IT MODERNISATION RECOVERY INCREMENT 1

Architecture Design Package (ADP)
NATO Operational Network

Effective date....... :	29-Jun-23
Version No........... :	2.2
Issued by .... :	ITM Project Office
Approved by .... :	Detlef Janezic, Chief Architecting & Engineering

Table of Amendments

Version	Date	Summary of Changes
0.1	2 June 22	Initial Version - Created New Chapter-Paragraph Layout
0.2	13 June 22	Reshuffled version after EntArch Coordination Aim to Simplify ADP to Serve as Index for SDPs
0.21	01 July 22	Creation of a new editing version and changes in document structure
0.9	12 July 22	Creation of review ready version covering updated: • CIS Drivers, CIS Principles and SDP Requirements Traceability • Nodal and service architecture • IDD • Availability and IT Continuity Services Model
0.91	13 Sep 22	Creation of version for review by TDA Design Board Members
1.0	11 Oct 22	Creation of baseline version feeding the ITM Recovery Increment 1 project and work packages
1.1	19 Dec 22	Working version towards version 2.0
2.0	19 Dec 22	Checkpoint 1 ITM Recovery Increment 1 high-level architecture design package.
2.1	25 Apr 23	Update DC location Corrected service terminology consistency with Figure 3-2 across ADP §3.5 Cyber Security Perspective: References and terminology; update §3.5 Data Diode as a service; update Figure 3-49 NATO ON Cyber Security Services; update §3.5.5.2 Data Loss Prevention Architecture.
2.2	29 June 23	Re-aligned the DevSecOps and IREEN environment to include the NSF

Stakeholders Details

Role	Name	Signature
Author	Marc van Selm Marc.Vanselm@ncia.nato.int Enterprise Architect, NCI Agency	Marc van Selm Digitally signed by Marc van Selm Date: 2023.06.29 12:32:19 +02'00'
Reviewer	Martin Diepstraten Martin.Diepstraten@ncia.nato.int POLARIS Technical Design Authority, NCI Agency	Martin Diepstraten Digitally signed by Martin Diepstraten Date: 2023.06.29 13:09:57 +02'00'
Approver	Detlef Janezic Detlef.Janezic@ncia.nato.int Agency Technical Design Authority	Detlef Janezic Digitally signed by Detlef Janezic Date: 2023.06.30 10:52:41 +02'00'

Table of Contents

List of Tables

List of Figures

Executive Summary

The current NATO Information Technology infrastructures, now operated by NATO Communications and Information (NCI) Agency, evolved over many years, in a piecemeal fashion. As a result, it does not adequately respond to the operational needs of the user communities it supports, does not enable acceptable continuity of operations and disaster recovery options, does not present an acceptable security posture, and presents a significant cost risk to NATO as maintenance costs continually increase.

NATO identified the requirement for a modernised IT infrastructure supporting the NATO Enterprise Approach and in accordance to the NATO Atlantic Council Endorsed requirements specified in the Statement or Requirements 2021 (SOR 2021). The NATO Core Services Programming Strategy addresses which requirements are to be achieved in each of three ITM Recovery project increments:

- Increment 1: Operational Network (up to an including NS classification level) for the NATO command Structure
- Increment 2: Protected Business Network (up to and including NR classification) level for the NATO Enterprise.
- Increment 3: Achieve Enterprise Level for the Operational Network and higher Data Centre (Cloud) Availability, Capacity and Resiliency levels.

This ADP will focus on ITM Recovery Increment 1: Achieve ITM Modernisation for the Operational Network (ON) supporting the NATO Command Structure, but will identify areas relevant for future proofing its evolution planned for ITM Recovery Increment 3.

This IT Modernisation (ITM) Recovery Increment 1 effort comprises of the delivery of the following top-level services:

1. Infrastructure as a Service (IaaS),
2. Client Provisioning Services (CPS),
3. Enterprise Core Services (ECS),
4. Enterprise Cyber Security Services (the C3 taxonomy refers as: CIS Security Services), and
5. Enterprise Service Management and Control (SMC)

These top-level services leverage private cloud technologies enabling service elasticity, resiliency, and agility.

These top-level, highly available, services are provided at all four levels of the logical architecture (Data Centre, enhanced node, standard node and remote node). This architecture specifies redundant network paths, redundant hardware, clustering, extensive instrumentation, automation and orchestration, and logical and physical separation to enforce security zones. This architecture, and subsequent design, will enable the NCI Agency to measure its service capabilities and cost efficiency capabilities.

This Architecture Design Package (ADP) is a project level architecture and reflects the overarching NATO Operational Network (ON) architecture. This ADP shall be considered as the umbrella document informing the more detailed engineering level Service Design Packages (SDPs) and Interface Definition Documents (IDDs). The NATO ON Architecture and Design, comprised by the ADP, 4 SDP’s and IDDs, when viewed together, describes an objective representation of the relevant

services, systems, organisational entities, and their interrelationships. The NATO ON architecture and design’s modular nature enables future architecture evolution, new service development, and site-level expansion.

The ADP addresses the following architecture elements:

- It identifies four key CIS drivers (cloud, cyber security, SMC and digital desktop) and it address how the NATO ON will support these drivers through architectural principles.
- It provides the following high level architecture views and concepts:
  - The service taxonomy
  - The node and network architecture
  - The Cyber Security Architecture
  - The SMC Architecture
- It provides the methodology to identify and document service interfaces.
- It provides the framework for service availability and Business Continuity including the methodology to calculate service availability targets, infrastructure service disaster recovery (DR) scenarios, and NATO ON applications’ end-to-end services availability and continuity of services targets.

1. Introduction

The Architecture Design Package (ADP) is the primary record of the NATO ON architecture, documented at project level, for the NATO's IT-Modernisation Recovery solution.

This architecture reflects the requirements as stated and assigned to the scope of ITM Recovery Increment 1 in the Project Proposal, the SOR 2021 and the Core Services Programming Strategy. It was developed following a disciplined approach, leveraging architecture development best practices and standards, to ensure that the delivered solution satisfies project requirements and constraints. The ADP includes a set of internally consistent views into the architecture that conform to the NATO Architecture Framework, version 4, the content of which is traceable to project requirements. These views are accompanied with descriptive narratives and definitions that enable common understanding.

The ADP will be updated as the architecture evolves over the life of the ITM Recovery projects (e.g. increment 1, 2, 3) and eventually additional projects. This ADP, being a project level architecture, is a component of the larger NATO ON architecture and will be after completion of the ITM projects be managed as such.

1.1. Purpose and Scope

This ADP is currently a project level technology architecture[1] in support of the ITM Recovery Increment 1 project. Although the ADP is primarily technical, it touches on business, information and application architecture where relevant. The ADP's focus is on the NATO Operational Network (ON), but only as far as relevant for ITM Increment 1. This ADP records (not define) capability level aspects to provide traceability. For ease of reference, we refer to this project level architecture as the "ITM ADP" in order to remind the reader of the project level scope of this ADP. The project scope of this ADP implies that the NATO ON architecture is broader than what is relevant for ITM Recovery Increment 1 and therefore broader than what this ADP documents.

Foremost, the purpose of this ADP is to be the one reference architecture definition document for all architects and engineers during the implementation of the entire ITM projects. The document will be continuously updated throughout the execution of the project.

This ADP describes the NATO ON communications and information systems (CIS) services, and where relevant underpinning business services, and their relationships to one another and to their environment, to be delivered by the ITM projects to satisfy stated requirements. It also defines linkages to the architecture principles that guide the architecture design process. This ADP describes a high-level description of the components, and when coupled with the more detailed, focused service design package (SDP), Interface Definition Documents (IDD) and Interface Definition Table (IDT) documents, through which a full, detailed view of the NATO ON architecture and Design is achieved. The ITM ADP, SDPs and IDDs together reduce project risk for the implementation/detailed design and future work by:

- Providing an objective design representation that satisfies stated requirements
- Forming the basis for defining and validating solution designs to be implemented
- Supporting modelling and analysis of the design's quality characteristics, with an emphasis on service availability and service recoverability
- Providing an integration framework where all interfaces are formally identified and described

[1] As defined by the NATO Enterprise Architecture Policy [12]

- Enabling design evaluation and implementation options by informing impact assessments on requirements and existing design
- Enabling assessment of the design’s support for operational needs and requirements
- Forming a firm basis for clear definitions of service interfaces and enabling the development of strong Service Level Agreements (SLAs)/OLAs for services internal and external to the scope and boundaries of the NATO ON services realized by ITM
- Facilitating communication and common understanding across all project stakeholders
- To provide the foundation for derived products such as:
    - CIS description: the Cyber Security Design need for the accreditation process
    - Statement of Work informing the technical implementation scope
    - Architecture Views that can be used as architecture building blocks for various architecture activities
    - Architecture Definition Documents (such as for IaaS) that provide more holistic architecture perspective of a certain ITM service area.

For managing requirements traceability from high-level capability/enterprise architecture requirements down to implementation level requirements there is a key linkage with requirements management through the Requirement Traceability Matrices (RTM) managed through the requirements management toolset operated adjacent and in synchronisation with the requirements artefacts managed in the architecture toolset (which is a subset of the entire requirements managed in ITM).

The architecture is intended to be modular and extensible in nature in order to enable new requirements and requirement changes to be captured in future iterations of the ADP.

The key ADP and related document dependencies as described above are visualised in Figure 1-1:

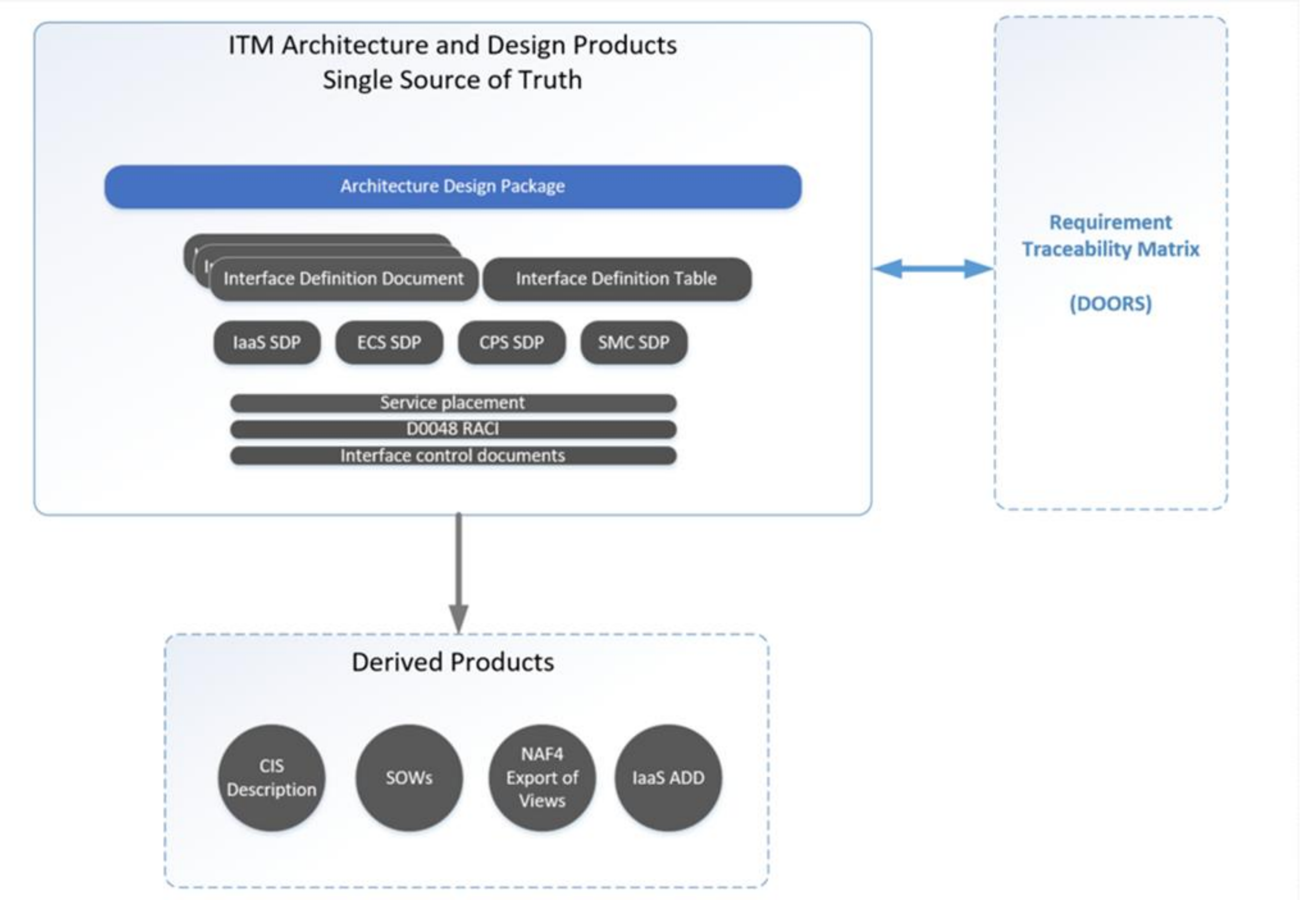

ITM Architecture and Design Products
Single Source of Truth
Architecture Design Package
Interface Definition Document
Interface Definition Table
IaaS SDP
ECS SDP
CPS SDP
SMC SDP
Service placement
D0048 RACI
Interface control documents
Requirement Traceability Matrix
(DOORS)
Derived Products
CIS Description
SOWs
NAF4 Export of Views
IaaS ADD

Figure 1-1 ADP document dependencies

1.1.1. Architecture Context

The architecture is a project level architecture and therefor primarily reflects the context of the ITM Recovery Increment 1 project. ITM will transform the way IT services are provided to users across the NATO enterprise, including the NATO Command Structure (NCS), the NATO Headquarters (NHQ), elements of the NATO Force Structure, and NATO agencies. This effort will modernise, consolidate, and centralise the infrastructure and service management, by abstracting CIS services from dedicated physical assets. This approach enables CIS services to be provided according to predefined standards and measurable service level agreements (SLA). This approach of abstracting to services, as compared to physical assets, will enable a higher-quality, more flexible, resilient, and secure set of CIS capabilities at transparent services cost to the user community.

Phase one of the architecture development effort, presented in the ADP, reflects the scope of the ITM Recovery Increment 1 efforts.

1.1.2. Architecture Views

The architecture was developed from the following architecture guidance sources:

1. NATO Architecture Framework (NAF), version 4
2. AC/322-D(2021)0017, C3Taxomomy Baseline 5.0, 30 August 2021, at https://tide.act.nato.int/tidepedia/index.php?title=C3_Taxonomy.
3. NATO Interoperability Standards and Profiles, Volumes 1-3, dated 6 June 2016

The architecture views and diagrams that are introduced in this document are compliant with the NATO Architecture Framework version 4. Any exceptions to this are noted in text accompanying the artefacts.

The architecture views in ArchiMate are managed and maintained in the NCI Agency ARIS toolset. Extracts of views can be made available upon request in the ArchiMate Open Exchange File format.

Table 1-1 summarizes the ADP architecture views, aggregated per NAFv4 viewpoint, by paragraph within this ADP. Note that architects have decided to model some views addressing multiple NAFv4 viewpoints where they assessed this approach better responds to the concerns addressed.

