUST use the pre-release identifier “te”.
11. Beta versions MAY contain some untested functionality and/or a number of relatively minor software deficiencies; they are often not yet integrated into the wider software environment and have undergone only software engineering testing by the developer team. Because of the low maturity status, these releases are not expected to run stably and SHALL NOT be used operationally. The focus of testing beta releases is detecting and reducing impacts to users.
  12. Pre-release versions have a lower precedence than the associated normal version. A pre-release version indicates that the version is unstable and might not satisfy the intended compatibility requirements as denoted by its associated normal version.
  13. Precedence refers to how versions are compared to each other when ordered. Precedence MUST be calculated by separating the version into major, minor, patch and build metadata in that order. Precedence is determined by the first difference when comparing each of these identifiers from left to right as follows: Major, minor, patch versions and build number are always compared numerically.

## ANNEX B: VERSIONING PATTERN FOR WEB SERVICES

The correct handling of interface versioning has been a difficult issue faced by developers of distributed systems. Unfortunately versioning has not been built into the Web services architecture, requiring developers to solve the problem through the application of patterns and best practices. Changes in an interface and the associated WSDL document can either be backwards-compatible or non-backwards-compatible, respectively.

The types of changes that are backwards compatible are:

- *Addition of new WSDL operations to an existing WSDL document.* If existing service consumers are unaware of a new operation, then they will be unaffected by its introduction.
- *Addition of new XML schema types within a WSDL document that are not contained within previously existing types.* Even if a new operation requires a new set of complex data types, as long as those data types are not contained within any previously existing types (which would in turn require modification of the parsing code for those types), then this type of change will not affect an existing service consumer.

There are many other change types that are not backwards-compatible; these include:

- Removing an operation
- Renaming an operation
- Changing the parameters (in data type or order) of an operation
- Changing the structure of a complex data type.

Software developer should use different strategies for handling the two different types of changes.

For backwards-compatible changes, the WSDL document and the existing Web service must be updated. It is recommended that every new edition of a WSDL document be stored in a version-control system, and that for the web service a unique version number in accordance with the Versioning Specification in Annex A is assigned (increasing the minor part of the version number). However, this is purely for the convenience of the Web service developers, and is not required by the implementers of the Web service consumers.

For non-backwards-compatible changes, another approach shall be used. When the interface to a service changes in a non-backwards-compatible way, in reality an entirely new service is being created. In this situation, developers should use unique XML namespaces to clearly delineate the versions of a document that are compatible or not. It is recommended to use a simple naming scheme that appends a date or a version stamp in accordance with the Version specification in Annex A to the end of a namespace definition that semantically (and specifically) denote the particular namespace. The actual mechanism by which this is done depends on whether the SOAP binding is done using the literal- or SOAP-encoded use style in WSDL. In literal encoding, the namespace is specified in the definition of the messages as part of the XML schema namespace definitions; in SOAP encoding, it can be specified within the SOAP binding element. Regardless of the mechanism chosen, a specific namespace value is sent along with every SOAP message and result. This allows a Web service implementation to correctly determine what to do with an incoming message, based on the namespace value.

If the namespace has changed, developers have to determine what to do with old service consumers. In case of a major version change the previous service may be retired and a failure on the server end should be generated if a request for an older namespace is received. For minor version changes, both versions of the web service have to be maintained and deployed, at least for the transitional period until all of the older service consumers have moved over to the new WSDL.

Namespace document shall contain the following annotation:

This namespace URI will only be used to refer to this version of this specification: different URIs will be used for any and all new versions of the specification except as follows: This namespace URI may be reused in any update of the specification which is made for the purpose of clarification or bug fixes. These changes will be minor in that they do not (a) change the meaning or validity of existing documents written using the namespace, or (b) affect the operation of existing software written to process such documents.



### ANNEX C: SWID TAG USAGE

The following table lists the element and values to be used in software identification tag files for NATO Software, whilst the swid tag schema defines the usage of several elements as optional, all following elements shall be maintained for NATO Software.

Element	Description/Values	ISO-19777 Obligation Category
entitlement_required_indicator	<i>true</i> for serialized/activated  <i>false</i> for trial/unlicensed  Format: boolean	mandatory
product_title	Configuration Item Name (product, application or component), string composed of 2 to 128 alphanumeric characters.  Example: "iGeoSIT Server"	mandatory
product_version		
<ul style="list-style-type: none"> <li>▪ name</li> </ul>	string version (major, minor), Example "2.0.0 RC1"	mandatory
<ul style="list-style-type: none"> <li>▪ numeric <ul style="list-style-type: none"> <li>○ major</li> </ul> </li> </ul>	Software with the same name but different major versions is not interchangeable.  Format: unsigned integer  A higher version number might indicate a significant change of a product interface where backward compatibility cannot be assumed. Major version zero (0) is for initial development when anything may change at any time.	mandatory
<ul style="list-style-type: none"> <li>○ minor</li> </ul>	The minor version number indicating significant enhancement with the intention of backward compatibility.  Format: unsigned integer  Restarts at 0 with each subsequent major version release.	mandatory
<ul style="list-style-type: none"> <li>○ review</li> </ul>	Patch or revision release number;  Format: unsigned integer  Restarts at 0 with each subsequent minor version release.	mandatory
<ul style="list-style-type: none"> <li>○ build</li> </ul>	The build number is used to identify incremental development baselines during software development.  Format: unsigned integer  A difference in build number represents a recompilation of the source code. Different build numbers might also be used when the processor, platform, or compiler changes. Build number is never reset, even across major releases.	mandatory
product_category	Identifies and categorizes the type of software this SWID tag refers to. For possible codes, refer to <a href="http://www.unspsc.org">www.unspsc.org</a> . Most codes for software will be found in the 4323xxxx section of the code (see Annex F).	optional
<ul style="list-style-type: none"> <li>▪ commodity_title</li> <li>▪ code</li> </ul>		
software_creator	For NATO Software, the following values shall be used:	mandatory
<ul style="list-style-type: none"> <li>▪ name</li> <li>▪ regid</li> </ul>	<ul style="list-style-type: none"> <li>▪ North Atlantic Treaty Organization</li> <li>▪ regid.1997-08.int.nato[,additional naming authority]</li> </ul> For software owned by a third party software_creator represents the registered name of the original software creator	

Element	Description/Values	ISO-19777 Obligation Category
	<p>Example: Adobe Reader</p> <ul style="list-style-type: none"> <li>▪ Adobe Systems Incorporated</li> <li>▪ regid.1986-12.com.adobe</li> </ul>	
software_licensor		mandatory
<ul style="list-style-type: none"> <li>▪ name</li> <li>▪ regid</li> </ul>	<ul style="list-style-type: none"> <li>▪ North Atlantic Treaty Organization</li> <li>▪ regid.1997-08.int.nato [,additional naming authority]</li> </ul> <p>For software developed or acquired by a NATO body the additional naming authority shall bear the full name of tbody, e.g. <i>NATO Communications and Information Agency</i></p>	
software_id		mandatory
<ul style="list-style-type: none"> <li>▪ unique_id</li> <li>▪ tag_creator_regid</li> </ul>	<ul style="list-style-type: none"> <li>▪ Universally Unique Identifier (UUID), generated in accordance with IETF RFC 4122 (reference G) or another identifier which uniqueness within the context of regid.1997-08.int.nato must be guranteed</li> <li>▪ regid.1997-08.int.nato [,additional naming authority]</li> </ul>	
component_of	Used to provide child / parent information related to the application or group, for example that the application is a component of software X.	optional
<ul style="list-style-type: none"> <li>▪ unique_id</li> <li>▪ tag_creator_regid</li> </ul>	<ul style="list-style-type: none"> <li>▪ unique_id = identifier of parent application</li> <li>▪ tag_creator_regid = regid of who provided conformation of component relationship</li> </ul>	
complex_of	Used to provide child/parent information related to the application, for example that this application is the parent of package a, package b, package c.	optional
<ul style="list-style-type: none"> <li>▪ unique_id_1</li> <li>▪ unique_id_2</li> <li>▪ unique_id ...</li> <li>▪ tag_creator_regid</li> </ul>	<ul style="list-style-type: none"> <li>▪ unique_id_1 = identifier of child application 1</li> <li>▪ unique_id_2 = identifier of child application 2</li> </ul> <p>(NOTE: The number of child components/applications will vary, add lines as required)</p> <ul style="list-style-type: none"> <li>▪ tag_creator_regid = regid of who provided conformation of child/ parent relationship</li> </ul> <p><i>This element would only be present if the software was a parent of other software items</i></p>	
tag_creator		mandatory
<ul style="list-style-type: none"> <li>▪ name</li> <li>▪ regid</li> </ul>	<ul style="list-style-type: none"> <li>▪ North Atlantic Treaty Organization</li> <li>▪ regid.1997-08.int.nato [,additional naming authority]</li> </ul>	
tag_type	Tag_type is a TagVault.org extension. Provides a way to clearly identify the tagged element and enables building the tag relationship model. Possible values: {application, component, feature, group, patch, media}	n/a
ConfidentialityLabel	ConfidentialityLabel is a NATO specific extension in accordance with STANAG / ADatP-4774 used to indicate the Security classification of the Software. If the software is classified the entire SWID tag MUST be digitally signed.	n/a
abstract_application_info	Provides brief information on application	optional

Element	Description/Values	ISO-19777 Obligation Category
license_linkage <ul style="list-style-type: none"> <li>▪ activation_status</li> <li>▪ channel_type</li> <li>▪ customer_type</li> </ul>	Defines the channel and type of license (i.e. OEM vs. Volume) that can affect the user's rights. See ISO/IEC 19770-2:2009 for guidance.	optional
serial_number	This is the product reconciliation information, and can be used to validate the product against a bespoke license agreement.	optional

Multiple levels of relationships can be specified. The high level perspective of this structure is shown below:

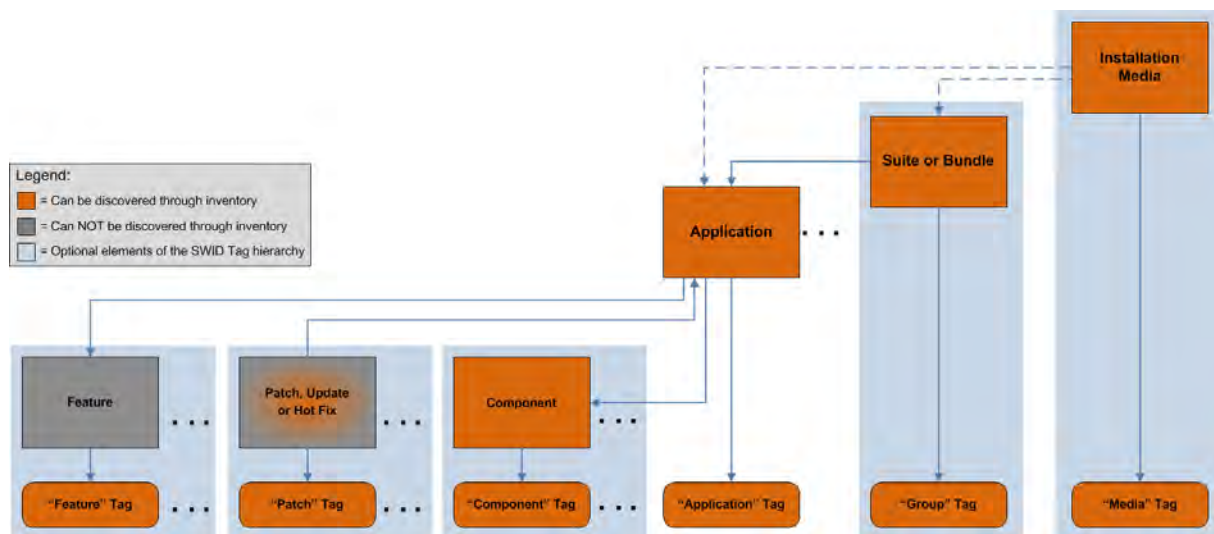


Figure 2: Relationship between different SWID Tags

These relationships include both parent to child (*complex\_of*) and child to parent relationships (*component\_of*) and also include an element that indicates *tag\_type*. Using this structure, it is possible to identify software at the level required for the specific task. In security content automation, this may entail finding a suite or a bundle and identifying all installed applications that belong to that bundle. It may also entail the identification of a patch (that identifies the application or component it applies to) and automatically receiving an exception when a patch becomes available and there are components, applications or suites that exist within an infrastructure, but have not yet been patched.

#### Media tags:

- A "Media" *tag\_type* is used to identify the files and data used to install software.
- A "Media" *tag\_type* will generally not be used for license reconciliation, but if digitally signed, may be used to validate that the installation files are exactly the same as what was published by the publisher.
- A "Media" *tag\_type* may also reference other tags to indicate which "Group(s)" or "Application(s)" may be installed by using the media.

#### Group tags:

- A "Group" *tag\_type* represents a suite or bundle of applications that are licensed as a group of items instead of individually.

- A Suite will often be comprised of multiple related applications as in the case of Microsoft Office – the applications are office productivity applications.
- A Bundle will often be comprised of multiple different applications that are grouped together as in the case of a new computer purchase that bundles multiple software titles together in an OEM bundle.

#### Application tags:

- An “Application” *tag\_type* is a software entity that is acquired for installation and use.
- An “Application” can be instantiated by a single executable file, comprised of multiple files, and/or one or more subordinate software entities referred to as “components”.
- The Use Case of an “Application” with one or more “Components” can involve Intellectual Property (IP) from a single or multiple publishers.

#### Component tags:

- A “Component” *tag\_type* is a software item that may not have been developed by the application owner (examples, include OEM components, software libraries that may need to be independently identified or open source software that is not built directly into the application).
- The “Component” *tag\_type* allows a software item to be identified as related to an application’s installation and is expected to be included as part of the applications entitlement. For example, an application that includes Microsoft SQL Express Edition should include a reference to a component tag indicating that SQL Express Edition is related to this application.

#### Patch tags:

- A “Patch” *tag\_type* represents an update to an application that is typically not a full product upgrade (which would include a new software ID tag), but is a fix to product that only modifies portions of the product.
- A patch is generally added to the set of installed applications/features/components after the fact.
- It is useful to the automation of IT processes if a patch identifies which item it modifies.

#### Feature tags:

- A “Feature” *tag\_type* represents two or more licensable “products” packaged WITHIN a SINGLE “Application” that require separate entitlement to enable their use.

In addition a SWID tag may contain addition data such as:

#### Payload data

- Filename, size, file hash(es)
- Process information
- Other resources (dev entries, registry settings, etc)

#### Digital Signatures

- All data can be signed at production time

#### Other links

- References to other installers/additional related software
- Referenced payload data
- Other software dependency requirements
- Supplemental information (customer provided, licensing details specified, etc)
- Structural information (identifies how software packages are related to one another).

**ANNEX D:  
SAMPLE SWID TAG FILES**

**File:** C:\ProgramData\regid.1997-08.int.nato\regid.1997-08.int.nato iGeoSIT-Win-en\_GB-2.0.0.swidtag

```
<?xml version="1.0" encoding="utf-8"?>

<swid:software_identification_tag xmlns:ns2="http://www.w3.org/2000/09/xmldsig#"
xmlns:swid="http://standards.iso.org/iso/19770/-2/2009/schema.xsd">
  <swid:entitlement_required_indicator>false</swid:entitlement_required_indicator>
  <swid:product_title>iGeoSIT 2.0 Server</swid:product_title>
  <swid:product_version>
    <swid:name>2.0.0</swid:name>
    <swid:numeric>
      <swid:major>2</swid:major>
      <swid:minor>0</swid:minor>
      <swid:build>2821</swid:build>
      <swid:review>0</swid:review>
    </swid:numeric>
  </swid:product_version>
  <swid:software_creator>
    <swid:name>North Atlantic Treaty Organization</swid:name>
    <swid:regid>regid.1997-08.int.nato,NATO Communications and Information Agency</swid:regid>
  </swid:software_creator>
  <swid:software_licensor>
    <swid:name>NATO Communications and Information Agency</swid:name>
    <swid:regid>regid.1997-08.int.nato, NATO Communications and Information Agency</swid:regid>
  </swid:software_licensor>
  <swid:software_id>
    <swid:unique_id>iGeoSIT_Server-Win-en_GB-2.0.0</swid:unique_id>
    <swid:tag_creator_regid>regid.1997-08.int.nato</swid:tag_creator_regid >
  </swid:software_id>
  <swid:component_of>
    <swid:unique_id>iGeoSIT-Win-en_GB-2.0.0</swid:unique_id>
    <swid:tag_creator_regid>regid.1997-08.int.nato</swid:tag_creator_regid >
```

```

</swid:component_of>
<swid:tag_creator>
  <swid:name>...</swid:name>
  <swid:regid>...</swid:regid>
</swid:tag_creator>
<swid:product_category> ... </swid:product_category>
<swid:product_family> ... </swid:product_family>
<swid:complex_of> ... </swid:complex_of>
<Payload date="08-18-2014" deviceId="NRNATO-3509X7Z4.NR.NCIA" >
  <File name="foo.txt"
    filesystem:attributes="hidden readonlysystem"
    SHA256:hash="9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08"
    MD5:hash="098f6bcd4621d373cade4e832627b4f6"
    SHA1:hash="a94a8fe5ccb19ba61c4c0873d391e987982fbbd3"/>
</Payload>

<extended_information>
<!-- TagVault.org extension -->
<tag_type xmlns="http://www.tagvault.org/tv_extensions.xsd">application</tag_type>
<!-- NATO Confidentiality Label extension -->
<ConfidentialityLabel xmlns="http://www.nato.int/2014/06/nl/cl" ReviewDateTime="2019-04-01T09:00:00Z">
  <ConfidentialityInformation xmlns="http://www.nato.int/2014/06/nl/cl">
    <PolicyIdentifier xmlns="http://www.nato.int/2014/06/nl/cl">NATO</PolicyIdentifier>
    <Classification xmlns="http://www.nato.int/2014/06/nl/cl">UNCLASSIFIED</Classification>
    <Category xmlns="http://www.nato.int/2014/06/nl/cl" Type="PERMISSIVE" TagName="Context">
      <GenericValue xmlns="http://www.nato.int/2014/06/nl/cl">NATO-7</GenericValue>
    </Category>
  </ConfidentialityInformation>
  <CreationDateTime xmlns="http://www.nato.int/2014/06/nl/cl">2014-04-01T09:00:00Z</CreationDateTime>
</ConfidentialityLabel>

</extended_information>
</software_identification_tag>
</swid:software_identification_tag>

```



C:\ProgramData\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft Microsoft Office Professional Plus  
2013.swidtag

```
<?xml version="1.0" encoding="utf-8"?>
<software_identification_tag xmlns="http://standards.iso.org/iso/19770/-2/2009/schema.xsd">
<entitlement_required_indicator>true</entitlement_required_indicator>
  <product_title>Microsoft Office Professional Plus 2013</product_title>
  <product_version>
    <name>15.0.4420.1017</name>
    <numeric>
      <major>15</major>
      <minor>0</minor>
      <build>4420</build>
      <review>1017</review>
    </numeric>
  </product_version>
  <software_creator>
    <name>Microsoft Corporation</name>
    <regid>regid.1991-06.com.microsoft</regid>
  </software_creator>
  <software_licensor>
    <name>Microsoft Corporation</name>
    <regid>regid.1991-06.com.microsoft</regid>
  </software_licensor>
  <software_id>
    <unique_id>90150000-0011-0000-0000-00000000FF1CE</unique_id>
    <tag_creator_regid>regid.1991-06.com.microsoft</tag_creator_regid>
  </software_id>
  <tag_creator>
    <name>Microsoft Corporation</name>
    <regid>regid.1991-06.com.microsoft</regid>
  </tag_creator>
  <extended_information>
    <tag_type xmlns="http://www.tagvault.org/tv_extensions.xsd">application</tag_type>
  </extended_information>
</software_identification_tag>
```

## ANNEX E: DEFINITIONS OF TERMS

This annex defines a set of common terms used within this document. Those terms that have been imported from International Standards such as ISO19770-2 are indicated by stating the respective ISO Standard number and appending the particular subsection citation to the overall reference citation separated by a colon.

**Bundle:** A grouping of products which is the result of a marketing/licensing strategy to sell entitlements to multiple products as one purchased item. A bundle can be referred to as a “suite”, if the products are closely related and typically integrated (such as an office suite containing a spreadsheet, word processor, presentation and other related items) [ISO/IEC 19770-5:2013].

**Component:** An entity with discrete structure, such as an assembly or software module, within a system considered at a particular level of analysis [ISO19770-2:4.1.3]. Component refers to a part of a whole, such as a component of a software product, a component of a software identification tag, etc.

**Configuration Item:** An item or aggregation of hardware or software or both that is designed to be managed as a single entity [ISO19770-2:4.1.5]. Configuration Items are characterized by their attributes and their relationships to other CIs; this information is recorded in a Configuration Record for each Configuration Item (CI) within the Configuration Management System and is maintained throughout its Lifecycle by Configuration Management. CIs are under the control of Change Management. CIs may vary widely in complexity, size and type, ranging from an entire system including all hardware, software and formal documentation, to individual IT Services and Service Level Agreements or to a single module, a minor hardware component or a single software package.

**Definitive Media Library:** One or more locations in which the definitive and approved versions of all software Configuration Items are securely stored. The Definitive Media Library may also contain associated CIs such as licenses and documentation. The Definitive Media Library is a single logical storage area even if there are multiple locations. All software in the Definitive Media Library is under the control of Change and Release Management and is recorded in a Configuration Management System.

**Deployment:** The activity responsible for movement of new or changed hardware, software, documentation, Process, etc. to the Live Environment. [ITIL V3]

**Maintenance Release:** Maintenance, bug fix or patch releases are version changes designed to fix identified critical problems such as security vulnerabilities and other bug and might also address improvements to usability or performance. It typically excludes new features or changes of the Human Machine Interface (HMI), Application Programming Interface (API), service interfaces or the data structure – unless fixing a defect or security vulnerability requires such changes. Third party systems can most likely use the systems further without modification.

Two categories of maintenance release are identified: Emergency and Routine and will be processed accordingly.

**Major Release:** Incrementing the major release number is generally a programmatic or life-cycle management decision. It is typically indicated by major enhancements and improvements such as the addition of key features to the functional baseline of a system; including major changes to the HMI concept, API, service interfaces, data structures and templates as well as new interfaces or a modified/enhanced control concept it can also include a change to the underlying platform(s) (i.e. a computer or hardware device and/or associated operating system, or a virtual environment, on which software can be installed or run). It may also refer as to the increment to an initial release.



**Minor Release:** Minor release numbers are incremented when minor enhancements and improvements to the existing features of a functional baseline are made. It includes new features and can include minor changes of the HMI, API, service interfaces, data structure or templates. Fundamental changes e.g. of the HMI concept are not to be expected though. A new minor release should maintain all interfaces introduced since the previous major release.

**Release:** A collection of new and/or changed configuration items which are tested and introduced into a production environment together [ISO19770-2:4.1.21] to implement one or several approved changes.

**software creator:** The person or organization that creates a software product or package. This entity might or might not own the rights to sell or distribute the software [ISO/IEC 19770-5:2013].

**software product:** A complete set of software designed for delivery to a software consumer or end-user that may contain computer programs, procedures and associated documentation and data [ISO/IEC 19770-5:2013].

**ANNEX F:  
CLASSIFICATION OF SOFTWARE**

The United Nations Standard Products and Services Code (UNSPSC) is an open, global, multi-sector standard for efficient, accurate five level hierarchical classification of products and services. Most codes for software will be found in the 4323xxxx section of the code set:

<b>Code</b>	<b>Commodity Title</b>
43230000	Software
<b>43231500</b>	<b>Business function specific software</b>
43231501	Helpdesk or call center software
43231503	Procurement software
43231505	Human resources software
43231506	Materials requirements planning logistics and supply chain software
43231507	Project management software
43231508	Inventory management software
43231509	Bar coding software
43231510	Label making software
43231511	Expert system software
43231512	License management software
43231513	Office suite software
43231514	Sales and marketing software
43231515	Mailing and shipping software
43231516	Audit software
43231517	Procedure management software
<b>43231600</b>	<b>Finance accounting and enterprise resource planning ERP software</b>
43231601	Accounting software
43231602	Enterprise resource planning ERP software
43231603	Tax preparation software
43231604	Financial analysis software
43231605	Time accounting software
<b>43232000</b>	<b>Computer game or entertainment software</b>
43232001	Action games
43232002	Adventure games
43232003	Sports games
43232004	Family software
43232005	Music or sound editing software
<b>43232100</b>	<b>Content authoring and editing software</b>
43232101	Pattern design software
43232102	Graphics or photo imaging software
43232103	Video creation and editing software
43232104	Word processing software
43232105	Charting software
43232106	Presentation software
43232107	Web page creation and editing software

Code	Commodity Title
43232108	Calendar and scheduling software
43232110	Spreadsheet software
43232111	Optical character reader OCR or scanning software
43232112	Desktop publishing software
<b>43232200</b>	<b>Content management software</b>
43232201	Content workflow software
43232202	Document management software
43232203	File versioning software
43232204	Embedded text entry software
43232205	Fonts software
<b>43232300</b>	<b>Data management and query software</b>
43232301	Categorization or classification software
43232302	Clustering software
43232303	Customer relationship management CRM software
43232304	Data base management system software
43232305	Data base reporting software
43232306	Data base user interface and query software
43232307	Data mining software
43232309	Information retrieval or search software
43232310	Metadata management software
43232311	Object oriented data base management software
43232312	Portal server software
43232313	Transaction server software
43232314	Business intelligence and data analysis software
<b>43232400</b>	<b>Development software</b>
43232401	Configuration management software
43232402	Development environment software
43232403	Enterprise application integration software
43232404	Graphical user interface development software
43232405	Object or component oriented development software
43232406	Program testing software
43232407	Requirements analysis and system architecture software
43232408	Web platform development software
43232409	Compiler and decompiler software
<b>43232500</b>	<b>Educational or reference software</b>
43232501	Foreign language software
43232502	Computer based training software
43232503	Spell checkers
43232504	Route navigation software
43232505	Multi-media educational software
43232506	Encyclopedia software
43232507	Dictionary software
43232508	Phonebook software

Code	Commodity Title
43232509	Voice synthesizer and recognition software
43232510	Geographic information system
<b>43232600</b>	<b>Industry specific software</b>
43232601	Aviation ground support software
43232602	Aviation test software
43232603	Facilities management software
43232604	Computer aided design CAD software
43232605	Analytical or scientific software
43232606	Compliance software
43232607	Flight control software
43232608	Industrial control software
43232609	Library software
43232610	Medical software
43232611	Point of sale POS software
43232612	Computer aided manufacturing CAM software
43232613	Manufacturing execution system MES software
43232614	Computer aided design CAD and computer aided manufacturing CAM system
43232615	Facial recognition software
43232616	Legal management software
43232617	Meteorological control software
43232618	Radar image treatment software
43232619	Satellite image treatment software
<b>43232700</b>	<b>Network applications software</b>
43232701	Application server software
43232702	Desktop communications software
43232703	Interactive voice response software
43232704	Internet directory services software
43232705	Internet browser software
<b>43232800</b>	<b>Network management software</b>
43232801	Network monitoring software
43232802	Network operating system enhancement software
43232803	Optical network management software
43232804	Administration software
43232805	Internet protocol IP multimedia subsystem software
<b>43232900</b>	<b>Networking software</b>
43232901	Access software
43232902	Communications server software
43232903	Contact center software
43232904	Fax software
43232905	LAN software
43232906	Multiplexer software
43232907	Storage networking software
43232908	Switch or router software

Code	Commodity Title
43232909	WAN switching software and firmware
43232910	Wireless software
43232911	Network connectivity terminal emulation software
43232912	Gateway software
43232913	Bridge software
43232914	Modem software
43232915	Platform interconnectivity software
43232916	Infrared data transfer irda software
<b>43233000</b>	<b>Operating environment software</b>
43233001	Filesystem software
43233002	Network operation system software
43233004	Operating system software
43233005	Computer firmware
43233006	Virtual machine software
43233200	Security and protection software
43233201	Authentication server software
43233203	Network security or virtual private network VPN management software
43233204	Network security and virtual private network VPN equipment software
43233205	Transaction security and virus protection software
43233400	Utility and device driver software
43233401	Compact disc CD server software
43233402	Data conversion software
43233403	Data compression software
43233404	Compact disc CD or DVD or sound card software
43233405	Device drivers or system software
43233406	Ethernet driver software
43233407	Graphics card driver software
43233410	Printer driver software
43233411	Screen saver software
43233413	Voice recognition software
43233414	Storage media loading software
43233415	Backup or archival software
43233416	Codec stacks
43233417	Handwriting recognition software components
43233418	Memory drivers
43233419	Multimedia stacks
43233420	Text to speech conversion software
43233421	Video drivers
43233500	Information exchange software
43233501	Electronic mail software
43233502	Video conferencing software
43233503	Network conferencing software
43233504	Instant messaging software

<b>Code</b>	<b>Commodity Title</b>
43233505	Ambient music or advertising messaging software
43233506	Map creation software
43233507	Mobile operator specific standard software
43233508	Mobile operator specific application software
43233509	Mobile messaging service software
43233510	Mobile internet services software
43233511	Mobile location based services software
43233512	Ring tone software
43233600	Electrical Equipment software
43233601	Motor Drive Software
43233602	Power Monitor Software
43233603	Programmable Logic Control Software
43233700	System management software
43233701	Enterprise system management software

Source: <https://www.unspsc.org/>

**ANNEX G:  
REQUEST FOR DEVIATION/WAIVER**

Request for Deviation/Waiver: Identification of Software Assets			
Project No and Name			
Project Description			
Requested by:		Request Date:	
Waiver is requested for the following parts of the Instruction:			
<input type="checkbox"/> Software Versioning	<input type="checkbox"/> Naming Convention	<input type="checkbox"/> Release to Production	
<input type="checkbox"/> SWID Tags	<input type="checkbox"/> Product Documentation	<input type="checkbox"/> Marking of Distribution Media	
Justification for deviation			
<p><i>&lt;The justification must include the rationale why the corporate policy can not be implemented at this time. Please indicate the impacts to the project with respect to cost/resources and schedule, and highlight conflicts with NATO agreed policies and directives. &gt;</i></p>			
Plan to achieve compliance			
<p><i>&lt;Please lay out how and when you will achieve compliance with this Instruction&gt;</i></p>			
Mitigation Actions			
<p><i>&lt;Please identify mitigation actions on how you plan to ensure that corporate functions can be executed in a coherent way&gt;</i></p>			
Request for Deviation/Waiver Approval/Rejection			
<input type="checkbox"/> Approved	<input type="checkbox"/> Approved with caveats	<input type="checkbox"/> Rejected	
Caveats			
Date		Signature Dir SStrat	



This page is left intentionally blank.





NATO Communications and Information Agency  
Agence OTAN d'information et de communication

**INTERIM**

**Standard Operating Procedure  
SOP 23.01  
ENTERPRISE IT CHANGE MANAGEMENT**

Effective date: 5 March 2020 (*Precise date as per Approver's e-signature date*)  
Revision No: Original  
  
Issued by: Chief Operating Officer SMC – Change & Configuration Authority  
  
Approved by\*: Chief Operating Officer \_\_\_\_\_

### Approved by

Name	Organizational Element	Position	Date
Ludwig Decamps	COO	COO	December 2019
Signature:			

### Document Owner

Name	Organizational Element	Position	Date
Angelo Talarico	COO	SMC Branch Head	December 2019
Signature:			

### Table of Amendments

Amendment No	Date issued	Remarks
0.1	01 Nov 2018	Initial Draft
0.2	07 Feb 2019	Process comments and finalize workflow
03	23 Feb 2019	Final Draft
0.9	16 Oct 2019	Process all SL feedback and alignment with ITSM Toolset.
1.0	22 Jan 2020	Minor modification for publication

### Author / Contributor Details

Organisation	Name	Contact Email/Phone
COO - SMC	Michaël Danys	<a href="mailto:Michael.danys@ncia.nato.int">Michael.danys@ncia.nato.int</a>
COO - SMC	Ayse Uras	<a href="mailto:Saniye-Ayse.Uras@ncia.nato.int">Saniye-Ayse.Uras@ncia.nato.int</a>
COO - SMC	Tarulata Patel	<a href="mailto:Tarulata.Patel@ncia.nato.int">Tarulata.Patel@ncia.nato.int</a>
COO - SMC	Arnaud Bautista	<a href="mailto:Arnaud.bautista@ncia.nato.int">Arnaud.bautista@ncia.nato.int</a>

### Coordinated / Informed with

Organisation	Name	Contact Email/Phone
SStrat	Torsten Graeber Rob van Engelshoven	<a href="mailto:Torsten.graeber@ncia.nato.int">Torsten.graeber@ncia.nato.int</a> <a href="mailto:rob.vanengelshoven@ncia.nato.int">rob.vanengelshoven@ncia.nato.int</a>
DSO	Romeo Rosario Alain Dupret James Burley	<a href="mailto:Romeo.rosario@ncia.nato.int">Romeo.rosario@ncia.nato.int</a> <a href="mailto:Alain.dupret@ncia.nato.int">Alain.dupret@ncia.nato.int</a> <a href="mailto:James.burley@ncia.nato.int">James.burley@ncia.nato.int</a>
AMDC2	Dirk Wessel	<a href="mailto:Dirk.wessel@ncia.nato.int">Dirk.wessel@ncia.nato.int</a>
C2	Joel Varanda Douglas Smith	<a href="mailto:Joel.varanda@ncia.nato.int">Joel.varanda@ncia.nato.int</a> <a href="mailto:Douglas.smith@ncia.nato.int">Douglas.smith@ncia.nato.int</a>
NSII	Elma Mujollari Colin Bent	<a href="mailto:Elma.mujollari@ncia.nato.int">Elma.mujollari@ncia.nato.int</a> <a href="mailto:Colin.bent@ncia.nato.int">Colin.bent@ncia.nato.int</a>
CES	Bruce Devin Adrian Lutea	<a href="mailto:Bruce.devin@ncia.nato.int">Bruce.devin@ncia.nato.int</a> <a href="mailto:Adrian.lutea@ncia.nato.int">Adrian.lutea@ncia.nato.int</a>

**(NCI Agency) Required metadata:**

The document referenced below is requested to be uploaded to the RECCEN

Please scan in colour and enable OCR.

Metadata Fields:	Metadata:
Originator	COO SMC Change and Configuration Authority
Classification	NATO UNCLASSIFIED
Title	Enterprise IT Change Management
Reference No	
Date	January 2020
Disposal Information	
Issuer	SMC - Change & Configuration Authority
Approver(s)	COO
Document Owner	Angelo Talarico
Lead Author	Michaël Danys
Supporting Author	Arnaud Bautista and Ayse Uras

**This document supersedes or replaces:**

Document Reference/ID:	Action:
NCSA SMD CMQC Configuration Change Proposal Version 3.0	Supersedes

Table of Contents

1	REFERENCES.....	8
2	DISCLAIMER.....	8
3	INTRODUCTION.....	8
4	PURPOSE.....	8
5	SCOPE.....	9
5.1	Out of Scope.....	9
6	APPLICABILITY.....	9
7	PRINCIPLES.....	9
8	HIGH LEVEL PROCESS.....	11
9	DISTRIBUTED AUTHORITY MODEL.....	12
9.1	Change Authorities.....	12
9.1.1	Change Advisory Board (CAB).....	13
9.1.2	Emergency CAB (ECAB).....	14
9.1.3	Enterprise CAB.....	15
9.1.4	NCI Agency Default Model of Distribution.....	15
9.1.5	Recorded and Authorized Deviations of the standard Distribution Model.....	16
9.2	IT Change Escalation and Transfer of Authority.....	16
9.2.1	Transfer of Change Category.....	16
9.2.2	Change Authority Escalation.....	17
9.3	Stakeholders.....	18
9.3.1	CSU (CIS Support Unit).....	18
9.3.2	NCI Agency Programme Offices (POs) & Service Lines (SLs).....	18
10	ROLES & RESPONSIBILITIES.....	19
10.1	IT Change Management Process Owner.....	19
10.2	IT Change Manager.....	20
10.3	IT Change Authority.....	21
10.4	IT Change Initiator.....	21
10.5	IT Change Implementer.....	22
10.6	IT Transition Planning and Support Manager.....	22
10.7	Service Validation and Testing Manager.....	22
10.8	Release & Deployment Manager.....	23
10.9	Configuration Manager.....	24
10.10	NATO Quality Assurance Representative.....	24
10.11	Service Delivery Manager.....	25
10.12	CAB Member.....	25
10.13	CAB Chairperson.....	25
10.14	Subject Matter Expert.....	26
11	IT CHANGE TYPES & CATEGORIZATION.....	26
11.1	Change Types.....	26
11.1.1	Normal Change.....	27
11.1.2	Standard Change.....	27

11.1.3 Emergency Change..... 28

11.2 Change Categories..... 28

12 REQUEST TYPES..... 30

13 CHANGE CLASSIFICATION..... 31

13.1 Impact Categories..... 31

13.2 Urgency Categories..... 33

13.3 Priority Categories ..... 34

14 RISK CATEGORIES..... 35

14.1 Probability of Risk..... 36

14.2 Risk Level Identification..... 37

15 CHANGE PROCEDURE ..... 38

15.1 Triggers ..... 39

15.1.1 Inputs ..... 39

15.1.2 Outputs ..... 40

15.2 Process Workflow..... 40

15.2.1 Standard Change (CAT1) - Generic..... 41

15.2.2 Normal Change (CAT2 – 4) - Generic ..... 42

15.2.3 Emergency Change - Generic ..... 42

15.3 Process Workflow Step Description ..... 43

15.4 Change Models ..... 43

16 SMC ENTERPRISE TOOLSET ..... 45

16.1 Change Management Module..... 45

16.1.1 Change Lifecycle..... 45

16.1.2 Change Approvals ..... 47

17 DOCUMENT CONTROL..... 48

17.1 Updates and Publication ..... 48

ANNEX A ABBREVIATIONS ..... 49

ANNEX B RACI MATRIX..... 51

ANNEX C KPI & MONITORING ..... 53

ANNEX D CHANGE MODEL TEMPLATE ..... 55

ANNEX E DISTRIBUTED CHANGE AUTHORITY DEVIATIONS ..... 56

ANNEX F DETAILED STANDARD CHANGE (CAT1) – GENERIC ..... 57

ANNEX G DETAILED NORMAL CHANGE (CAT2-4) – GENERIC..... 61

ANNEX H DETAILED EMERGENCY CHANGE - GENERIC..... 67

ANNEX I DETAILED WORKFLOW STEP DESCRIPTION..... 72

List of figures

Figure 1: Simplified Process Flow ..... 11

Figure 2: Change Authority Escalation Flow..... 18

Figure 3: IT Change Management & Related Processes..... 38

Figure 4: Generic Process Workflow - Standard Change (CAT1)..... 41

Figure 5: Generic Process Workflow - Normal Change (CAT2-4) ..... 42

Figure 6: Generic Process Workflow - Emergency Change (CAT2-3) ..... 43

Figure 7: Generic Process VS Change Model..... 44

Figure 8: ITSM Phases to Process Phases ..... 46

Figure 9: ITSM Change Lifecycle ..... 47

Figure 10: Generic Process Workflow - Standard Change (CAT1) - Phase 1 ..... 57

Figure 11: Generic Process Workflow - Standard Change (CAT1) - Phase 2 ..... 57

Figure 12: Generic Process Workflow - Standard Change (CAT1) - Phase 3 ..... 58

Figure 13: Generic Process Workflow - Standard Change (CAT1) - Phase 4 ..... 58

Figure 14: Generic Process Workflow - Standard Change (CAT1) - Phase 5 ..... 59

Figure 15: Generic Process Workflow - Standard Change (CAT1) - Phase 6 ..... 59

Figure 16: Generic Process Workflow - Standard Change (CAT1) - Phase 7 ..... 60

Figure 17: Generic Process Workflow - Standard Change (CAT1) - Phase 8 ..... 60

Figure 18: Generic Process Workflow - Normal Change (CAT2-4) - Phase 1..... 61

Figure 19: Generic Process Workflow - Normal Change (CAT2-4) - Phase 2..... 61

Figure 20: Generic Process Workflow - Normal Change (CAT2-4) - Phase 3..... 62

Figure 21: Generic Process Workflow - Normal Change (CAT2-4) - Phase 4..... 63

Figure 22: Generic Process Workflow - Normal Change (CAT2-4) - Phase 5..... 64

Figure 23: Generic Process Workflow - Normal Change (CAT2-4) - Phase 6..... 65

Figure 24: Generic Process Workflow - Normal Change (CAT2-4) - Phase 7..... 66

Figure 25: Generic Process Workflow - Normal Change (CAT2-4) - Phase 8..... 66

Figure 26: Generic Process Workflow - Emergency Change (CAT2-3) - Phase 1..... 67

Figure 27: Generic Process Workflow - Emergency Change (CAT2-3) - Phase 2..... 67

Figure 28: Generic Process Workflow - Emergency Change (CAT2-3) - Phase 3..... 68

Figure 29: Generic Process Workflow - Emergency Change (CAT2-3) - Phase 4..... 68

Figure 30: Generic Process Workflow - Emergency Change (CAT2-3) - Phase 5..... 69

Figure 31: Generic Process Workflow - Emergency Change (CAT2-3) - Phase 6..... 70

Figure 32: Generic Process Workflow - Emergency Change (CAT2-3) - Phase 7..... 71

Figure 33: Generic Process Workflow - Emergency Change (CAT2-3) - Phase 8..... 71

List of tables

Table 1: High Level Process Flow Description .....	12
Table 2: Default Change Authority Distribution Model .....	16
Table 3: Change Authority Escalation Matrix.....	17
Table 4: NCI Agency Change Categories.....	29
Table 5: ITIL VS NCI Agency Change Terminology .....	30
Table 6: Change Request Types Submission Matrix.....	31
Table 7: Impact Categories.....	33
Table 8: Urgency Categories.....	34
Table 9: Priority Category Matrix .....	35
Table 10: Risk Categories.....	36
Table 11: Risk Probability .....	36
Table 12: Risk Level Identification.....	37
Table 13: IT Change Management Triggers.....	39
Table 14: IT Change Management Inputs .....	39
Table 15: Change Input supporting documents .....	40
Table 16: IT Change Management Outputs .....	40
Table 17: ITSM Approval Phases Description.....	48
Table 18: Abbreviations.....	50
Table 19: RACI Matrix - Change Phase VS Role .....	51
Table 20 - Process CSFs & KPI's .....	53
Table 21: IT Change Management Metrics .....	54
Table 22: Process Workflow Step Description .....	84

## ENTERPRISE IT CHANGE MANAGEMENT

### 1 REFERENCES

- a) AD 06.00.13 Service Change Management, December 2016;
- b) AGENCY SOI Minimum Information Input in Application and Technology Portfolio (A&TP) for RFC Validation published in NCIA Routine Order - Week 28 Dated 14 Jul 2017;
- c) AD 01.01 - Agency Policy on Management and Control of Directives, Notices, Processes, Procedures and Instructions, May 2014;
- d) SOP 06.04.02 Request Fulfilment, April 2019;
- e) AC/322-D/0047-REV2(INV), INFOSEC Technical & Implementation Directive on Cryptographic Security and Cryptographic Mechanisms;
- f) SDIP 29/2, Facility Design Criteria and Installation of Equipment for the Processing of Classified Information;
- g) AD 06.00.03 Risk Management, August 2014;
- h) AD 06.00.06, Agency Quality and Compliance Management Policy;
- i) AC/322-D(2017)0016 (INV), Technical and Implementation Directive on Supply Chain Security for COTS CIS Security Enforcing Products;
- j) NCI Agency Enterprise Information and Communication Technology Service Delivery Model: Part I – The Static Case, 30 November 2016;
- k) NCI Agency Enterprise Service Delivery Model: Implementation Plan 2019, 17 October 2018.

### 2 DISCLAIMER

This SOP has been in production for over a year and has received many comments. It has met an 80 percent threshold for completeness and accuracy. Although, not quite the finished article it is being released as an interim document to coincide with the transition of Change Management from CAMs to ITSM. The Interim SOP will be reviewed 6 months from authorising signature.

### 3 INTRODUCTION

The primary task of NCI Agency is the delivery of Computer Information Systems (CIS) services for NATO and other Customers. The availability of IT services is crucial in supporting Customer and the Agency business processes. A critical requirement is to manage changes effectively and efficiently without any detrimental impact to the operational IT Services, therefore, affecting the business of our Customers or NCI Agency.

Change Management is the process responsible for controlling the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services.

A Change is the addition, modification or removal of anything that has an effect on IT services and changes the status of a Configuration Item (CI). This shall include changes to all architectures, processes, tools, metrics and documentation specific to the change, as well as changes to IT services and other CIs. All changes must be recorded and managed in a controlled way.

### 4 PURPOSE

The purpose of this Standard Operating Procedure (SOP) is to describe the common Enterprise IT Change Management procedures. It will standardize the approach and methodology across the NCI Agency to ensure that all IT related change on any NCI Agency managed network is tracked, approved and executed accordingly.

The primary objectives of this SOP are:

- Ensure that IT changes are recorded and evaluated;
- Respond to Request For Changes (RFCs) that will align services with business needs;
- Respond to changing business requirements;



- Ensure that authorized changes are implemented in a controlled manner;
- Ensure the changes are fit for use and fit for purpose<sup>1</sup>;
- Optimize overall business risk related to IT Change Management.

## 5 SCOPE

The scope of this SOP covers the addition, modification or removal of, services or a service component, and associated documentation, of all IT services, systems, software, patches, hardware, and products on all security domains/networks operated, managed, controlled or maintained, locally or centrally, or contracted by NCI Agency. It will further discuss:

- Interaction requirements between IT Change Management and Release & Deployment Management (RDM);
- Change Evaluation Process for CAT 3 and 4 changes only;
- Engineering Change Proposals (ECPs) and Projects driven by a Project Manager, which overlap with IT Change Management.

### 5.1 Out of Scope

- Business Change. This SOP does not apply to AirC2 Capabilities. Changes relative to those capabilities will be handled in accordance with the NATO Joint AirC2 Life cycle Configuration Management Plan and sub-sequent AMDC2 CM SOPs.
- Organization Change;
- Process Documentation Change;
- Change Proposal (ChP) (Covered by SPM);
- Cryptographic equipment in accordance with Ref e) & f);
- Distribution of NATO software to a nation, an international organization or any other third party. Separate documents, policies and directives will govern these processes.

## 6 APPLICABILITY

This SOP applies to all Agency personnel involved in change management across all areas of its operation. Moreover, all NCI Agency elements, internal and/or contracted who are involved in the delivery, provision and support of services and service components.

## 7 PRINCIPLES

All IT changes shall be controlled. Any modification to a configuration item done without applying the defined process shall be recorded and reported as an unauthorised change.

Furthermore:

- The Business and its management shall commit to proper execution of IT Change Management;
- IT Change Management shall be used in all phases of the Service Lifecycle, and in particular, coordinate and support the information exchange requirements within the NCI Agency related to an IT Change;

---

<sup>1</sup> The value of a service offered is defined by fitness for use and fitness for purpose. IT Change Management, due to Release & Deployment being out of scope, will validate if both criteria are met. Fit for purpose: Does the change allow the customer to do what was requested based on requirements specification or test results covering these. Fit for use: The ability of the change to meet its agreed requirements (capacity, reliability, continuity and security).



- IT Change Management shall reinforce the NCI Agency's approved Service Portfolio, by ensuring changes are in line with the Service Roadmaps, and pipeline services when applicable;
- The emergency change process shall only be used to fix identified errors or critical security and safety vulnerabilities;
- Emergency changes shall be managed in accordance with the foreseen emergency procedures. In such a situation, the process execution may be compressed. However, if any IT Change Management activities are skipped, those activities shall be conducted retrospectively;
- Be in line with Strategic Planning and Requirements Management and shall deliver added business value;
- The impact of a change need to be identified and its consequences evaluated, understood and considered. This includes effects on other services or shared infrastructures as well as the effects on the service being changed and possible effects on the service performance targets mentioned in the Service Level Agreement (SLA) and Service Operational Agreements (OLA);
- Reports will be produced and utilized to facilitate decision making at each point an authorization is required;
- Ensure that IT Change Management process shall be measured;
- Any RFC originating from a Customer, which is not covered by an SLA, Programme of Work (PoW) or other funding means shall be requested to submit a Customer Request Form (CRF) for that RFC;
- All Lessons Identified followed by applicable lessons learned shall be incorporated into Continual Service Improvement (CSI);
- Quality Assurance principle shall be applied to the IT Change Management process and its execution.

## 8 HIGH LEVEL PROCESS

This Chapter offers a simplified overview of the Enterprise IT Change Management process.

This simplified process flow depicts the phases each RFC goes from submission to closure.

The phases<sup>2</sup> are numbered 1 through 8 and are used later in the document for identification purposes.

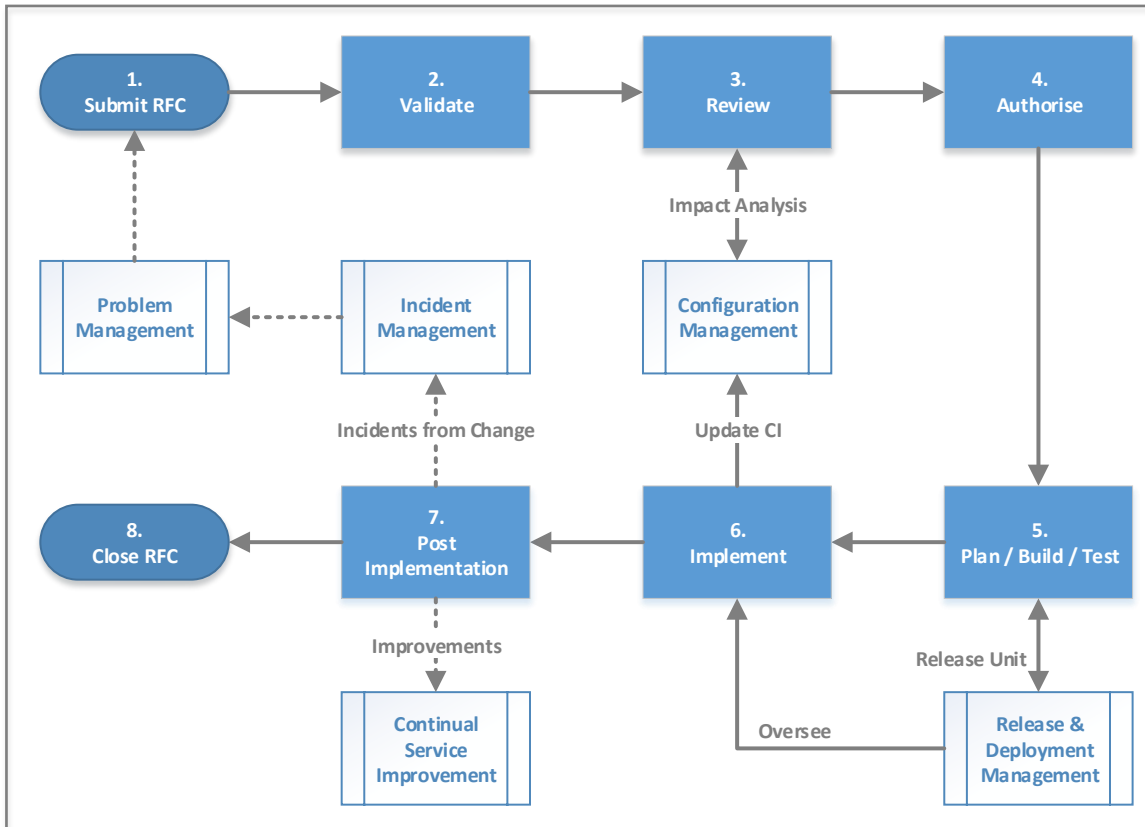


Figure 1: Simplified Process Flow

<sup>2</sup> These phases are related to the description of the process, more information on how these phases are implemented in the toolset is available in chapter 17 SMC ENTERPRISE TOOLSET.

High Level Process flow Description:

Phase	Description
<b>1. Submit RFC</b>	An RFC is created. The Change Initiator shall document the request and provide required supporting information.
<b>2. Validate</b>	The RFC is screened for completion and categorized. This may include Customer validation.
<b>3. Review</b>	The content of the RFC is analysed and evaluated from multiple perspectives to assess impact, complexity, and feasibility in preparation for the Change Authority to make an informed decision.
<b>4. Authorise</b>	Phase in which the RFC shall be authorized by the Change Authority for execution.
<b>5. Plan / Build / Test</b>	The authorised change is prepared for implementation by SMEs. This phase may require coordination with other Agency elements.
<b>6. Implement</b>	The change is implemented into the production environment by SME based on the previous phase deliverables.
<b>7. Post Implementation</b>	Change management assesses the implementation. Based on the size of the change this can include Early Life Support, Post Implementation Review and interaction with other processes.
<b>8. Close RFC</b>	Closure activities are performed and the change initiator is informed about the change closure.

Table 1: High Level Process Flow Description

## 9 DISTRIBUTED AUTHORITY MODEL

SMC Branch under COO is accountable for the Enterprise Change Management process, across all security domains including mission networks. It distributes change authority to the Organisational Elements (OE) i.e. SLs and CSUs, allowing them change, configuration planning and control whilst remaining under SMC governance.

OEs are mandated to create their own Distributed CABs (DCAB) for their own “Domain” to control the changes to service configuration baselines in terms of core and support services i.e. platforms, infrastructure and software.

### 9.1 Change Authorities

The Change Authority is the person or Board responsible for authorizing an IT Change to be processed and implemented.

The IT Change Authority for NCI Agency lies with the Enterprise CAB, chaired by COO SMC Branch.

The Change Authority for a specified scope of change can be distributed to another entity within the NCI Agency, under the distributed authority model as detailed above.

Any distribution of authority to DCABs shall be authorized by the Enterprise CAB, to assess the appropriate maturity, impact and ensure management support.

By default, CAT 1 and CAT 2 changes (chapter 11.2) are distributed to OEs. In limited cases, CAT 3 Changes may also be considered; described in Chapters 9.1.4 & 9.1.5.

IT Change Managers shall escalate a change to the appropriate approval body when the risk is deemed too high, see Table 3: Change Authority Escalation Matrix. For changes not distributed that remain with SMC, the highest level of escalation will be to the NCI Agency Executive Board.

The management level at which a change is authorized shall rest with the Change Authority accountable for accepting the risk and remediation.

Change Authority can be distributed to the following:

- Directorates;
- Service Lines;
- CIS Support Units (CSU);
- Lifecycle Configuration Control Board or similar body
- NATO Operations for which the NCI Agency is delivering IT Services;
- NATO Exercises for which the NCI Agency is delivering IT Services.

#### 9.1.1 Change Advisory Board (CAB)

The CAB represents a coordinated entity, consisting of two or more people that shall convene at regular intervals to discuss IT Change related matters. The CAB usually consists of representatives of IT and the Business.

This SOP does not differentiate between other terminologies used within NCI Agency to describe its function. Project boards, Programme boards, Working Groups etc. are all considered a CAB when they hold decision authority related to IT Changes or provide advice to their relevant Change Authority.

The CAB delivers support to the IT Change Manager in the assessment of an RFC or by authorizing, when delegated, the submitted RFCs.

The objective of the CAB is to ensure that all change requests are adequately assessed from an operational, architectural, service interdependency, technical viewpoint. Assessing *“fit for purpose”* and *“fit for use”*.

The CAB members shall selectively be chosen to ensure that all changes presented at the CAB are assessed correctly with the right expertise and from every aspect of the business.

The CAB shall convene at least once per week or shall be cancelled if no RFC is presented.

The CAB members shall actively participate in the CAB activities including the decision-making.

The CAB body shall consist of guests invited to provide SME input based on the discussed changes and preferably have static representatives from, not limited to:

- IT Change Management (Mandatory)
- Service Validation and Testing (Mandatory)
- Service Asset & Configuration Management (Mandatory)
- Information / Cyber Security (Mandatory)
- Release & Deployment Management (Mandatory if not actioned by IT Change Management)
- Quality Management (Highly preferred)
- Change Initiator (As required)
- Customer or Agency’s Customer representative (As required)
- Service Delivery Manager (When applicable)

- Subject Matter Experts (As required)
- Vendor / Supplier representative (As required)

The CAB shall come to unanimous decision between its members. If no consensus is found, the decision shall be escalated to a higher change authority.

The CAB Chairperson has the option to open the CAB for anyone to attend as long as it does not disrupt the operation of the CAB. Whether done or not, any CAB Meeting Minutes shall be public record, which can be consulted by anyone in the NCI Agency or, on request, by the Customer.

The CAB Chairperson shall be closely affiliated to IT Change Management in order to understand the process flow.

The CAB Chairperson is also responsible for the organization of the CAB and the agenda items.

The CAB Agenda shall consist of:

- Required participation;
- Review and approval of the previous meeting minutes;
- Review of previously implemented changes with focus on implementations that caused incidents and problems including rolled back or backed out changes;
- Review all RFCs up for authorization including emergency change;
- Review RFCs for escalation;
- Any Other Business (AOB) or topic to be discussed in next CAB.

In addition, the scope of the agenda is limited to the previous implementation period and the period between the current CAB and the next one scheduled.

It is the responsibility of CAB participants to obtain and review the meeting agenda and previous minutes prior to each CAB meeting.

Changes may be rejected by the CAB if a change is not represented by either the Change Initiator or his/her representative; lacks appropriate approvals; lacks appropriate documentation; or issues/concerns are raised at the CAB, which can have an impact on NCI Agency services. Before rejection, the CAB can request additional information before making a final verdict.

Following each CAB, meeting minutes will be drafted and distributed to each CAB member/attendee and published following the CAB Chairperson approval.

Each RFC will have its work log updated based on the recorded CAB minutes and listed actions/tasks.

#### 9.1.2 Emergency CAB (ECAB)

An Emergency Change Advisory Board (ECAB) can only be triggered when a change request is raised as an Emergency Change Type (Chapter 11.1.3) and validated by the IT Change Manager. An ECAB can help outside of the Normal CAB schedule.

The ECAB has the responsibility for assessing, and approving the emergency change being presented. The conditions for a RFC to be regarded as emergency change and the composition of ECAB shall be defined by the chairperson of the normal CAB. *As an example: a CAT2 Change in a SL of Emergency Type will be actioned by the ECAB within that SL. A CAT 3 Emergency Change will, by default, be actioned by SMC IT Change Management or according to the distribution model in place.*

Since the time for assessing, approving and testing is limited for emergency change, it is important not to implement any change without verification and validation of the impact, unless there is no alternative (e.g. impending major service interruption, grave security risk, etc.).

The ECAB follows the same rules as the Normal CAB but allows for:

- Validation and authorization without the full CAB board present;
- Validation and authorization can take place without all required input which is normally required for a normal change request;
- Testing may be reduced or in exceptional cases omitted;
- Reflecting the changes in the Configuration Management Database (CMDB)/Configuration Management System (CMS) can be deferred but has to happen before closure of the change;
- In all cases, every skipped activity or delivery of required input criteria shall be performed as soon as possible after the emergency is resolved.

After the approval of an emergency change, the ECAB Chairperson will formally notify the Normal CAB about the outcome.

### 9.1.3 Enterprise CAB

Is the highest Change Authority Board in the NCI Agency, it will manage Category 3 and 4 change that has a major disruption and/or impact on the delivery of a service/s to the Customer or NCI Agency.

The Enterprise CAB body shall consist of members mentioned in chapter 9.1.1 Change Advisory Board (CAB) and additionally from:

- Service Line Change Management POC (As required)
- Service Portfolio Management (As required)
- Strategy/Enterprise Architecture (As required)
- Operations Centre ASI Coordination Cell (As required)
- CSU Representatives (When Applicable)

All stakeholders listed above will be informed of the Enterprise CAB agenda and minutes

The enterprise CAB shall convene at least one time per week. The Agenda will state the required attendees; each attendee shall review the Agenda to ensure they are prepared for the CAB.

### 9.1.4 NCI Agency Default Model of Distribution

Table 2 shows the default model of distribution for Change Categories.

Default Model of Change Distribution	NCI Agency Entity			
	Enterprise CAB	Service Line	CSU	NATO Operations & Exercises
Change Category	1	X	X	X
	2		X	X
	3	X	X <sup>3</sup>	X <sup>5</sup>
	4	X		X <sup>5</sup>

Table 2: Default Change Authority Distribution Model

9.1.5 Recorded and Authorized Deviations of the standard Distribution Model

Any deviation of the standard distribution model shall be assessed and authorized by the Enterprise CAB and recorded in Annex E Distributed Change Authority.

Deviations to the default NCI Agency Change Authority Distribution model are granted after an Enterprise CAB evaluation. Changes to this model will be submitted through RFC.

Additional rights are provided through a deviation to the standard distribution model, the entity receiving the additional rights shall be responsible to execute the process according to NCI Agency standards and shall keep the Enterprise CAB informed. Upon escalations, the Enterprise CAB shall be consulted.

9.2 IT Change Escalation and Transfer of Authority

It is imperative that an escalation process in in place for changes that require a higher change authority to make a decision.

There are two types of escalation, transfer of change category and the escalation to a higher Change Authority.

9.2.1 Transfer of Change Category

During the lifecycle of a change request, it is possible that the initial change category changes. This can be due to the result of validation activities, change of requirements and/or recommendation from stakeholders.

If the change category becomes higher than what is currently within the acting Change Authority’s rights of distribution, the IT Change Manager shall transfer the change request to the right Change Authority Identified. See Chapter 9.1 to understand to whom the change should be assigned to.

<sup>3</sup> Cat 3 distributed to Service Lines for changes, which remain within the Service Line, meaning no impact on other Service Lines and no impact on Customer services outside of agreed maintenance windows for the affected Service.

<sup>4</sup> Cat 3 distributed to CSUs only granted by default for services part of the local SLA which are locally supported, managed and provisioned.

<sup>5</sup> NATO Operations & Exercises have distributed authority to fully control IT Change Management within their Area of Responsibility (AoR). This delegation is only applicable if the RFC is not affecting any other entity, in this case the Enterprise CAB stay the default authority for CAT 3-4. This includes baseline changes or changes to Release Packages under Agency Configuration Management control.



*Example: The IT Change Manager of a CAT2 Change identifies that the Request is not covered within the described boundaries of CAT2 (e.g. Not within SLA boundaries) as the request is for a new service. The IT Change Manager shall reassign the Change Request to a CAT4 Change authority, by default SMC Enterprise CAB.*

### 9.2.2 Change Authority Escalation

The main driver to escalate the authorization of a change request to a higher change authority is driven by the risk assessment at described levels of risk and based on the category of change; a higher change authority will be consulted.

Every IT Change has an associated risk; it is for the IT Change Manager to assess the risk from the information provided or request support in establishing the risk

Table 3: Change Authority Escalation Matrix below assists in identifying the correct Change Authority for any change versus risk possibility.

Change Authority Escalation by Change Category		Change Category			
		1	2	3	4
Risk Level	5	Ent-CAB	Ent-CAB	Exec. Board	Exec. Board
	4	CAB	Ent-CAB	Ent-CAB	Exec. Board
	3	CAB	CAB	Ent-CAB	Ent-CAB
	2	IT Change Manager	IT Change Manager	Ent-CAB *	Ent-CAB
	1	Tool	IT Change Manager	Ent-CAB *	Ent-CAB

*\* Or CAB in CSU / SL when distributed by Enterprise CAB*

Table 3: Change Authority Escalation Matrix

Change authority escalation flow is depicted in Figure 2 below.

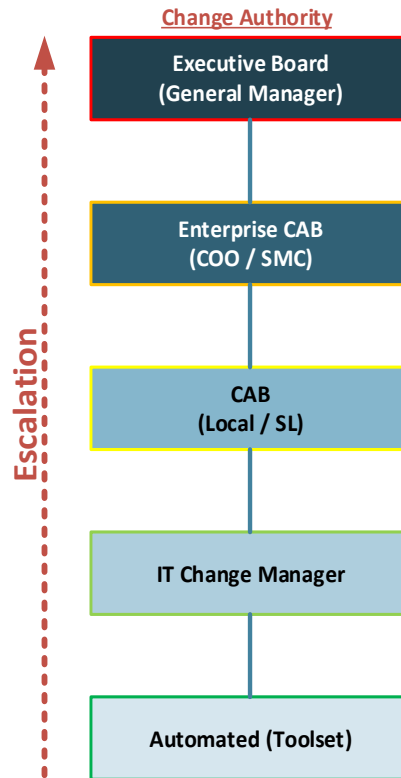


Figure 2: Change Authority Escalation Flow

Each Agency Change Authority shall formally document its own escalation and make that information available.

**9.3 Stakeholders**

In addition to Enterprise IT Change Management, there are 2 other important stakeholders in the execution of IT Change Management.

**9.3.1 CSU (CIS Support Unit)**

CSUs maintain control of local CIS systems and services and will therefore follow the direction as detailed in this SOP. Responsibilities include:

- Managing all Standard (CAT 1) and Minor Changes (CAT 2) or as described in 9.1.4 and configuration activities related to the Customers they support, but not limited to end user equipment patching, installation and software parametrisation, logistics support, etc.
- Update the impacted CIs into the CMDB as per local agreement.

**9.3.2 NCI Agency Programme Offices (POs) & Service Lines (SLs)**

Programme Offices and Service Lines will follow the directions as detailed in this SOP related to IT Change Management. Responsibilities include:

- Manage all Changes for each category when scope is limited to their own entity as described in 9.1.4 ;
- Update the impacted CI’s into the CMDB as per local agreement

## 10 ROLES & RESPONSIBILITIES

RACI Matrix mapping defined Roles to each of the generic change workflow steps can be found in Annex B).

Roles describe the profile and responsibility of a person or entity related to IT Change Management and will be used throughout the document.