Table 1-1. NAF4 Artefact Description and Document Location

View	Description	Document Location
C7	CIS Drivers	Paragraph 2.1
A8	CIS Principles	Paragraph 2.2
S1	Service Taxonomy	Paragraph 3.2
S2	Service Structure	Paragraph 3.3.1
L1	Node types	Paragraph 3.3.1
L2	Service delivery	Paragraph 3.3.1
P1	Location types	Paragraph 3.3.1
P2	Service hosting	Paragraph 3.3.1
L3	Node Connectivity	Paragraph 3.3.2 + 3.3.3
C1	SMC Capability	Paragraph 3.4.3
S2	SMC Service Integration	Paragraph 3.4.5
S4	SMC Functions	Paragraph 3.4.1.1
S3	SMC Interfaces	Paragraph 3.4.6
C1	Cyber Security Capability	Paragraph 3.5.2
S2	Cyber Security Service Integration	Paragraph 3.5.5
S4	Cyber Security Functions	Paragraph 3.5.3
S8	Cyber Security Service Policy	Paragraph 3.5.3 + 3.5.4
S3	Interface Definition	Section 4
C7 / S8 / L8 / P8	Availability and IT Continuity	Section 5

1.2. Document Organisation

The Architecture Design Package complies with SOW requirement 17.3.11. The ADP organisation with a brief section description is depicted in Table 1-2.

Table 1-2. ADP Document Organisation

Section	Section Heading	Section Content
Executive Summary	Executive Summary	Background and high level summary of the ADP
Section 1	Introduction	Introduction to the ADP
Paragraph 1.1	Purpose and Scope	Reason for the document and scope of the content
Paragraph 1.2	Document Organisation	Structure of the ADP
Paragraph 1.3	Points of Contact	Personnel of Interest
Paragraph 1.4	Glossary of Abbreviations, Acronyms and Terminology	Glossary of Terms
Paragraph 1.5	Reference Documents	Documents needed to understand the complete ITM solution

Section	Section Heading	Section Content
Section 2	CIS Drivers, CIS Principles and SDP requirements traceability	Introduction to CIS Drivers and Principles
Section 2.1	CIS Drivers	CIS Driver Definitions and goals and objectives
Paragraph 2.2	CIS Principles	Identifies specific SOW requirements being addressed
Section 3	Architecture Perspectives	Introduction of the key architecture views driving the NATO ON design
Paragraph 3.2	Services Perspective	Provision of Generic Services & Subservices Structure
Paragraph 3.3	Infrastructure Perspective	Definitions of ITM type of nodes and functions supporting end-2-end network architecture
Paragraph 3.4	Service Management and Control Perspective	SMC architecture addressing the Enterprise-Domain-Element architecture functions and options, introduction of SMC related interfaces.
Paragraph 3.4	Cyber Security Perspective	Addressing the key Cyber Security functions, policy compliancy methodology and introduction of the Cyber Security Services integration aspects.
Section 4	Interface Definition Methodology	Introduction to the Architecture Interface Definition method
Paragraph 4.1	Interface Definition Model	Architecture model showing how interfaces are identified and specified
Paragraph 4.2	Interface Definition elements	Identification of Work Package 7 IER, services and technical interfaces. Linkage to the Interface Definition Document Table [50] for the details.
Section 5	Availability and IT Continuity of Services Model	Availability and IT Continuity of Services
Paragraph 5.1.1	Generic Availability and IT continuity of Service Model	Introduction to Availability and IT Continuity of Services
Paragraph 5.2	ITM Service Availability Model and Service Levels	Design, analysis, and models for availability and MTTR/MTBF SLT compliance
Paragraph 5.3	ITM Continuity of Service Model and Service Levels	Design, analysis, and models for availability and RTO/RPO SLT compliance
Paragraph 5.4	KPIs	IaaS/ECS/CPS SMC domain and element level KPI parameter definition guidance
Paragraph 5.5	NATO ON Availability Implementation Strategy	Design strategy for the availability and disaster recovery design

1.3. Points of Contact

The primary owners of this ADP are the NCIA Polaris Programme Technical Design Authority as the approval authority and the ITM Project Architect as the Custodian.

1.4. Glossary of Abbreviations, Acronyms and Terminology

Table 1-3 lists common abbreviations and acronyms found throughout this document.

Table 1-3. Glossary

Acronym or Term	Definition
ACPV	Asset, Configuration, Patch and Vulnerability Management
LAN	Local Area Network
ADP	Architecture Design Package
A_i	Intrinsic Availability
AFPL	Approved Fielded Product List

Acronym or Term	Definition
BPS	Boundary Protection Service
CI	Configuration Item. A configuration any service component, infrastructure element, or other item that needs to be managed in order to ensure the successful delivery of services.
COI	Community of Interest
Coloured Cloud	A Coloured Cloud (CC) is a military grade IP encrypted network overlay, including the associated CIS Nodes (clients and infrastructure), belonging to a particular information security domain. In this context a security domain is referred to as a “colour”, where the colour is used to denote a particular security classification. In simple terms, a CC can be understood as a type of a virtual private network (VPN) overlay including all server and client systems attached to the VPN.
Coloured Cloud Access	The Coloured Cloud Access (CCA) refers to the functionality and the associated infrastructure node that makes up the local instance of CC at a point of presence.
COTS	Commercial off the Shelf
CPS	Client Provisioning Services
CSOC	Cyber Security Operations Centre
CTD	Contractor Technical Director
DAG	Database Availability Group
Data Centre	Key centralised IaaS location where the bulk of computing and storage will take place
DC	Data Centre
DCI	Data Centre Interconnect
DLP	Data Loss Prevention
ECS	Enterprise Core Services
EN	Enhanced Node – Location with enhanced computing capabilities in order to support applications that are not deemed to have the ability to centralise for technical or other reasons, and to provide an enhanced level of graceful degradation should communications be interrupted.
Entity	Entity in this architecture is defined as any singular, identifiable and separate object, referring to individuals, organizations, systems, to bits of data or even to distinct system components that are considered relevant. An external entity refers to individuals, organizations or systems beyond the physical scope of this architecture.
ETEE	Education Training Exercise Evaluation
ESMC	Enterprise Service Management and Control
FMECA	Failure Mode Effects Criticality Analysis
HA	High Availability
H-to-H	Human to Human
IA	Information Assurance
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
IdAM	Identity Access Management
IDD	Interface Definition Document
IDT	Interface Definition Table
IREEN	IREEN is an ITM Reference Environment. In the context of ITM Rec Increment 1, it is an environment providing the reference of services in the scope of the project ITM Rec Increment 1. As part of ITM Rec Increment 1, two reference environments are leveraged, IREEN ON@NU and IREEN ON@NS.
IT	Information Technology
ITM	IT Modernisation
MPLS	Multiprotocol Label Switching
MTBF	Mean Time Between Failure
MTTR	Mean Time to Repair

Acronym or Term	Definition
NAF	NATO Architecture Framework
NATO	North Atlantic Treaty Organisation
NCI Agency	NATO Communication and Information Agency
NCIRC	NATO Computer Incident Response Centre
NCS	NATO Command Structure
NFR	Non-Functional Requirement. Non-functional requirements prescribe how a system or service must perform in terms such as performance, capacity and/or resilience. Non-functional requirements also direct how a system of service must be implemented with respect to constraints such as rules, standard, certain technologies or methodologies and policies.
NHQ	NATO Headquarters
NISP	NATO Interoperability Standards Profile
NPKI	NATO Public Key Infrastructure
NR	NATO Restricted Network
NS	NATO Secret Network
NSF	NATO Software Factory
NU	NATO Unclassified Network
ON	NATO Operational Network
OOB	Out-Off-Band – Refers to the dedicated management/console network leveraged when incidents cannot be fixed via inline mechanism.
RN	Remote Node – Location client where end-user devices and a campus LAN is provided, but all other services will be centrally provisioned.
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDP	Service Design Package
SIOP	Service Interoperability Point
SIOP5	The interface between the NCI Coloured Cloud Access function and the Campus Local Area Network
SLA	Service Level Agreement
SLT	Service Level Target
SMC	Service Management and Control
SN	Standard Node – Location with limited amount of computing in support of local user services access.
SOC	Service Operations Centre – A set of end-user equipment, collocated at either a Data Centre or Enhanced Node used to support Purchaser operators in the provision of IT services to the NATO users.
SOP	Standard Operating Procedure
SOW	Statement of Work
SRM	Site Recovery Manager
U1	Static User – A user that is working at an authorised user location in any of the Static HQ locations.
U2	Mobile User – A static user will also be able to securely access the IT services from a remote location (e.g., by using the Internet).
U3	Administrator – IT support users that are responsible to administer, manage, and maintain the IT services.
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine
VPN	Virtual Private Network
VRF	Virtual Router Forwarding
WAN	Wide Area Network

1.5. Reference Documents

The NATO Enterprise and the NATO ON, which primarily serves the NATO Enterprise, is very complex. It is expected that readers of this document are familiar with the reference documents listed in Table 1-4. These reference documents provide the necessary additional supporting details for the full contextual understanding of the interdependency information, presented in this document.

Table 1-4. References

Ref.	Document	Description
Governance		
1	C-M(2015)0041-REV2, Annex 10, NATO Cloud Computing Policy, 7 January 2016	NATO policy that provides the cloud level definitions and introduces the Cloud First principle
2	NATO Enterprise Statement of Requirement / Minimum Enterprise Requirement for Common Consultation, Command and Control (C3) Capability by 2021 (SOR/MER 21), MCM-0294-2018. April 2018.	Minimum Enterprise Requirements that are addressing the need for IaaS, ECS, CPS services in form of requirements statements.
3	Information Technology – Modernisation (ITM) & Core Services – Programming Strategy. ACT/CAPDEV/CAP/TT-4638. SACT, October 2021.	Workout and mapping from Bi-SC on requirements for NATO ON.
4	NATO Standard ADatP-34, NATO Interoperability Standards and Profiles, Edition N, Version 1, 26 May 2021, at https://tide.act.nato.int/mediawiki/tidepedia/images/9/9a/NISP-v14-release.pdf	NATO interoperability standards which apply to many of the NATO ON services.
5	AC/322-D(2015)0014-REV3 The NATO Enterprise Approach for the delivery of C3 Capabilities and the provision of ICT services, dated 14 December 2015.	Documents provide information about which NATO entities belong to the NATO Enterprise Scope
6	AC/322-D(2017)-0030 NATO Enterprise C&I Vision, dated 25 July 2017.	Document provides information about the C&I Vision and steps towards achieving this vision.
7	C-M(2015)0041-REV2 Annex 7: Software Policy	Document provides guidance on NATO acquired software and its lifecycle and addresses evolutionary and continual development
Architecture		
10	AC/322-D(2018)0002, NATO Architecture Framework, Version 4, 25 January 2018, https://tide.act.nato.int/mediawiki/em/index.php/NAF_4	NATO Architecture Framework which defines the architecture method and views used in this document.
11	AC/322-D(2021)0017, C3Taxomomy Baseline 5.0, 30 August 2021, at https://tide.act.nato.int/tidepedia/index.php?title=C3_Taxonomy.	Services taxonomy that provides the underlying services definitions as used in this document.

Ref.	Document	Description
12	C-M(2015)0041-REV2, Annex 9, Enterprise Architecture Policy	C3 Policy
SMC		
21	Enterprise SMC vs Domain SMC – Architectural Approach 2.0, NCI Agency Internal Working Document	Providing the Architecture Guidance for Enterprise, Domain, Element SMC functions and Service Interfaces.
Cyber		
30	AC/322-D/0048-REV3, Technical and Implementation Directive on CIS Security	The lead cyber security guidance document that informs the minimum level cyber security measures to be taken at the CIS level, commonly referred to as D/0048
31	NATO Communications and Information (NCI) Agency Technical Report 2017/NCB010400/13, "CIS Security Capability Breakdown Version 2.0", Sébastien Gay, NCI Agency, The Hague, 2017 (NATO Unclassified)	This document describes the Communications and Information System (CIS) Security Capability Breakdown Version 2.0, providing a comprehensive map of CIS Security capabilities and a common terminology.
32	Interface Definition Document User and Device Credentials – Operational Network, 1.01 Draft 01 https://polaris.nr.nato/itmrecinc1/_layouts/15/ WopiFrame.aspx?sourcedoc=/itmrecinc1/ Engineering%20Space/WP2/ITM%20IDD%20-%20UDC%20-%20DRAFT.docx&action=default	Describes Interface Definition Document (IDD) User And Device Credentials – Operational Network (Draft) - PKI Interfaces
33	Interface Definition Document 'DLP Discovery'	This IDD provides a high level overview of the DLP Discovery ('data at rest') architecture and identifies the DLP Discover interfaces and dependencies on other services.
34	NCIA/TR/2021/CTO/12723, Guidance for D/0048 Revision 3 compliance in ITM Recovery, 13 September 2021.	Maps D/0048 requirements to NATO ON services requirements and explains the implementation requirements for countermeasures.
35	NATO Comprehensive Cyber Defence Policy Action plan (Annex 1 to PO(2022)0065, 14 February 2022, NATO Restricted)	This Action Plan identifies actions based on the NATO Comprehensive Cyber Defence Policy.
Network Services		
41	NATO Communications Infrastructure (NCI), NCI SDS – Core and Access Network Design Description, Contract: CO-13735-NCI, 18 March 2019	Describes the NCI Network Core and Access
42	NATO Communications Infrastructure (NCI), NCI SDS – Core Document Contract : CO-13735-NCI, 25 February, 2019	Describes the NCI high-level network design

Ref.	Document	Description
Project		
50	Interface Definition Document Table, document 2.2.2	Identifies the exchanges across services relevant for the NATO ON and the respective interfaces
Workforce Design		
60	The global skills and competency framework for the digital world. SFIA version 8.	https://sfia-online.org/en/sfia-8
Commercial Standards		
70	ISO 9241	International Organization for Standardization (ISO) Human-computer interaction.

2. CIS Drivers, CIS Principles and SDP requirements traceability

This chapter will introduce the key governing requirements that can be considered to be the top-level requirements that the NATO ON services shall comply with. The structure and organisation on how to manage and maintain traceability from top-level requirement to detailed implementation/design level will be addressed in this chapter as well as well.

For the ADP level requirements and its traceability to Service Design Package (SDP) level the following definitions as used:

- **CIS Drivers** are the key tenants, or the architecture goals, for the NATO ON services, which are realized by Infrastructure as a Service (IaaS), Enterprise Core Services (ECS) and Client Provisioning Services (CPS), as the services that are most visible to the user, and the Enterprise Service Management and Control (SMC) services and the Enterprise Cyber Security services in support of IaaS, ECS and CPS. The CIS drivers are the parent/root structure from which to inform the CIS principles. The CIS Drivers are introduced in section 2.1
- **CIS Principles** guide the design, implementation and evolution of the architecture. They are enduring, and inform and support an organisation in fulfilling its mission. The architecture principles, documented herein, represent the NCI Agency's high-level objectives for the NATO ON services. Details on how the architecture design and subsequent service designs adhere to and address these principles are included in the following sections. The CIS principles are introduced paragraph 2.2
- **Requirement Traceability from CIS principles to Service Design Package (SDP).** This is expressed by means of a requirements traceability matrix, identifying which NATO ON service implementations fulfil which CIS principles, worked out in the Service Design Packages specific paragraphs and sections.

Figure 2-1 below depicts the requirements traceability model that is in place covering for requirements governance at the capability level, as well as the ITM project implementation level.

The project area of responsibility, addressed in this ADP, includes:

- The ADP driven CIS Drivers, CIS Principles and the SDP traceability matrix.
- The Solution Requirements (SRS and User Stories, which shall be traceable to ADP and SDP).