One person can fill one or more roles but accountability remains with one person. The only exception to this rule is the roles of Service Validation and Testing (SVT) Manager and Release and Deployment Manager (RDM); cannot be the same person due to possible conflict of interest.

ITIL differentiates between a Process Owner, Manager and Practitioner. In order to simplify roles within NCI Agency the role of Manager and Practitioner will be combined until further notice.

Where applicable, roles and responsibilities are in accordance with ESDM, responsibilities listed below are specific to IT Change Management.

### 10.1 IT Change Management Process Owner

**Profile:** The person fulfilling this role is accountable for ensuring that the process is performed according to the agreed and documented process and is meeting the aims of the process definition. There will be only one IT Change Management Process Owner across NCI Agency.

**Actor:** COO Service Management & Control Branch Chief

**Responsibilities:** The IT Change Manager Process Owner shall:

- Carry out the responsibilities as listed in the RACI model found at Annex B;
- Ensure that the IT Change Management process is fit for purpose;
- Ensure that there is optimal fit between people, process, technology/tool and governance;
- Ensure that proper internal Key Performance Indicators (KPI) are set;
- Ensure that quality reports are produced, distributed and utilized;
- Assist with and ultimately be responsible for the process design;
- Define the KPIs to evaluate the effectiveness and efficiency of the process and design reporting specification;
- Review KPIs and take the action required following the analysis;
- Address any issues with the performance of the process;
- Review and initiate improvements in the tool, process, governance mechanisms and people;
- Work with other process owners to ensure that there is an integrated approach to service transition;
- Promote the evolving vision of IT Change Management to the NCI Agency;
- Function as a point of escalation when required;
- Ensure that the process, roles, responsibilities and documentation are regularly reviewed and audited;
- Interface with relevant teams ensuring adequate resources to support IT Change Management process;
- Designates an IT Change Management Process Manager for process execution as part of IT Change Management.

## 10.2 IT Change Manager

**Profile:** The IT Change Manager is responsible for the overall IT change management process. One or more IT Change Managers can exist but there shall be one IT Change Manager nominated by site or Area of Responsibility (AoR) where IT Change Management operates to have the overall lead role.

**Actor:** Any NCI Agency employee executing the function of IT Change Management.

**Responsibilities:** All IT Change Managers shall:

- Carry out the responsibilities as listed in the RACI model found at Annex B;
- Verify that all changes submitted meet all agreed criteria and return to Change Initiator with reason for rejection when this criterion is not met;
- Present all RFC to the CAB; issues an agenda, and circulate all RFC to CAB members in advance of the meeting to allow prior consideration;
- Convene and chairs CAB meetings, when assigned the CAB Chairperson role;
- Responsible for the overall change process operation and for ensuring all participants comply with the change policy process and procedures;
- Ensures decisions or recommendations made during the CAB meeting are recorded in the minutes, communicated and available for interested parties;
- Receive, accept, review or re-allocate a priority, in collaboration with the Initiators, for all RFCs;
- Assesses RFCs to ensure:
  - Originators provide complete information requirements for the category and type of change;
  - Appropriate assignment of categories and priorities;
  - Change initiators provide all prerequisites based on Category (CAT) of Change, in order to formally accept an RFC;
  - Identifies an RFC for escalation if required;
- Obtain validation for changes by creating/assigning tasks to the appropriate support groups;
- Escalate all RFCs that require CAB review;
- Coordinate impact assessment, planning and authorization of RFCs in cooperation with members of the CAB;
- Supports the CAB Chairperson by updating and highlighting RFCs, which need action or decisions during CAB meetings, issues meeting agendas and supports CAB minute's development;
- Supports the CAB Chairperson, by supplying administrative support;
- After consideration of the advice given by the CAB or ECAB, authorize acceptable Changes;
- Ensure that appropriate actions have been planned to minimize the risk of failure and the impact on users during change implementations;
- Coordinate with the Release & Deployment Manager to ensure the timing of implementation does not conflict with other planned changes or events;

- Liaise with Service Area Owners, System Delivery Managers, Project Managers to ensure that IT Change Management is in place throughout the complete life cycle of all assigned systems and services;
- Authorize, escalates or rejects RFCs within the boundaries of the SLA;
- Close RFCs;
- Ensure that the IT Change Management KPIs are tracked and reported;

In case, multiple Change Managers exist within one Area of Responsibility (AoR) an experienced individual will be in the lead role. On top of the responsibilities above, this person shall:

- Provide advice, guidance and support to other IT Change Managers;
- Act as an escalation route for other IT Change Managers;
- Analyse requirements for potential escalations to Service Portfolio Management.

### 10.3 IT Change Authority

**Profile:** Depending on the complexity, risk level or decision-making required for the change request, different levels of approval may be required. In addition, the IT Change Management Process Owner for specific purposes and scope, can delegate the approval to a subordinated Change Authority. There will be different change authority levels and these are discussed in chapter 9.1 Change Authority delegation.

**Actor:** Any NCI Agency personnel or Board assigned with this Authority.

**Responsibilities:** The change authority shall:

- Carry out periodic review of change categories;
- Participate in the change review before changes are closed;
- Attend CAB meetings to discuss and review changes when required;
- Formally authorize changes at agreed points in the change lifecycle.

### 10.4 IT Change Initiator

**Profile:** This person responsible for initiating the RFC.

**Actor:** Any user of NCI Agency services both internal and external.

**Responsibilities:** The Change Initiator shall:

- Initiates the change by raising an RFC with all required information;
- Carry out risk assessment, testing/back-out plans, and impact analysis of the change and attach the results into the RFC;
- Is accountable and responsible for the change in question being accurate and fit for purpose;
- Ensure business impact, date and timing of outage, business communications have been agreed and issued;
- Monitor the raised RFC through the process and implementation;
- Review changes proposed by IT Change Management and answer additional questions when required;
- Ensure post implementation review information is provided when requested;
- Attend CAB meetings to provide further information when required.

### 10.5 IT Change Implementer

**Profile:** Change Implementers are responsible for deploying and, when applicable, validating the change coordinated by the Release and Deployment Manager. They can be represented by NCI Agency staff members, Service Owners or vendors. The Change Implementer may be internal or external (vendor/ user base).

**Actor:** Any NCI Agency personnel, contractor or service provider required to perform activities in order to successfully implement the change.

**Responsibilities:** The IT Change Implementer shall:

- Perform deployment of the requested Change;
- Develops the remediation/back-out plan and implement as necessary;
- Records results of the change implementation;
- Conducts initial post-implementation review to determine if desired results were achieved;
- Update RFC requesting deployment to record the implementation and any lessons learned;
- Liaise with the RDM Manager for status update on the deployment/implementation where applicable.

### 10.6 IT Transition Planning and Support Manager

**Profile:** The TPS Manager role ensures overall coordination of a large amount of activities and deconflicts where required. This role is only active on large scale changes and performed by the Project Manager (PM) in order for the IT Change Manager to focus on the proper handling of the Change.

**Actor:** Any NCI Agency employee assigned to perform coordination activities in support of Change Management process.

**Responsibilities:** The TPS Manager shall:

- Budget and account for service transition activities and resources;
- Manage and coordinate requests for resources;
- Coordinate activities across changes and people;
- Monitor change progress, identifying issues, risks and deviations;
- Contacts necessary parties to coordinate supporting processes;
- Communication with stakeholders.

### 10.7 Service Validation and Testing Manager

**Profile:** SVT Manager can be represented by NCI Agency staff members, SME or the user of a service. They ensure the performance of testing and validating activities. Depending on the type of change, one or more stakeholders can fulfil this role with a different performance focus.

**Actor:** Any person, identified by IT Change Management, required to perform validation or executing tests to correctly assess fit for purpose and fit for use of the related change.

**Responsibilities:** the SVT Manager shall:

- Be responsible for the development of test plans;
- Administer test assets and components;
- Execute the test plan, validating and verifying the desired outcome of the change;
- Record, analyse, diagnose and report the test results;

- SVT Managers are organized, but not limited, in three main areas of NCI Agency:
  - Independent Validation & Verification (IV&V):
    - Shall assess the RFC from the IV&V perspective for testing focused on the fit for purpose and provide recommendations.
  - Cyber Security:
    - Shall assess the RFC from a security perspective including penetration and vulnerability testing and provide recommendations.
  - User / Service Owner:
    - Shall assess the change request from a Fit for Use perspective and provide recommendations.

### 10.8 Release & Deployment Manager

**Profile:** Release and Deployment Manager focuses on the transitions from initiation to testing and release of a change request and ensures that the integrity of the live environment is safeguarded by releasing only validated and authorized components.

**Actor:** Any NCI Agency employee executing the function of RDM Manager, in case this function does not exist the IT Change Manager covers this role.

**Responsibilities:** The Release & Deployment Manager shall:

- Ensure a release plan that includes a roll-back plan is developed for all releases.
- Ensure releases are built and adequately tested prior to rollout to LIVE environment.
- Ensure effective communication about releases to relevant parties.
- Ensure appropriate documentation and training is provided to relevant parties on releases.
- Ensure necessary approvals are taken from change management and other interested parties for releases.
- Validate risk assessment and impact assessment;
- Obtain scope of evaluation for RFCs raised;
- Liaise with all necessary parties to coordinate build of the test environment, testing and implementation;
- Provide guidance for the release package during service design stage;
- Ensure Known Error Database (KEDB) is updated;
- Coordinate release documentation and communication;
- Review results of the tests performed;
- Review draft and final Approved Service Interruption (ASI);
- Present items ready for deployment at the CAB;
- Maintain a Forward Release Schedule;
- Coordinate early life support;
- Coordinate planned releases with key stakeholders (OpsCen, Resource Manager, SME's, Operational Sponsors and SDM).

### 10.9 Configuration Manager

**Profile:** The Configuration Manager is required to ensure that the overarching intention and policies of configuration management are employed throughout the service management lifecycle and with specific consideration for every aspect and complexity of the complete service.

**Actor:** Any NCI Agency employee executing the function of Configuration Manager who has been delegated the authority to update the CMDB.

**Responsibilities:** The Configuration Manager shall:

- Develop configuration management plans and procedures;
- Propose/agree interfaces with change management, problem management, release management, service operations, logistics, finance and administration functions;
- Maintain and manage the CMDB(s);
- Conduct regular configuration audits;
- Be the custodian of all master copies of software, assets and documentation Cis.
- Manage and maintain the Definitive Media Library (DML);
- Manage and maintain the Approved Field Product List (AFPL).

### 10.10 NATO Quality Assurance Representative

**Profile:** The NQAR controls the results of a process execution in order to ensure that the final product implements its original requirements. In addition, the NQAR performs quality assurance checks in order to assure that the process is executed in accordance to its definitions and quality criteria, as defined in NATO (including NCI Agency) policy documents.

**Actor:** Quality Assurance Engineer.

**Responsibilities:**

- The NQAR is a permanent member of the Enterprise CAB;
- As preparation to CAB meetings, the NQAR provides an initial assessment of the RFCs in scope, to ensure all procedural and RFCs Release Package Validation pre-requisites are met;
- During the IT Change Management System or Service "Evaluation" process phase, the NQAR attends all Test Readiness and Review coordination meetings by providing "fit for use" and "fit for purpose" quality observations;
- NQAR provides a formal assessment (Certification) containing all relevant RFC identified observations together with a recommendation on RFC Approval/Rejection to the IT Change Authority in support to RFC risk and impact assessments;
- The NQAR monitors the IT Change Management process to ensure it is compliant to the approved NATO policies and Quality Management System (QMS);
- The NQAR conducts independent random quality audits to verify IT Change Manage Process integrity against Key Quality Indicators. The quality assurance engineer produces an Assurance report;
- As per Continual Service Improvement (CSI), the NQAR records quality observations in the NCI Agency CSI register and ensures the follow-up of these observations.



### 10.11 Service Delivery Manager

**Profile:** For each service there will be an assigned Service Delivery Manager (SDM) that will be directed and be responsible to the accountable Service Owner for the day-to-day delivery of the service.

**Actor:** Any NCI Agency employee who gets delegated the responsibility of a service from the Service Owner.

**Responsibilities:** The Service Delivery Manager shall:

- Oversight of the establishment and maintenance of the service baseline;
- The correct planning for the delivery of the service, documented in a 'service delivery plan,' and correct expenditure of the service budget against the plan;
- Negotiating with SLs, CSUs or other OU (e.g. CSSC) for the allocation of capacity needed to support the delivery of their services.
- Monitoring and reporting of KPIs and associated metrics for their assigned services;
- The planning and execution of transition of new/modified capability into service operations;
- Advance coordination of all planned service outages, planned changes, or other service disruptions with the Ops Cen Duty Control Office;
- Validate the request for emergency changes for Services within own AoR;
- Representing the SO at the CAB and other bodies as directed by the SO, mandatory representation for emergency changes;
- The proactive monitoring of the service in order to identify issues and take advance action to prevent degradation of services;
- CSI for the assigned service, including the delivery of all agreed efficiency and effectiveness targets for the service;
- Creation and maintenance of templates and other material to be used by personnel involved in delivery of the service;

### 10.12 CAB Member

**Profile:** CAB Members are selectively chosen to assess agenda items from both a technical and business perspective based on their expertise.

**Actor:** Any NCI Agency employee, service provider or Customer (representative) selected by IT Change Management to have a valuable contribution to the operation of the CAB.

**Responsibilities:** The CAB Member shall:

- Circulate RFCs up for evaluation within their AoR and coordinate feedback;
- Remain neutral and provide recommendation not influenced by others but based on available information and expertise;
- Review and make recommendation on the authorization of an RFC or change;
- If authorized, come to a consensus on the authorization of an RFC or change.

### 10.13 CAB Chairperson

**Profile:** The CAB Chairperson is a normal member of the CAB he/she shares the same responsibilities as other CAB members in addition to the ones specific to the CAB Chairperson role. Usually the CAB Chairperson is given to a senior IT Change Manager.

**Actor:** Any NCI Agency employee, preferably executing a function of IT Change Management, assigned to facilitate the CAB operation.

**Responsibilities:** The CAB Chairperson shall:

- Plan, schedule, manage, facilitate and chair the CAB meetings;
- Select RFCs up for review at CAB meetings;
- Convene ECAB meetings when required;
- Select successful and failed changes up for review at the CAB meetings;
- Ensure decision or recommendation made during the CAB are communicated and available for consultation;
- If the CAB also has the role of Change Authority, and no consensus can be found, the CAB Chairperson has the final decision authority or the option to escalate to a higher decision authority if risk is deemed too high and will provide and record justification of the decision.

#### 10.14 Subject Matter Expert

**Profile:** Subject Matter Experts are responsible for assessing, planning and monitoring Change Management for their functional department and specific technology platform. They function as the point of contact between different departments for the Change Management process.

**Actor:** Any NCI Agency employee, service provider or Customer which has specific expertise in the area covered by a change.

**Responsibilities:** The SME shall:

- Provide impact assessment and interaction/dependencies of change activities with other Service management processes;
- Contribute to the risk analysis, receive and stores, risk reports;
- Ensure that the back-out plan is valid and complete;
- Support the RDM Manager, in the planning and maintenance of the Change Schedule, when the Change Management process impacts the deployment timelines;
- Produce and issue status updates using CMDB and related information sources.

### 11 IT CHANGE TYPES & CATEGORIZATION

This chapter will provide the main definition related to the internal working and processing of IT Changes.

The produced solution below is a combination of ITIL best practices together with the chosen technology that will support IT Change Management that being BMC Remedy ITSM.

IT Change Management reserves the rights to change any category or type of the change request at any time in the process, after validation, based on findings, experience or when the needs or requirements change.

#### 11.1 Change Types

Within IT Change Management, the first differentiation between changes is based on the type of change. Within the NCI Agency will adhere to the three types defined by ITIL.

Change types are used to define which process should be triggered. The type is mainly used by the IT Change Manager and toolset to determine the workflow of completing this ticket

The Change type may be unknown by the Change Initiator. Within the NCI Agency, the type of changes will be translated to Change Categories (Table 5: ITIL VS NCI Agency Change Terminology) to determine who will action a change, who will be the Change Authority, which process the change will follow and the prerequisites required for that change.

BMC Remedy ITSM defines Change type as Change Class. In addition to normal, standard and emergency change class (which will be discussed in this chapter), other Change Classes exist however they are mainly for internal use by the IT Change Manager. The other classes not described here are Latent, Expedited and the No Impact class. Latent Change will retrospectively record a Change that already took place.

#### 11.1.1 Normal Change

A Normal change is a change that is not a standard change or emergency Change.

Normal changes are more complex and have more impact than standard changes, but do not need to be implemented immediately as emergency changes.

Governed by all the processes defined in the IT Change Management process and require approval on a case-by-case basis.

This type will be the most frequently used and defines the workflow for both normal and emergency changes.

The Change Authority for a normal change will review and update the impact, risk and scope of the change.

A request for a normal change can be used to introduce new services or decommission services to the organization or the Customer. These Changes can be initiated by the NCI Agency or in some cases by one of its Customers.

#### 11.1.2 Standard Change

A standard change is a pre-authorized changed with low risk, low cost, low impact and relatively common which can follow a known procedure or work instruction. Standard change are largely re-populated based on previously agreed requirements.

Standard changes shall follow a simplified process compared to normal change to facilitate quick resolution of the change request due to limited validation.

Standard changes are closely associated to Service Request Fulfilment but there is no direct one-to-one relationship between the two. They differ from each other on two points. Compared to a standard change a service request is:

- A request based on an entry in the Service Catalogue;
- Documented and recorded in the Approved Service Request (ASR) list.

Every low risk, low cost, low impact request that is not documented and not know as a Service Request part of the ASR list will be a Standard Change.

Every standard change shall follow a generic change model. When the standard change is frequently returning a specific change model can be defined to streamline the change request. Once a specific change model is defined, it can become a candidate to transform into a Service Request and be recorded on the ASR list.

The change model of a standard change shall show that:

- Repeatable work instructions or procedures are available;
- The impact is proven to be low;

- Deployment plan is documented and previously tested;
- Communication and notification on process is documented;
- Verification steps are documented and results know;
- Back-out plan is document and tested.

Any standard change that does not comply with the above statements will be handled as a normal change.

CSI will be in place to review standard changes at regular intervals to determine which standard change can be transformed into a service request.

The CAB will review all newly proposed service requests and authorize or reject the move from standard change to request fulfilment.

### 11.1.3 Emergency Change

An emergency change is a change that must be implemented as soon as possible; delayed implementation can have a detrimental impact to the organization, operations or Customer.

IT Change Management shall evaluate the emergency change for correct classification based on one of the following:

- Actual service interruption with a moderate to high risk to breach SLAs;
- A potential service interruption requiring immediate prevention;
- Security related which requires immediate remediation;
- Operational related with a significant impact on the business or Customer.

The Change Initiator needs to be available and willing to provide all or as much information he/she can provide, including the rationale for it to be an emergency change, for IT Change Management to have a clear understanding of the request.

If the request is correctly raised as an emergency change, the IT Change Manager shall call for the ECAB as soon as possible in order to evaluate, assess and reject or authorise the change with the highest priority.

An emergency chance does not guarantee that the change will be authorised and implemented.

An emergency change shall follow the Normal IT Change Management process described but will be executed with highest priority and the possibility for execution of the change to take place even when validation is not yet completed (when circumstances requires it).

## 11.2 Change Categories

Changes are categorized as CAT 1 to CAT 4 in NCI Agency whereas they are categorized as Standard, Minor, Significant or Major within the ITIL framework.

Categorization helps Change Managers and other involved parties to group changes in terms of eventual use, coverage, impact and potential risks.

	NCI Agency Change Categories			
	CAT 1	CAT 2	CAT 3	CAT 4
Originates from	Any user consuming NCI Agency services	Any user consuming NCI Agency services, Sponsor, Service Owner / SDM	Sponsor, Service Owner / Service Delivery Manager (SDM)	Sponsor, Service Owner / Service Delivery Manager (SDM)
Service Catalogue	Adheres to the NCI Agency Service Catalogue	Minor change to a service within the NCI Agency service catalogue	Significant revision to a service within the NCI Agency service catalogue	New to service catalogue
Implementation resource	Can be implemented with local resources	Can be implemented with local resources	Beyond local capabilities for implementation	Requires a significant amount of resource allocation, testing or engineering
SLA boundaries	Is within SLA boundaries	Is within SLA boundaries	Beyond SLA boundaries	Beyond SLA boundaries
Work instructions or procedures	Work instructions or procedures available	Work instructions as is or to be modified	Work instructions as is or to be modified	Work instructions to be created
Change type procedure followed	Follows the Standard Change Type Procedure	Follows the Normal Change Type Procedure	Follows the Normal Change Type Procedure incl. Change Eval.	Follows the Normal Change Type Procedure incl. Change Eval.
Service Outage	No	No or limited	Yes	Yes

Table 4: NCI Agency Change Categories

It is important to correctly identify and assign the right change category, as this will determine who the default change authority is and what escalation path is available when risk increases. Detailed information on this can be found in Chapter 9 DISTRIBUTED AUTHORITY MODEL.

During change category identification, lowest change category is to be used unless at least one of the criteria matches in a higher change category.

There is a strong relationship between the ITIL defined change Types, ITIL defined change categories and NCI Agency change categorization as described below:

ITIL Change Type		Standard Change	Normal Change			Emergency Change
ITIL Change Category		Standard Change	Minor Change	Significant Change	Major Change	
NCI Agency Change Categories	CAT1	X	-	-	-	-
	CAT2	-	X	-	-	X
	CAT3	-	-	X	-	X
	CAT4	-	-	-	X	-

Table 5: ITIL VS NCI Agency Change Terminology

An Emergency Change Type can only be applicable to:

- CAT2/Minor Changes Category;
- CAT3/Significant Changes Category.

In very rare occasions, it would be possible to have an Emergency Change Type be applicable for a CAT4 / Major Change Category when a new service has to be implemented with highest urgency on very short notice to address a severe finding/Customer request.

An Emergency Change Type cannot be applied to a CAT1/Standard Change Category. If that would be the case then either the Change is wrongly classified as CAT1/Standard Change or Emergency is being confused with Urgency.

Change Authority describes who the responsible authority is to manage the change. For CAT 1 and 2 changes, the Change Authority will be the CSU/SL. Usually these are change requests from the customer, within the same SL or between SL which have minimal impact on service offering and availability. CAT 3 and 4 changes are managed by Enterprise IT Change Management.

## 12 REQUEST TYPES

There is a clear distinction between what request a Change Initiator raises and the change itself. It needs to be clear that a change request is not the same as the change itself. One is purely a request from a user to the service provide while the other is the change implementation itself.

There are 3 types of Change Requests:

- **Service Request (SR):** Although actioned through the Request Fulfilment process, a large majority of SR at one point in time used to be an RFC. Over time the execution of the RFC became, well known, documented and standard resulting in it becoming an SR, also known as a preapproved standard change. No further detail will be given to this Change Request type in this SOP. See Request Fulfilment SOP, Ref d).
- **Request For Change (RFC):** An RFC is the formal request to IT Change Management for a change to be made. The RFC will be evaluated be IT Change Management before being authorized as a change to be implemented.
- **Change Proposal (ChP) / Customer Request Form (CRF):** A CRF is the NCI Agency version of a change proposal which is the formal request to NCI Agency for the feasibility of a significant (CAT3) or major (CAT4) change. See Service Change Management Ref a).
  - A Change Proposal originates from Service Portfolio Management (SPM) Process;
  - A Change proposal is a short description of what must be done (changed or new service);

- It is possible that the implementation of change proposals is part of a service agreement with the Customer. In these Cases the Customer shall submit an Engineering Change Proposal (ECP) for the modification of a provided service.

Change Request Type		Change Categories			
		CAT1	CAT2	CAT3	CAT4
Requested by	NCI Agency	SR/RFC	RFC	RFC	RFC
	Customer	SR/RFC	RFC	CRF / ECP	CRF

Table 6: Change Request Types Submission Matrix

Request Type options from a Customer point of view:

- The Users of the Customer are able to create SR and RFC for the CAT 1 and 2 Change Categories as these are, for the majority, requests already covered and funded through an SLA. The CAT 3 and 4 Changes from the Customer do not flow as an RFC but as a Change Proposal, i.e. a CRF or ECP.
- For CAT 3 Change requests from the Customer the Change Proposal is usually a request for new capabilities/requirement implementation in an existing service offering. While the service is already available and maintained under an SLA it does not mean that new requirement and capability development is part of this offering, in which case a CRF is required. In some cases, new capability development and Customer requirement implementation is part of an SLA, PoW or other pre-agreed means of funding, to facilitate these requests an ECP change model will be available.
- For CAT 4 requests from the Customer this is very clear as it's a new capability or service which is requested for which the Agency needs to formally investigate and identify how the requested capability can be provided as a new service, following the Customer Request Form (CRF) Process.

Request type options from an NCI Agency internal point of view:

- SR and RFC process differentiation is already covered in previous chapters of this document.
- For CAT 3 & 4 changes will be processed as RFCs. Although out of scope of this document it is usually seen as the Agency process to approve new internal projects or modifications of services, this is particularly important as one of the major outcomes of this process is the allocation of funding to execute the proposed change.

For every authorized Change Proposal, a new RFC shall be raised for the actual implementation of the change in order to correctly plan the implementation and identify the impact on services. This includes all changes to the production environment done under the umbrella of a project, SLA, PoW or other approved means of funding in order to avoid any unplanned/unauthorized change to take place which can result in an interruption of service without prior knowledge or authorization.

### 13 CHANGE CLASSIFICATION

#### 13.1 Impact Categories

Impact is a measure of the effect on an incident, problem, or change. Impact is often based on how service levels will be affected.

Impact can be measured by the number of people affected, the criticality of the system, or the loss of revenue because of the service degradation or disruption.

Impact is derived from the following criteria:

- **Scope:** Who could be affected? Widespread, large, limited, or localized?
- **Customer Impact:** What impact will the Customer experience?
- **IT Resource impact:** Who is required to implement the change?
- **Complexity:** How difficult is it to implement (relationship & dependencies)?
- **Availability:** What outage is required?
- **Roll-back:** What is the impact of backing-out of the change?
- **SLA Targets:** Is there any agreement impacted (MoA, MoU, SLA, SSP, OLA, UC)?

In order to determine which level of impact shall be selected the general rule is:

- Lowest impact by default and can go higher when:
  - At least 3 of the criteria matches in the table below;
  - When unsure, select the higher Impact Category.

Impact (I)	Weight	Criteria
<b>Extensive</b>	<b>1</b>	<ul style="list-style-type: none"> <li>• <b>Scope:</b> Widespread.</li> <li>• <b>Customer Impact:</b> Impacts several Customers, major planned disruption to critical systems or impact to mission critical services.</li> <li>• <b>IT Resource Impact:</b> Involves IT resources from two or more workgroups and crosses IT divisions or involves expertise not currently staffed, or requires external SMEs.</li> <li>• <b>Complexity:</b> High complexity requiring technical and business coordination.</li> <li>• <b>Availability:</b> Change outage greater than 1 hour and affecting clients during Business hours. Lengthy install and back-out plan ready in standby to be implemented.</li> <li>• <b>Roll-back:</b> Affects critical data or server security and the back-out would likely extend the window timeframe.</li> <li>• <b>SLA targets:</b> Impacts SLA during business hours.</li> </ul>
<b>Significant</b>	<b>2</b>	<ul style="list-style-type: none"> <li>• <b>Scope:</b> Large.</li> <li>• <b>Customer Impact:</b> Impacts several Customers, significant disruption to critical systems or mission critical services.</li> <li>• <b>IT Resource Impact:</b> Involves IT resources from two or more workgroups within the same IT division, or involves expertise that has limited staffing, or requires external SMEs.</li> <li>• <b>Complexity:</b> Significant complexity requiring technical coordination only. No business coordination required.</li> <li>• <b>Availability:</b> Change outage less than 1 hour during Business Hours or greater than 1 hour during non-Business hours.</li> </ul>



Impact (I)	Weight	Criteria
		<ul style="list-style-type: none"> <li>• <b>Roll-back:</b> Affects non-critical data or security and has a moderate back-out plan, which would not extend window timeframe.</li> <li>• <b>SLA targets:</b> Impacts SLA during business hours.</li> </ul>
<b>Moderate</b>	<b>3</b>	<ul style="list-style-type: none"> <li>• <b>Scope:</b> Limited.</li> <li>• <b>Customer Impact:</b> Impacts a minimal number of users, minimal impact to a portion of a business unit or non-critical service.</li> <li>• <b>IT Resource Impact:</b> Involves IT resources from one workgroup within same IT division / department.</li> <li>• <b>Complexity:</b> Low complexity requiring no technical coordination.</li> <li>• <b>Availability:</b> Change outage less than 1 hour during Non-Business hours and affecting clients during that period only.</li> <li>• <b>Roll-back:</b> No security issues and simple back-out plan.</li> <li>• <b>SLA targets:</b> Minor/non-relevant/no impact on SLA targets.</li> </ul>
<b>Minor</b>	<b>4</b>	<ul style="list-style-type: none"> <li>• <b>Scope:</b> Localized.</li> <li>• <b>Customer Impact:</b> No impact to the business, as well as no impact to critical systems or services.</li> <li>• <b>IT Resource Impact:</b> Involves a single IT resource from a workgroup (e.g. CSU, OpsCen).</li> <li>• <b>Complexity:</b> Maintenance type of change.</li> <li>• <b>Availability:</b> No outage expected.</li> <li>• <b>Roll-back:</b> No back-out plan needed.</li> <li>• <b>SLA targets:</b> No effect on SLA targets.</li> </ul>

Table 7: Impact Categories

### 13.2 Urgency Categories

Urgency is a measure of how long it will be until the delay of a change has a significant business impact. For example, a high impact change may have low urgency if the impact will not affect the business until 6 months later e.g. End of life of an IT product.

Defined by the Change Initiator and reflects how quickly a change must be implemented, or the time available to reduce the impact of the change on the business. The default value of the Urgency field is Low.

Urgency can be derived based on the following criteria:

- **Scope:** Why does it require urgent processing?
- **Schedule:** The operational reason it requires urgent processing?
- **Security:** What are the security implications?

In order to determine which level of Urgency shall be selected the general rule is:

- Lowest Urgency by default and can be higher when at least 1 of the criteria matches in the table below;

Urgency (U)	Weight	Criteria
<b>Critical</b>	<b>1</b>	<ul style="list-style-type: none"> <li>• <b>Scope:</b> Service Outage of Core / Critical components</li> <li>• <b>Schedule:</b> Requires immediate processing</li> <li>• <b>Security:</b> Major security impact.</li> </ul>
<b>High</b>	<b>2</b>	<ul style="list-style-type: none"> <li>• <b>Scope:</b> Service Outage of low to medium components or to prevent an imminent core service outage</li> <li>• <b>Schedule:</b> Requires fast processing / VIP</li> <li>• <b>Security:</b> Significant security impact.</li> </ul>
<b>Medium</b>	<b>3</b>	<ul style="list-style-type: none"> <li>• <b>Scope:</b> No Service Outage but soon required, or to prevent a possible service outage</li> <li>• <b>Schedule:</b> Normal processing timeframe</li> <li>• <b>Security:</b> Minor security impact</li> </ul>
<b>Low</b>	<b>4</b>	<ul style="list-style-type: none"> <li>• <b>Scope:</b> No Service Outage</li> <li>• <b>Schedule:</b> Nice to have / processing when time permits</li> <li>• <b>Security:</b> Not security related.</li> </ul>

Table 8: Urgency Categories

### 13.3 Priority Categories

Priority is a category that is based on Impact and Urgency. It identifies the importance IT Change Management assigns to the change request. Priority indicates the order in which to process the changes. It is influenced by considerations such as risk and resource availability, but its primary driver is the combination of Urgency and Impact.

The Default Priority Categorization mapping is assigned as:

Priority		Urgency			
		1	2	3	4
Impact	1	1	1	2	2
	2	1	2	3	3
	3	2	3	3	4
	4	2	3	4	4

Table 9: Priority Category Matrix

### 14 RISK CATEGORIES

The risk category defines the level of risk that a change can have on the business due to unknown factors during the evaluation, complexity of the change or being unaware of the full scope of the impacted services.

Risk categorization and risk analysis is a complex matter. There is no mathematical formula that can correctly determine the risk of executing an IT change.

In order to determine the risk associated with an IT Change correctly we will have to take multiple factors into account, an overview of those, not limited to:

- Correct impact/urgency assignment;
- Back-out plan possibility and availability;
- Performance of the IT Change Manager;
- Affected CIs and their dependency relationships;
- Knowledge of the IT Change Implementer.

The Change initiator shall answer all mandatory questions to the best of their ability in order to identify the possible Risk Level. IT Change Management shall assess the risk based on provided information, experience and criteria on the risk levels based on Ref g).