Considering the wider requirements traceability context the figure shows, the linkage of CIS Drivers to the CIS principles is provided via the NATO ON Capability Requirements as documented in the ITM & Core Services Programming Strategy. The linkage is illustrated in the diagram below. Note that the CIS principles are also linked to C3 policy, which is covering all of NATO CIS, including those focussed on ITM. Furthermore, observe that the ITM & Core Service Programming Strategy is strongly linked to the Bi-SC SOR and the C&I Vision.

The four types of requirements traceability matrices (RTM) created and maintained within the project, and illustrated in Figure 2-1, are:

- CIS Principles/CIS Drivers to Capability Requirements (influence relationship);
- CIS Principles to Solution Requirements and SDPs (influence relationship);
- Solution Requirements to Capability Requirements (realization relationship); and
- Solution Requirements to detailed implementation artefacts (detailed design, interface control documentation, etc.) (Realization relationship).

The focus of the requirements and requirements traceability modelling in this document is on the introduction of CIS drivers and principles and provide a traceability mapping to the capability requirements. Traceability modelling of the various types of requirements dependencies as depicted in Figure 2-1 is not performed utilising the architecture tools (e.g. Archimate/ARIS), but performed via the ITM requirements management processes and supported by the DOORS toolset as depicted in the scoping Figure 2-1 provided in section 1.1.

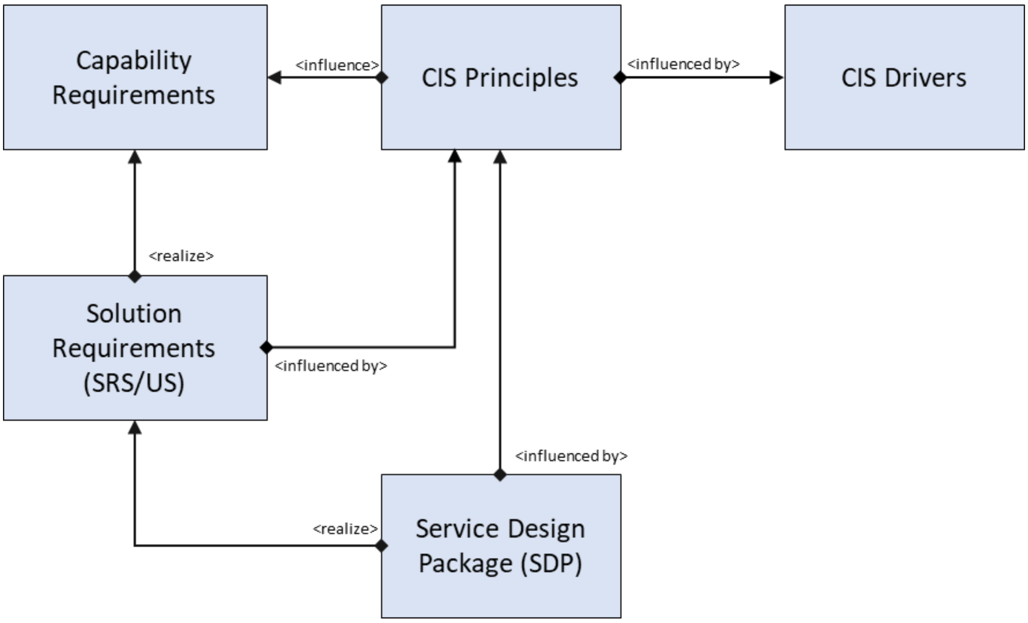


Figure 2-1 CIS Drivers, Principles, SDP traceability (not modelled in ArchiMate)

2.1. CIS Drivers

The ArchiMate standard defines a driver as follows: A driver represents an external or internal contribution that motivates an organization to define its goals and implement the changes necessary to achieve them.

The following four key CIS drivers are identified (each identified through a representative term):

1. Cloud
2. Cyber Security
3. Service Management and Control
4. Digital Desktop

In the remainder of this section each of these drivers will be further defined.

2.1.1. CIS Driver 1: Cloud

As context to this driver, the NATO Enterprise Cloud Computing policy (reference [1]) promotes NATO to adopt a Cloud Computing Business model where:

- ICT solutions will be designed with the expectation that the infrastructure has already been designed and will be provisioned, when needed.

- ICT solutions will be hosted on infrastructure owned[2], operated and maintained by the Cloud Service Provider.
- Service providers will be responsible for acquiring, running and maintaining the cloud infrastructure on which NATO ON services are realized.

Note: Although in line with NATO Enterprise C&I Vision (reference [6]), the general aim for the NATO ON is to achieve cost efficiency through maximum use of the same standardized Services (para 3.4 of NATO Enterprise Vision). However, the NATO Enterprise Vision and NATO Cloud Computing Policy both suggests that the maximum use of evolving cloud based solutions should be pursued. (cloud first principle)

Key CIS Driver 1 “Cloud” is to enable the NCI Agency to provide effective and cost-efficient Infrastructure as a Service (IaaS) Private Cloud capability that:

- Supports IT services up to the NATO SECRET (NS) level on the Operational Network (ON) infrastructure
- Supports ICT provider and end-user business continuity and disaster recovery needs;
- Provides increased operational flexibility and agility
- Provides increased service availability and resiliency that meets user needs; Increased service levels (as per SOR/MER 21 (reference [2]) Service Level Targets change compared to SOR 19)
- Reduces ICT resource requirements time and effort to deploy and manage application services
- Implements a remote, mobile support model and move to self-service and automated processes
- Improves management processes and procedures – increased effectiveness, efficiency and consistency of service realization
- Improves the security posture of the CIS services through centralised, standardised and agile CIS security operations effectiveness in a way that is fully integrated with the IaaS Private Cloud service delivery capability
- Improves Support of for DevSecOps paradigm; including infrastructure as a code for faster deployment, updating, lifecycle-management, patching and overall improved security posture.
- Enables Enterprise Core Services to assume cloud based features (such as Database Services, Portal Services) as a step-up to further Platform as a Service (PaaS) Cloud enablement

2.1.2. CIS Driver 2: Cyber Security

Achieve a higher maturity level for Cyber Security of CIS services and improve the abilities for proactive Cyber Security and faster response to security infractions considering the ever-growing Cyber Threat Landscape in order to achieve:

- Enhanced security through compliance with the revised NATO C3 Board endorsed Technical and Implementation Directive on CIS Security (reference [30]) and with the SOR/MER 2021 extent security requirements (reference [2]). The directive requires additional minimum level (new) CIS security requirements with implications for Identity and Access Management (IAM) and more specifically in the area of privileged access management (PAM).

[2] In the context of the NATO ON architecture, the “ownership” concept refers to having “possession and control”. That means that the service provider has a right to use the infrastructure. The legal context under which such is granted, nor the legal constraints of such, is not relevant for this architecture.

- Integrated IaaS Private Cloud Cyber Security following the security by design principle.
- To establish a modern set of cyber security functions to achieve the security level required for delivery of CIS Services. Most cyber security functions will be based on the current approach, updated to be effective and efficient in the new private cloud provisioning model. This includes preventive functions such as endpoint protection, network and communications protection, as well as defensive functions for monitoring, detection, and response.
- The CIS segmentation model and the corresponding boundary protection functions that were previously developed for the NATO ON, will be reused and adapted if needed. The initial NATO ON cyber security endpoint baseline will be used, although it will be updated to account for new technology and updated policy.
- New functions will be implemented for user authentication, device authentication, and privileged access management. These functions will establish the baseline for all future implementations.
- The cyber security functions for monitoring, detection, and response will be implemented following the current approach with the necessary adjustments in capacity and management. System logs will be collected according to the current approach, and new infrastructure components and Enterprise Core Services will be analysed for the monitoring information to be collected.
- All cyber security management and monitoring will be integrated with the Cyber Security Operations Centre (CSOC). The cyber security services in the NCI Agency service catalogue (“SEC services”) will be updated to cover the NATO ON services and will be subsequently used to ensure continuous cyber security coverage.

2.1.3. CIS Driver 3: SMC

Achieve an efficient, performant and dependable service delivery through well-designed Service Management and Control (SMC) capability for the IaaS Private Cloud. The NATO ON IaaS Private Cloud Service Management and Control (SMC) capability (comprising people, process and technology) will provide a set of common and consistent processes and associated tools supporting workforce to achieve the following goals:

- The Domain (IaaS/ECS/CPS) SMC technology toolset will integrate and interoperate with the Enterprise-SMC (E-SMC) toolset. That shall provide a holistic view of all services across the infrastructure. E-SMC governs and enforces the agreed IT Service management policies through the embedding and integrating of the processes and controls.
- The NATO ON adopts the Enterprise Asset and Configuration Management 3-tiered model:
  - Tier 1 Asset, Configuration, Patch and Vulnerability Management (ACPV) governance, i.e. strategic decision making
  - Tier 2 Enterprise SMC, i.e. technical management
  - Tier 3 Element and Domain SMC, i.e. technical assets
- Via the Element and Domain SMC (Tier 3) and Enterprise SMC (Tier 2) data and information will be provided to support the ACPV governance level (Tier 1).
- The SMC implements a scalable, three-level, hierarchical technical architecture:
  - At the lowest level, there are Element SMC systems. Element SMC systems are typically vendor-specific and manage the lowest level of service components within the infrastructure.

  - The second level is comprised of Domain SMC systems. Domain SMC systems operate within an SMC Domain in order to manage and control systems from multiple vendors that provide similar functionality within the infrastructure.
  - At the third level, the highest, level are the Enterprise SMC systems. E-SMC systems aggregate and process data from domain and element SMC systems to provide a service view. This layer provides operators and commanders with relevant and actionable information regarding services (Service Situational Awareness / Recognised CIS Picture).

- From an ITM Recovery Increment 1 viewpoint, note the following: The SMC contributions, realized by ITM, shall be seen as contributing activity to achieve the overarching Enterprise SMC capability via a programmatic approach. The three architecture levels are documented and detailed in the paragraph 3.4.

- Achieve SMC Processes impacting IaaS/ECS/CPS Service Design, Management and Delivery – 17 ITILv3 (2011) based ICT service management processes: Incident Management, Change Management, Change Evaluation, Request Fulfilment, Service Asset and Configuration Management, Release and Deployment Management, Event Management, Problem Management, Knowledge Management, Service Level Management, Availability Management, Capacity Management, Access Management, Service Validation and Testing, Information Security Management, IT Services Continuity Management, Financial Management for IT.

- People – organisation aspects (organizational functions, roles and responsibilities), training and instructional will be mapped to the 3-tier Organisation model (introduced above) that includes the ESOC organisation. Key driver for the organisation and process design is to achieve the non-technical part of the Service Level Requirements so the IT provider can fulfil the SOR and SLA requirements from the Customer.

- A key foundational deliverable, of ITM Recovery Increment 1, that shall be achieved as soon as possible is a quality based Configuration Management Database (CMDB) and processes, for the NATO ON services realized, to enable ITM Recovery Increment 1 to exercise full configuration control from the outset of the project. This foundational function is essential to manage implementation and low level design change simultaneously across the various ITM Recovery Increment 1 Work Packages. Up-to-date configuration information is also an essential input for test and validation activities. This CMDB deliverable is a core component of the Agency effort to support the Asset, Configuration, Patch and Vulnerability Management (ACPV) initiative. The C (Configuration) aspect is immediately impacted by the delivery of ITM Recovery Increment 1 to provide a valid operational inventory and a manageable service impact capability

- An aligned goal is to contribute for a part to the implementation of NATO Cyber Adaptation urgent reforms as actioned in the NATO Comprehensive Cyber Defence Policy Action plan [35] regarding the prioritised requirement on ACPV, to improve obsolescence management and asset replacement planning.

2.1.4. CIS Driver 4: Digital Desktop

Change and disruption, well-illustrated by the COVID19 pandemic, makes that a flexible, agile, mobile force is critical to the success of NATO. Moreover, all indications are that this change and the need to be prepared for increasing uncertainty in terms of the strategic environment are unlikely to diminish. (From reference [3]). Furthermore, today data is predominantly digital and ever increasing in quantity and fidelity. Such an environment drives the need for the ability for staff to work, share and collaborate across the Enterprise and the Alliance large, regardless of physical location of the people, data and systems.

In summary, this driver instigates the need for agile CIS services, the need for operational efficiencies and foremost the need for business continuity. Such is translated in the concept of a digital desktop, which gives staff the freedom to work, collaborate, access and share information as, where and when required. The concept of digital desktop is a subset of the digital desktop, which not only covers the desktop but the staff's working environment at large.

The CIS Driver "Digital Desktop", as elaborated above, leads to a key objective to offer the user a service-based desktop experience and a step toward a cloud-based desktop and desktop applications through a demand model, considering:

- Desktop and desktop application performance,
- Similar look and feel independent of the client platform and location from where the users access the network;
- Access to the user data in Switching between desktop sessions;
- Mobility of the user profile,
- Desktop is single point of entry for Human-2-Human (H-2-H) communications and team-based collaboration.
- On demand ordering of access to required applications.

2.2. CIS Principles

In the remainder of this section the CIS principles are introduced and mapped its Parent CIS Driver.

2.2.1. CIS principles linked to CIS Driver1: Cloud

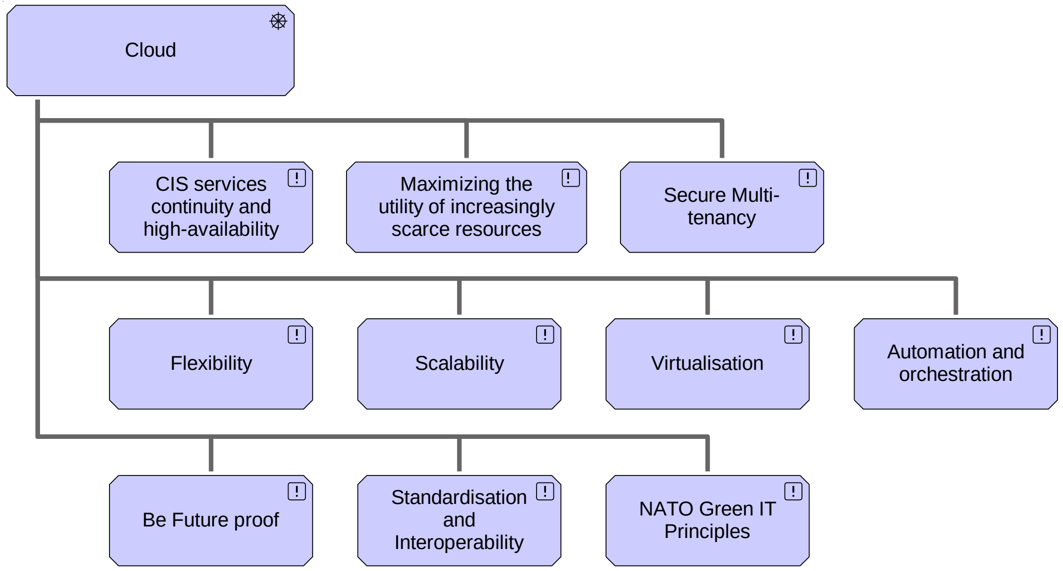

Cloud
CIS services continuity and high-availability
Maximizing the utility of increasingly scarce resources
Secure Multi-tenancy
Flexibility
Scalability
Virtualisation
Automation and orchestration
Be Future proof
Standardisation and Interoperability
NATO Green IT Principles

Figure 2-2 CIS Principles to Driver1: Cloud mapping

2.2.1.1. CIS Services Continuity and High Availability

The NATO ON architecture is designed to meet the service's continuity and availability requirements. The NATO ON architecture addresses the high availability requirements by addressing both the operational and intrinsic availability.