Risk Level	Weight	Criteria
<b>Low Risk</b>	<b>1</b>	A risk that will have little or no impact on achieving outcome objectives. (e.g. No SLA Breach, few users impacted)
<b>Medium Risk</b>	<b>2</b>	A risk that will have a minor impact on achieving desired results to the extent that one or more stated outcome objectives will fall below goals but well above minimum acceptable levels. (e.g. No SLA Breach, service degradation)
<b>High Risk</b>	<b>3</b>	A risk that will have a moderate impact on achieving desired results to the extent that one or more stated outcome objectives will fall well below goals but above minimum acceptable levels. (e.g. No SLA Breach, severe degradation)

Risk Level	Weight	Criteria
<b>Very High Risk</b>	<b>4</b>	A risk that will have a significant impact on achieving desired results to the extent that one or more stated outcome objectives will fall below acceptable levels. (e.g. SLA Breach)
<b>Critical Risk</b>	<b>5</b>	A risk that will have a severe impact on achieving desired results, to the extent that one or more of its critical objectives will not be achieved. (e.g. Multiple SLA Breaches)

Table 10: Risk Categories

The default risk level is 1. Risk assessment is done based on Change Initiator and SME input with the Change Manager making the evaluation.

The Risk level will determine the Change authority for a specific change. Table 3: Change Authority Escalation Matrix will help to identify the right change authority for the identified risk.

**14.1 Probability of Risk**

The identification of the correct risk level is achieved based on the impact of the change and the probability of a risk event to occur.

Probability of Risk defines how likely a risk event is to occur. We differentiate between:

Risk Probability	Weight	Criteria
<b>Very Likely</b>	<b>1</b>	The Change is known to be a difficult implementation or has guaranteed issues that can't be mitigated before the execution of the change starts.
<b>Likely</b>	<b>2</b>	The Change has never been executed before or preparation shows likelihood of issues to occur that can't be mitigated during preparation.
<b>Unlikely</b>	<b>3</b>	The Change has been previously executed with no unexpected issues.
<b>Rare</b>	<b>4</b>	The Change has been previously executed numerous times with no unexpected issues.

Table 11: Risk Probability

### 14.2 Risk Level Identification

The below matrix maps out impact versus the risk probability and will define the risk level of a particular change.

Risk Level Identification		Impact			
		1	2	3	4
Risk Probability	1	5	4	3	3
	2	4	4	3	2
	3	3	3	2	2
	4	3	2	2	1

Table 12: Risk Level Identification

Risk level will be set in the IT Service Management Toolset in order to identify the correct Change Authority based on the Category of Change.

### 15 CHANGE PROCEDURE

This chapter covers the workflows for standard, normal and emergency IT Changes, in addition to process Triggers, Inputs and Outputs.

Change models shall be developed to support the generic change process. They shall also be developed to optimize the process flow for specific IT changes, whereby the generic process does not meet the requirements.

IT Change Management has the following relationships with other processes and activities. Figure 3: IT Change Management & Related Processes depicts those relationships.

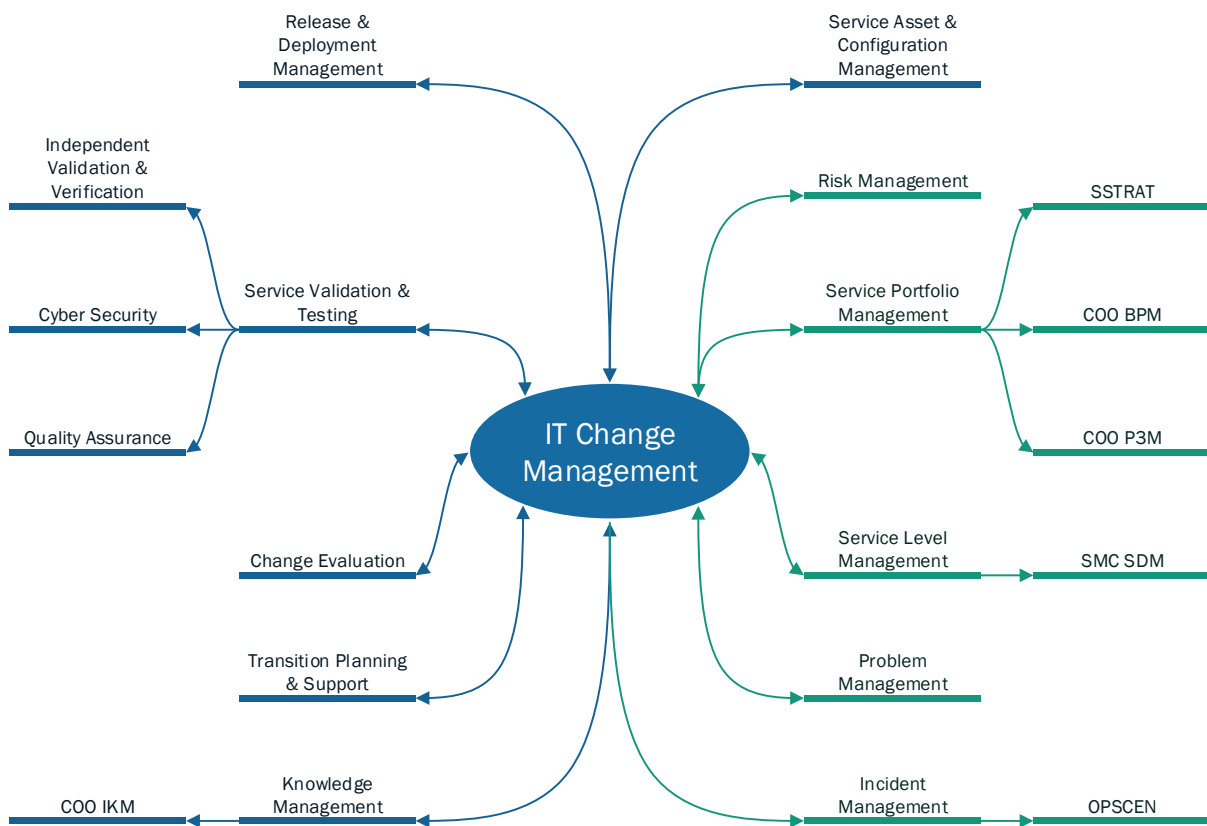


Figure 3: IT Change Management & Related Processes

### 15.1 Triggers

Common triggers for IT Change Management are, but not limited to:

Event/Information Product	From Process	Remark
<b>Problem Records</b>	Problem Management	To action Problem Management findings.
<b>Incident Records</b>	Incident Management	To assist incident resolution.
<b>Project or Program Requirements</b>	Any Process	Already approved Projects or PoW with funding.
<b>New business requirements / Strategic / Legal / Regulatory</b>	Service Portfolio Management	Change Proposal, Customer Request Form.
<b>Service Decommission</b>	Any Process	Driven by Service Delivery Manager / Resource Manager.
<b>SLA</b>	Service Level Management	New functional or non-functional negotiated requirements.
<b>Service Improvement Plans</b>	Continual Service Improvements	Optimizations for Service Delivery
<b>Operational Requirements</b>	Any Process	In support of business / Customer.

Table 13: IT Change Management Triggers

#### 15.1.1 Inputs

Input to the Change Management process are, but not limited to:

Information Product	From Process	Remark
<b>RFC</b>	Change Management	On Creation of the RFC.
<b>Change Proposals</b>	SPM	SPM or COO.

Table 14: IT Change Management Inputs

Any additional input / information that can be useful for the evaluation or implementation of the change shall be provided to IT Change Management in order to increase the success rate of the requested change. As example:

0002 Information Product	From Process	Remark
<b>Service Design Package</b>	Any Process	Can included means for change, build, transition release, support, test, evaluation, deploy and remediation. If already available should include roll-back plan, support plan, interface design.
<b>Test / Evaluation reports and/or interim test / evaluation reports</b>	Any Process	If already exists, including results.

0002 Information Product	From Process	Remark
<b>Assets or configuration items (e.g. baseline, release package)</b>	Any Process	That require a change, are new or to be decommissioned.
<b>Funding</b>	Any Process	Funding for the activity needs to be clear and available.
<b>Justification</b>	Any Process	Change must be properly motivated to justify the change request.

Table 15: Change Input supporting documents

### 15.1.2 Outputs

The IT Change Management Process delivers as output:

Information Product	To Process	Remark
<b>Rejected and cancelled RFC</b>	-	Change Initiator informed.
<b>Authorized RFC</b>	SVT / CM / RDM	Further processing of the change.
<b>Change Proposal feasibility Study</b>	SPM / COO	To make informed decision on the Proposal's existence.
<b>Change Schedule</b>	RDM	When the change will be implemented.
<b>Change to Service or Infrastructure</b>	Operations	Result from authorized change, Implementation.
<b>New, changed or disposed CIs</b>	CM	Update CMDb / CMS
<b>Change documents, records and reports</b>	KM	Part of the SKMS.
<b>Service Design Package</b>	RDM	Basis for RDM to plan the build, test and deployment.
<b>Post Implementation Review (PIR)</b>	CSI	When required, post implementation review is done and passed to CSI for process optimization.
<b>Closed RFC</b>	-	Change Initiator informed when change is formally closed.

Table 16: IT Change Management Outputs

### 15.2 Process Workflow

This chapter describes the generic process workflows from for Standard Change (CAT1), Normal Change (CAT2-4) and Emergency Change. The 3 generic workflows follow 8 phases, each of these phases are described in the simplified flow.

These 3 generic workflows are the foundation for change models. Change models will be used to document how change requests of a specific category flow through the process, which steps of the generic workflow can be skipped and which entities need to be tasked to achieve a correct outcome of the change requested. Whenever a specific change model does not exist, one of the generic change models shall be used to submit an RFC.



### 15.2.1 Standard Change (CAT1) - Generic

The Standard Change Process flow describes the steps from submission to closure of a standard Change, also known as a CAT1 Change. This is the most simplistic of workflows for which minimal validation, authorization and review is required.

A detailed description of each work step is documented in Annex I Detailed Workflow Step Description.

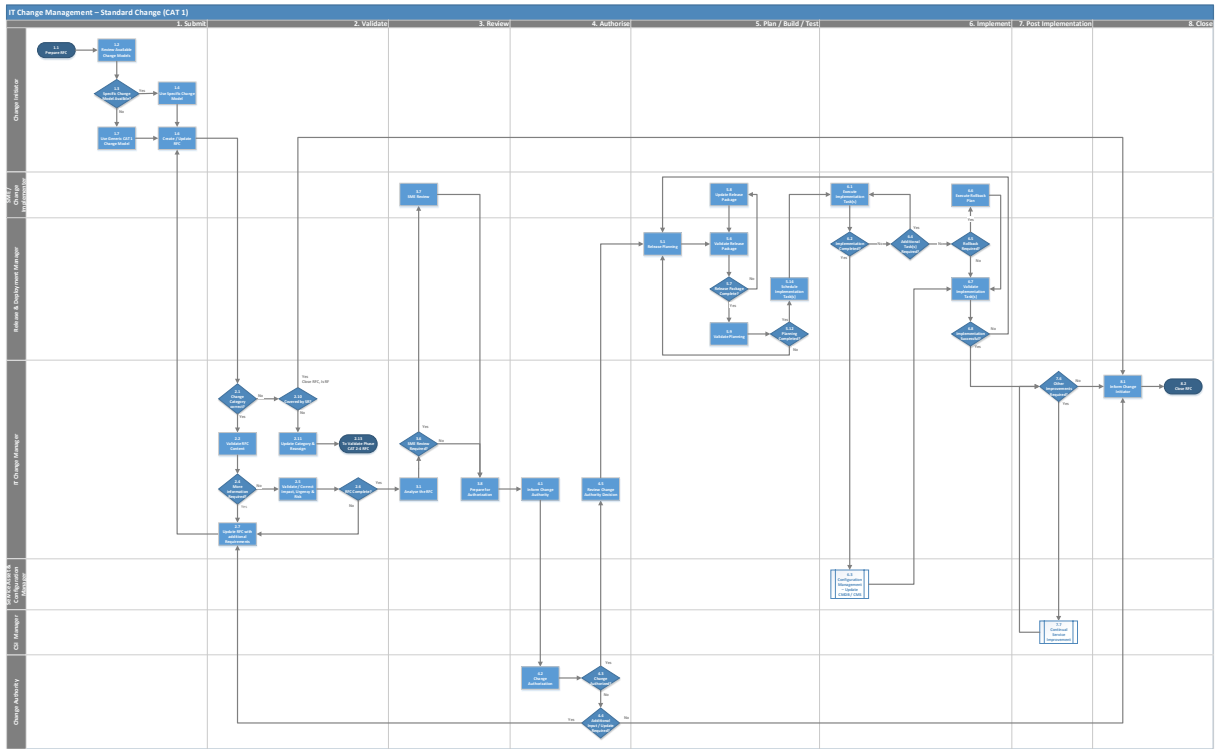


Figure 4: Generic Process Workflow - Standard Change (CAT1)

The complete process flow visualized above can be found in more detail as part of Annex F Detailed Standard Change (CAT1) – Generic or on the SMC portals referenced in chapter 17.1 Updates and Publication.

### 15.2.2 Normal Change (CAT2 – 4) - Generic

The Normal Change Process flow describes the steps from submission to closure of a normal Change, also known as CAT2, 3 or 4 Changes. This workflow covers all IT change management scenarios and is the default RFC process flow if no specific change model exists.

The Normal Change process is applicable to Emergency Changes with minor deviations in the work steps. Execution time is the main difference between the two.

A detailed description of each step is documented in Annex I Detailed Workflow Step Description.

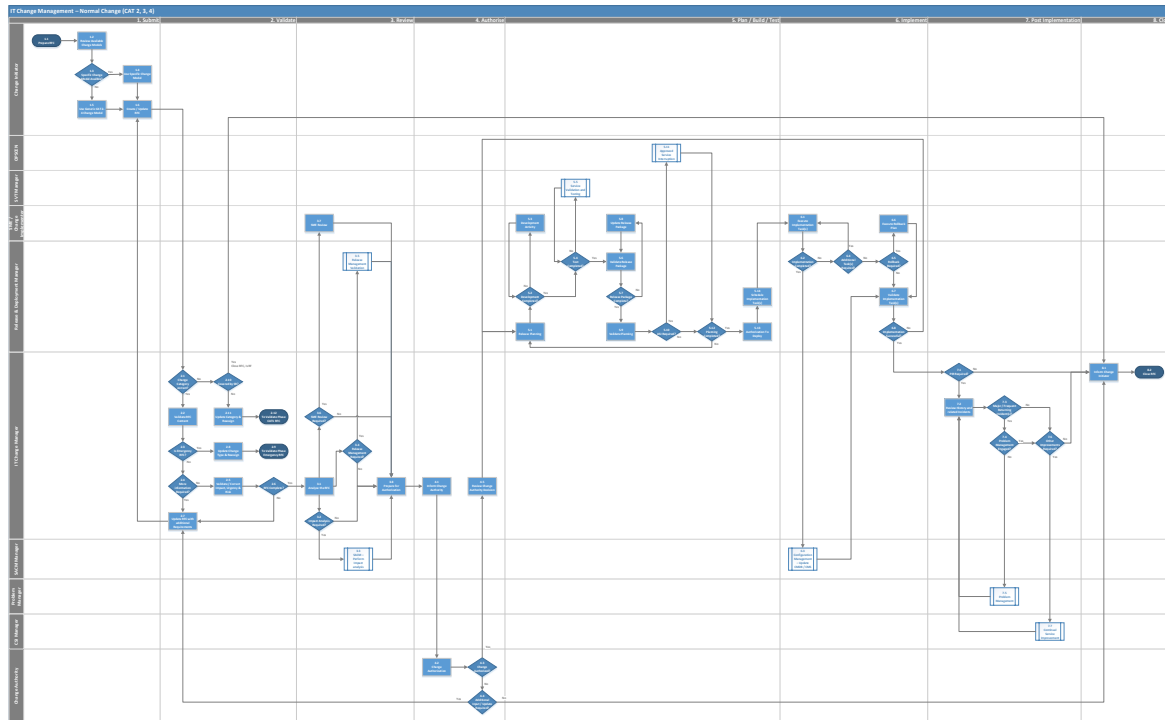


Figure 5: Generic Process Workflow - Normal Change (CAT2-4)

The complete process flow visualized above can be found in more detail as part of Annex G Detailed Normal Change (CAT2-4) – Generic or on the SMC portal referenced in chapter 17.1 Updates and Publication.

### 15.2.3 Emergency Change - Generic

The Emergency Change process flow describe the steps from submission to closure of an Emergency RFC; typically, this will only be applicable on CAT2 and CAT3 changes.

Overall, the normal change process is sufficient but due to the urgency of the emergency change, it is possible that some steps are performed without completion of a previous step. As a result, an additional validation is required after the normal workflow has been executed to certify that everything is properly completed, recorded and actioned.

A detailed description of each step is documented in Annex I Detailed Workflow Step Description.

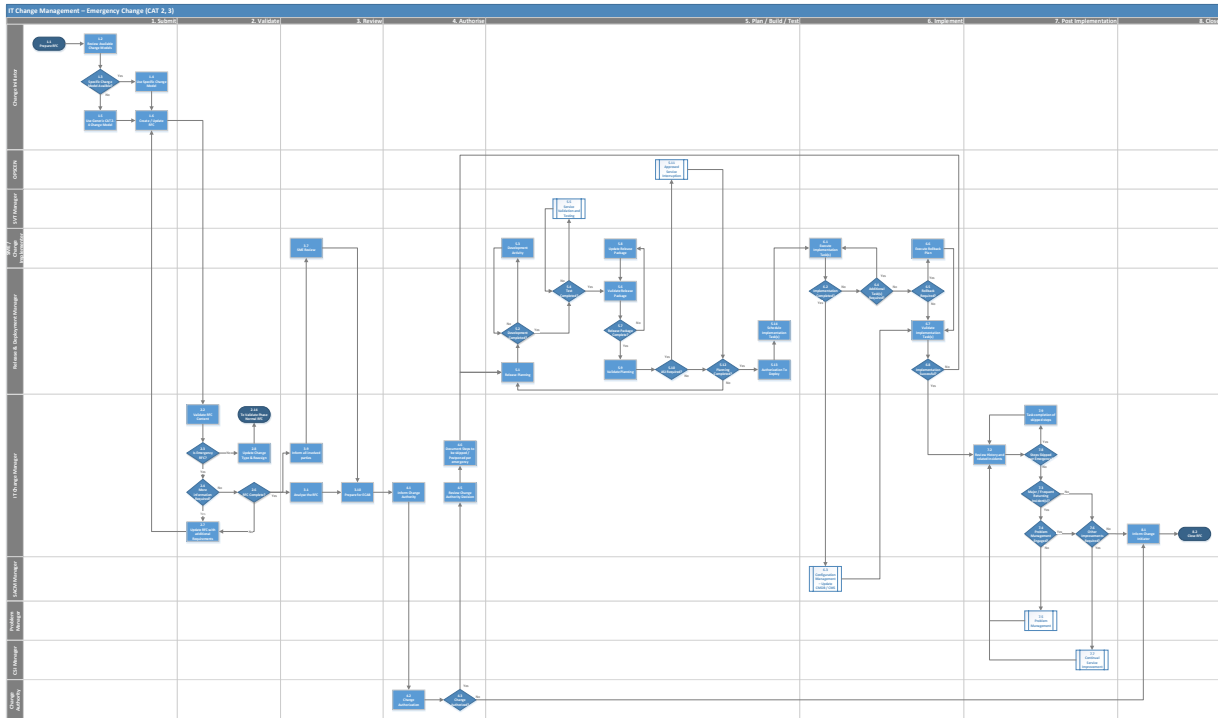


Figure 6: Generic Process Workflow - Emergency Change (CAT2-3)

The complete process flow visualized above can be found in more detail as part of Annex H Detailed Emergency Change - Generic or on the SMC portals referenced in chapter 17.1 Updates and Publication.

### 15.3 Process Workflow Step Description

Workflow step description for each of the activities described in the 3 generic workflows can be found in Annex I Detailed Workflow Step Description.

### 15.4 Change Models

As previously discussed, change models are predefined workflows based on the generic workflow, which specify how a change request needs to be actioned based on what is requested.

The goals of using change models is that after the process matures, 95% or more of the submitted changes can be facilitated by using a change model (Template). This will allow for more accurate, consistent data capture and processing of the RFC, allowing shorter timescales to be achieved.

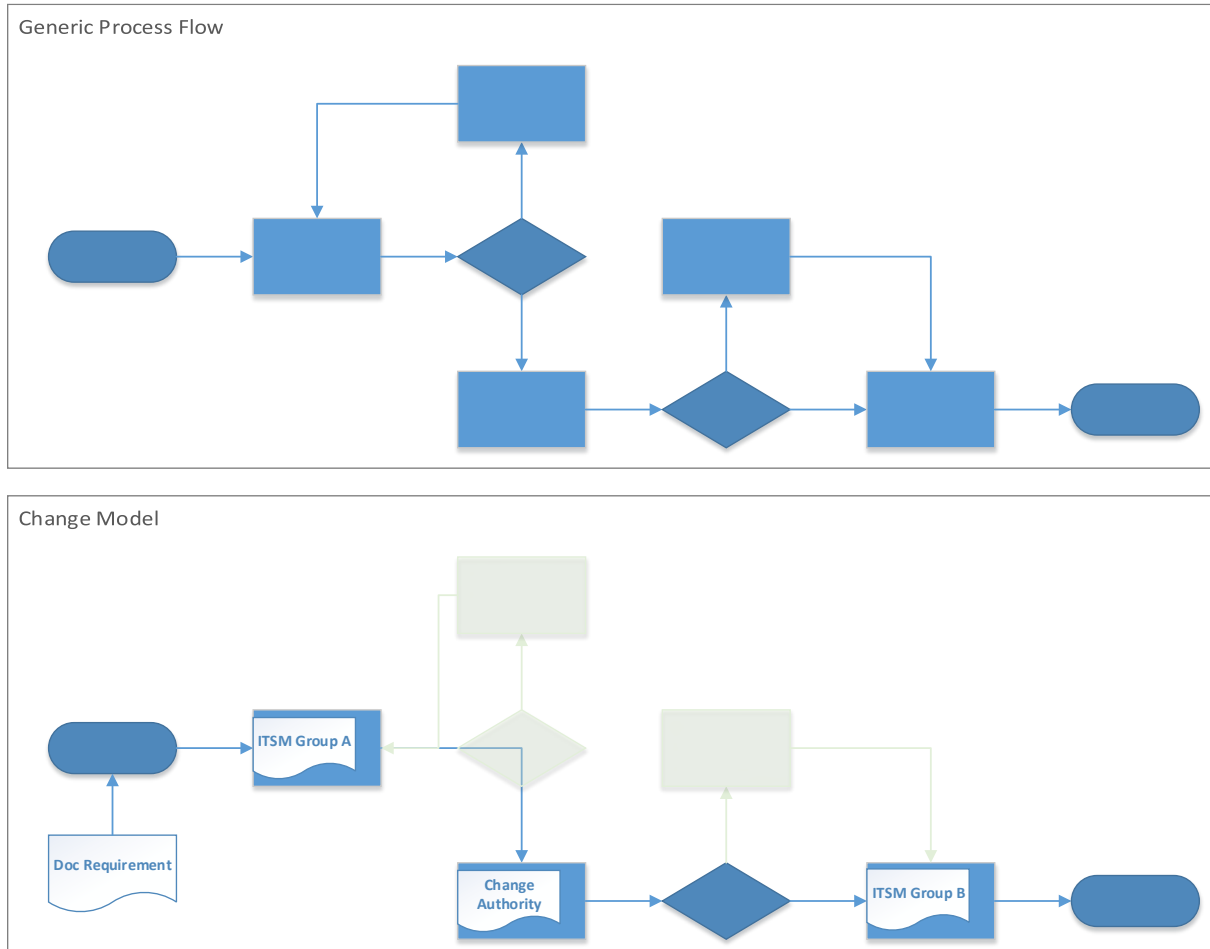


Figure 7: Generic Process VS Change Model

As visualized in the above diagram an (not representative) example of the normal generic process flow is listed at the top. A change model is developed based on the generic process flow but not all steps are necessary (Faded green). At the same time additional documentation requirements are defined; functional group assignment stipulated for both RFC and associated tasks and change authority designated.

The Enterprise toolset allows templates to be defined that stipulate the process, simplifies the information gathering and streamlines the requests raised by the Change Initiator through the workflow.

Change models will be managed by SMC CCA and authorized by the Enterprise CAB, unless delegated. This shall guarantee that no duplication of a change model exists.

New change models can be created submitted to the Enterprise CAB; template for new Change Model Request is available in Annex D Change Model Template.

When specific change models are developed for CAT2-4 Changes, they will start with the described Generic Normal Change process as a foundation and identify which steps can be excluded.

Each change model will describe the required information and documentation required during the submission of the RFC. *As an example: An RFC for configuration change in an application might just require proper justification, CI affected and expected impact. An RFC for rollout of software to every device will require a justification, affected CI list, expected impact or downtime analysis, deployment plan, funding confirmation, AFPL validation, communication plan, etc....*

All available change models and their template will be available in the ITSM toolset for selection when creating an RFC and on the SMC portal on Reach and NS (location in chapter 17 DOCUMENT CONTROL) as reference for submission requirements, workflow process, and task assignment and escalation paths.

## **16 SMC ENTERPRISE TOOLSET**

BMC Remedy ITSM is the Change Management toolset.

Change Requests shall be raised through the Self Service portal; BMC MyIT.

Changes shall not be raised using the BMC ITSM mid-tier console; this is reserved for management of the change request.

### **16.1 Change Management Module**

Within ITSM, the Change Management Module will be used for all change management activities from CAT 1 to CAT 4. Request Fulfilment will be completed in the Work Order Module as part of the Approved Service Request List.

In order to make a RFC in ITSM a CRQ shall be raised.

#### **16.1.1 Change Lifecycle**

The ITSM Change Management module follows 5 lifecycle Phases: Initiate, Review & Authorize, Plan & Schedule, Implement and Closed.

Each phase can be mapped to the to the change management procedure described in this SOP, see Figure 8: ITSM Phases to Process Phases

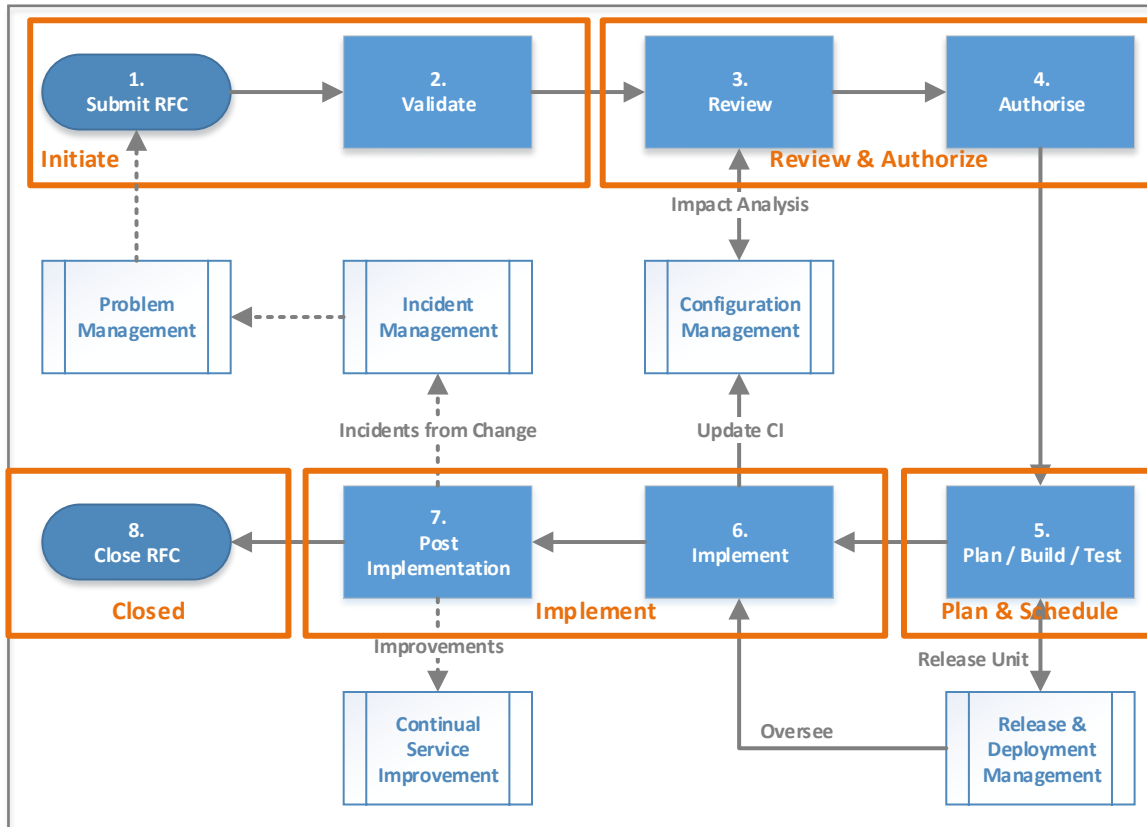


Figure 8: ITSM Phases to Process Phases

### 16.1.2 Change Approvals

The Toolset has a built in capability to deal with multiple type of approvals throughout the lifecycle of a change. As depicted In Figure 9, there are 4 possible stages of approval during the lifecycle.

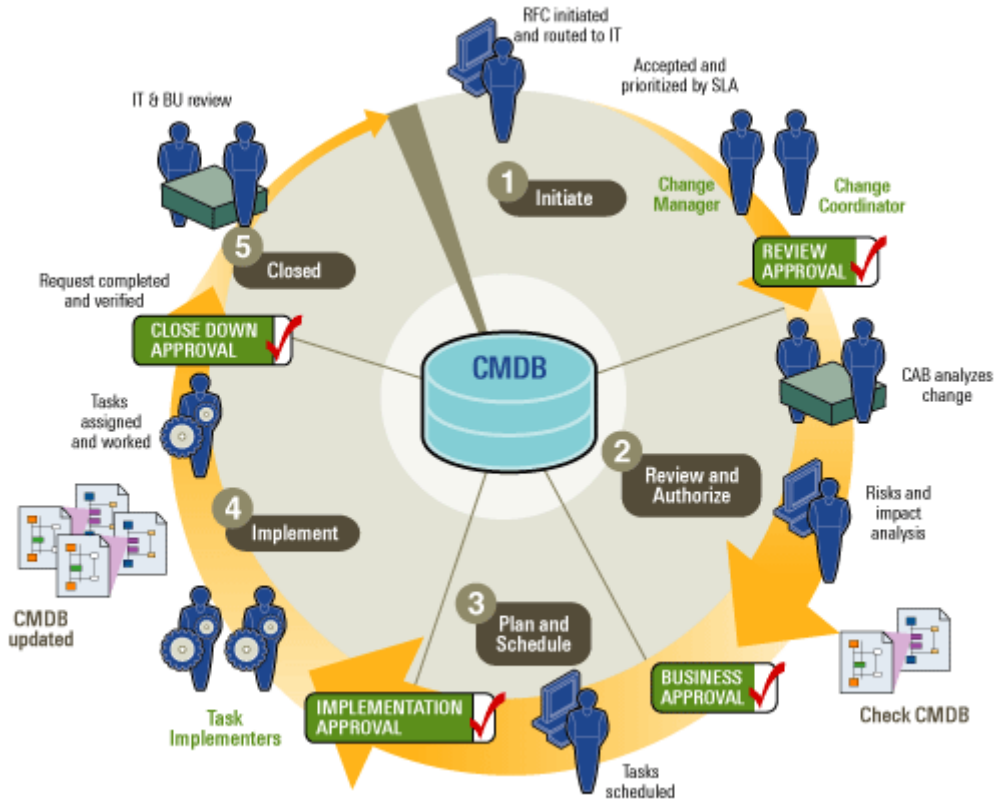


Figure 9: ITSM Change Lifecycle

Each of these approval phases have their own value and use cases. Table 17: ITSM Approval Phases Description provides an overview of the most common.

Approval Phase	Description
<b>Review Approval</b>	The Review Approval can take place at the end of the Initiate Phase ( <i>Validation</i> ). Main purpose is to ensure all required input is provided and is valid before processing to the review of this change. The Change Manager can validate or, a Customer Approval step can be inserted. This can allow the Customer to accept each change request raised by their user before it gets to the Agency.
<b>Business Approval</b>	The Business Approval can take place at the end of the Review and Authorize Phase ( <i>Authorize</i> ). Main purpose is the acceptance of the Change by the Change Authority and the authorization for preparing the change to take place. This Authorization is usually given after evaluation and analysis by the IT Change Manager, SDM and or SME’s with or without CAB involvement. It is the official acceptance by the Agency of the RFC to be a change that will implemented at a point in time.
<b>Implementation Approval</b>	The Implementation Approval can take place at the end of the Plan and Schedule Phase (Plan, Build, Test). Main purpose is the

Approval Phase	Description
	review of all scheduled activities for the implementation of that change and the final authorization before changes are done on the production environment. Usually this decision is based on presented implementation plan, ASI coordination completed, etc.
<b>Close Down Approval</b>	The Close Down Approval can take place at the end of the Implementation Phase. Main purpose is to validate that the change was correctly implemented, no additional activities are required and/or no roll-back plan needs to be executed. After this validation, the Change Initiator can be informed about change implementation before the RFC is closed.

Table 17: ITSM Approval Phases Description

During the requirement specification of a change model it will become clear, which approval gates are required for that particular use case. By default the Review Approval, Implementation Approval and Close Down approval are present in all templates unless otherwise stated or described.

**17 DOCUMENT CONTROL**

The NCI Agency Quality Management System, as described in the AD 06.00.06, Agency Quality and Compliance Management Policy, Ref h), establishes the objectives, policy, principles and processes for QM in the Agency. It also identifies Process Quality Management as one of the Quality Management Domains. Quality Management will occur within the context of the Agency Quality Management System (QMS), which follows the ISO 9001:2015 practice and is based on a Plan-Do-Check-Act (PDCA) cycle. The NCI Agency QMS is predicated on the principle of “Quality Built In.” It is, therefore, inherently part of any process design and implementation.

The IT Change Management Process Owner is overall accountable for Managing Process Quality for the IT Change Management process.

Process Quality Management is one of the five quality management domains, as identified in the QMS. The Manage Process Quality process is further detailed in PDED 06.01.04 Manage Process Quality.

**17.1 Updates and Publication**

This interim SOP will be published as a formal Agency document and put under configuration control. For process, assurance and control purposes the IT Change Management Process Owner will implement and maintain a record of all the related process documentation.

This interim SOP will be reviewed after 6 months and reissued as a full SOP.

The latest and official version of this document may be obtained on SMC intranet page on both NR and NS network. Reach: <https://dis.nr.ncia/smc/CCA/SitePages/Home.aspx> NS: <https://nww.portal.ncia.nato.int/nchg/smd/cqm/>.

Annexes will be hosted on the above link as a separate document and will have its own version control to facilitate Continual Service Improvement on the IT Change Management process.

It is the responsibility of the users of this document to ensure that they are using the most recent version available.

Revisions to this SOP will fall under the Change Management Process.



**Annex A ABBREVIATIONS**

Abbreviation	Full Wording
<b>A&amp;TP</b>	Application and Technology Portfolio
<b>AFPL</b>	Approved Fielded Product List
<b>AoR</b>	Area Of Responsibility
<b>ASI</b>	Approved Service Interruption
<b>ASR</b>	Approved Service Request
<b>BPM</b>	Business Planning Management
<b>CAB</b>	Change Advisory Board
<b>CAT</b>	Category
<b>CCA</b>	Change & Configuration Authority
<b>ChP</b>	Change Proposal
<b>CI</b>	Configuration Item
<b>CIS</b>	Computer Information System
<b>CM</b>	Configuration Management
<b>CMDB</b>	Configuration Management Database
<b>CMS</b>	Configuration Management System
<b>COO</b>	Chief Operating Office
<b>CRF</b>	Customer Request Form
<b>CS</b>	Cyber Security
<b>CSI</b>	Continual Service Improvement
<b>CSSC</b>	CIS Sustainment Support Centre
<b>CSU</b>	CIS Support Unit
<b>DML</b>	Definitive Media Library
<b>DSO</b>	Directorate Service Operations
<b>ECAB</b>	Emergency Change Advisory Board
<b>ECP</b>	Engineering Change Proposal
<b>ESDM</b>	Enterprise Service Delivery Model
<b>IKM</b>	Information Knowledge Management
<b>ITIL</b>	Information Technology Infrastructure Library
<b>ITSM</b>	Information Technology Service Management
<b>IV&amp;V</b>	Independent Validation & Verification
<b>KM</b>	Knowledge Management
<b>KPI</b>	Key Performance Indicator

Abbreviation	Full Wording
<b>NCI Agency</b>	NATO Communication and Information Agency
<b>NQAR</b>	NATO Quality Assurance Representative
<b>OPSCEN</b>	Operations Centre
<b>OU</b>	Organizational Unit
<b>P3M</b>	Portfolio, Programme and Projects Management
<b>PDCA</b>	Plan-Do-Check-Act
<b>PIR</b>	Post Implementation Review
<b>PM</b>	Project Manager
<b>PO</b>	Programme Office
<b>PoW</b>	Programme of Work
<b>QA</b>	Quality Assurance
<b>QMO</b>	Quality Management Office
<b>QMS</b>	Quality Management System
<b>RDM</b>	Release & Deployment Management
<b>RFC</b>	Request For Change
<b>RM</b>	Resource Manager
<b>RO</b>	Routine Order
<b>CM</b>	Configuration Management
<b>SDM</b>	Service Delivery Manager
<b>SDP</b>	Service Design Package
<b>SKMS</b>	Service Knowledge Management System
<b>SL</b>	Service Line
<b>SLA</b>	Service Level Agreement
<b>SMC</b>	Service Management & Control
<b>SME</b>	Subject Matter Expert
<b>SOI</b>	Standard Operating Instruction
<b>SOP</b>	Standard Operating Procedure
<b>SPM</b>	Service portfolio Management
<b>SR</b>	Service Request
<b>SSTRAT</b>	Service Strategy
<b>SVT</b>	Service Validation & Testing
<b>TPS</b>	Transition Planning and Support

Table 18: Abbreviations

**Annex B RACI MATRIX**

RACI matrix based on the described roles from Chapter 10 and the generic process phases as defined in Chapter 8 HIGH LEVEL PROCESS.

RACI Remarks<sup>6</sup>

Phase \ Role	PO IT Change Management	IT Change Initiator	Service Delivery Mgr.	IT Change Manager	Release & Deployment Manager	SACM Manager	SME	TPS Manager	IT Change Authority	CAB Member	CAB Chairperson	NOAR	SVT Manager	IT Change Implementer
1. Submit RFC		R - A		C - I										
2. Validate		C - I		R - A										
3. Review		C - I	R - C	R - A	R - C	R - C	R - C							
4. Authorise		C - I	R - C	R	C	C	C	C - I	A - R	C	C	C	C	I
5. Plan / Build / Test		I	R - A	C - I	R	I	R - C	C - I					R - C	C - I
6. Implement		I	R - A	C - I	R	R - I	C - I	C - I	I	I	I	I	I	R
7. Post Implementation		I	R - I	R - A	R - I	I	C - I	C - I	I	I	I	C - I		C
8. Close RFC		C - I		R - A										

Table 19: RACI Matrix - Change Phase VS Role

<sup>6</sup> The Process Owner of IT Change Management is overall accountable for the IT Change Management Process and IT Change Management at Enterprise Level;  
 When the matrix mentioned more than one selection it's due to different level of involvement based on the change category;  
 Split between roles with both accountability and responsibility will be addressed at later stage (e.g. split between IT Change Manager and IT Change Coordinator).

Phase \ Role	IT Change Initiator	Service Delivery Mgr.	IT Change Manager	Release & Deployment Manager	SACM Manager	SME	TPS Manager	IT Change Authority	CAB Member	CAB Chairperson	NQAR	SVT Manager	IT Change Implementer
1. Submit RFC	R - A		C - I										
2. Validate	C - I		R - A										
3. Review	C - I	R - C	R - A	R - C	R - C	R - C							
4. Authorise	C - I	R - C	R	C	C	C	C - I	A - R	C	C	C	C	I
5. Plan / Build / Test	I	R - A	C - I	R	I	R - C	C - I					R - C	C - I
6. Implement	I	R - A	C - I	R	R - I	C - I	C - I	I	I	I	I	I	R
7. Post Implementation	I	R - I	R - A	R - I	I	C - I	C - I	I	I	I	R - C		C
8. Close RFC	C - I		R - A										

**Annex C KPI & MONITORING**

The objectives of the IT Change Management process are listed in Chapter 4. Achievement of those objectives is dependent on the IT Change Management process to be executed in accordance with documented procedures and ensuring the quality of executing the procedures remains high. At all costs, unauthorized changes need to be prevented as these can affect Customer services and service availability, which cannot be prevented or stopped until the service is interrupted and detected by Event Management or Incident Management.

The Critical Success Factors (CSF) and KPIs listed below are therefore focused on those aspects that must be implemented as an initial step towards improving process maturity. The CSFs and KPIs will be reviewed and updated in future reviews of the SOP to take into account lessons learned and improvements in IT Change Management process maturity.

Critical Success Factor (CSF)	Key Performance Indicator (KPI)	Internal Target
<b>Responding to NATO IT Business needs while maximizing value</b>	1. Number of Change Requests	<b>Not yet applicable</b>
	2. Average time for each phase	<b>Not yet applicable</b>
	3. Backlog of change requests older than X weeks	<b>Not yet applicable</b>
	4. Changes Closed successfully	<b>&gt;= 95%</b>
<b>Optimizing overall business risk</b>	5. Number of changes where remediation is invoked	<b>&lt;= 5%</b>
	6. Percentage of failed Changes	<b>&lt;= 2%</b>
	7. Number of Unauthorized Changes	<b>&lt;= 1%</b>
<b>Make efficient use of resources required to handle RFCs</b>	8. Percentage Timeliness and Quality of change implementation	<b>Not yet applicable</b>
	9. Percentage of Emergency Changes	<b>Not yet applicable</b>
	10. Average Cumulative time for each phase	<b>Not yet applicable</b>

Table 20 - Process CSFs & KPI's

Besides the above listed KPIs, IT Change Management will track the below metrics for trend analysis and historical comparison purpose. This activity will mainly be captured in weekly or monthly reports generated from the toolset.

All metrics listed below shall have the possibility to apply filters on the following data fields:

- Changes by Type
- Changes by Category
- Changes by Status
- Changes by Location

Metrics	Simplified Calculation
<b>% Closed Successful</b>	# of changes "Closed Successful"/total number of changes
<b>% Closed Failed</b>	# of changes "Closed Failed"/total number of changes
<b>% Open</b>	# of changes that are in the following status: ("Submitted," "Reviewed," "Provisional," "Pending," "Resubmitted," and "Scheduled")/total number of changes
<b>% Rejected</b>	# of changes that are in the following status: ("Rejected")/total number of changes
<b>% of Cancelled</b>	# of changes that are in ("Cancelled" and "Draft")/total number of changes
<b># of Emergency</b>	Total # of Emergency changes
<b># of Normal</b>	Total # of Normal changes
<b>Total # of Changes per week/month</b>	Shows the total number of RFCs
<b>% of Emergency</b>	# of Emergency changes/total number of changes
<b>% of Normal</b>	# of Normal changes/total number of changes

Table 21: IT Change Management Metrics



## **Annex D CHANGE MODEL TEMPLATE**

This change model template is used to document and request a new specific change model. It will document which steps in the process are part of the model, what information needs to be provided by the Change Initiator, etc... Additional information will be added by IT Change Management for Change Management purposes (Escalation, SME required, Tasking, etc....)

All available change models are available on SMC portal, see Chapter 17.

The change model Template document is also available on the SMC portal or through a Change Request in the MyIT Self-Service Portal.

**Annex E DISTRIBUTED CHANGE AUTHORITY DEVIATIONS**

The below table describes the deviations from the default Change Authority model as described in Chapter 9.1 Change Authority

Change Authority	Category	CAT 3	CAT 4	Date Delegation Granted	Remarks
Entity		X	X	DD/MM/YYYY	



**Annex F DETAILED STANDARD CHANGE (CAT1) – GENERIC**

Below you will find the complete process flow described in 15.2.1 Standard Change (CAT1) - Generic but split over each phase for ease of use and readability.

Phase 1: Submit

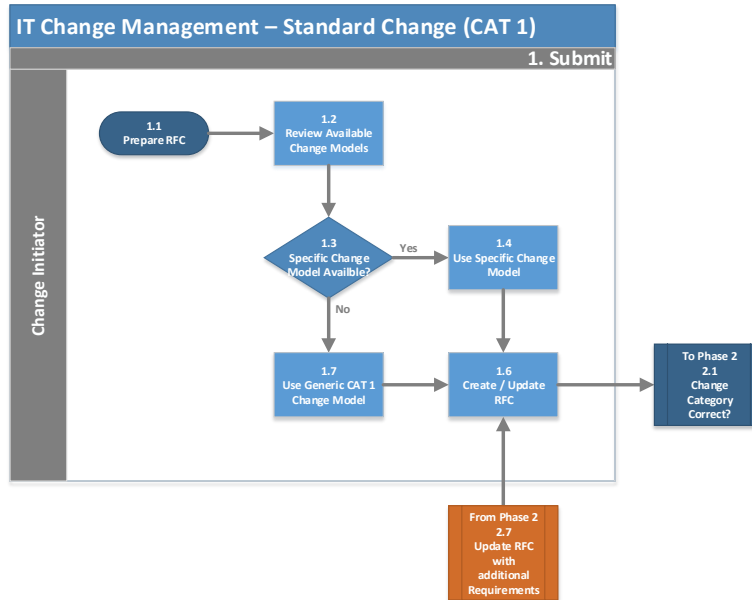


Figure 10: Generic Process Workflow - Standard Change (CAT1) - Phase 1

Phase 2: Validate

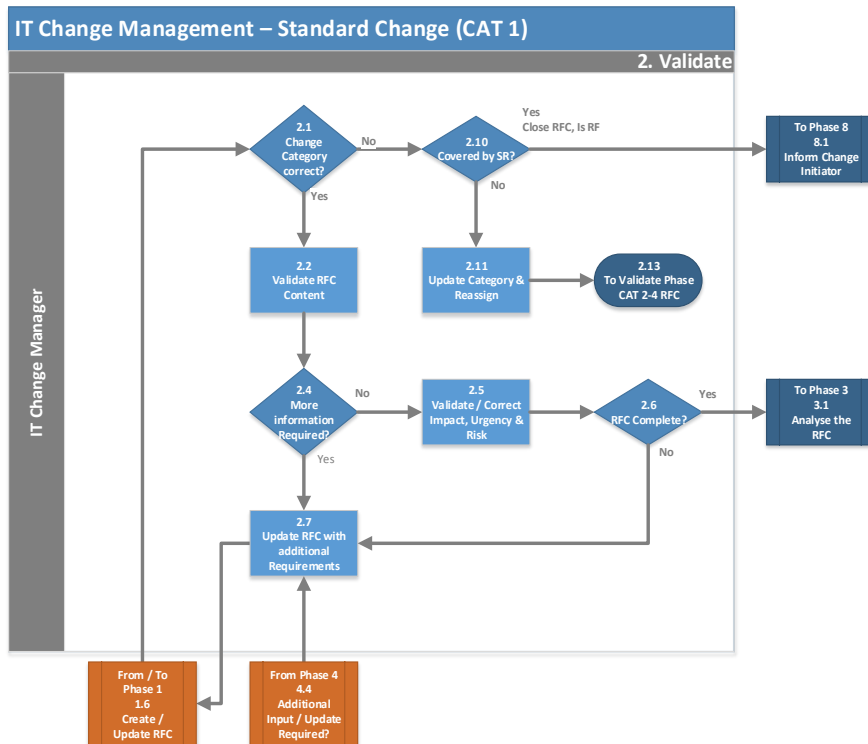


Figure 11: Generic Process Workflow - Standard Change (CAT1) - Phase 2

Phase 3: Review

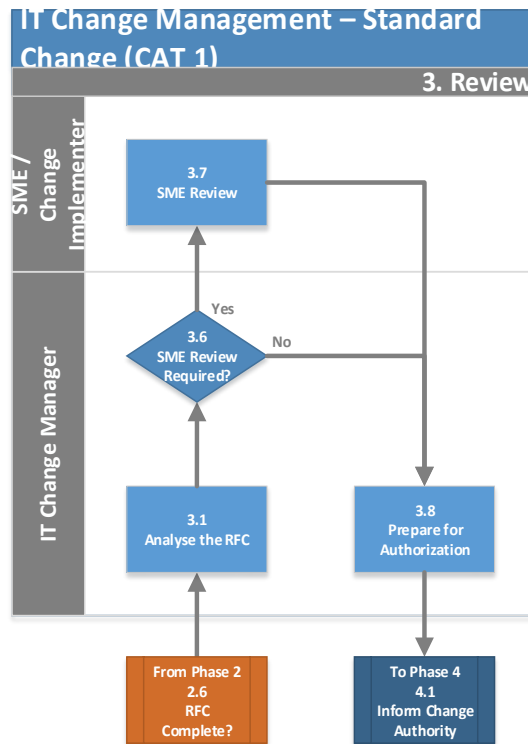


Figure 12: Generic Process Workflow - Standard Change (CAT1) - Phase 3

Phase 4: Authorise

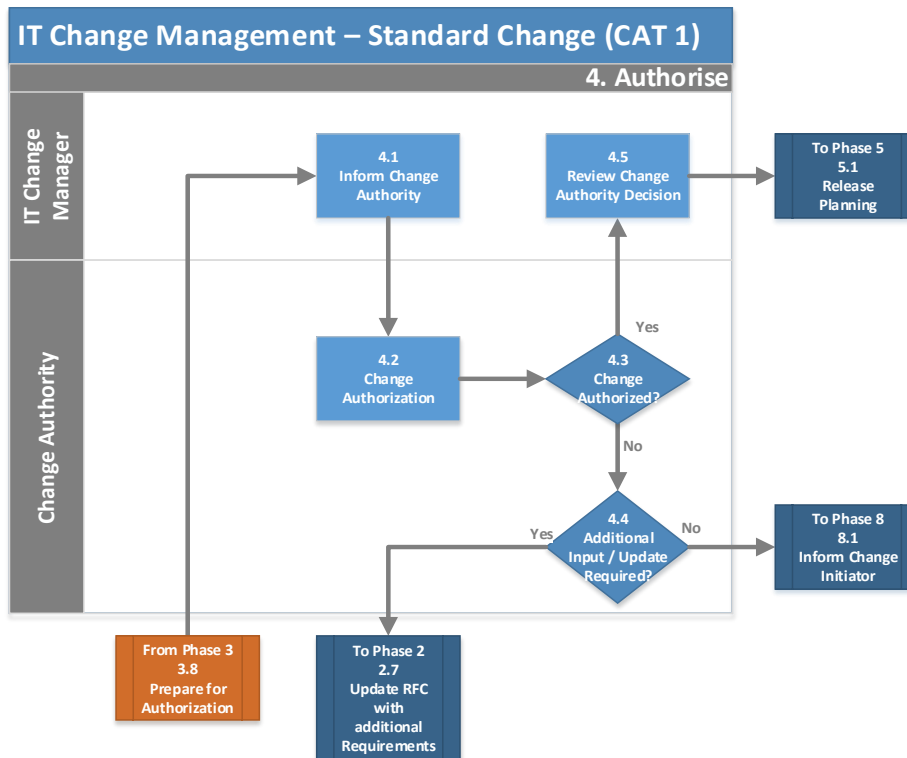


Figure 13: Generic Process Workflow - Standard Change (CAT1) - Phase 4

Phase 5: Plan / Build / Test

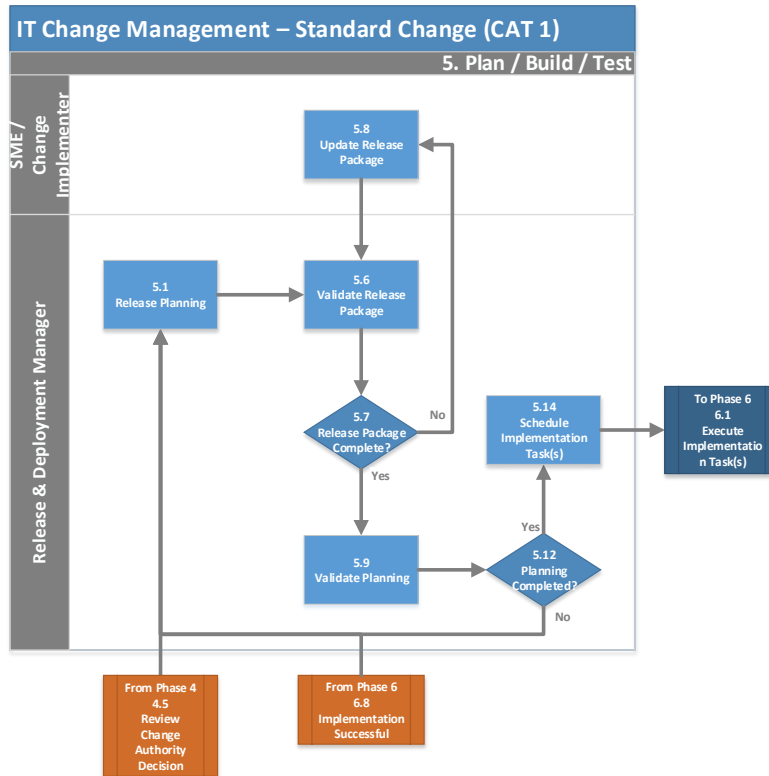


Figure 14: Generic Process Workflow - Standard Change (CAT1) - Phase 5

Phase 6: Implement

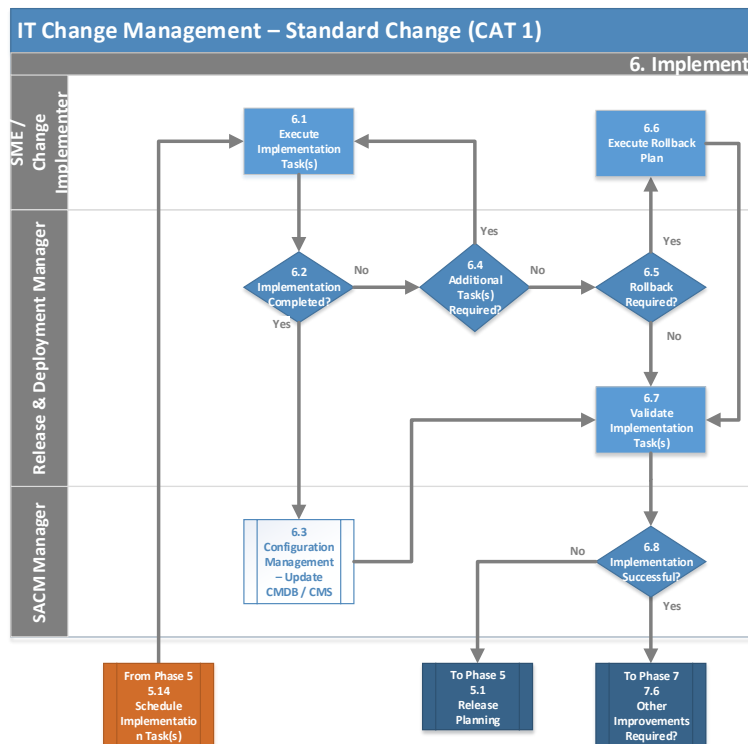


Figure 15: Generic Process Workflow - Standard Change (CAT1) - Phase 6

Phase 7: Post Implementation

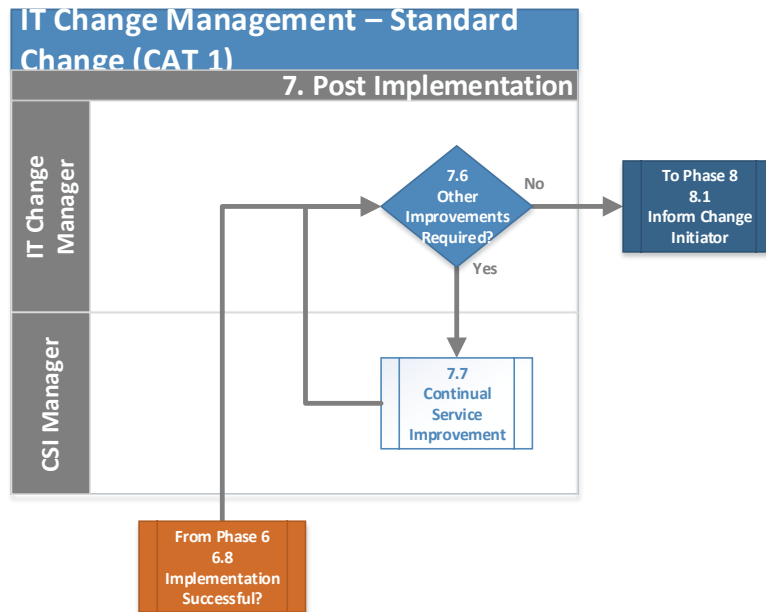


Figure 16: Generic Process Workflow - Standard Change (CAT1) - Phase 7

Phase 8: Close

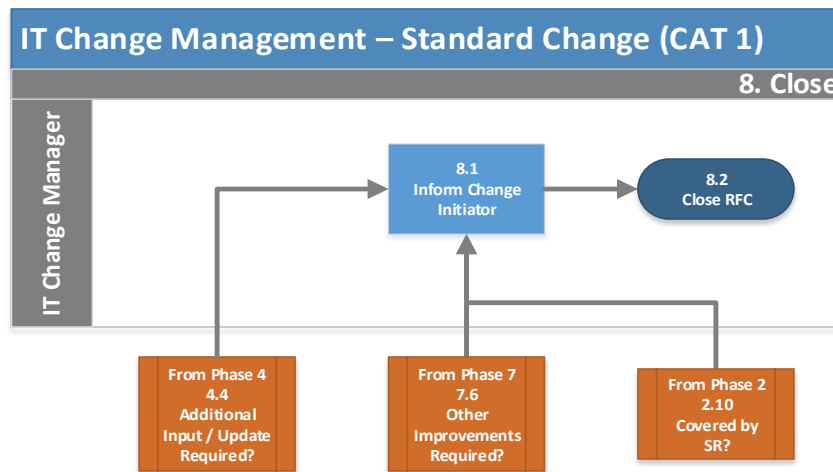


Figure 17: Generic Process Workflow - Standard Change (CAT1) - Phase 8

**Annex G DETAILED NORMAL CHANGE (CAT2-4) – GENERIC**

Below you will find the complete process flow described in 15.2.2 Normal Change (CAT2 – 4) - Generic but split over each phase for ease of use and readability.