Operational availability is explained in detail in each of the four Services Design Packages (SDP): Infrastructure as a Service (IaaS), Client Provisioning Services (CPS), Enterprise Core Services (ECS), and Service Management and Control (SMC) support high availability operations by leveraging redundant hardware, clustering, load balancing, and redundant network paths. Operational availability is further enhanced by the Service Management control plane that is constantly monitoring, logging and adjusting via prescribed event-driven automation of the various N enclaves for SLA/OLA compliance.

Intrinsic availability is addressed by the mean time between failure (MTBF) and mean time to repair (MTTR) analysis. Please note that intrinsic availability has a different meaning for each of the Infrastructure Nodes and associated User Nodes, including the campus network. Each SDP accounts for those differences in their detailed designs.

We avoid single points of failure using redundant hardware. Load balancing is employed to realize highly available and geographically distributed services.

Our event management process enables information collection, such as Syslog, for failure detection.

2.2.1.2. Maximizing the Utility of Increasingly Scarce Resources

The NATO ON design supports the consolidation of services to reduce the overall administrator and maintenance resources, optimising the use of physical assets and resources in providing services to users, and reducing the Total Cost of Ownership (TCO) of the service lifecycles. This principle is achieved through centralised management, virtualisation, pooled resource sharing, consolidation of services, automation, and dynamic allocation of resources.

2.2.1.3. Secure Multi-Tenancy

The NATO ON design supports secure multi-tenancy by allowing multiple NATO Communities of Interest (COIs) to share the same infrastructure while complying with applicable NATO security regulations and requirements. Key considerations in supporting this principle include tenant identification and security requirements assessments for each to assure sufficient isolation while optimizing resource use.

2.2.1.4. Scalability

The NATO ON design supports scaling to increase capacity (scale up and out) and to decrease capacity (scale down). [3]

2.2.1.5. Virtualization

The NATO ON design supports virtualisation through logical-level decoupling from specific hardware solutions and dependencies achieved through virtualisation methods, technologies and techniques.

[3] Driven by the private cloud/on-premise constraint that the infrastructure cannot be shared with many tenants as would be the case for Public Cloud scenarios – for the ON - a 25% automatic scale out capacity/performance scalability KPI is set. Capacity/Performance upgrades beyond this level are understood to take more time due to the required infrastructure-facility upgrades that may be required.

2.2.1.6. Automation and Orchestration

The NATO ON design supports the automation of management and administration of NATO ON services to achieve efficiencies, including effective and timely services delivery, across the entire service life-cycle. This includes self-service capabilities for users.

2.2.1.7. Be Future Proof

The NATO ON design and solution are sustainable and 'future-proof' for the lifecycle of the project. The design leverages a modular approach to capacity using industry-leading Commercial Off-the-Shelf (COTS) products evaluated against vendor development lifecycle and product-usable lifecycle. Product selection is focused on industry-standard ports and protocols, resulting in a reduction of risk associated with vendor support, product upgrades or functionality enhancements. All products in the design will comply with Integrated Logistics Support (ILS) guidance on maintenance periods as part of the overall lifecycle support and logistics concept.

2.2.1.8. Standardisation and Interoperability

The NATO ON design focuses on the use of COTS products and provides further standardisation based on functionality and location across the enterprise. The NATO ON design's logical and physical interfaces are founded on open industry standards and protocols.

2.2.1.9. Green IT

The NATO ON monitors and reports resource and energy consumption.

The NATO ON design optimizes the infrastructure footprint and energy consumption through virtualisation and consolidation of services.

2.2.2. CIS principles linked to CIS Driver2: Cyber Security

The Cyber Security Driver gives rise to the following principles:

1. Security by Design: Security is considered from the onset following a holistic approach;
2. Identity and Access Management: the key enabler for secure access to services;
3. Cyber monitoring and response to cyber security related events/risks.

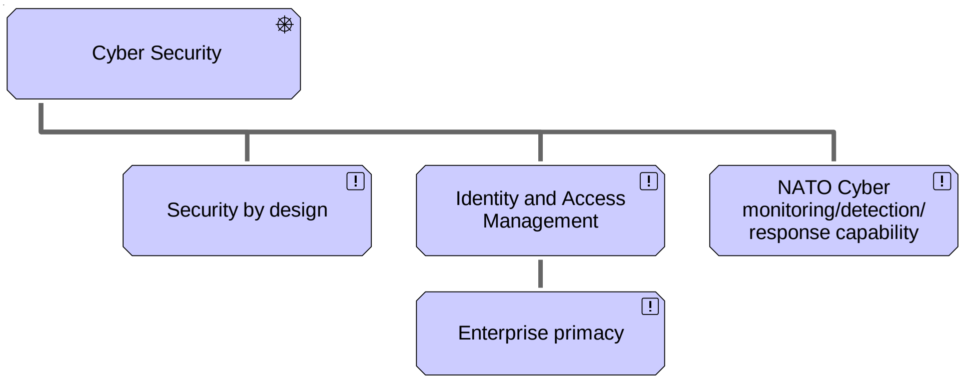

Cyber Security
Security by design
Identity and Access Management
NATO Cyber monitoring/detection/ response capability
Enterprise primacy

Figure 2-3 CIS Principles to Driver2: Cyber Security

2.2.2.1. Security by Design

Provide Integrated IaaS Private Cloud Cyber Security as the security by design principle. Each of the IaaS services shall be designed and implemented following a risk based security by design principle considering:

- Inclusion of preventive functions such as endpoint protection, network and communications protection;
- Inclusion of defensive functions for monitoring, detection, and response;
- Alignment with the life-cycle management of the various IaaS hardware and software elements following the NCIA AFPL change management procedure;
- Compliancy with NATO security policy.

See Section 3.5 for more coverage of the Security by Design approach.

2.2.2.2. Identity and Access Management / Enterprise primacy

Provide a NATO Enterprise Level Identity and Access Management including a Privileged Access Management, capability that will support administrative roles, to achieve a given task (formally recorded), in-given-time, with minimum necessary required access rights (least privilege).

Employ an enterprise perspective of coherence placing interoperability, agility and management of “total cost of ownership” at the forefront.

2.2.2.3. NATO Cyber monitoring/detection/response capability

Provide a monitoring/detection/response capability that will:

- Have increased capacity to include new NATO ON Nodes into its coverage;
- Integrate with the Enterprise Logging capability that will collect and centralize logs from all endpoints, creating a data lake to be utilized by different entities for different purpose;
- Perform accurate data management and data integration of IaaS-related Cyber Security services through the CSOC supported by integration with SMC and leveraging the Configuration Management Database (CMDB; see 2.1.3).

2.2.3. CIS principles linked to CIS Driver3: SMC

The Asset, Configuration, Patch and Vulnerability Management (ACPV) principles define that the IaaS SMC Configuration Management function has to deliver accurate SMC data management and data integration services in order to feed ACPV information services.

In this 3-tier Enterprise Asset Configuration and Management capability, where Tier-1 covers Strategic Decision Making, Tier 2 Technical Management, and Tier 3 technical assets.

In paragraph 3.3, capabilities related to Configuration Item (CI) discovery, configuration management and service capacity are providing information about operational configuration and service impact views, feeding service enabled views to the strategic tier-1 ACPV level.

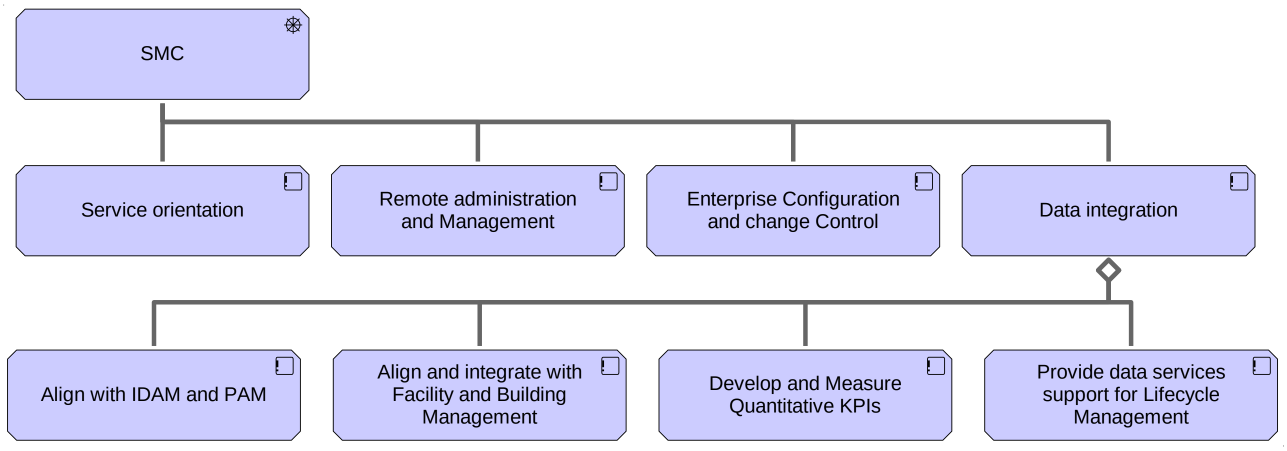

SMC
Service orientation
Remote administration and Management
Enterprise Configuration and change Control
Data integration
Align with IDAM and PAM
Align and integrate with Facility and Building Management
Develop and Measure Quantitative KPIs
Provide data services support for Lifecycle Management

Figure 2-4 CIS Principles to Driver3: SMC

2.2.3.1. Service orientation

SMC data services shall support a service based approach where the CIS services tree is for 100% mapped to the hardware and software assets to the granularity needed to provide the services and provide reports/data about the CIS services configuration, performance and capacity. No hardware or software assets or any other components contributing to CIS services shall be managed “outside the controls” of the SMC function.

2.2.3.2. Enterprise configuration and change control

All configuration changes that impact a service to any of the systems, hardware and software assets, that realize NATO ON services, shall be formally managed, recorded, reported about, archived and audited.

- SMC data shall use data integration services interfaces that map to the data models and interfaces governed by the Enterprise SMC (ESMC) provided data integration services guidance (e.g. ESMC is broker for interoperability with other services such as Enterprise Resource Planning and Portfolio Management Services).

2.2.3.3. SMC data shall use data integration services interfaces

The SMC Data and Data integration services shall support the following in support of (aggregating) the following principles:

- Align with IDAM and PAM: SMC data services shall use and align with IDAM and PAM services and identity data (relate to people and device entities).
- Align and integrate with Facility and Building Management related systems considering Data that need to be shared around HVAC, facility and rack locations, space and building (room) access controls.
- Develop and Measure Quantitative KPIs (metering) that can be fully correlated to the Service Level Requirements and Service Level Targets used in the Service Level Agreements of Operational Level Agreements that are exercised for the IaaS related services as advertised in the NCIA catalogue of services (see reference [20]). Use the service levels as per SOR/MER 21 Service Level Targets
- Provide data services support for lifecycle management of the IaaS Automation and Orchestration Functions. The Automation and Orchestration functions shall not “duplicate” or

come up with “alternative data models” authoritative IaaS/ECS/CPS asset data that is available via the SMC data services; it shall interface directly or via a mediation/translation layer.

- Provide data services that support full lifecycle management of all IaaS/ECS/CPS hardware/software services (including alignment with portfolio and catalogue management).

2.2.3.4. Remote Administration and Management

Remote administration and management of all NATO ON services, following approved Standard operating Procedures (SOPs) and from allowed locations, is a core design principle. The NATO ON design allows authenticated and authorised administrative capabilities from any location, in particular the SOCs, and has an extensive array of remote management capabilities.

2.2.4. CIS principles linked to CIS Driver4: Digital Desktop

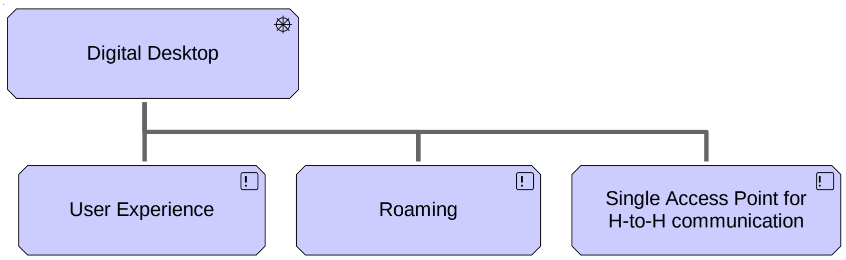


Figure 2-5 CIS Principles to Driver4: Digital Desktop

2.2.4.1. User Experience

The NATO ON design offers a consistent and standardised end-user experience, as defined in reference [70], the ON and shall be designed to offer satisfactory service response times. The subcomponents of each service that supports this architecture principle are described in the following paragraphs. The application enables user interaction to convey activity and responsiveness. COTS applications conform to industry norms for human interaction.

2.2.4.2. Roaming

The NATO ON design provides users on the ON and network the ability to remain engaged in business processes while roaming within NATO facilities. The NATO ON design addresses the roaming by using roaming user profiles and central application provisioning irrespective of the client device location or type (thin or thick).

2.2.4.3. Single Access Point for H-2-H Collaboration

The Digital Desktop will enable a single point of access for a user to collaborate and share information. For the scope of ITM Recovery Increment 1 this is translated to access to the key ECS services: Skype for Business, Portal and Email. These services enable a user to create calendar based collaboration (team) events, share information and check presence of the team.

3. Architecture Perspectives

3.1. Introduction of Architectural Perspectives

This view introduces an overview of the various architectural perspectives that are relevant for the ITM Recovery Increment 1 project. The diagram in Figure 3-1 below, and the list of covered architectural perspectives provided in the text below Figure 3-1, serves as an “index” for the architectural perspectives, or viewpoints, described herein.

The diagram in Figure 3-1 identifies key aspects that are relevant for NATO ON services from an ITM project viewpoint. Aspects covered include organizational elements, business services, technical services, infrastructure, nodes and supporting infrastructure and services. The following paragraphs, which are listed below Figure 3-1, detail the architectural perspectives that the architects consider critical. The following paragraphs refer back to the key aspects identified in the diagram below and provide further detail from their respective viewpoints.

Note, this view must not be seen as a layered stack such as the Open Systems Interconnection model (OSI model) nor must be seen like a taxonomy like NATO C3 Taxonomy. Rather, this view illustrates the context of various architectural viewpoints allowing for establishing relationship between viewpoints in a coherent manor.

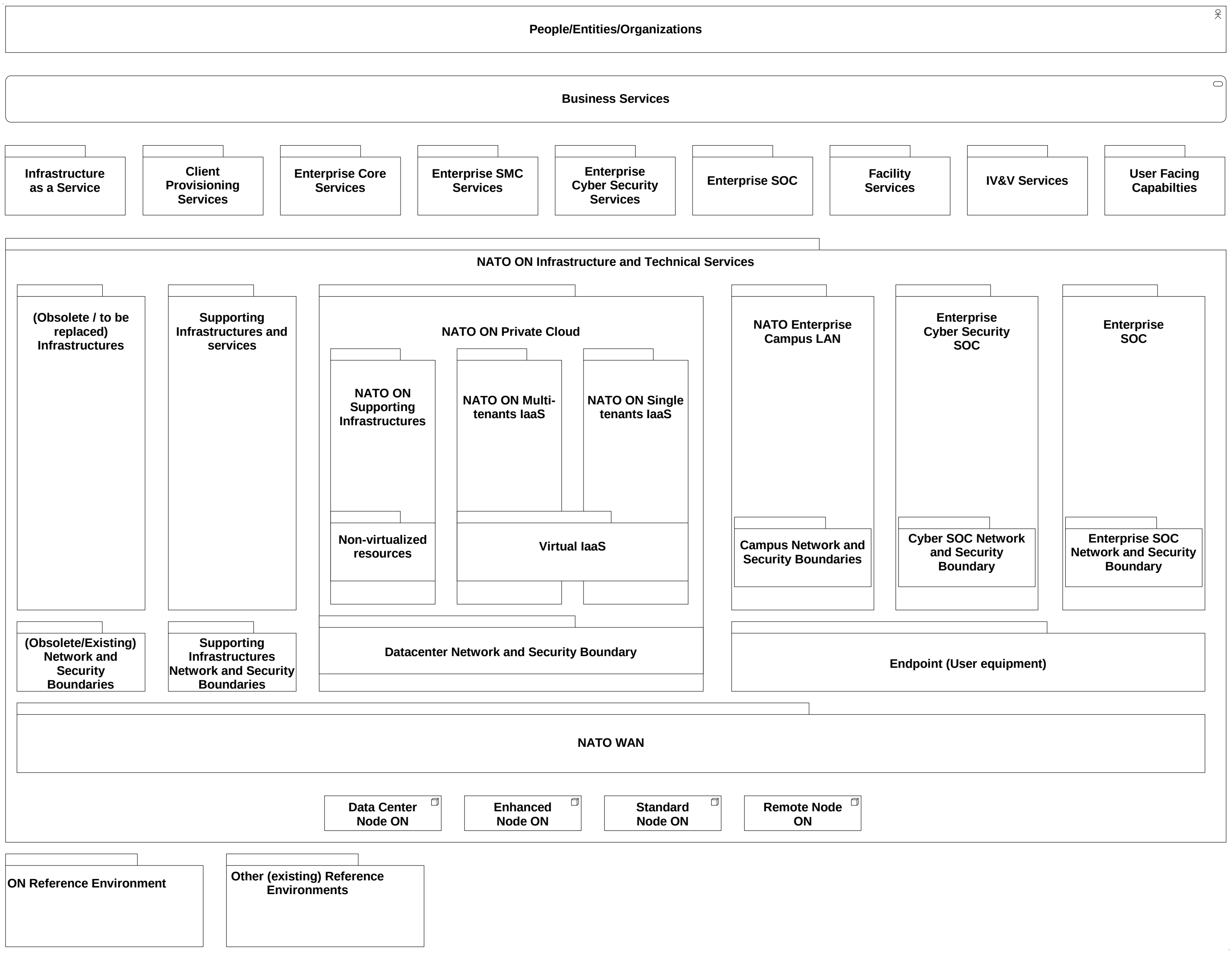

People/Entities/Organizations
Business Services
Infrastructure as a Service
Client Provisioning Services
Enterprise Core Services
Enterprise SMC Services
Enterprise Cyber Security Services
Enterprise SOC
Facility Services
IV&V Services
User Facing Capabilties
NATO ON Infrastructure and Technical Services
(Obsolete / to be replaced) Infrastructures
Supporting Infrastructures and services
NATO ON Private Cloud
NATO ON Supporting Infrastructures
NATO ON Multi-tenants IaaS
NATO ON Single tenants IaaS
Non-virtualized resources
Virtual IaaS
NATO Enterprise Campus LAN
Campus Network and Security Boundaries
Enterprise Cyber Security SOC
Cyber SOC Network and Security Boundary
Enterprise SOC
Enterprise SOC Network and Security Boundary
(Obsolete/Existing) Network and Security Boundaries
Supporting Infrastructures Network and Security Boundaries
Datacenter Network and Security Boundary
Endpoint (User equipment)
NATO WAN
Data Center Node ON
Enhanced Node ON
Standard Node ON
Remote Node ON
ON Reference Environment
Other (existing) Reference Environments

Figure 3-1 Overview of Architectural Perspectives

The following perspectives (viewpoints) are covered:

- Services (§ 3.2)
- Infrastructure (§ 3.3), broken down in a nodal decomposition (§ 3.3.1), WAN transport (§ 3.3.2), networking infrastructure (§ 3.3.3) and IT infrastructure (§ 3.3.4)
- Service Management and Control (§ 3.4)
- Cyber Security (§ 3.5)
- Lifecycle Management and DevSecOps (§ 3.6)

Note for traceability purposes, Cyber Security Services, as referred to above and used throughout this ADP, are in the NATO C3 Taxonomy (C3T) referred to as “CIS Security Services” (as covered in the C3T’s Technical Services layer) and “CIS Security Applications” (as covered in the C3T’s User-

Facing Capabilities layer). The term “Cyber Security” is used herein to align with common industry terminology.

3.2. Services Perspective

NATO ON Services are realized though technical and business services working in concert.

The NATO ON Service Tree, addressed by this ADP, is presented in Figure 3-2 below.

The focus of this ADP is the realization of:

- the Infrastructure as a Service (IaaS), identified as ON-Infra;
- the Client Provisioning Services (CPS), identified as ON-CPS;
- the Enterprise Core Services (ECS), identified as ON-ECS;
- the SMC Services, identified as ON-SMC; and
- the Cyber Security Services, identified as ON-CS.

The SMC Services and Cyber Security Services are supporting the IaaS, CPS and ECS - as part of the NATO ON services.

The scope of this ADP is ON Services for the NATO Enterprise, hence the prefix “Enterprise” used throughout this ADP such as Enterprise Core Services (ECS). Observe that Enterprise Core Services (ECS) is specialization of Core Services, as identified in the C3 Taxonomy, focussed at the NATO Enterprise. Across this ADP, Enterprise Core Services and Core Services may be used interchangeably. Equally, Infrastructure Services and Infrastructure as a Service (IaaS) may be used interchangeably.

Because of the ADP’s focus, the view below considers a pure technical viewpoint. That implies that this view solely describes the CIS services that are realized by ITM; business services are not elaborated in this specific view.

As illustrated in the introduction to this “Architecture Perspectives” section (previous paragraph), the NATO ON Services also cover additional services beyond the scope of ITM. Many of these are already-existing services. A portion of these services, outside the scope of ITM, must be interfaced with. These interfaces are covered in the Interface Definition Document (IDD) Table (reference [50]).

Note that the term “ITM Recovery Services” is used, in the diagram in Figure 3-2 below, to remind us of the project level scope of this view. Having said that, the diagram does illustrate that the ITM Recovery Services are part of the larger whole of the NATO ON Services. When reviewing this view, please remember that, in order to keep the diagrams from getting too “busy”, only CIS services that are relevant for ITM Recovery Increment 1 are represented.

This Service Taxonomy, NAFv4 S1, in Figure 3-2 below, shows the structure of the CIS services and sub-services provisioned through the NATO ON design. This Service Taxonomy organises the required services into categories to manage the service design complexity and to ease the harmonisation of CIS architecture across the enterprise.

The level of decomposition reflected in this Service Taxonomy facilitates tracing to the Service Design Packages (SDP) that articulate the detailed design of these services. Each of the “leaf-level” services defined in this Service Taxonomy is further decomposed and described in the individual SDPs.

For ease of reference (specifically for the stakeholders that this view is intended for), Figure 3-2 below uses terminology already used throughout the ITM documentation produced earlier. Consequently, this view does not fully adhere to the NATO C3 Taxonomy (C3T) (reference [11]), but uses terminology expected to be more familiar to the stakeholders.

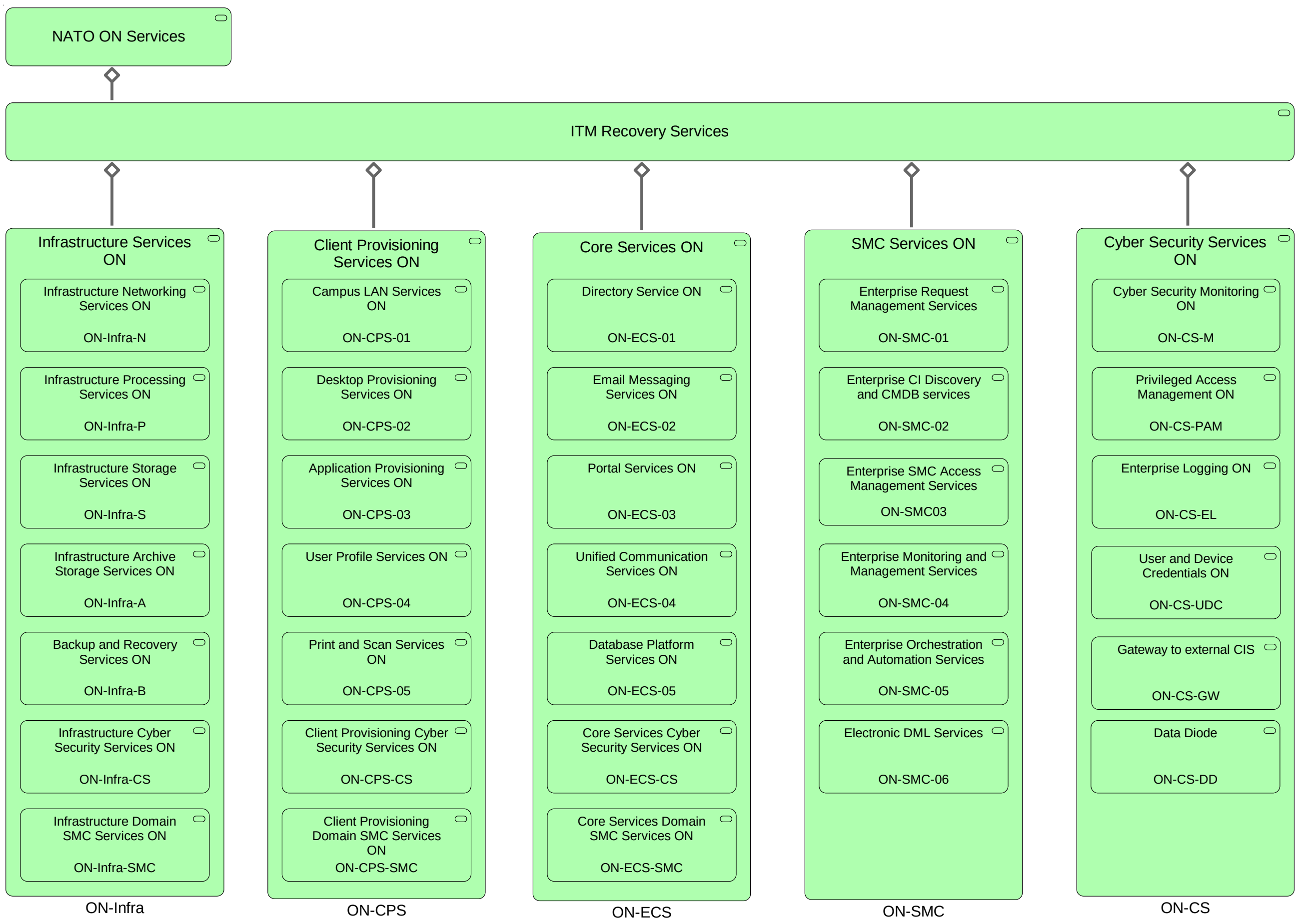

NATO ON Services
ITM Recovery Services
Infrastructure Services ON
Infrastructure Networking Services ON
ON-Infra-N
Infrastructure Processing Services ON
ON-Infra-P
Infrastructure Storage Services ON
ON-Infra-S
Infrastructure Archive Storage Services ON
ON-Infra-A
Backup and Recovery Services ON
ON-Infra-B
Infrastructure Cyber Security Services ON
ON-Infra-CS
Infrastructure Domain SMC Services ON
ON-Infra-SMC
ON-Infra
Client Provisioning Services ON
Campus LAN Services ON
ON-CPS-01
Desktop Provisioning Services ON
ON-CPS-02
Application Provisioning Services ON
ON-CPS-03
User Profile Services ON
ON-CPS-04
Print and Scan Services ON
ON-CPS-05
Client Provisioning Cyber Security Services ON
ON-CPS-CS
Client Provisioning Domain SMC Services ON
ON-CPS-SMC
ON-CPS
Core Services ON
Directory Service ON
ON-ECS-01
Email Messaging Services ON
ON-ECS-02
Portal Services ON
ON-ECS-03
Unified Communication Services ON
ON-ECS-04
Database Platform Services ON
ON-ECS-05
Core Services Cyber Security Services ON
ON-ECS-CS
Core Services Domain SMC Services ON
ON-ECS-SMC
ON-ECS
SMC Services ON
Enterprise Request Management Services
ON-SMC-01
Enterprise CI Discovery and CMDB services
ON-SMC-02
Enterprise SMC Access Management Services
ON-SMC03
Enterprise Monitoring and Management Services
ON-SMC-04
Enterprise Orchestration and Automation Services
ON-SMC-05
Electronic DML Services
ON-SMC-06
ON-SMC
Cyber Security Services ON
Cyber Security Monitoring ON
ON-CS-M
Privileged Access Management ON
ON-CS-PAM
Enterprise Logging ON
ON-CS-EL
User and Device Credentials ON
ON-CS-UDC
Gateway to external CIS
ON-CS-GW
Data Diode
ON-CS-DD
ON-CS

Figure 3-2. NATO ON Service Tree – confined to ITM Recovery Increment 1 scope[4]

3.3. Infrastructure Perspective

3.3.1. Nodal decomposition

From a high-level the NATO ON architecture can be summarized as shown below. The diagrams in Figure 3-3 - Figure 3-9 shows active structure and service realization views.

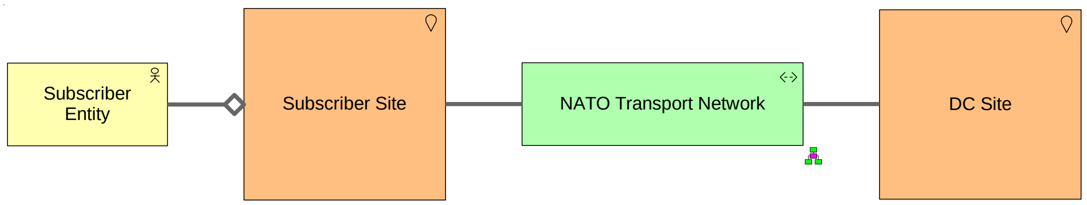


Figure 3-3. High Level NATO ON architecture

[4] The wider IDAM perspective covers, in addition to the Core Services Directory Services and Cyber Security Services PAM, integration with other services like NEDS, NPKI and Personnel Management Services. The wider IDAM perspective is not covered in this version of the ADP.

The “Subscriber Entity”, modelled in Figure 3-3 above, represents the organisations that are hosted at a “Subscriber Site” (a location). These Subscriber Entities are served with CIS services from a “DC Site”.

Note that, although not explicitly modelled in Figure 3-3 above, a Data Centre (DC) Site may physically host both the DC and a user community (the Subscriber Site). That means subscribers and DC are collocated at the same location. However, at this level of abstraction, the architecture is agnostic to that and permits collocated or not collocated Subscriber / DC Sites.

The NATO Transport Network, realized by the NATO Communications Infrastructure (NCI), provides the wide area network (WAN) communications between sites.