Phase 1: Submit

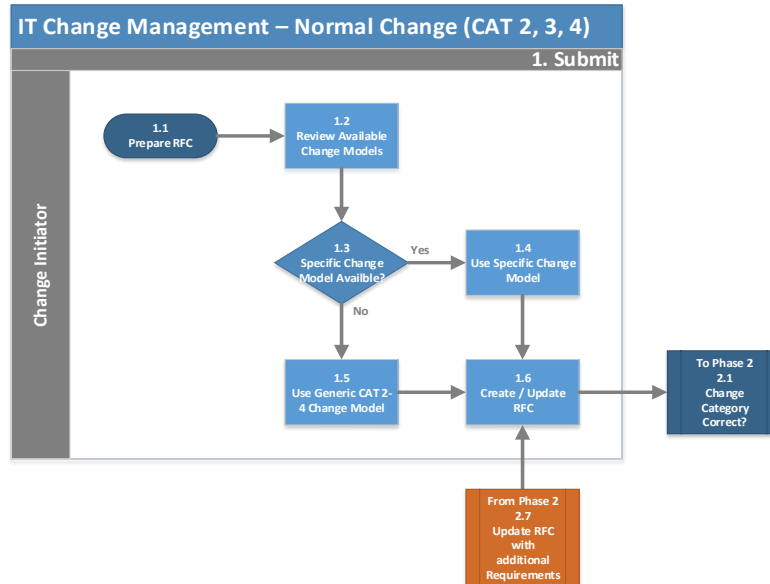


Figure 18: Generic Process Workflow - Normal Change (CAT2-4) - Phase 1

Phase 2: Validate

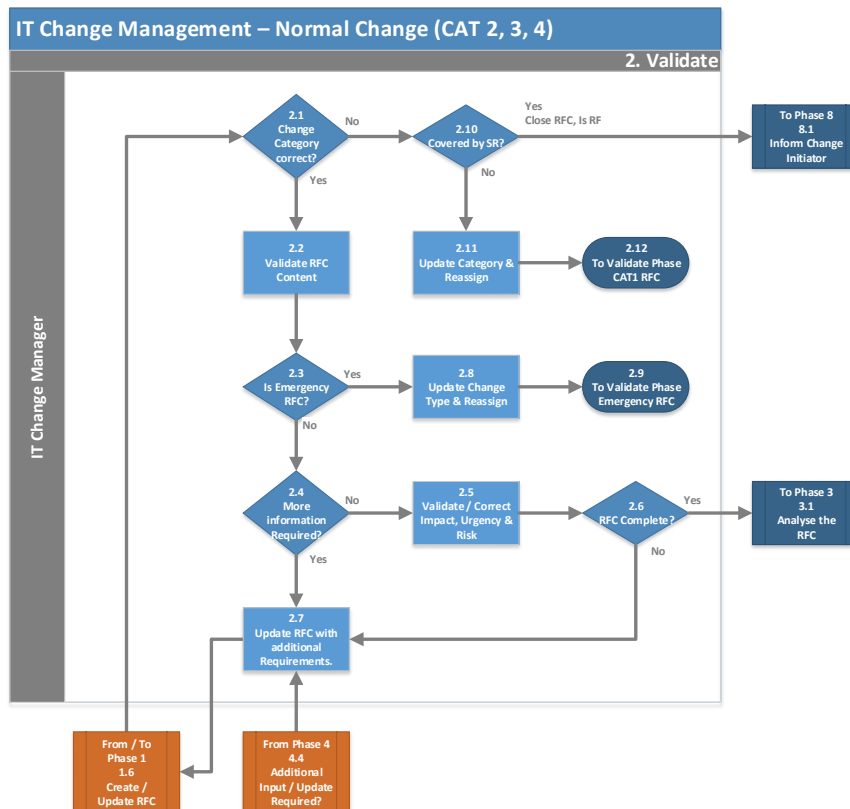


Figure 19: Generic Process Workflow - Normal Change (CAT2-4) - Phase 2

Phase 3: Review

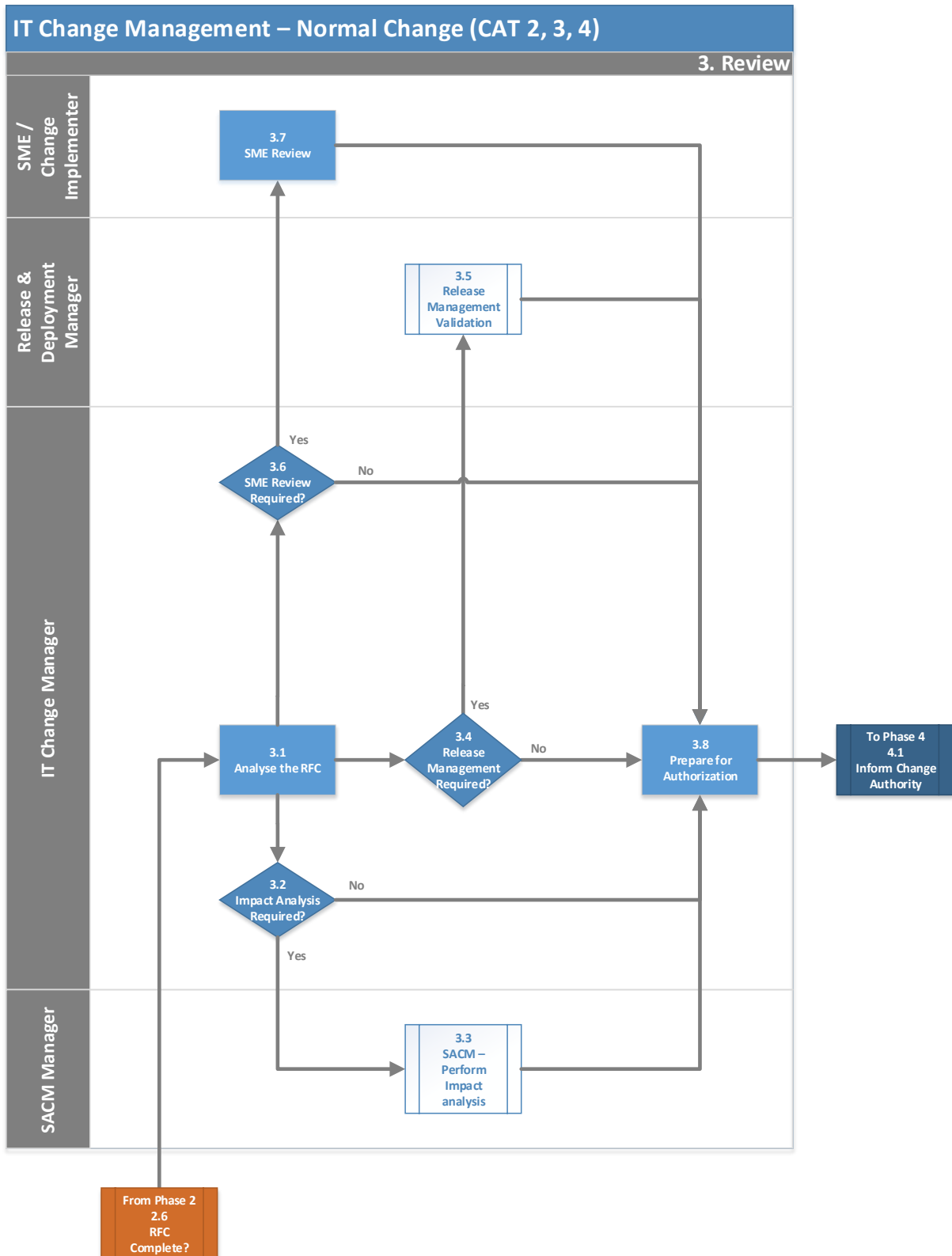


Figure 20: Generic Process Workflow - Normal Change (CAT2-4) - Phase 3

Phase 4: Authorise

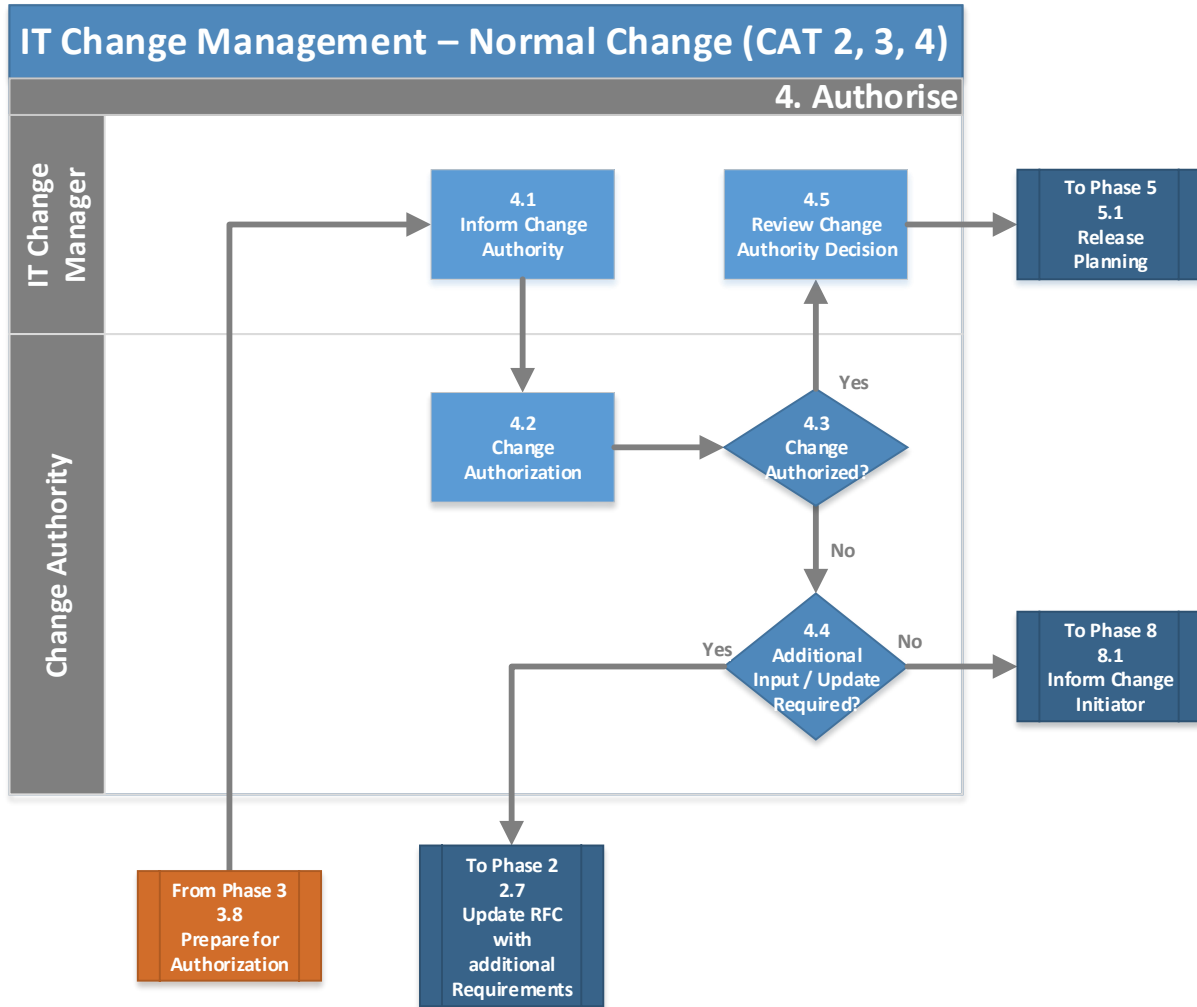


Figure 21: Generic Process Workflow - Normal Change (CAT2-4) - Phase 4

Phase 5: Plan / Build / Test

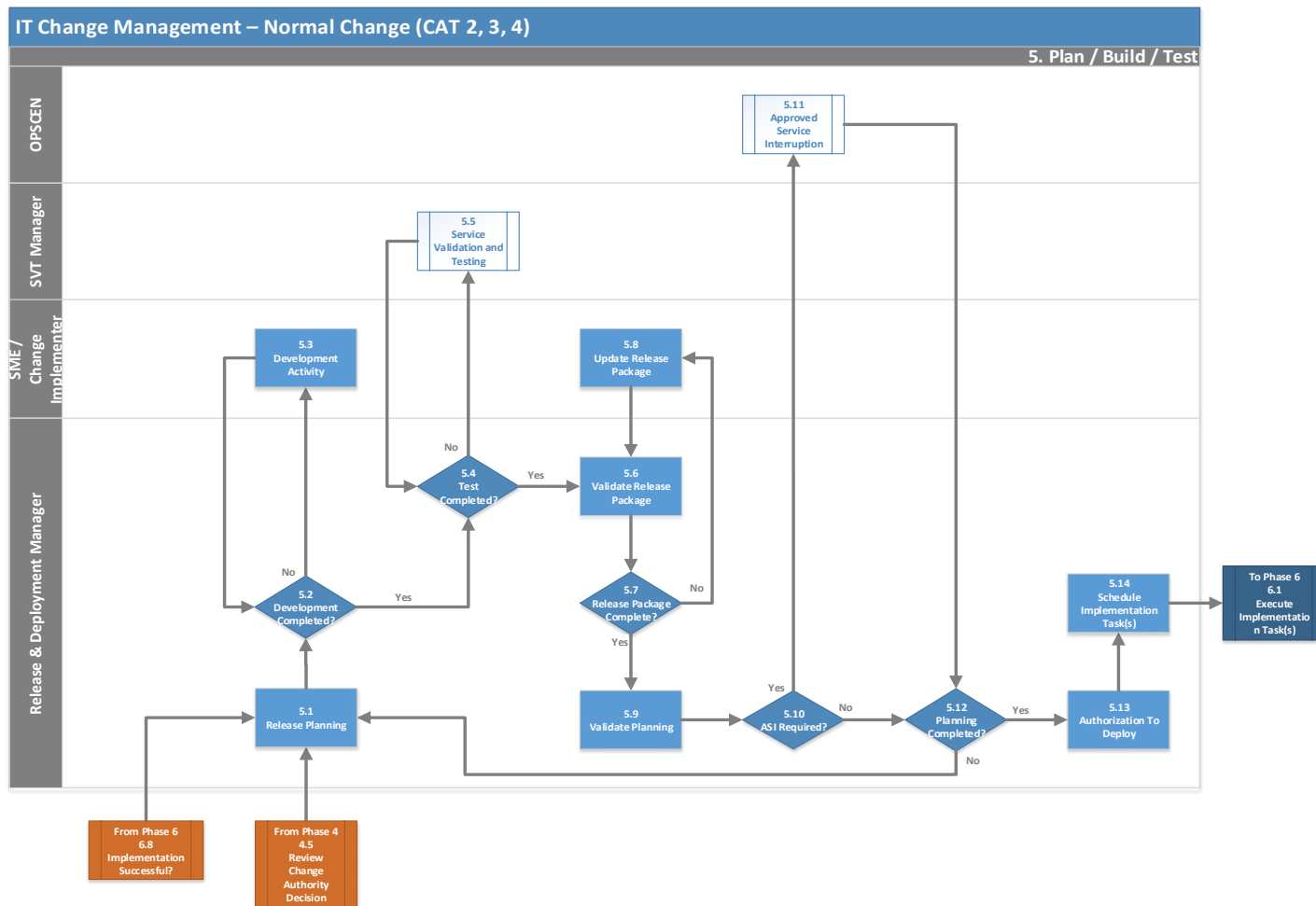


Figure 22: Generic Process Workflow - Normal Change (CAT2-4) - Phase 5



Phase 6: Implement

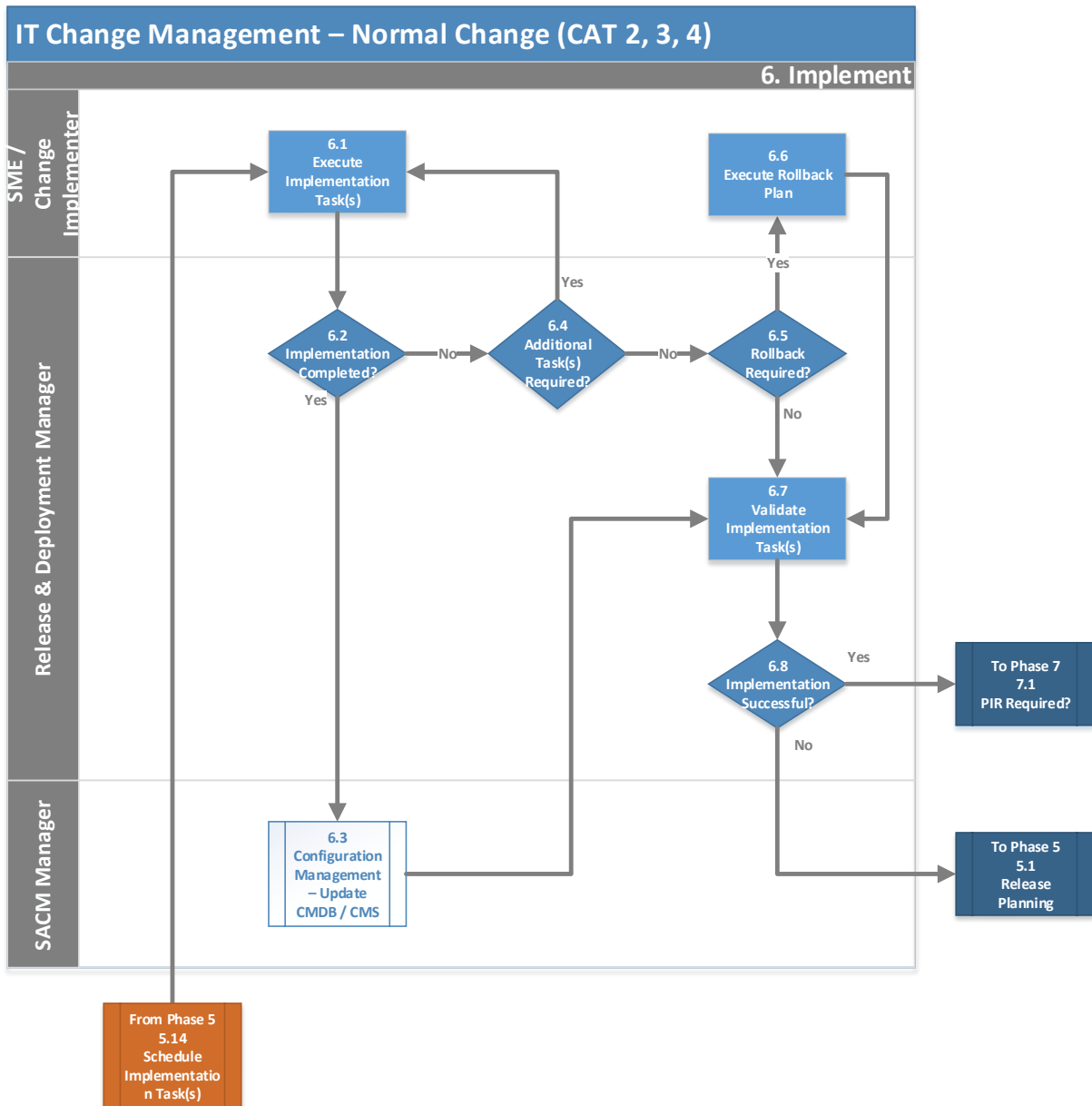


Figure 23: Generic Process Workflow - Normal Change (CAT2-4) - Phase 6

Phase 7: Post Implementation

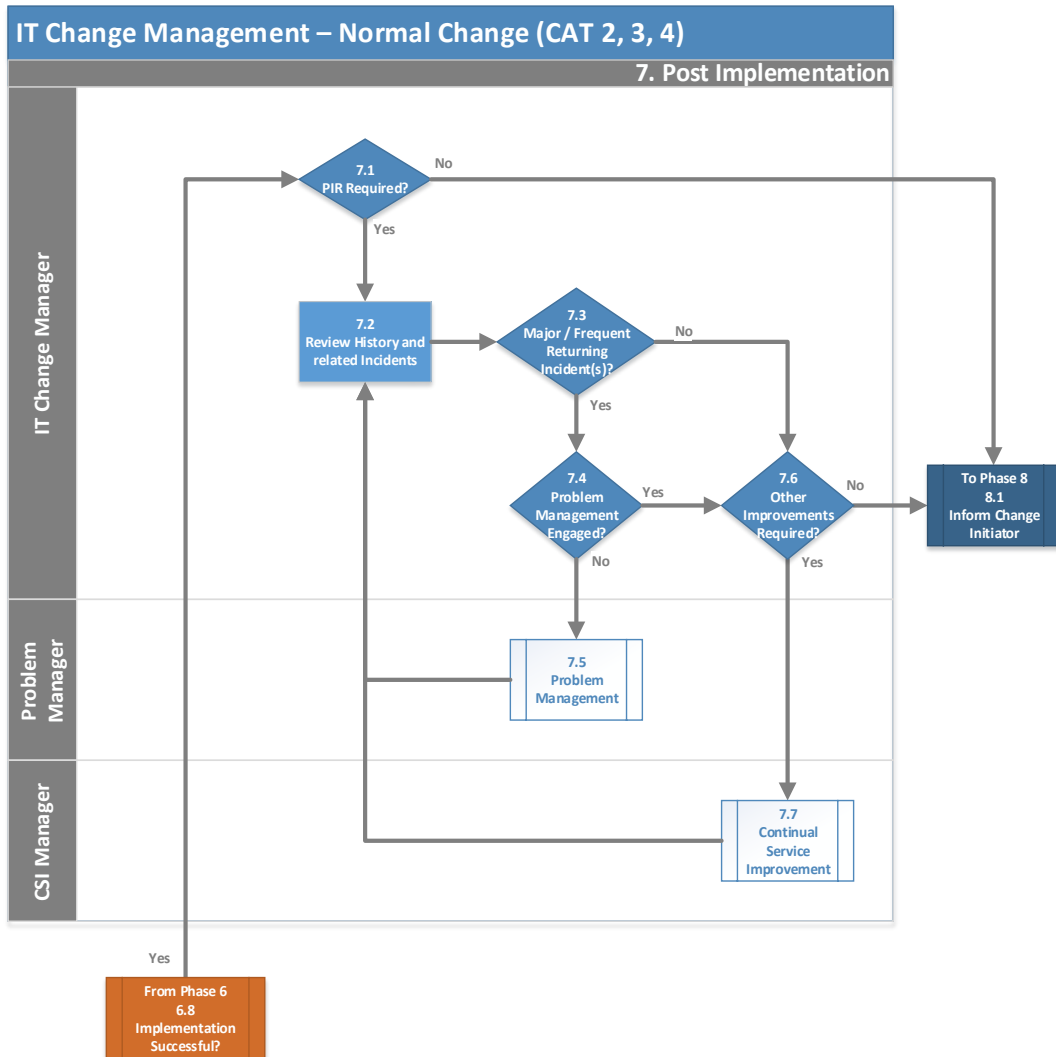


Figure 24: Generic Process Workflow - Normal Change (CAT2-4) - Phase 7

Phase 8: Close

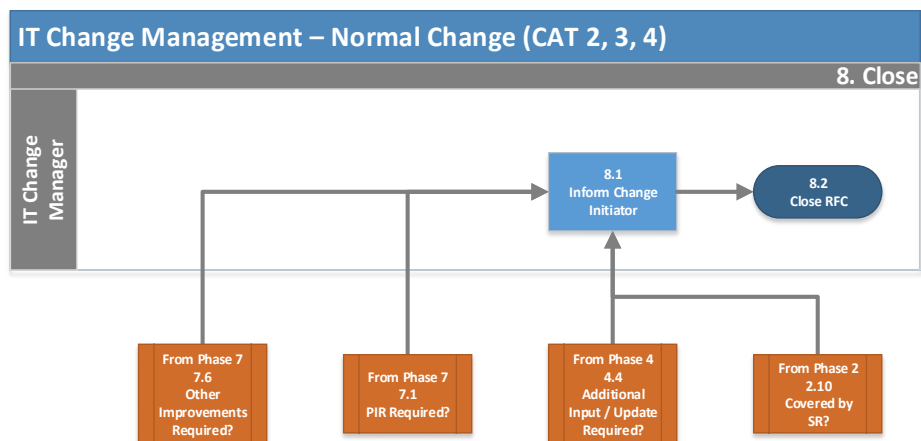


Figure 25: Generic Process Workflow - Normal Change (CAT2-4) - Phase 8

**Annex H DETAILED EMERGENCY CHANGE - GENERIC**

Below you will find the complete process flow described in 15.2.3 Emergency Change - Generic but split over each phase for ease of use and readability.

Phase 1: Submit

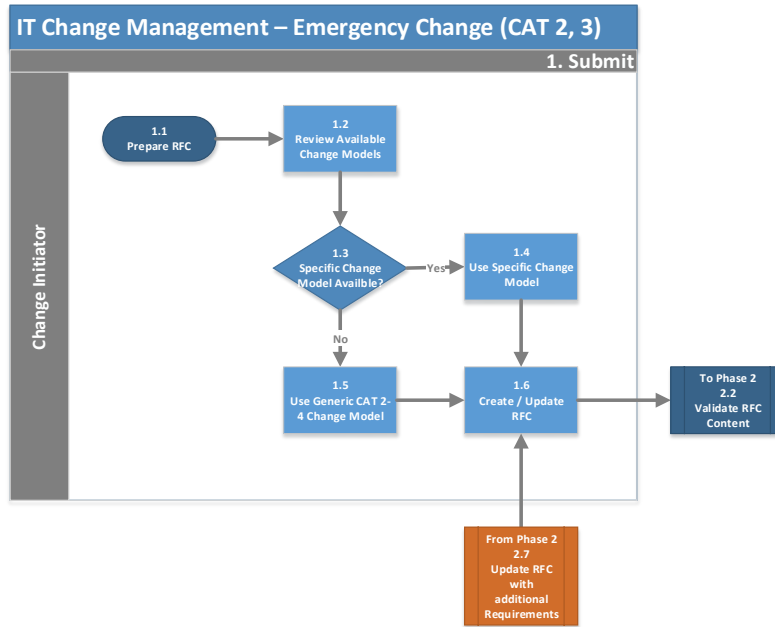


Figure 26: Generic Process Workflow - Emergency Change (CAT2-3) - Phase 1

Phase 2: Validate

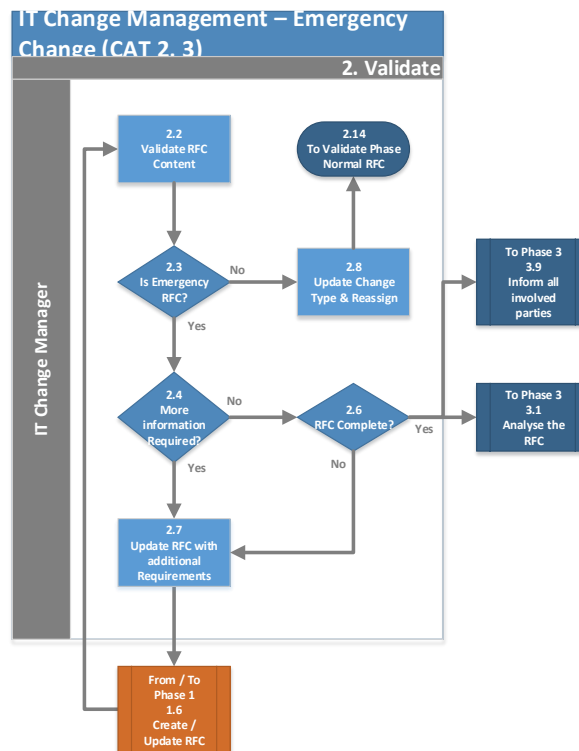


Figure 27: Generic Process Workflow - Emergency Change (CAT2-3) - Phase 2

Phase 3: Review

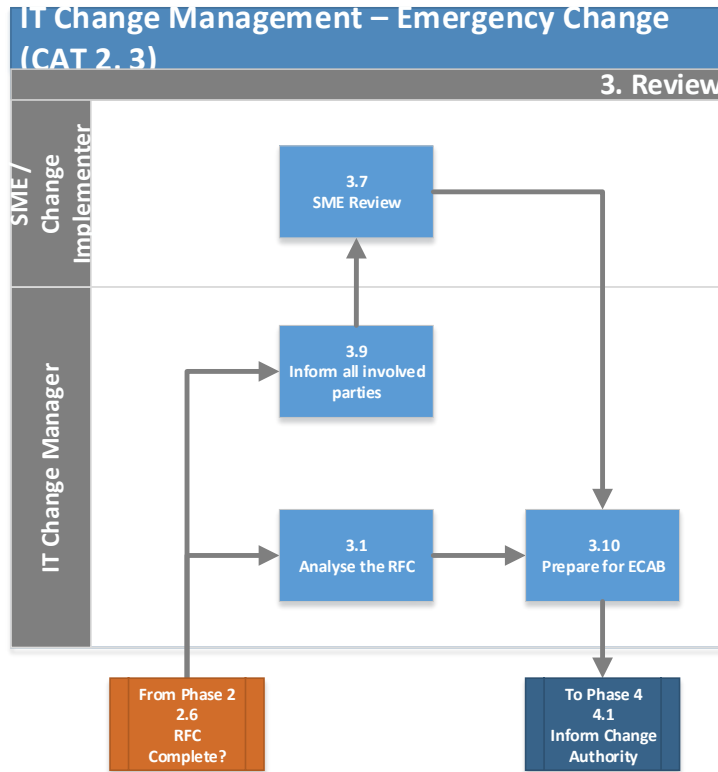


Figure 28: Generic Process Workflow - Emergency Change (CAT2-3) - Phase 3

Phase 4: Authorise

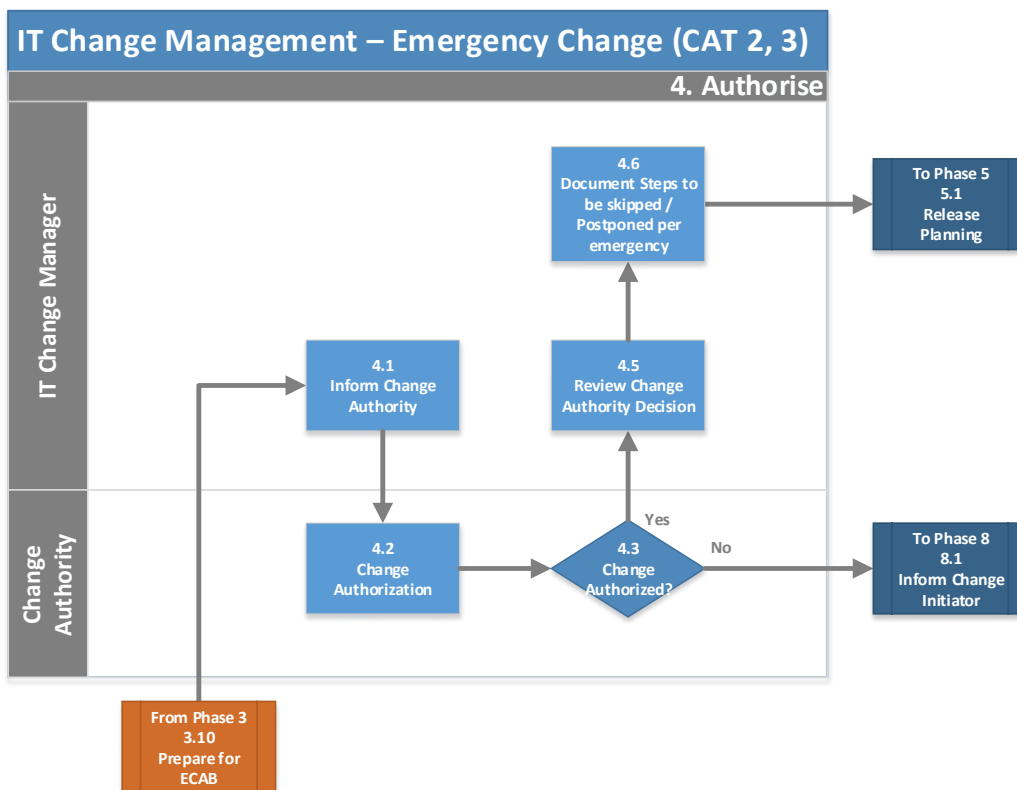


Figure 29: Generic Process Workflow - Emergency Change (CAT2-3) - Phase 4

Phase 5: Plan / Build / Test

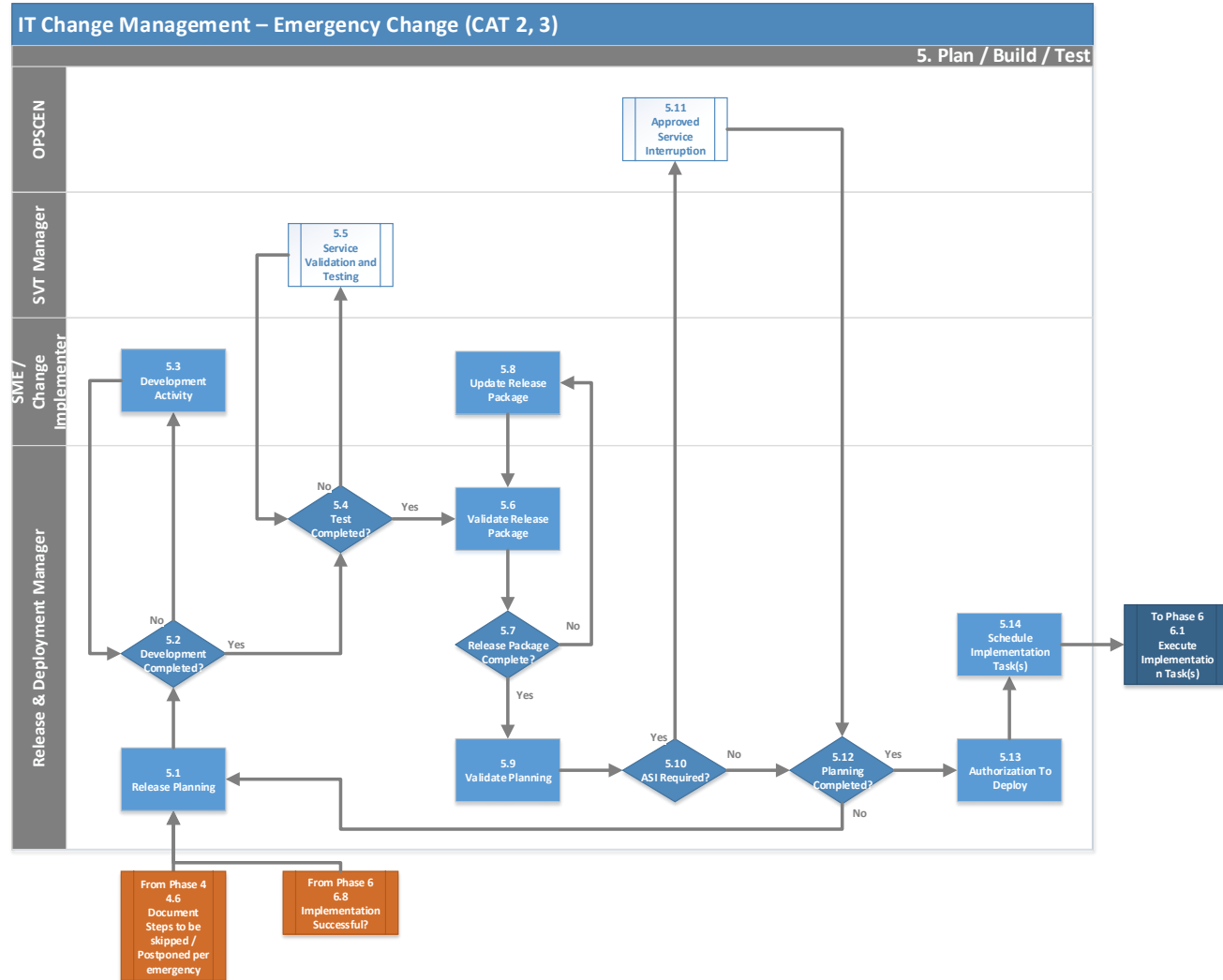


Figure 30: Generic Process Workflow - Emergency Change (CAT2-3) - Phase 5

Phase 6: Implement

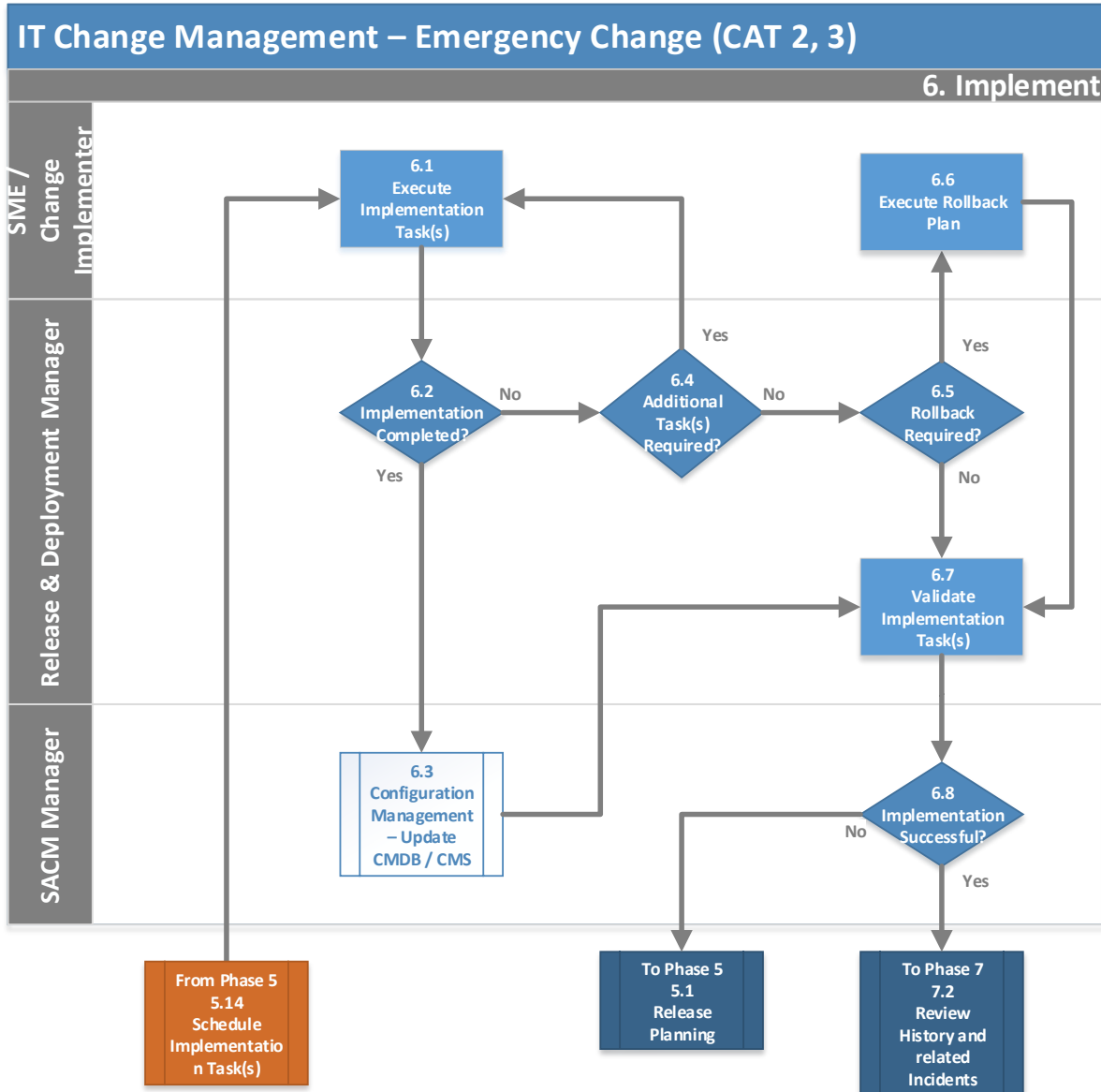


Figure 31: Generic Process Workflow - Emergency Change (CAT2-3) - Phase 6

Phase 7: Post Implementation

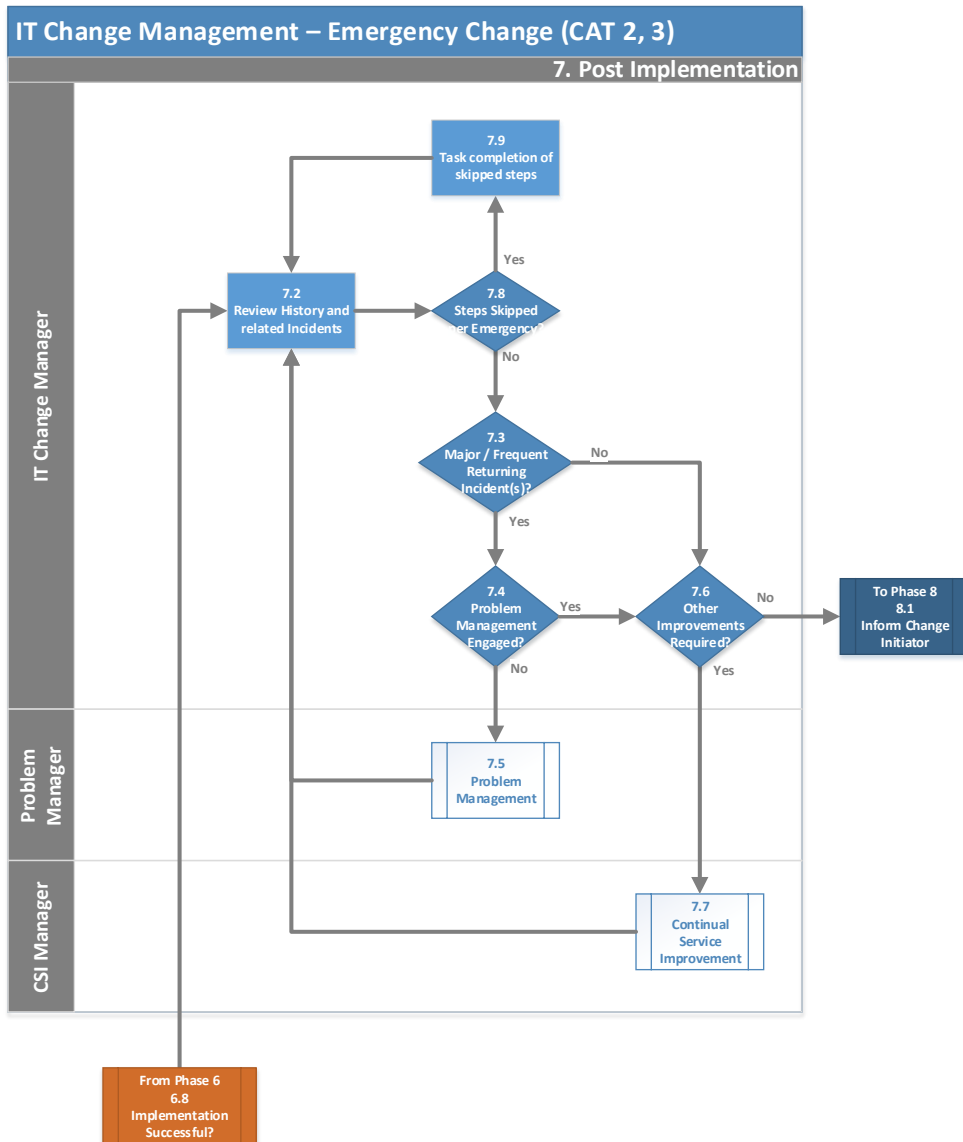


Figure 32: Generic Process Workflow - Emergency Change (CAT2-3) - Phase 7

Phase 8: Close

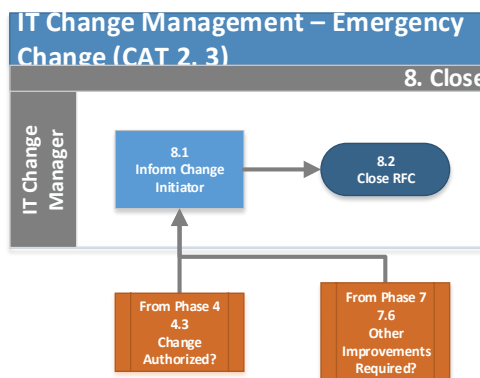


Figure 33: Generic Process Workflow - Emergency Change (CAT2-3) - Phase 8

**Annex I DETAILED WORKFLOW STEP DESCRIPTION**

Below table describes the activities performed during each step of the previously described process flows.