Commensurate to the user requirements, with respect to accessibility, performance and resiliency, Subscriber Sites come in three flavours. The following flavours of Subscriber Site exist:

- Standard Node (SN) site: local enabling infrastructure supporting local client IT access and user access to applications and Enterprise Core Services in the Data Centre. A SN serves the typical requirements of users at a location served by the IaaS.
- Enhanced Node (EN) site: providing the same client IT support as standard nodes but with local infrastructure to support critical local data and application services. An EN is a step up from the SN with edge computing infrastructure serving local users with critical services.
- Remote Node (RN) site: remote client access to the Data Centres, no local infrastructure. A RN is a cost effective simplified Access Node that only locally hosts the minimum to “power” User Equipment accessing all services from the DC.

Considering the DC Site and the above introduced three flavours of Subscriber Sites, the NATO ON architecture considers the following flavours (specializations) of the NATO Enterprise Static Site.

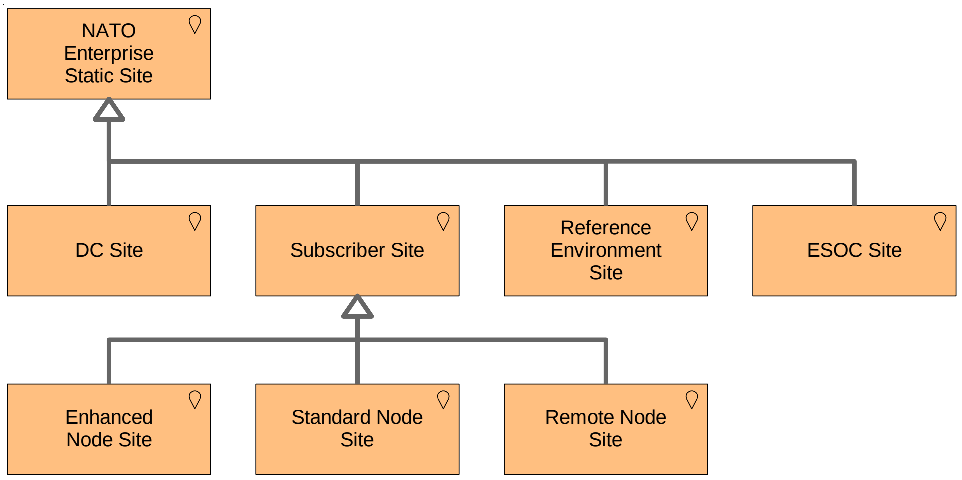


Figure 3-4 Breakdown of the NATO Enterprise Static Site into flavours

Using the NATO Enterprise Static Sites, introduced in above, the view in Figure 3-5 below shows the CIS services’ active structure focused on the type of node, which are: Data Centre, Enhanced, Standard, Remote, Reference.

When comparing Figure 3-3 and Figure 3-4 note that, in addition to the DC Site and the Subscriber site, two additional site types exist. The first is the “Reference Environment Site”. The Reference Environment Site covers the NATO Software Factory (NSF) cloud and on-premises environment. The on-premises environment is also referred to as the “ITM Reference Environment” (IREEN). Whilst the on-premises part of the so-called Reference Environment Site is hosting IREEN, this architecture considers the Reference Environment Site as a hybrid environment.

In the context of ITM Rec Increment 1, IREEN is an environment providing the reference of services in the scope of the project. As part of ITM Rec Increment 1, two reference environments are leveraged, IREEN ON@NU and IREEN ON@NS.

IREEN ON@NU will be one building block for the NATO Enterprise Reference System NERS. Ultimately the NERS includes the full reference for NATO ON, which is beyond the scope of the ITM Recovery Increment 1 project. The Reference node type, as part of IREEN ON@NU, can be configured to model a DC, an Enhanced Node (EN), a Standard Node (SN) or a Remote Node (RN). The second additional site type is the “ESOC Site”. The ESOC refers to the Enterprise Service Operations Centre (ESOC).

In Figure 3-5 below, the CIS nodes that are in scope of ITM are marked green. The other nodes, marked grey, are provided as context. Basically the active structure in scope of ITM is made up of the NATO CIS User Node and the NATO Infrastructure Node.

Note that this view below is logical and distinguishes between infrastructures (Infra Node ON), from where the CIS services are provided, and the user access (User Node ON). Architecturally the user access and infrastructure have a different purpose and in turn consist of different building blocks. Infrastructure Nodes and User Nodes are therefore independently modelled herein. However, in principle, each NATO CIS User Node is collocated with one of the 5 NATO Infrastructure Nodes as shown.

The view in Figure 3-5 below decomposes the generic NATO CIS Node into a CIS User Node, an Infrastructure Node, a Communications Access Node and a Transport Node. The nodes in scope of this increment are green, the other nodes (marked in grey) are shown to provide context.

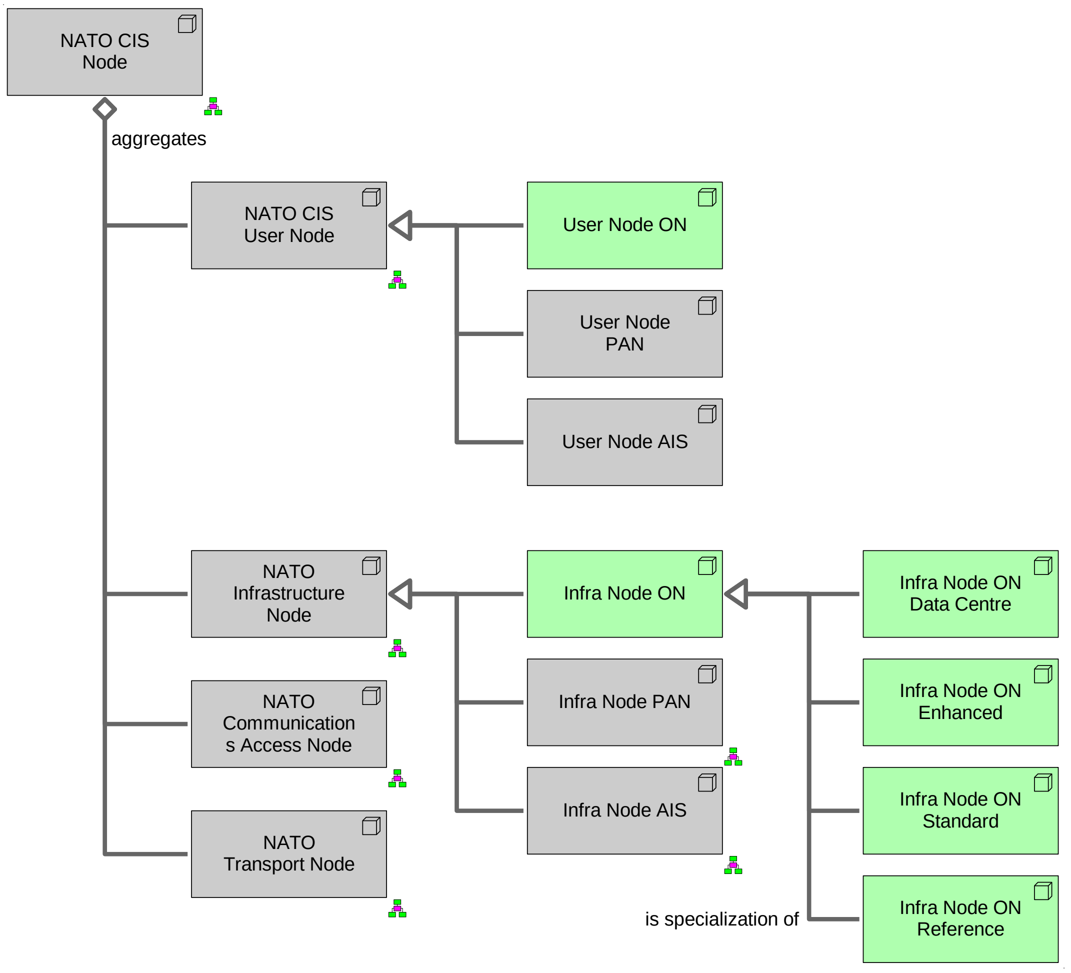


Figure 3-5 NATO CIS Node Types

When reviewing the diagram above, note that the grey nodes are not in scope of ITM Recovery Incr. 1 but included to provide context with respect to the NATO CIS.

Further observe that the diagram above shows no “Infra Node ON Remote”. This is because the Remote Node (RN) has no local infrastructure.

Finally, note that the “Infra Node ON Reference” is a type of Infra Node ON that can emulate each of the other “Infra Node ON” node types. I.e. Infra Node ON Reference can realize a reference implementation for the Infra Node ON Data Centre, for the Infra Node ON Enhanced and for the Infra Node ON Standard.

The view in Figure 3-6 below shows the decomposition of the generic NATO CIS Node. This view shows that a CIS Nodes is made up of a NATO CIS User Node, a NATO Infrastructure Node, a NATO Communications Access Node (context only, not in scope of ITM) and a NATO Transport Node (context only, not in scope of ITM). Referring back to the statement that an RN is not equipped with an Infra Node, the view in Figure 3-6 below is generic. In the case of the RN, the Infra Node ON is a "null building block" (i.e. is empty).

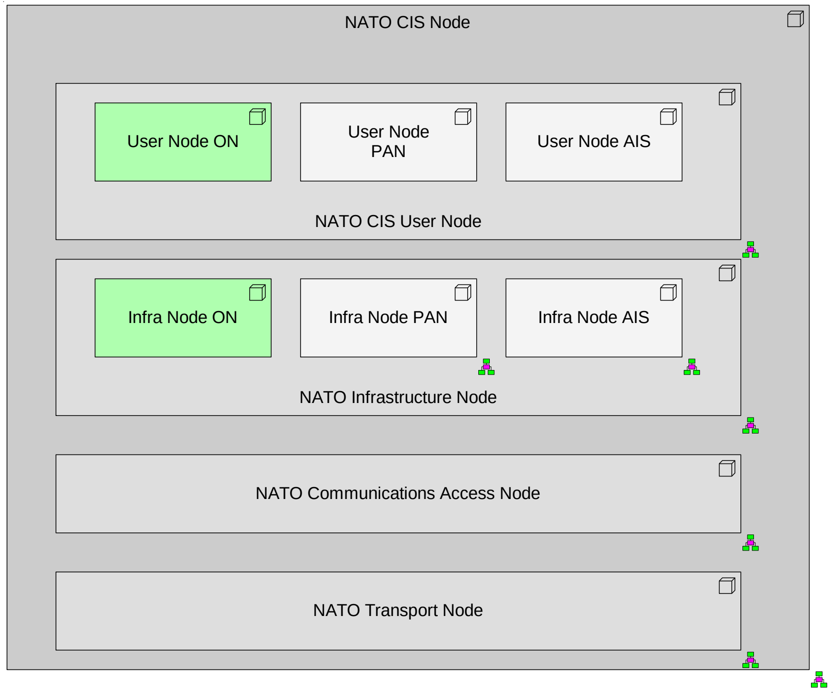


Figure 3-6 The NATO CIS Node Decomposition

When reviewing the diagram above, note that the grey nodes not in scope of ITM Recovery Incr. 1 but included to provide context.

Figure 3-7 below shows the sites in scope of ITM Recovery Increment 1. Sites are grouped by type, which are:

- Data Centre Site,
- Enhanced Node Site,
  Standard Node Site,
- Remote Node Site,
- ESOC Site and
- Reference Environment Site.

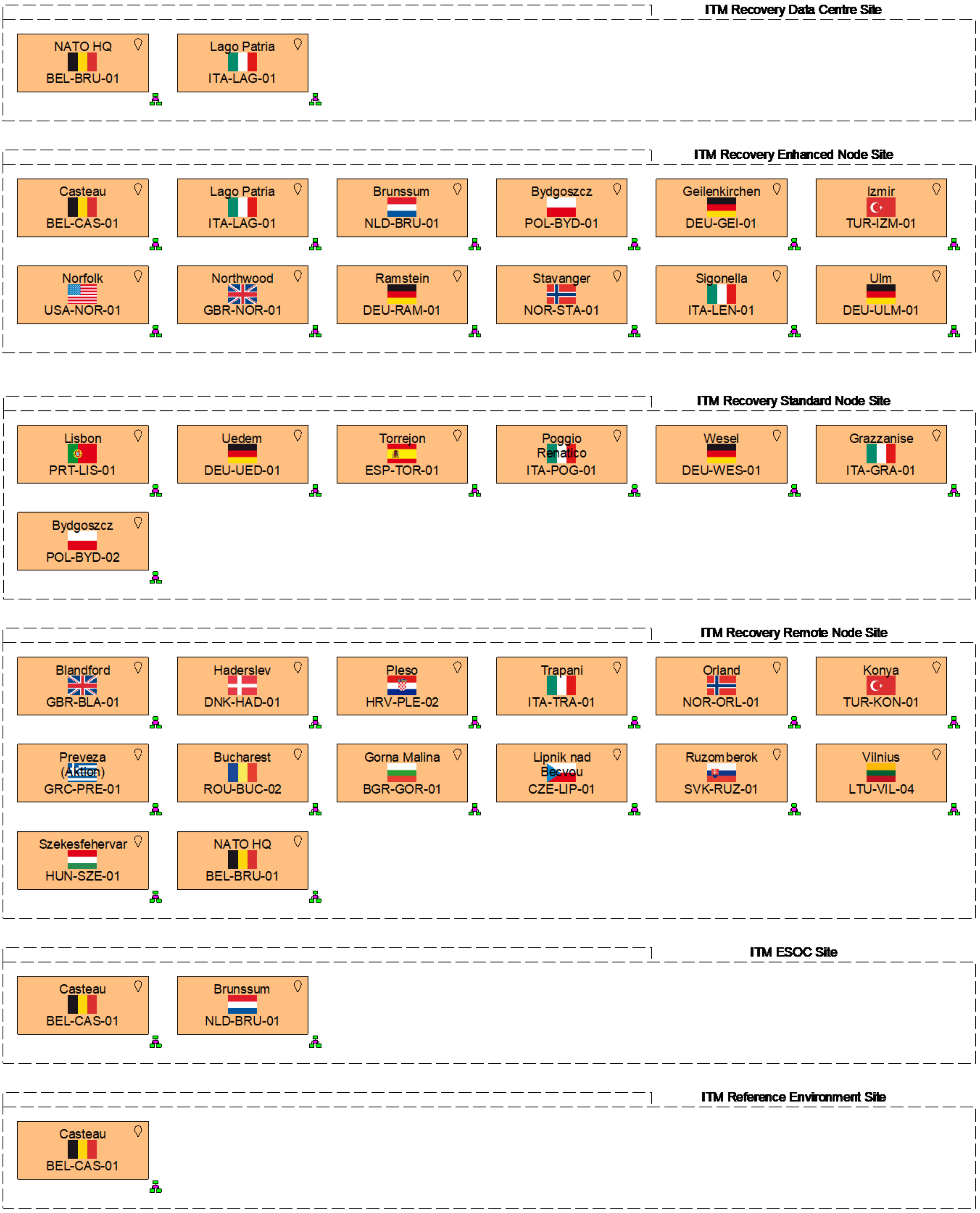


Figure 3-7 Sites where ITM Recovery Increment 1 realizes NATO ON services

When reviewing the groupings of sites in the diagram above, note that ITA-LAG-01 is included in the Data Centre Site group and in the Enhanced Node Site group. Technically the Infra Nodes in both sites are aggregated within the Infra Node ON Data Centre (and therefore hosted in the same site).

This is so because there is very limited benefit in establishing an Infra Node ON Enhanced separate from the DC and in the same location (especially in the same facility/room). However, strictly considering the performance and resiliency, for the users at these sites the resemblance to a Remote Node is high. That means that the infrastructure availability levels are equal to those of an Enhanced Node. In the hypothetical case where the DC would be relocated to another site, while the user community remains, the Enhanced Node functionality would reside on-site at ITA-LAG-01.

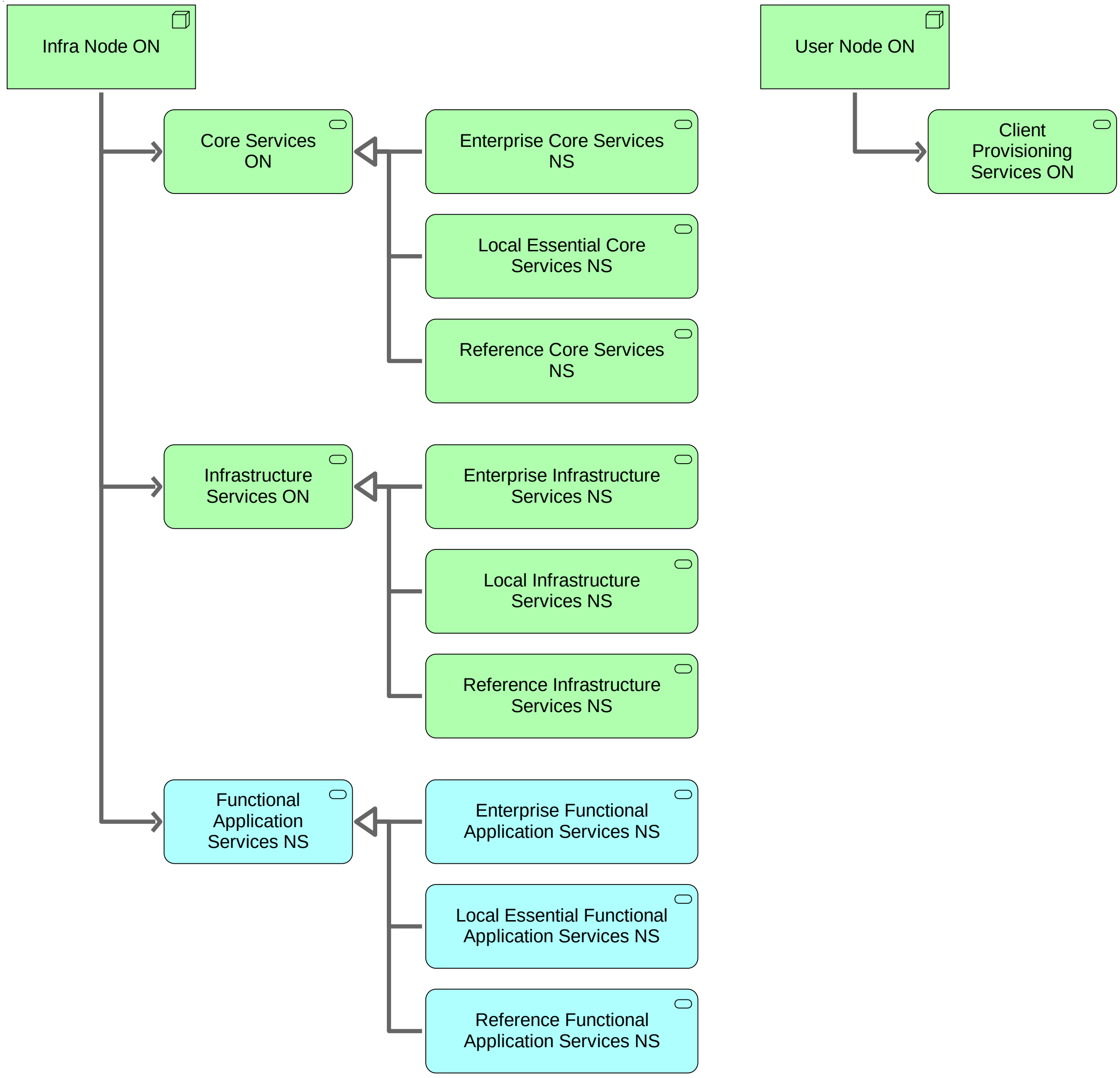

Infra Node ON
User Node ON
Core Services ON
Enterprise Core Services NS
Local Essential Core Services NS
Reference Core Services NS
Client Provisioning Services ON
Infrastructure Services ON
Enterprise Infrastructure Services NS
Local Infrastructure Services NS
Reference Infrastructure Services NS
Functional Application Services NS
Enterprise Functional Application Services NS
Local Essential Functional Application Services NS
Reference Functional Application Services NS

Figure 3-8 Service delivery by the Infra Node ON and User Node ON

Distributing the services introduced in the Service delivery by the Infra Node ON and User Node ON view above, the view Service Hosting per Node type in Figure 3-9 below. This view shows how the decomposition of services, as introduced in Figure 3-8 above, is realized across various site and node types.

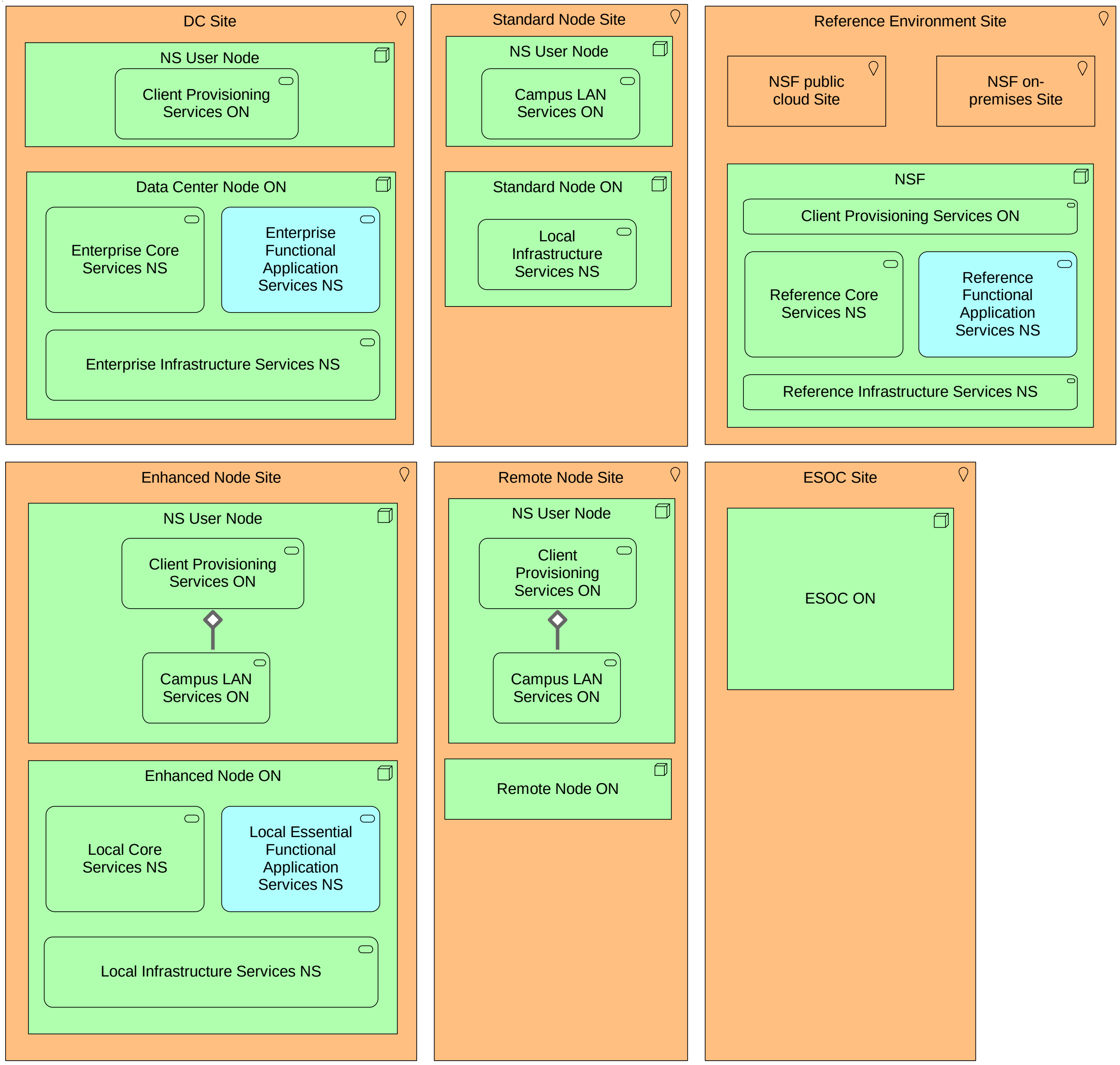

DC Site
NS User Node
Client Provisioning Services ON
Data Center Node ON
Enterprise Core Services NS
Enterprise Functional Application Services NS
Enterprise Infrastructure Services NS
Standard Node Site
NS User Node
Campus LAN Services ON
Standard Node ON
Local Infrastructure Services NS
Reference Environment Site
NSF public cloud Site
NSF on-premises Site
NSF
Client Provisioning Services ON
Reference Core Services NS
Reference Functional Application Services NS
Reference Infrastructure Services NS
Enhanced Node Site
NS User Node
Client Provisioning Services ON
Campus LAN Services ON
Enhanced Node ON
Local Core Services NS
Local Essential Functional Application Services NS
Local Infrastructure Services NS
Remote Node Site
NS User Node
Client Provisioning Services ON
Campus LAN Services ON
Remote Node ON
ESOC Site
ESOC ON

Figure 3-9 Service Hosting per Node Type

Services are provided from the DC, but where necessary for resiliency or performance reasons, local instances exist. This applies to the *Local* Infrastructure Services NS at the SN and EN, and the *Local* Core Services NS at the EN. These are instances of “edge services” serving users within the specific site, strongly integrated with the DC. Note the illustration of this hierarchy in Figure 3-10 below.

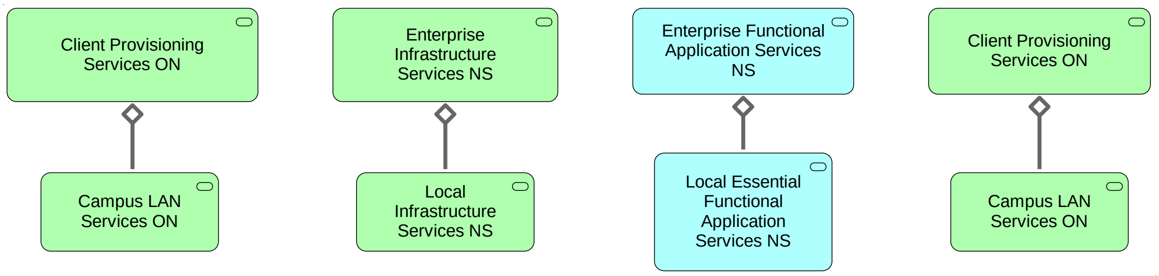

Client Provisioning Services ON
Campus LAN Services ON
Enterprise Infrastructure Services NS
Local Infrastructure Services NS
Enterprise Functional Application Services NS
Local Essential Functional Application Services NS
Client Provisioning Services ON
Campus LAN Services ON

Figure 3-10 Service Hierarchy

3.3.2. WAN Transport

The Wide Area Network (WAN) transport is realized by the NATO communication Infrastructure (NCI) (reference [41]). The diagram below introduces the part of the overall context that is most relevant for the WAN Transport perspective documented herein.

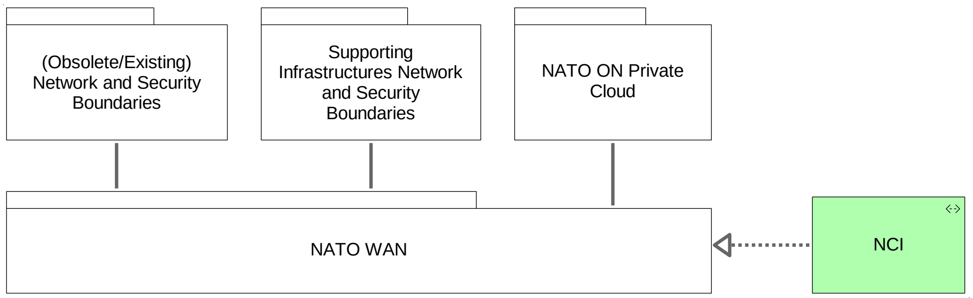

(Obsolete/Existing) Network and Security Boundaries
Supporting Infrastructures Network and Security Boundaries
NATO ON Private Cloud
NATO WAN
NCI

Figure 3-11 WAN Transport Context

Note: the NCI is not part of the ITM scope. This architecture considers the WAN as an enabling service (a dependent service) for the NATO ON services. Conversely, the Campus LAN and, where applicable to connect distant buildings hosting users served by ON Services, any extension of the Campus LAN involving cryptographic devices, is in scope of ITM.

The figures below present the connectivity of the different Enhanced, Standard and Remote nodes to the Data Centres, as provided by the NCI. All lines depicted in the diagrams correspond to Ethernet Virtual Circuits (EVC) initially operating at 1 Gbps. In the case of the NCI nodes serving the Enhanced Nodes and Standard nodes, connectivity to the NCI Core Nodes serving the Data Centres is provided with physical diversity (i.e. separate EVCs towards two Data Centres, carried over separate transmission infrastructure). Conversely, the NCI nodes serving the Remote Nodes are connected over a single EVC and transmission line. Data Centres are interconnected via high speed lines (e.g100 Gbps). Note that this capacity is shared amongst all services, with a fixed capacity share allocated to NATO ON.

All the views identify the NCI Nodes by the location identified and by the capacity of the node (NCI 40G or NCI 5G).

The figures below provide different views of the WAN topology for the Enhanced Nodes, the Standard Nodes, and the Remote Nodes.