Step	Activity	Detailed
1.1	Prepare RFC	<p><b>Previous Step:</b> None</p> <p><b>Main Actor:</b> Change Initiator</p> <p><b>Description of step:</b> Change Initiator is preparing the submission of the RFC. A proper understanding of what to request (Requirements), where it is required (New / modification of existing CIS), why it's required (Justification) and optionally by when (Timeframe) the change is required. Being able to answer these questions is key correctly raising the RFC.</p> <p><b>Output:</b> Understand of the RFC that will be raised.</p>
1.2	Review available Change Models	<p><b>Previous Step:</b> 1.1</p> <p><b>Main Actor:</b> Change Initiator</p> <p><b>Description of step:</b> The Change Initiator will review the available change models / templates available for selection, which is closest related to the Change Request that will be made.</p> <p><b>Output:</b> Understanding of the available change models.</p>
1.3	Specific Change Model available?	<p><b>Previous Step:</b> 1.2</p> <p><b>Main Actor:</b> Change Initiator</p> <p><b>Description of step:</b> Did the Change Initiator identify a specific change model or not?</p> <p><b>Output:</b> Yes or No Decision.</p>
1.4	Use specific Change Model	<p><b>Previous Step:</b> 1.3</p> <p><b>Main Actor:</b> Change Initiator</p> <p><b>Description of step:</b> The Change Initiator has found a change model Matching his requirements. This change model Shall now be used in the next step when submitting the RFC.</p> <p><b>Output:</b> Change model identified.</p>
1.5	Use generic CAT 2-4 Change Model	<p><b>Previous Step:</b> 1.3</p> <p><b>Main Actor:</b> Change Initiator</p> <p><b>Description of step:</b> When no change model / Template is available that can facilitate the RFC that will be submitted the generic change model for CAT 2-4 shall be selected.</p> <p>As this is not a specific change model it is important for the Change Initiator to provide as much information as possible in the description of the request as no specific questions will be posed in the generic change model.</p> <p><b>Output:</b> Generic change model identified.</p>



Step	Activity	Detailed
1.6	<b>Create / Update RFC</b>	<p><b>Previous Step:</b> 1.4, 1.5, 1.7, 2.7</p> <p><b>Main Actor:</b> Change Initiator</p> <p><b>Description of step:</b> The Change Initiator completes the template of the chosen change model. It is required to complete every field, answer any question and attach the requested documents to the RFC that the change model requires in order for IT Change management to complete the review phase. Not providing all required information will result in a delay of processing the change request. At a minimum during this stage the Change Initiator shall always provide:</p> <ul style="list-style-type: none"> <li>• RFC Classification</li> <li>• A description of the request</li> <li>• the impact &amp; urgency of the RFC</li> <li>• Is emergency or not?</li> <li>• Justification</li> <li>• Funding (SLA, Project, PoW, ...)</li> <li>• CIs affected (Workstation, Servers, Application names, identifiers, ...)</li> </ul> <p><b>Output:</b> Complete RFC created and submitted to IT Change Management.</p>
1.7	<b>Use generic CAT 1 Change Model</b>	<p><b>Previous Step:</b> 1.3</p> <p><b>Main Actor:</b> Change Initiator</p> <p><b>Description of step:</b> When no change model / Template is available that can facilitate the RFC that will be submitted the generic change model for CAT 1 shall be selected.</p> <p>As this is not a specific change model it is important for the Change Initiator to provide as much information as possible in the description of the request as no specific questions will be posed in the generic change model.</p> <p><b>Output:</b> Generic change model identified.</p>
2.1	<b>Change category correct?</b>	<p><b>Previous Step:</b> 1.6</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> Review if the chosen change category is the right one for the request raised.</p> <p><b>Output:</b> Yes or No Decision.</p>
2.2	<b>Validate RFC content</b>	<p><b>Previous Step:</b> 1.6, 2.1</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> Review if all provided information and selections are made when the Change Initiator created the RFC.</p>

Step	Activity	Detailed
		<b>Output:</b> Initial review of the RFC content completed
2.3	Is emergency RFC?	<p><b>Previous Step:</b> 2.2</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> Review if the RFC is a candidate for emergency based on IT Change Manager knowledge / experience and the justification provided.</p> <p><b>Output:</b> Yes or No Decision.</p>
2.4	More information Required?	<p><b>Previous Step:</b> 2.2, 2.3</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> Is any of the required input missing?</p> <p><b>Output:</b> Yes or No Decision.</p>
2.5	Validate / Correct Impact, Urgency & Risk	<p><b>Previous Step:</b> 2.4</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> Review of the Impact, Urgency and calculate Priority and update the Risk value if required.</p> <p><b>Output:</b> Correct Prioritization and Risk value logged.</p>
2.6	RFC complete?	<p><b>Previous Step:</b> 2.4, 2.5</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> Is all required information provided and clear for further processing of the RFC?</p> <p><b>Output:</b> Yes or No Decision.</p>
2.7	Update RFC with additional requirements	<p><b>Previous Step:</b> 2.4, 2.6, 4.4</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> Reach out to the Change Initiator and request the additional information required for processing of the RFC.</p> <p><b>Output:</b> Change Initiator informed and requested to provide additional input on the RFC.</p>
2.8	Update Change Type & Reassign	<p><b>Previous Step:</b> 2.3</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> It is important before executing any other steps in the workflow that the Change Type is correctly set as this has an influence on how the RFC will be processed.</p> <p><b>Output:</b> Updated RFC with correct Change Type.</p>
2.9	To validate phase emergency RFC	<p><b>Previous Step:</b> 2.8</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> RFC will be reassigned to the correct IT Change Management group for further processing.</p>

Step	Activity	Detailed
		<b>Output:</b> RFC Continues in another workflow.
2.10	Covered by SR?	<p><b>Previous Step:</b> 2.1</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> Whether a Service Request Template already exists for the requested capability. IT Change Management will not process RFC, which are actioned through Service Request Fulfilment.</p> <p><b>Output:</b> Yes or No Decision.</p>
2.11	Update Category & reassign	<p><b>Previous Step:</b> 2.10</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> It is important before executing any other steps in the workflow that the Change Category is correctly set as this has an influence on how the RFC will be processed.</p> <p><b>Output:</b> Updated RFC with correct Change Category.</p>
2.12	To validate phase CAT 1 RFC	<p><b>Previous Step:</b> 2.11</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> RFC will be reassigned to the correct IT Change Management group for further processing of the RFC.</p> <p><b>Output:</b> RFC Continues in another workflow.</p>
2.13	To validate phase CAT 2-4 RFC	<p><b>Previous Step:</b> 2.11</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> RFC will be reassigned to the correct IT Change Management group for further processing of the RFC.</p> <p><b>Output:</b> RFC Continues in another workflow.</p>
2.14	To validate Phase normal RFC	<p><b>Previous Step:</b> 2.8</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> RFC will be reassigned to the correct IT Change Management group for further processing of the RFC.</p> <p><b>Output:</b> RFC Continues in another workflow.</p>
3.1	Analyse the RFC	<p><b>Previous Step:</b> 2.6</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> In depth review of the requested capability. Based on this analysis IT Change Management will be able to determine if they require input from additional stakeholders.</p> <p><b>Output:</b> IT Change Manager understand what is requested and knows who to engage for proper analysis</p>
3.2	Impact analysis required?	<p><b>Previous Step:</b> 3.1</p> <p><b>Main Actor:</b> IT Change Manager</p>

Step	Activity	Detailed
		<p><b>Description of step:</b> Based on the initial analysis performed, the IT Change Manager needs to determine if Configuration Management needs to be involved, mainly for impact assessment.</p> <p><b>Output:</b> Yes or No Decision.</p>
3.3	SACM – Perform impact analysis	<p><b>Previous Step:</b> 3.2</p> <p><b>Main Actor:</b> SACM Manager</p> <p><b>Description of step:</b> Analysis if the mentioned impacted Cis are correct and on request of IT Change Management perform evaluation on which related Cis or Services are impacted.</p> <p><b>Output:</b> Impact analysis and assessment report</p>
3.4	Release Management required?	<p><b>Previous Step:</b> 3.1</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> Based on the initial analysis performed, the IT Change Manager needs to determine if Release Management needs to be involved. This mainly applicable for larger change scope or when existing or new, commonly used, Release Package needs to be updated or created.</p> <p><b>Output:</b> Yes or No Decision.</p>
3.5	Release Management Validation	<p><b>Previous Step:</b> 3.4</p> <p><b>Main Actor:</b> Release &amp; Deployment Manager</p> <p><b>Description of step:</b> Review the RFC and evaluate the current state of the Release Package that will deliver the requested capability. When applicable the Release Manager will usually engage the Transition Planning and Support Manager / Project Manager in case of larger change requests.</p> <p><b>Output:</b> Release Management assessment report.</p>
3.6	SME review required?	<p><b>Previous Step:</b> 3.1</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> Based on the initial analysis performed, the IT Change Manager needs to determine if Subject Matter Experts need to be engaged for analysis of the request.</p> <p><b>Output:</b> Yes or No Decision.</p>
3.7	SME review	<p><b>Previous Step:</b> 3.6, 3.9</p> <p><b>Main Actor:</b> SME</p> <p><b>Description of step:</b> IT Change Management usually does not have in depth expertise in the requested change and will rely on SMEs to evaluate the feasibility and coverage of the requested capability properly. SME in this context also refers to the review of Licenses, infrastructure and evaluation of expected costs.</p> <p><b>Output:</b> Assessment of requested capability report.</p>

Step	Activity	Detailed
3.8	Prepare for authorization	<p><b>Previous Step:</b> 3.2, 3.3, 3.4, 3.5, 3.6, 3.7</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> The IT Change Manager bundles all received assessment and ensure all relevant outcome is available and ready to be shared with the Change Authority to support the authorization steps.</p> <p><b>Output:</b> Summary report for the Change Authority</p>
3.9	Inform all involved parties	<p><b>Previous Step:</b> 2.6</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> All identified stakeholders are made aware of the emergency RFC and requested to review and prepare their assessment of the request. Due to the fast pace of an emergency request, a report is usually not required but feedback will be collected and recorded in the meeting minutes of the Emergency CAB.</p> <p><b>Output:</b> High priority communication and review request to involved parties.</p>
3.10	Prepare for ECAB	<p><b>Previous Step:</b> 3.1, 3.7</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> IT Change Management shall prepare and understand the requested change. Close interaction with the Change Requestor will be required for proper briefing during the Emergency CAB</p> <p><b>Output:</b> IT Change Management understanding of the request and prepared to present.</p>
4.1	Inform Change Authority	<p><b>Previous Step:</b> 3.8, 3.10</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> IT Change Management usually does not have in depth expertise in the requested change and will rely on SMEs to properly evaluate the feasibility and coverage of the requested capability.</p> <p><b>Output:</b> ECAB Scheduled</p>
4.2	Change authorization	<p><b>Previous Step:</b> 4.1</p> <p><b>Main Actor:</b> Change Authority</p> <p><b>Description of step:</b> The Change Authority will review, discuss and evaluate the presented RFC and rule a commonly agreed way forward on the requested change.</p> <p><b>Output:</b> Meeting minutes including the authorization or rejection of the change.</p>

Step	Activity	Detailed
4.3	Change Authorized?	<p><b>Previous Step:</b> 4.2</p> <p><b>Main Actor:</b> Change Authority</p> <p><b>Description of step:</b> Whether the Change Authority authorized the change to take place or not.</p> <p><b>Output:</b> Yes or No Decision.</p>
4.4	Additional input / update required?	<p><b>Previous Step:</b> 4.3</p> <p><b>Main Actor:</b> Change Authority</p> <p><b>Description of step:</b> If the Change Request was not authorized does the Change Authority require additional information to make an educated decision?</p> <p><b>Output:</b> Yes or No Decision.</p>
4.5	Review Change Authority decision	<p><b>Previous Step:</b> 4.3</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> The IT Change Management reviewed the Change Authority's ruling and documents the outcome in the RFC. IT Change Management will take all remarks from the Change Authority into account and ensure this information is shared with other stakeholders in upcoming phases of the RFC.</p> <p><b>Output:</b> Update RFC with decision from the Change Authority.</p>
4.6	Document steps to be skipped / postponed per emergency	<p><b>Previous Step:</b> 4.5</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> For an Emergency RFC it is possible that the Change Authority decides that steps in upcoming phases of the IT Change Management process can be skipped. IT Change Management will document and track the skipped steps for review during Phase 7: Post Implementation.</p> <p><b>Output:</b> Deviated task log and activities recorded in the RFC.</p>
5.1	Release planning	<p><b>Previous Step:</b> 4.5, 4.6, 5.12, 6.8</p> <p><b>Main Actor:</b> Release &amp; Deployment Manager</p> <p><b>Description of step:</b> Release Management will review the RFC and identify required activities which results in a Release package that is ready for implementation.</p> <p><b>Output:</b> Required activities identified for implementation.</p>
5.2	Development completed?	<p><b>Previous Step:</b> 5.1, 5.3</p> <p><b>Main Actor:</b> Release &amp; Deployment Manager</p> <p><b>Description of step:</b> Is any development required or already completed?</p> <p><b>Output:</b> Yes or No Decision.</p>

Step	Activity	Detailed
5.3	Development activity	<p><b>Previous Step:</b> 5.2</p> <p><b>Main Actor:</b> SME</p> <p><b>Description of step:</b> Experts or developers will be engaged to create or prepare a solution / service which meets the requirements of the requestor.</p> <p><b>Output:</b> Developed solution that meets Change Initiator's requirements.</p>
5.4	Test completed?	<p><b>Previous Step:</b> 5.2, 5.5</p> <p><b>Main Actor:</b> Release &amp; Deployment Manager</p> <p><b>Description of step:</b> Is any test required or as testing already performed?</p> <p><b>Output:</b> Yes or No Decision.</p>
5.5	Service Validation and Testing	<p><b>Previous Step:</b> 5.4</p> <p><b>Main Actor:</b> Service Validation and Testing Manager</p> <p><b>Description of step:</b> Independent Validation and Verification of the solution will take place. Testing will ensure that the solution meets the Change Initiator's requirements, is compatible with the existing IT landscape and is secure for use.</p> <p><b>Output:</b> Test report including recommendations / remediations.</p>
5.6	Validate Release Package	<p><b>Previous Step:</b> 5.1, 5.4, 5.8</p> <p><b>Main Actor:</b> Release &amp; Deployment Manager</p> <p><b>Description of step:</b> Release Management will review and validate all the findings during the Plan / Build / Test phase and identify the areas that have to be addressed before the Release Package is ready for implementation.</p> <p><b>Output:</b> Release Package assessment report</p>
5.7	Release Package complete?	<p><b>Previous Step:</b> 5.6</p> <p><b>Main Actor:</b> Release &amp; Deployment Manager</p> <p><b>Description of step:</b> Is the Release Package complete and ready for implementation? The Release Package should include but not limited to:</p> <ul style="list-style-type: none"> <li>• The solution</li> <li>• Administrator documentation</li> <li>• Support plan</li> <li>• End-user documentation (when applicable)</li> <li>• Licenses (when applicable)</li> </ul> <p><b>Output:</b> Yes or No Decision.</p>

Step	Activity	Detailed
5.8	Update Release Package	<p><b>Previous Step:</b> 5.7</p> <p><b>Main Actor:</b> SME</p> <p><b>Description of step:</b> Updates the release package based on the Release Package assessment report provided by the Release Manager.</p> <p><b>Output:</b> Updated Release Package</p>
5.9	Validate planning	<p><b>Previous Step:</b> 5.7</p> <p><b>Main Actor:</b> Release &amp; Deployment Manager</p> <p><b>Description of step:</b> The Deployment Manager will review the suggested implementation plan, usually this is in coordination with the Change Implementer and SME's. The activities are planned towards a tentative release schedule.</p> <p><b>Output:</b> Agreed Deployment Plan</p>
5.10	ASI Required?	<p><b>Previous Step:</b> 5.9</p> <p><b>Main Actor:</b> Release &amp; Deployment Manager</p> <p><b>Description of step:</b> Is a service outage required to implement the requested capability in the RFC?</p> <p><b>Output:</b> Yes or No Decision.</p>
5.11	Approved Service Interruption	<p><b>Previous Step:</b> 5.10</p> <p><b>Main Actor:</b> OPSCEN</p> <p><b>Description of step:</b> Service Delivery Managers (SDM's) in coordination with the Deployment Manager will prepare and evaluate the Approved Service Interruption (ASI). The SDM will then facilitate required information to the OPSCEN to communicate impact to the affected customer/s (All user broadcast message). This process is greatly supported if an impact analysis was performed during the Analysis Phase.</p> <p><b>Output:</b> Approved ASI</p>
5.12	Planning completed?	<p><b>Previous Step:</b> 5.9, 5.10, 5.11</p> <p><b>Main Actor:</b> Release &amp; Deployment Manager</p> <p><b>Description of step:</b> Final review of the deployment plan based on outcome of the ASI processes and tentative release schedule. The complete plan should include but not limited to:</p> <ul style="list-style-type: none"> <li>• Deployment plan</li> <li>• Release schedule</li> <li>• Release Package</li> <li>• Roll-back plan</li> </ul> <p><b>Output:</b> Yes or No Decision.</p>



Step	Activity	Detailed
5.13	Authorization to deploy	<p><b>Previous Step:</b> 5.12</p> <p><b>Main Actor:</b> Release &amp; Deployment Manager</p> <p><b>Description of step:</b> When all activities are completed in this phase, Release &amp; Deployment authorize the implementation.</p> <p><b>Output:</b> Authorization to Deploy the Release Package</p>
5.14	Schedule implementation task(s)	<p><b>Previous Step:</b> 5.12, 5.13</p> <p><b>Main Actor:</b> Release &amp; Deployment Manager</p> <p><b>Description of step:</b> The Deployment Manager shall schedule the task(s) for implementation based on the authorized releases schedule and plan.</p> <p><b>Output:</b> Task(s) for implementation assigned</p>
6.1	Execute implementation task(s)	<p><b>Previous Step:</b> 5.14, 6.4</p> <p><b>Main Actor:</b> Change Implementer</p> <p><b>Description of step:</b> The Change Implementer will execute the assigned task in order to put the release package in the expected operational state according to the authorized deployment plan.</p> <p><b>Output:</b> Task Implementation Report</p>
6.2	Implementation completed?	<p><b>Previous Step:</b> 6.1</p> <p><b>Main Actor:</b> Release &amp; Deployment Manager</p> <p><b>Description of step:</b> Validate if the task(s) are completed.</p> <p><b>Output:</b> Yes or No Decision.</p>
6.3	Configuration Management – Update CMDB / CMS	<p><b>Previous Step:</b> 6.2</p> <p><b>Main Actor:</b> SACM Manager</p> <p><b>Description of step:</b> After the change to the IT landscape is in place, the Configuration Management Database shall be updated to reflect the current reality.</p> <p><b>Output:</b> CIs update in CMDB</p>
6.4	Additional task(s) required?	<p><b>Previous Step:</b> 6.2</p> <p><b>Main Actor:</b> Release &amp; Deployment Manager</p> <p><b>Description of step:</b> It is possible that new tasks originate from the implementation activities of previous tasks, activities overlooked or unplanned actioned required.</p> <p><b>Output:</b> Yes or No Decision.</p>
6.5	Rollback required?	<p><b>Previous Step:</b> 6.4</p> <p><b>Main Actor:</b> Release &amp; Deployment Manager</p> <p><b>Description of step:</b> If the implementation was unsuccessful, a rollback might be required.</p>

Step	Activity	Detailed
		<b>Output:</b> Yes or No Decision.
6.6	<b>Execute rollback plan</b>	<p><b>Previous Step:</b> 6.5</p> <p><b>Main Actor:</b> Change Implementer</p> <p><b>Description of step:</b> The rollback plan is executed as documented in the deployment plan. Any changes related to the implementation of this change are reversed to their original state.</p> <p><b>Output:</b> IT landscape restored as before implementation task(s) were initiated.</p>
6.7	<b>Validate implementation task(s)</b>	<p><b>Previous Step:</b> 6.3, 6.5, 6.6</p> <p><b>Main Actor:</b> Release &amp; Deployment Manager</p> <p><b>Description of step:</b> Review and evaluate the implementation according to how it is described in the deployment plan including the validation if the CMDB is updated according to the implemented change.</p> <p><b>Output:</b> Implementation phase completed.</p>
6.8	<b>Implementation Completed?</b>	<p><b>Previous Step:</b> 6.7</p> <p><b>Main Actor:</b> Release &amp; Deployment Manager</p> <p><b>Description of step:</b> Was the implementation of the change successful or are additional action required for completion?</p> <p><b>Output:</b> Yes or No Decision.</p>
7.1	<b>PIR required?</b>	<p><b>Previous Step:</b> 6.8</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> For emergency changes, a PIR is always required as emergency changes are usually implemented without all validation and analysis steps performed with level of detail. For normal changes, a PIR can be initiated by IT Change Management if too many unexpected incidents occurred, implementation did not fully go as expected or for audit purposes.</p> <p><b>Output:</b> Yes or No Decision.</p>
7.2	<b>Review history and related incidents</b>	<p><b>Previous Step:</b> 6.8, 7.1, 7.5, 7.9</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> Evaluate how the change was processed and the incidents that had this change as a root cause. Document the findings for briefing, sharing, learning and optimization with the aim to reduce impact on service(s) when executing planned changes.</p> <p><b>Output:</b> Post Implementation Review report.</p>
7.3	<b>Major / Frequent returning incident(s)?</b>	<p><b>Previous Step:</b> 7.2, 7.8</p> <p><b>Main Actor:</b> IT Change Manager</p>

Step	Activity	Detailed
		<p><b>Description of step:</b> Are there any incidents which were logged due to a major service interruption or if there were an unusual quantity of Incidents.</p> <p><b>Output:</b> Yes or No Decision.</p>
7.4	Problem Management engaged?	<p><b>Previous Step:</b> 7.3</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> Evaluate if Problem Management should be engaged.</p> <p><b>Output:</b> Yes or No Decision.</p>
7.5	Problem Management	<p><b>Previous Step:</b> 7.4</p> <p><b>Main Actor:</b> Problem Manager</p> <p><b>Description of step:</b> Perform an analysis on the Incident(s) related to the RFC as per Problem Management process.</p> <p><b>Output:</b> Problem Record logged and tracked.</p>
7.6	Other improvements required?	<p><b>Previous Step:</b> 6.8, 7.3, 7.4</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> Was anything else identified which was not already logged, addressed and resolution identified. Usually this question will lead to process optimization.</p> <p><b>Output:</b> Yes or No Decision.</p>
7.7	Continual Service improvement	<p><b>Previous Step:</b> 7.6</p> <p><b>Main Actor:</b> Continual Service Improvement Manager</p> <p><b>Description of step:</b> Continual Service Improvement process will look for a way to optimize the way the IT Change Management process is executed or which steps needs to be added, modified or removed.</p> <p><b>Output:</b> Positive improvements to way of working.</p>
7.8	Steps skipped per emergency?	<p><b>Previous Step:</b> 7.2</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> Where any steps bypassed or not fully execute due to the change being of emergency nature?</p> <p><b>Output:</b> Yes or No Decision.</p>
7.9	Task completion of skipped steps	<p><b>Previous Step:</b> 7.8</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> IT Change Management shall ensure that any step not executed will be completed to ensure that the change, even though already implemented, is properly documented and recorded in the RFC and CMDB.</p>



Step	Activity	Detailed
		<b>Output:</b> deferred steps completed.
8.1	<b>Inform Change Initiator</b>	<p><b>Previous Step:</b> 2.10, 4.3, 4.4, 7.1, 7.6</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> IT Change Management informs the Change Initiator about the completion of the change implementation. Change Initiator confirms change was implemented according to request</p> <p><b>Output:</b> Change Initiator confirms implementation of request.</p>
8.2	<b>Close RFC</b>	<p><b>Previous Step:</b> 8.1</p> <p><b>Main Actor:</b> IT Change Manager</p> <p><b>Description of step:</b> IT Change Management changes the status of the RFC to closed.</p> <p><b>Output:</b> RFC Closed</p>

Table 22: Process Workflow Step Description

**STANDARDIZATION  
AGREEMENT**

**ACCORD  
DE NORMALISATION**

# **STANAG 4107**

**MUTUAL ACCEPTANCE  
OF GOVERNMENT QUALITY  
ASSURANCE AND USAGE  
OF THE ALLIED QUALITY  
ASSURANCE PUBLICATIONS  
(AQAP)**

**ACCEPTATION DE SERVICES  
MUTUELS D'ASSURANCE  
OFFICIELLE DE LA QUALITÉ  
(AOQ) ET UTILISATION DES  
PUBLICATIONS INTERALLIÉES  
SUR L'ASSURANCE  
DE LA QUALITÉ (AQAP)**

**EDITION/ÉDITION 12**

**29 August/août 2022**



**NORTH ATLANTIC  
TREATY ORGANIZATION**

**ORGANISATION DU TRAITÉ  
DE L'ATLANTIQUE NORD**

**Published by  
the NATO STANDARDIZATION OFFICE  
(NSO)**

**Publié par  
le BUREAU OTAN DE NORMALISATION  
(NSO)**

**© NATO/OTAN**

**LETTER OF PROMULGATION****LETTRE DE PROMULGATION****STATEMENT**

The enclosed NATO standardization agreement (STANAG), which has been ratified by member nations, as reflected in the NATO Standardization Document Database (NSDD), is promulgated herewith.

**ENACTMENT**

This STANAG is effective upon receipt for use by the participating nations and NATO bodies.

**ACTIONS BY NATIONS**

Nations are invited to examine their ratification of the STANAG and, if they have not already done so, advise the NSO of their intention regarding its ratification and implementation.

Once implemented, Allies shall provide implementation details through the electronic reporting tool.

**SECURITY CLASSIFICATION**

This STANAG is a NATO non-classified document to be handled in accordance with C-M(2002)60.

**RESTRICTION TO REPRODUCTION**

This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database (<https://nso.nato.int/nso/>) or through your national standardization authorities.

**DÉCLARATION**

L'accord de normalisation OTAN (STANAG) ci-joint, qui a été ratifié par les pays membres dans les conditions figurant dans la Base de données des documents de normalisation OTAN (NSDD), est promulgué par la présente.

**ENTRÉE EN VIGUEUR**

Ce STANAG entre en vigueur dès réception aux fins d'application par les pays et les organismes OTAN participants.

**MESURES À PRENDRE PAR LES PAYS**

Les pays sont invités à examiner l'état d'avancement de la ratification du STANAG et à informer, s'ils ne l'ont pas encore fait, le NSO de leur intention concernant sa ratification et sa mise en application.

Dès que le STANAG est mis en application, les Alliés doivent fournir les informations y afférentes via l'outil de notification électronique.

**CLASSIFICATION DE SÉCURITÉ**

Ce STANAG est un document OTAN non classifié qui doit être traité conformément au C-M(2002)60.

**RESTRICTION DE REPRODUCTION**

Ce document de normalisation OTAN est produit par l'OTAN. Il peut être reproduit moyennant mention de la paternité de l'OTAN. L'OTAN n'exige aucune participation financière, à aucun stade, pour ses documents de normalisation, lesquels ne sont pas destinés à la vente. Ceux-ci sont disponibles dans la base de données des documents de normalisation OTAN (<https://nso.nato.int/nso/>) ou auprès de l'organisme national de normalisation.

## **ADDITIONAL INFORMATION**

This Edition of STANAG 4107 reflects the ratification of AQAP-2210, Edition B, which has been reviewed and updated together with its supporting guidance publication (AQAP-2210-SRD.1)

All other covered AQAPs remain unchanged and into effect.

Nations are asked to note that the nature of the agreement for mutual Government Quality Assurance and the use of AQAPs has not changed.

## **INFORMATIONS SUPPLÉMENTAIRES**

Cette édition du STANAG 4107 tient compte de la révision et de la mise à jour de l'AQAP-2210, dont l'édition B a été ratifiée, et du guide d'utilisation correspondant (AQAP-2210-SRD.1).

Toutes les autres AQAP couvertes par ce STANAG demeurent inchangées et restent en application.

Les pays sont invités à noter que la nature de l'accord concernant les services mutuels d'assurance officielle de la qualité et l'utilisation des AQAP n'a pas changé.



**Dimitrios SIGOULAKIS**  
Major General, GRC (A)  
Director, NATO Standardization Office

**Dimitrios SIGOULAKIS**  
Général de division, GRC (A)  
Directeur du Bureau OTAN  
de normalisation

## STANAG 4107 Edition/Édition 12

### MUTUAL ACCEPTANCE OF GOVERNMENT QUALITY ASSURANCE AND USAGE OF THE ALLIED QUALITY ASSURANCE PUBLICATIONS (AQAP)

### ACCEPTATION DE SERVICES MUTUELS D'ASSURANCE OFFICIELLE DE LA QUALITÉ (AOQ) ET UTILISATION DES PUBLICATIONS INTERALLIÉES SUR L'ASSURANCE DE LA QUALITÉ (AQAP)

#### AIM

The aim of this NATO standardization agreement (STANAG) is to respond to the following interoperability requirements.

#### INTEROPERABILITY REQUIREMENTS

To set forth the process, procedures, terms and conditions under which Mutual Government Quality Assurance of defence products is to be performed by the appropriate national authority of one NATO member nation, at the request of another NATO member nation or NATO organization; and to standardize the development, updating and application of AQAP on the basis of the concept of quality assurance in the procurement of defence products.

#### AGREEMENT

Participating nations agree to implement the following standards.

#### STANDARDS

- AQAP-2000, Edition 3
- AQAP-2070, Edition B
- AQAP-2105, Edition C
- AQAP-2110, Edition D
- AQAP-2131, Edition C
- AQAP-2210, Edition B
- AQAP-2310, Edition B
- AQAP-4107, Edition A

#### OTHER RELATED DOCUMENTS

None.

#### SUPERSEDED DOCUMENTS

This STANAG supersedes the following document:

STANAG 4107, Edition 11, dated 15 January 2019

#### BUT

Le présent accord de normalisation OTAN (STANAG) a pour but de répondre aux exigences d'interopérabilité suivantes.

#### EXIGENCES D'INTEROPÉRABILITÉ

Définir les processus, procédures, modalités et conditions régissant l'exercice mutuel de l'assurance officielle de la qualité des produits de défense par les autorités nationales compétentes d'un pays de l'OTAN, à la requête d'un autre pays de l'OTAN ou d'une organisation de l'OTAN; et normaliser l'élaboration, la mise à jour et la mise en application des AQAP, à partir du concept d'assurance de la qualité applicable à l'acquisition des produits de défense.

#### ACCORD

Les pays participants conviennent de mettre en application les normes suivantes.

#### NORMES

- AQAP-2000, Édition 3
- AQAP-2070, Édition B
- AQAP-2105, Édition C
- AQAP-2110, Édition D
- AQAP-2131, Édition C
- AQAP-2210, Édition B
- AQAP-2310, Édition B
- AQAP-4107, Édition A

#### AUTRES DOCUMENTS CONNEXES

Aucun.

#### DOCUMENTS ANNULÉS ET REMPLACÉS

Le présent STANAG annule et remplace le document suivant :

STANAG 4107, Édition 11, du 15 janvier 2019



## **NATIONAL RATIFICATION RESPONSE**

National responses are recorded in the NATO Standardization Document Database (NSDD).

Allies shall provide ratification details through the electronic reporting tool (e-Reporting).

## **IMPLEMENTATION OF THE AGREEMENT**

The implementation of STANAG 4107 requires nations to:

- have adequate infrastructure and processes to support their National Quality Assurance Authority's role,
- appoint a GQA focal point,
- establish competent GQA Representative resource with supporting processes and implement AQAP-2070,
- monitor and continually improve delivery of GQA Surveillance services,
- promote the use of contractual AQAPs for acquisition,
- proactively support NATO AC/327 Working Group 2.

NATO organizations shall:

- have the processes and resources to support the conduct of quality assurance activities across all stages of the lifecycle acquisition process.
- appoint a focal point for quality who shall ensure that this publication is applied to the organisation and engage as appropriate with nations for the provision of mutual GQA.
- promote the use of AQAPs for acquisition throughout the supply chain and proactively support NATO AC327 Working Group 2.

Partner Nations are invited to implement this STANAG noting that the provision of mutual GQA is reserved for NATO nations and agencies.

## **RÉPONSES NATIONALES AUX DEMANDES DE RATIFICATION**

Les réponses nationales sont consignées dans la Base de données des documents de normalisation OTAN (NSDD).

Les Alliés doivent rendre compte de leurs ratifications via l'outil de notification électronique (e-Reporting).

## **MISE EN APPLICATION DE L'ACCORD**

Les pays qui entendent mettre en application le STANAG 4107 doivent :

- disposer des infrastructures et des processus nécessaires, afin que l'autorité nationale pour l'assurance de la qualité puisse remplir ses fonctions ;
- désigner un point focal AOQ ;
- mettre en place un représentant pour l'AOQ aux compétences appropriées et les processus correspondants, et appliquer l'AQAP-2070 ;
- contrôler et améliorer continuellement la prestation de services de surveillance d'AOQ ;
- favoriser l'utilisation des AQAP de type contractuel pour les acquisitions ;
- soutenir de façon proactive le Groupe de travail 2 de l'AC/327 de l'OTAN.

Les organisations de l'OTAN doivent :

- disposer des processus et des ressources requises pour conduire les activités d'assurance de la qualité à toutes les étapes du processus d'acquisition ;
- désigner un point focal pour la qualité, qui veillera à ce que les dispositions de la présente publication soient appliquées au sein de l'organisation et qui, au besoin, se mettra en contact avec les pays pour la fourniture de services mutuels d'AOQ ;
- promouvoir l'utilisation des AQAP pour les acquisitions sur l'ensemble de la chaîne d'approvisionnement, et soutenir de façon proactive le Groupe de travail 2 de l'AC/327 de l'OTAN.

Les pays partenaires sont invités à appliquer le présent STANAG, étant entendu que la prestation de services mutuels d'AOQ est réservée aux pays membres et aux agences de l'OTAN.

This Edition of STANAG 4107 covers the release of AQAP 2210 Ed B. NATO requirements for software quality. Nations and NATO organisations are requested to use this contractual QA requirement when acquiring software.

Allies and NATO bodies shall provide implementation details through the electronic reporting tool (e-Reporting).

Partner nations are invited to provide their implementation details through the electronic reporting tool (e-Reporting).

#### **NATO EFFECTIVE DATE (NED)**

Not applicable.

#### **REVIEW**

This STANAG is to be reviewed in accordance with AAP-03. The result of the review is to be recorded within the NSDD.

#### **TASKING AUTHORITY**

This STANAG is supervised under the authority of:

CNAD LIFE CYCLE MANAGEMENT GROUP/  
GROUPE DE LA CDNA SUR LA GESTION DU CYCLE DE VIE  
(AC/327)

WORKING GROUP 2 ON QUALITY/  
GROUPE DE TRAVAIL 2 SUR LA QUALITÉ  
(WG/2)

#### **FEEDBACK**

Any comments concerning this STANAG shall be directed to:

**NATO Standardization Office  
(NSO)**

La présente édition du STANAG 4107 couvre l'Édition B de l'AQAP-2210, qui traite des exigences de l'OTAN pour la qualité des logiciels. Les pays et les organisations de l'OTAN sont invités à utiliser ces exigences contractuelles en matière d'assurance de la qualité lors de l'acquisition de logiciels.

Les Alliés et les organismes OTAN doivent rendre compte de leur mise en application via l'outil de notification électronique (e-Reporting).

Les pays partenaires sont invités à rendre compte de leur mise en application via l'outil de notification électronique (e-Reporting).

#### **DATE D'ENTRÉE EN VIGUEUR OTAN (NED)**

Sans objet.

#### **RÉEXAMEN**

Le présent STANAG doit être réexaminé conformément à l'AAP-03. Le résultat de ce réexamen doit être consigné dans la NSDD.

#### **AUTORITÉ DE TUTELLE**

Le présent STANAG est sous la responsabilité de :

#### **INFORMATIONS EN RETOUR**

Tous les commentaires concernant le présent STANAG doivent être adressés au :

**Bureau OTAN de normalisation  
(NSO)**

**Boulevard Léopold III  
1110 BRUXELLES – Belgique**

**STANDARDIZATION  
AGREEMENT**

**ACCORD DE  
NORMALISATION**

# **STANAG 4427**

**CONFIGURATION MANAGEMENT  
IN SYSTEM LIFE CYCLE  
MANAGEMENT**

**LA GESTION DE LA  
CONFIGURATION DANS LA  
GESTION DU CYCLE DE VIE  
DES SYSTÈMES**

**EDITION/ÉDITION 3  
18 December/décembre 2014  
NSO/1556(2014)LCMG/4427**



**NORTH ATLANTIC  
TREATY ORGANIZATION**

**ORGANISATION DU TRAITÉ  
DE L'ATLANTIQUE NORD**

**Published by  
THE NATO STANDARDIZATION OFFICE  
(NSO)**

**Publié par  
le BUREAU OTAN  
DE NORMALISATION (NSO)**

**© NATO/OTAN**

**LETTER OF PROMULGATION**

**LETTRE DE PROMULGATION**

**STATEMENT**

The enclosed NATO Standardization Agreement (STANAG), which has been ratified by member nations, as reflected in the NATO Standardization Document Database (NSDD), is promulgated herewith.

**IMPLEMENTATION**

This STANAG is effective upon receipt and ready to be used by the implementing nations and NATO bodies.

The partner nations are invited to adopt this STANAG.

**SUPERSEDED DOCUMENTS**

This STANAG supersedes the following documents:

STANAG 4427 Edition 2, February 2007  
STANAG 4159 Edition 2, September 1991

**ACTIONS BY NATIONS**

Nations are invited to examine their ratification of the STANAG and, if they have not already done so, advise the NSO of their intention regarding its implementation.

Nations are requested to provide to the NSO their actual STANAG implementation details.

**DÉCLARATION**

L'accord de normalisation OTAN (STANAG) ci-joint, qui a été ratifié par les pays membres dans les conditions figurant dans la Base de données des documents de normalisation OTAN (NSDD), est promulgué par la présente.

**MISE EN APPLICATION**

Ce STANAG entre en vigueur dès réception et est prêt à être mis en application par les pays et les organismes OTAN d'exécution.

Les pays partenaires sont invités à adopter ce STANAG.

**DOCUMENTS ANNULÉS ET REMPLACÉS**

Ce STANAG annule et remplace les documents suivants :

STANAG 4427 Edition 2, février 2007  
STANAG 4159 Edition 2, septembre 1991

**MESURES À PRENDRE PAR LES PAYS**

Les pays sont invités à examiner l'état d'avancement de la ratification du STANAG et à informer, s'ils ne l'ont pas encore fait, le NSO de leur intention concernant sa mise en application.

Les pays sont priés de fournir au NSO des informations détaillées sur la mise en application effective de ce STANAG.

**SECURITY CLASSIFICATION**

This STANAG is a NATO non classified document to be handled in accordance with C-M(2002)60.

**CLASSIFICATION DE SÉCURITÉ**

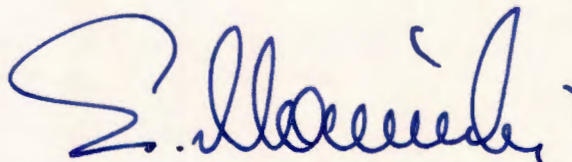
Ce STANAG est un document OTAN non classifié qui doit être traité conformément au C-M(2002)60.

**RESTRICTION TO REPRODUCTION**

No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member nations and Partnership for Peace countries, or NATO commands and bodies.

**RESTRICTION CONCERNANT LA REPRODUCTION**

Aucune partie de la présente publication ne peut être reproduite, incorporée dans une base documentaire, utilisée commercialement, adaptée ou transmise quelle qu'en soit la forme ou par les moyens électroniques ou mécaniques, de photocopie, d'enregistrement et autres sans l'autorisation préalable de l'éditeur. Sauf pour les ventes commerciales, cela ne s'applique pas aux États membres ou aux pays du Partenariat pour la paix, ni aux commandements et organismes de l'OTAN.



**Edvardas MAŽEIKIS**  
Major General, LTUAF  
Director, NATO Standardization Office

**Edvardas MAŽEIKIS**  
Général de division aérienne, LTUAF  
Directeur du Bureau OTAN de  
normalisation

**STANAG 4427 Edition/Édition 3**

**CONFIGURATION MANAGEMENT  
IN SYSTEM LIFE CYCLE  
MANAGEMENT**

**LA GESTION DE LA CONFIGURATION  
DANS LA GESTION DU CYCLE DE VIE  
DES SYSTÈMES**

**AIM**

The aim of this NATO standardization agreement (STANAG) is to respond to the following interoperability requirements.

**BUT**

Le présent accord de normalisation OTAN (STANAG) a pour but de répondre aux exigences d'interopérabilité suivantes.

**INTEROPERABILITY REQUIREMENTS**

To harmonize Configuration Management (CM) principles in national and multinational programmes to ensure armament systems and equipment meet the Alliances interoperability needs.

**EXIGENCES D'INTEROPÉRABILITÉ**

Harmoniser les principes de la gestion de la configuration appliqués dans les programmes nationaux et les programmes multinationaux pour que les équipements et les systèmes d'armement répondent aux exigences d'interopérabilité de l'Alliance.

**AGREEMENT**

In accordance with the NATO Policy for System Life Cycle Management, C-M(2005)0108, ratifying nations agree to implement the following standards.

**ACCORD**

Conformément aux dispositions de la politique OTAN de gestion du cycle de vie des systèmes (C-M(2005)0108), les pays participants conviennent de mettre en application les normes suivantes.

**STANDARDS**

ACMP-2000 Edition A Policy on Configuration Management  
ACMP-2009 Edition A Guidance on Configuration Management  
ACMP-2100 Edition A Configuration Management Contractual Requirements

**NORMES**

ACMP-2000 Edition A Politique sur la gestion de la configuration  
ACMP-2009 Edition A Directive sur la gestion de la configuration  
ACMP-2100 Edition A Exigences contractuelles en matière de gestion de la configuration

**OTHER RELATED DOCUMENTS**

AEDP-1 Engineering Documentation in Multinational Joint Projects  
ADATP-02 NATO Information Technology Glossary  
ISO 10007 Quality management systems – Guidelines for configuration management

**AUTRES DOCUMENTS CONNEXES**

AEDP-1 Documentation technique des projets multinationaux menés en commun  
ADATP-02 Glossaire OTAN des technologies de l'information  
ISO 10007 Systèmes de management de la qualité – Lignes directrices pour la gestion de la configuration

STANAG 4661 Product Life Cycle Support (PLCS)

STANAG 4661 Soutien du cycle de vie du produit

### **NATIONAL DECISIONS**

The national decisions regarding the ratification and implementation of this STANAG are provided to the NSO.

### **DÉCISIONS NATIONALES**

Les décisions nationales concernant la ratification et la mise en application du présent STANAG sont communiquées au NSO.

The national responses are recorded in the NATO Standardization Document Database (NSDD).

Les réponses nationales sont consignées dans la Base de données des documents de normalisation OTAN (NSDD).

### **IMPLEMENTATION OF THE AGREEMENT**

This STANAG is considered implemented when a nation has issued the necessary orders and instructions putting the contents of this agreement into effect.

### **MISE EN APPLICATION DE L'ACCORD**

Le présent STANAG est considéré comme mis en application quand un pays a transmis les ordres et instructions nécessaires pour l'entrée en vigueur des stipulations de l'accord.

Nations are invited to report on their effective implementation of the STANAG using the form in Annex H to AAP-03(J).

Les pays sont invités à rendre compte de la mise en application effective du présent accord au moyen du formulaire figurant à l'Annexe H à l'AAP-03(J).

Partner nations are invited to report on the adoption of the STANAG using the form in Annex G to AAP-03(J).

Les pays partenaires sont invités à rendre compte de l'adoption du présent STANAG au moyen du formulaire figurant à l'Annexe G à l'AAP-03(J).

### **REVIEW**

This STANAG is to be reviewed at least once every three years. The result of the review is recorded within the NSDD.

### **RÉEXAMEN**

Le présent STANAG doit être réexaminé au moins une fois tous les trois ans. Le résultat de ce réexamen est consigné dans la NSDD.

Nations and NATO bodies may propose changes, at any time, through a standardization proposal to the tasking authority (TA), where the changes will be processed during the review of the STANAG.

Les pays et les organismes OTAN peuvent, à tout moment, proposer des modifications en soumettant une proposition de normalisation à l'autorité de tutelle (TA), qui traitera ces modifications lors du réexamen du STANAG.

**TASKING AUTHORITY**

**AUTORITÉ DE TUTELLE**

This STANAG is supervised under the authority of:

Le présent STANAG est sous la responsabilité de :

CNAD Life Cycle Management Group (AC/327) /

Groupe sur la gestion du cycle de vie relevant de la CDNA (AC/327)

Secretary AC/327 / Secrétaire de l'AC/327

**CUSTODIAN**

**PILOTE**

The custodian of this STANAG is:

Le pilote du présent STANAG est :

NORWAY / NORVEGE

Norwegian Defence Logistics Organisation / Organisation logistique de la défense norvégienne

**FEEDBACK**

**INFORMATIONS EN RETOUR**

Any comments concerning this STANAG shall be directed to:

Tous les commentaires concernant le présent STANAG doivent être adressés à :

**NATO Standardization Office**  
**(NSO)**

**Bureau OTAN de normalisation**  
**(NSO)**

**Boulevard Léopold III**  
**1110 BRUXELLES – Belgique**



**NATO UNCLASSIFIED**  
Releasable to North Macedonia

16 July 2019

**DOCUMENT**  
AC/322-D(2019)0034 (INV)  
**Silence Procedure ends:**  
**29 Aug 2019 14:00**

**CONSULTATION, COMMAND AND CONTROL BOARD (C3B)**

**C3 TAXONOMY BASELINE 3.1**

**Note by the Secretary**

1. ACT invited the C3 Board (Enclosure 1), to endorse the Baseline 3.1 of the C3 Taxonomy, including the C3 Technical Services Taxonomy.
2. The version 3.1, presented at Enclosure 2, addresses the Nations' concerns represented during the previous approval process. Therefore, in accordance to the C3B's mandate, the C3 Taxonomy Baseline 3.1 is now offered to the Nations for approval under silence.
3. If the Action Officer does not hear to the contrary **by 14:00hrs on Thursday, 29 August 2019**, it will be assumed that Nations have approved the C3 Taxonomy Baseline 3.1.
4. To keep track of the correspondence related to this subject, Nations are also kindly requested to courtesy-copy all related communications, via NS WAN, to the C3 Board Secretariat at: "Mailbox NHQC3S-C3B(Secretariat)", C3BSecretariat@hq.nato.int.

(Signed) S. NDAGIJIMANA-MUNEZERO

Enclosure 1: ACT/CAPDEV/REQ/TT-1578/Ser:NU:0245, 12 July 2019  
Enclosure 2: C3 Taxonomy Baseline 3.1

2 Enclosures

Action Officer: Lori MacRae (5071)  
Original: English

**NATO UNCLASSIFIED**

-1-



**NATO UNCLASSIFIED**  
Releasable to NORTH MACEDONIA



**NORTH ATLANTIC TREATY ORGANIZATION**  
**ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD**  
HEADQUARTERS SUPREME ALLIED COMMANDER TRANSFORMATION  
7857 BLANDY ROAD, SUITE 100  
NORFOLK, VIRGINIA, 23551-2490



ACT/CAPDEV/REQ/TT-1578/Ser:NU:0245

TO: See Distribution

SUBJECT: **C3 TAXONOMY BASELINE 3.1**

DATE: 12 July 2019

REFERENCE(S):

- A. AC/322-D(12016)0017, C3 Taxonomy Baseline 2.0, 14 March 2016
- B. IMSM-0032-2019, Release of Baseline 3.0 - Consultation, Command and Control (C3) Taxonomy, 15 February 2019
- C. 6300 TSC FEJX-0140/TT-0988/Ser:NU0061, Consultation, Command and Control (C3) Taxonomy Baseline 3.0, 27 March 2019

1. The Consultation, Command and Control (C3) Taxonomy is a product developed by ACT to synchronize all C3 capability activities in NATO by connecting the Strategic Concept and Political Guidance through the NATO Defence Planning Process (NDPP) to traditional Communications and Information Systems (CIS) architecture and design constructs. The C3 Taxonomy was first published in July 2012. The C3 Board endorsed Baseline 2.0 in March 2016 with Reference A. Subsequently, with Reference B the Military Committee (MC) tasked this headquarters in February to complete Baseline 3.0 of the C3 Taxonomy. This new version was submitted before the end of the first quarter of 2019 with Reference C.

2. Baseline 3.0 contains two taxonomies, the C3 Taxonomy and the C3 Technical Services Taxonomy. The latter provides a more granular representation of the Community of Interest Services, Core Services and Communications Services. The products for each of the taxonomies are a poster and a report, plus a change log to explain the differences between this and the previous baseline.

3. The Architecture Capability Team (ACaT) has reviewed the baseline 3.0. Although it considers the update a minor uplift of Baseline 2.0 that doesn't address all the issues that have been raised by the Nations over the years, it considered the need for an update essential. The ACaT has offered to work with ACT to ensure required changes will be part of Baseline 4.0.

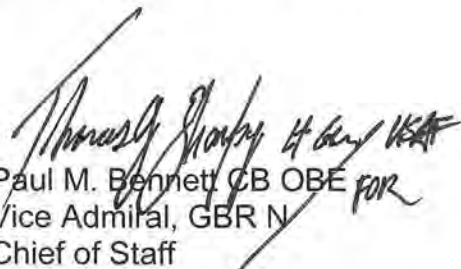
4. After ACaT review the baseline was sent to the Nations represented in the C3 Board for endorsement under silence procedure. Two nations interrupted the approval process with their concerns. In response, a new Baseline 3.1 version has been produced. This version addresses the concerns from Nations, inconsistencies in earlier submitted work and specifically, the request from the Architecture CaT to include a specified change log and a machine-readable data file for both the C3 Taxonomy and the C3 Technical Services Taxonomy.



**NATO UNCLASSIFIED**  
Releasable to NORTH MACEDONIA

5. This letter offers the C3 Board new versions of the poster and report for the C3 Taxonomy and C3 Technical Services Taxonomy (Enclosures 1 to 4) plus specified release notes with a register of change and deletion (Annexes A and B). Consequently, the enclosures to Reference C are withdrawn. Annex A to that letter is still relevant and accordingly, ACT aims to produce the next baseline before the end of the first quarter in 2020.
6. The machine-readable data file for the taxonomies is presented for download on ACT's Tidepedia website. The original data model and the contributing pages for the production of the new baseline are available online in ACT's Enterprise Mapping Wiki.
7. With this letter ACT invites the C3 Board to endorse Baseline 3.1 of the C3 Taxonomy, including the C3 Technical Services Taxonomy.
8. Should there be any questions, our point of contact is Mr. Peter Woudsma in the Federated Interoperability Branch, email [peter.woudsma@act.nato.int](mailto:peter.woudsma@act.nato.int) and telephone +1 757 747 4222.

FOR THE SUPREME ALLIED COMMANDER TRANSFORMATION:

  
Paul M. Bennett CB OBE *for*  
Vice Admiral, GBR N  
Chief of Staff

ANNEXES:

- A. Release Notes for the C3 Taxonomy, Baseline 3.1
- B. Release Notes for the C3 Technical Services Taxonomy, Baseline 3.1

ENCLOSURES:

1. Poster of the C3 Taxonomy
2. Report of the C3 Taxonomy
3. Poster of the C3 Technical Services Taxonomy
4. Report of the C3 Technical Services Taxonomy

**NATO UNCLASSIFIED**  
Releasable to NORTH MACEDONIA

DISTRIBUTION:

External –

Action:

Director General, International Military Staff  
Director, NATO Headquarters C3 Staff (NHQC3S)

Information:

NCIA  
NSPA  
SHAPE J6

Internal –

Information:

SACT  
DSACT  
DCOX CAPDEV  
DCOS R&M  
DCOS SPP  
DCOS JFD  
ACT/STRE  
ACT/SEE

## **RELEASE NOTES FOR THE C3 TAXONOMY, BASELINE 3.1**

### **INTRODUCTION**

1. The Baseline 2.0 version of the C3 Taxonomy was endorsed by the NATO C3 Board in March 2016. In February 2019 Allied Command Transformation was tasked by the Military Committee to produce a new version of the C3 Taxonomy to address the needs of the FMN community, and to harmonize with the NATO Interoperability Standards and Profiles (NISP) and FMN Spiral Specifications.
2. This document provides the release notes for the C3 Taxonomy Baseline 3.1, including a register of changes and deletions.

### **MAIN ISSUES**

3. The datasets that form the basis of the C3 Taxonomy are continuously changed and improved to find a better arrangement and definition of taxonomy elements and to accommodate changes that are being inspired by contemporary developments in technology, policies and implementations. This equally applies to the production of baseline 3.1.
4. Baseline 3.1 introduces the following main changes from baseline 2.0:
  - a. The groupings for CIS Security and for Service Management and Control (SMC) have been removed. These groupings were addressed in separate chapters in the report and visualized by dashed vertical selections on the taxonomy poster. They introduced a perception of stovepipes that was counter-intuitive to Service Oriented Architecture (SOA). Where appropriate, these groupings have been replaced by more specialized areas.
  - b. With the introduction of a new version of the Capability Hierarchy the role of a hierarchy framework separate from the capability codes and statements is no longer relevant. The new hierarchy is used in the current cycle of the NATO Defence Planning Process (NDPP). The taxonomy layer has been updated accordingly. The taxonomy report now includes the definitions of the capability areas that previously were only shown on the poster.
  - c. Ongoing development of the Community of Interest (COI) services required a need to reconsider the distribution of services between COI-Specific and COI-Enabling. Furthermore, the COI-Specific Services were categorized as "domain services" for the

**NATO UNCLASSIFIED**  
Releasable to NORTH MACEDONIA

operational domains (including cyberspace) and as "functional services" for the specialist areas of expertise (including Medical and CIS).

d. Recognizing several initiatives in C3 capability development and FMN spiral specifications, more emphasis was put on data. The taxonomy now includes elements for Data Science Services and Database Services, and in some instances the description of service elements have been consequently changed.

5. In the processing of baseline 3.0 by the NATO C3 Board, concerns were raised about the clarity and consistency in addressing the distinction between classified and non-classified information. The terminology in the taxonomy was deemed ambiguous or inappropriate, especially for the reference to security policies and security domains.

6. In response, it is acknowledged that NATO has distinct policies and directives for classified vs. non-classified information. However, it needs to be emphasized that the taxonomy is solution- and organization-agnostic. In other words: it is not an exclusive NATO taxonomy per se. As such, for instance, the reference to "security policies" in the text does not refer explicitly to the NATO Security Policy. The intent has always been to offer a taxonomy for a wider adoption past NATO, including nations and organizations. Nevertheless, in whatever form and function, the taxonomy should not disrupt its applicability for NATO in any context.

7. The following changes have been implemented in baseline 3.1 in order to establish compliancy with these concerns.

a. "CIS Security policies" are changed to "CIS Security measures".

b. "level of security for information" is changed to "levels of information security and management".

8. The result is a C3 Taxonomy that more accurately reflects the C3 landscape and provides a robust framework for architectural work in support of NATO Enterprise, Alliance, and Federation partners.

## **REGISTER OF CHANGES**

9. The following paragraphs list and clarify the changes that are made from baseline version 2.0 to 3.1. These changes are combined per layer and numbered in accordance with the corresponding chapters in the C3 Taxonomy Report.

10. The register does not include minor changes that do not alter the context and meaning of service definitions, such as grammatical and typographical errors.

## **C3 Taxonomy**

11. Nothing significant to report.

### **Operational Context**

12. Nothing significant to report.

### **Missions and Operations**

13. Nothing significant to report.

### **Policy and Guidance**

14. Nothing significant to report.

### **Mission Types and Tasks**

15. Paragraph 4.1.2 - In the paragraphs under "Mission Types and Tasks", updated the list to reflect the ongoing cycle of the NATO Defence Planning Process (NDPP).

### **Operational Capabilities**

16. Nothing significant to report.

### **Capability Hierarchy**

17. Paragraph 4.2.1 - Renamed "Capability Hierarchy, Codes and Statements" to "Capability Hierarchy" and changed description to follow the 2017 Bi-SC agreed Capability Hierarchy, which is the basis for the new NDPP cycle.

18. Paragraph 4.2.1.1 - Added "Capability Area R - Prepare".

19. Paragraph 4.2.1.2 - Added "Capability Area D - Project".

20. Paragraph 4.2.1.3 - Added "Capability Area E - Engage".

21. Paragraph 4.2.1.4 - Added "Capability Area L - Sustain".

22. Paragraph 4.2.1.5 - Added "Capability Area C - Consult, Command and Control".

23. Paragraph 4.2.1.6 - Added "Capability Area P - Protect".

24. Paragraph 4.2.1.7 - Added "Capability Area I - Inform".

### **Business Processes**

25. Paragraph 4.2.2 - For "Business Processes, note that the planning in the C3 Taxonomies Production Cycle aims to review this layer and produce a C3 Business Process Taxonomy together with Baseline 5.0 of the C3 Taxonomy.

26. Paragraph 4.2.2.1 - In "CIS Security Processes" changed "level of security for information" is changed to "levels of information security and management".

**Information Products**

27. Paragraph 4.2.3 - Changed the description of "Information Products" for clarification and a more specific definition of characteristics. Note that the planning in the C3 Taxonomies Production Cycle aims to review this layer and produce a C3 Information Product Taxonomy together with Baseline 4.0 of the C3 Taxonomy.

**CIS Capabilities**

28. Nothing significant to report.

**User-Facing Capabilities**

29. Nothing significant to report.

**User Applications**

30. Paragraph 5.1.1.2 - In "SMC Applications" changed "SMC policies" to "SMC measures".

**User Equipment**

31. Nothing significant to report.

**Back-End Capabilities**

32. Nothing significant to report.

**Technical Services**

33. Nothing significant to report.

**Community of Interest Services**

34. Nothing significant to report.

**COI-Specific Services**

35. Paragraph 5.2.1.1.1.1 - Renamed "Joint Services" to "Joint Domain Services". Changed the description for clarification of joint and combined forces.

36. Paragraph 5.2.1.1.1.2 - Renamed "Air Services" to "Air Domain Services".

37. Paragraph 5.2.1.1.1.3 - Renamed "Maritime Services" to "Maritime Domain Services".



**NATO UNCLASSIFIED**  
Releasable to NORTH MACEDONIA

- 38. Paragraph 5.2.1.1.1.4 - Renamed "Land Services" to "Land Domain Services".
- 39. Paragraph 5.2.1.1.1.5 - Added "Cyberspace Domain Services".
- 40. Paragraph 5.2.1.1.1.6 - Renamed "JISR Services" to "Intelligence and ISR Functional Services".
- 41. Paragraph 5.2.1.1.1.7 - Renamed "Electronic Warfare Services" to "Electronic Warfare Functional Services".
- 42. Paragraph 5.2.1.1.1.8 - Renamed "Environmental Services" to "Environmental Functional Services".
- 43. Paragraph 5.2.1.1.1.9 - Renamed "Logistics Services" to "Logistics Functional Services".
- 44. Paragraph 5.2.1.1.1.10 - Added "Medical Functional Services".
- 45. Paragraph 5.2.1.1.1.11 - Renamed "CIMIC Services" to "CIMIC Functional Services".
- 46. Paragraph 5.2.1.1.1.12 - Renamed "ETEE Services" to "ETEE Functional Services".
- 47. Paragraph 5.2.1.1.1.13 - Added "CIS Functional Services".

**COI-Enabling Services**

- 48. Paragraph 5.2.1.1.2.4 - Renamed "Battlespace Information Services" to "Operations Information Services".
- 49. Paragraph 5.2.1.1.2.5 - Merged "Modeling and Simulation Services" from "Modeling and Simulation Services" and "Modeling and Simulation Enabling Services". Changed the description for clarification.

**Core Services**

- 50. Nothing significant to report.

**Business Support Services**

- 51. Paragraph 5.2.1.2.1.1 - In "Business Support CIS Security Services" changed "CIS Security policies" to "CIS Security measures".
- 52. Paragraph 5.2.1.2.1.3 - Renamed "Unified Communication and Collaboration Services" to "Communication and Collaboration Services".
- 53. Paragraph 5.2.1.2.1.7 - Added "Data Science Services".

**Platform Services**

- 54. Paragraph 5.2.1.2.2 - Renamed "SOA Platform Services" to "Platform Services".
- 55. Paragraph 5.2.1.2.2.1 - Renamed "SOA Platform CIS Security Services" to "Platform CIS Security Services". Changed "CIS Security policies" to "CIS Security measures".
- 56. Paragraph 5.2.1.2.2.2 - Renamed "SOA Platform SMC Services" to "Platform SMC Services".
- 57. Paragraph 5.2.1.2.2.6 - Added "Database Services".

**Infrastructure Services**

- 58. Paragraph 5.2.1.2.3.1 - In "Infrastructure CIS Security Services" changed "CIS Security policies" to "CIS Security measures".
- 59. Paragraph 5.2.1.2.3.4 - Changed the description of "Infrastructure Storage Services" to focus on data rather than information.

**Information Systems Equipment**

- 60. Nothing significant to report.

**Communications Services**

- 61. Nothing significant to report.

**Communications Access Services**

- 62. Paragraph 5.2.1.3.1.1. - In "Communications Access CIS Security Services" changed "CIS Security policies" to "CIS Security measures".

**Transport Services**

- 63. Paragraph 5.2.1.3.2.1. - In "Transport CIS Security Services" changed "CIS Security policies" to "CIS Security measures".

**Transmission Services**

- 64. Paragraph 5.2.1.3.3.1. - In "Transmission CIS Security Services" changed "CIS Security policies" to "CIS Security measures".

**Communications Equipment**

- 65. Nothing significant to report.