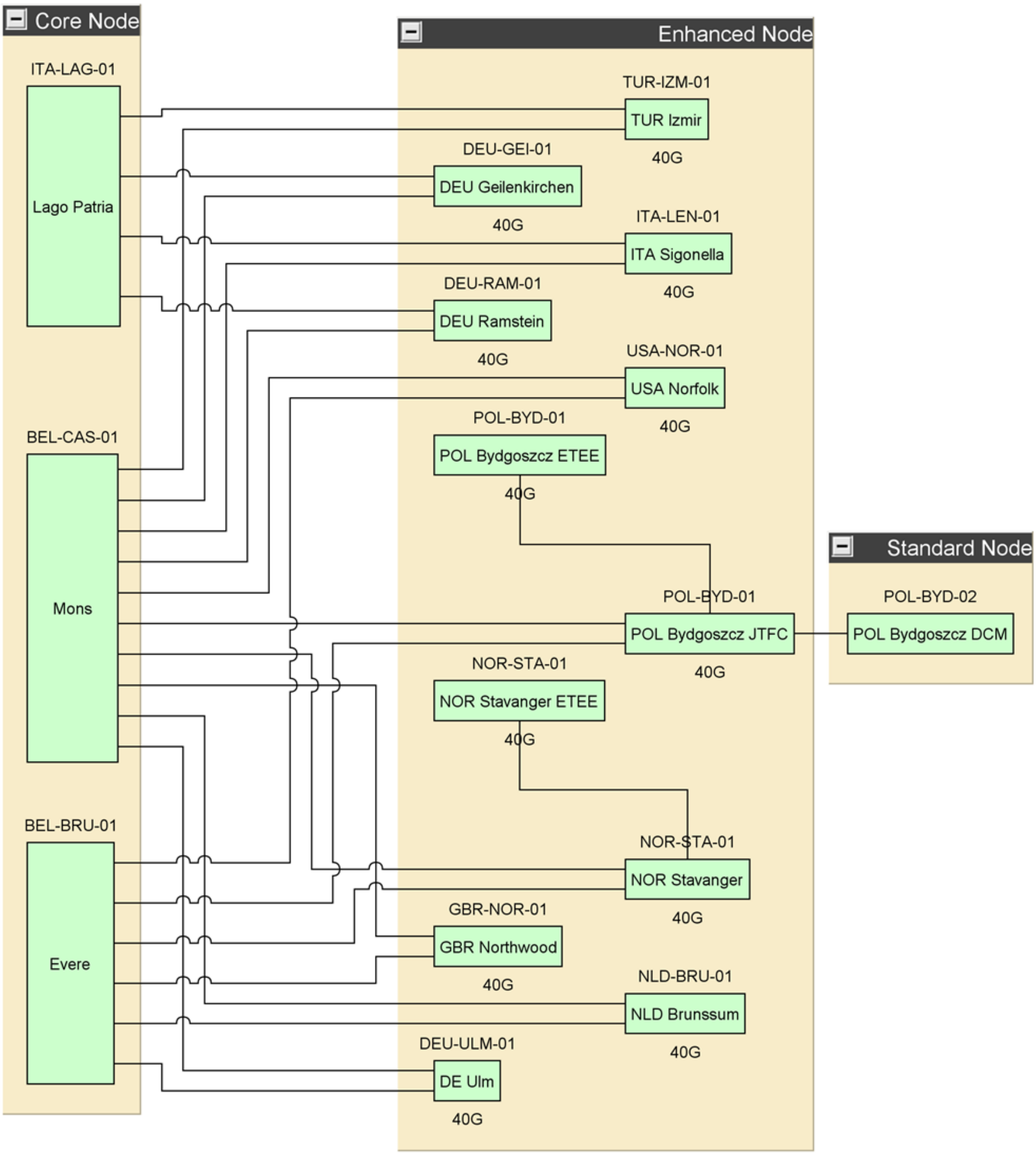


Figure 3-12 Enhanced Node WAN topology – NCI Node perspective

Note that the term “Core Node”, as used throughout this view, is introduced by the NCI architecture. The term Core Node is only relevant for the WAN transport scope.

Core Nodes refer to ITA-LAG-01, BEL-CAS-01 and BEL-BRU-01. Core Nodes are interconnected through a so-called “High Speed Core” (HSC). The Core Nodes are interconnected with 100Gbps circuits.

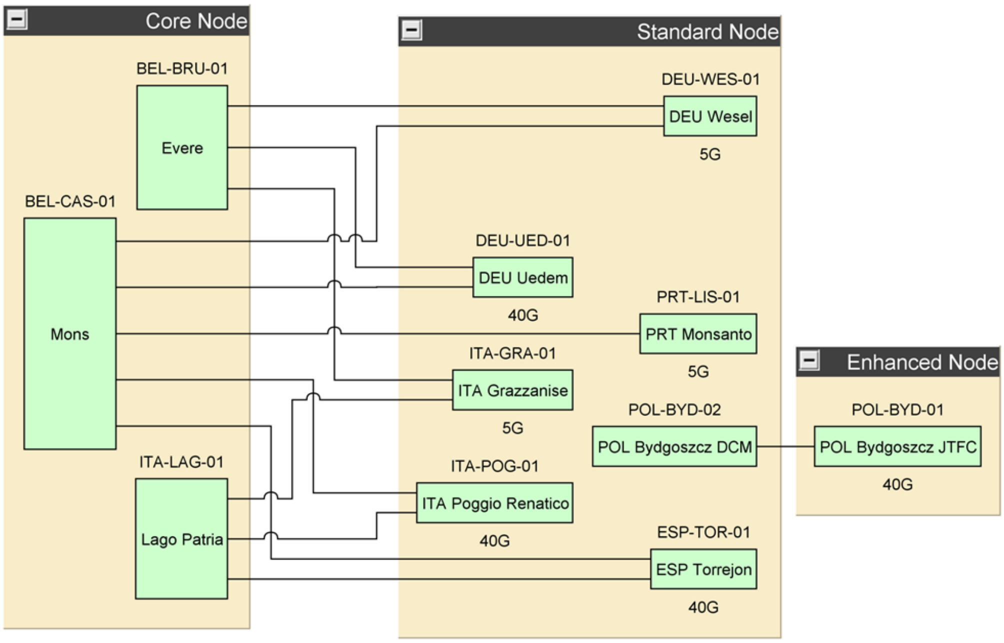


Figure 3-13 Standard Node WAN topology – NCI Node perspective

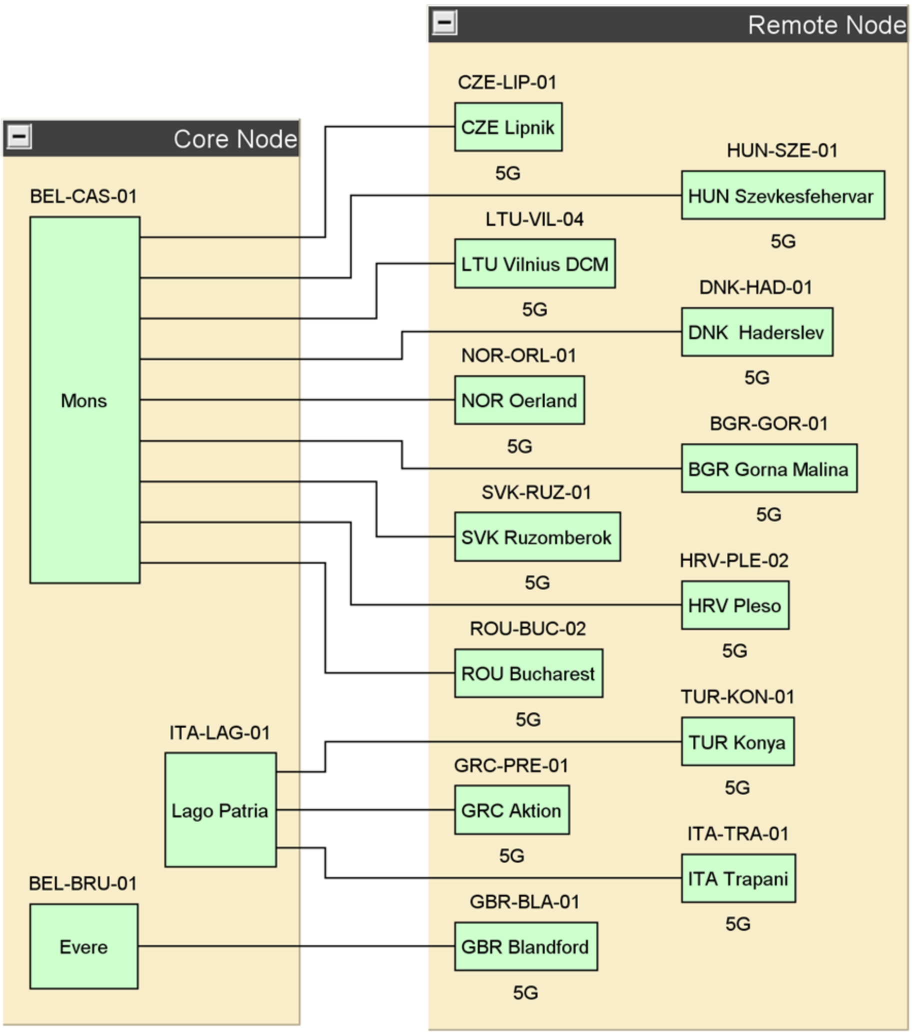


Figure 3-14 Remote Node WAN topology – NCI Node perspective

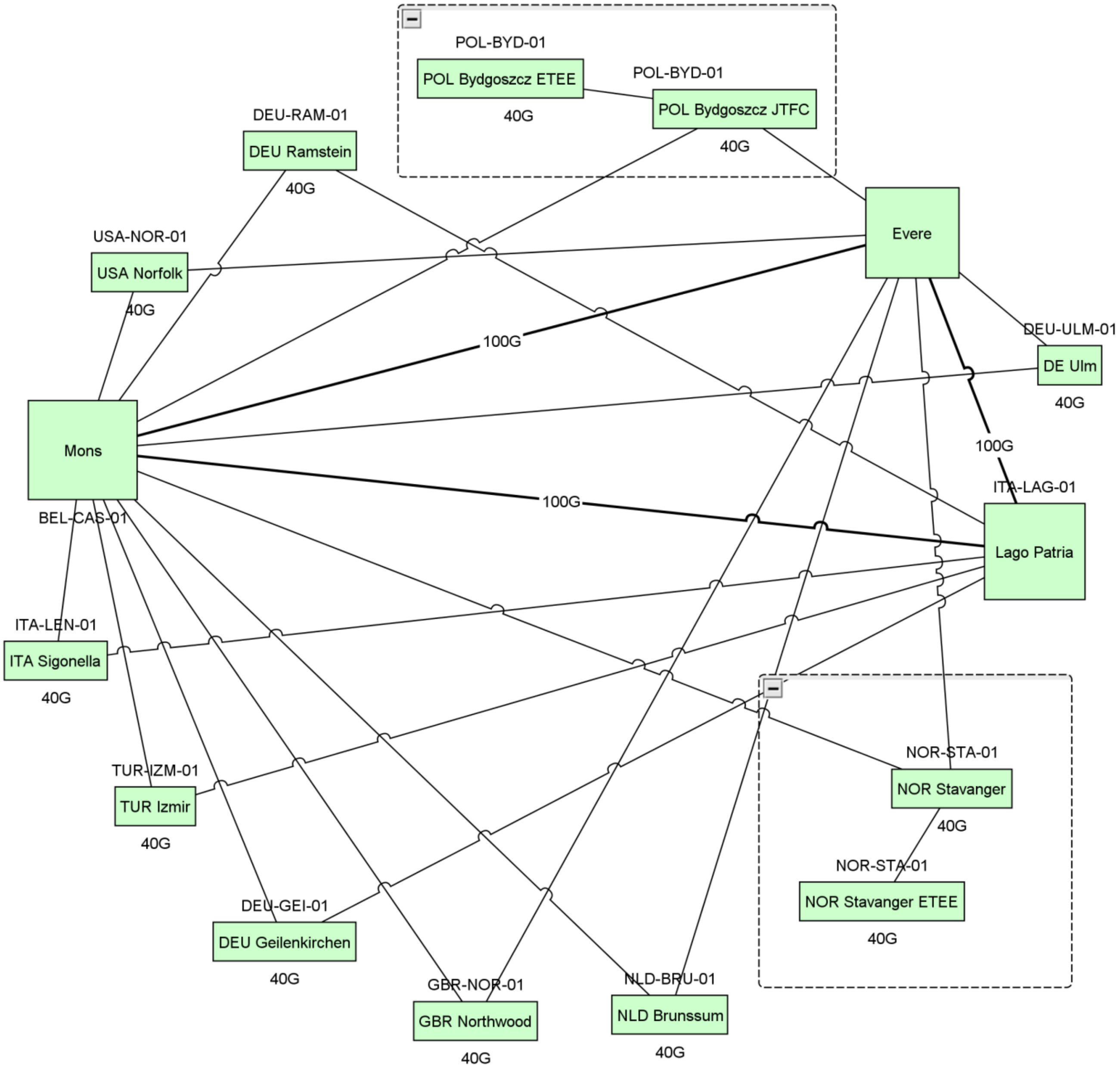


Figure 3-15 Enhanced Node network topology – Transport Perspective

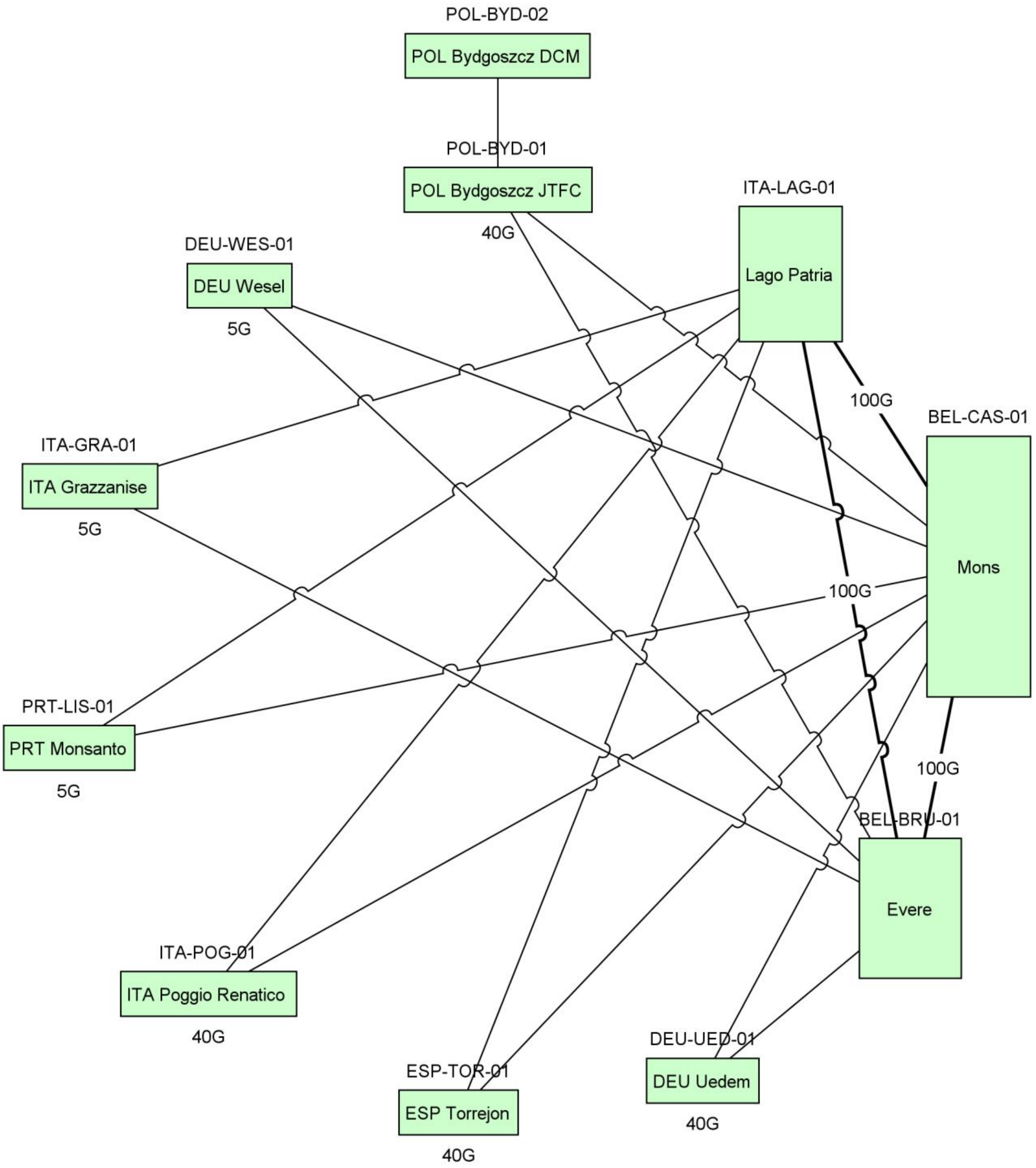


Figure 3-16 Standard Node network topology – Transport Perspective

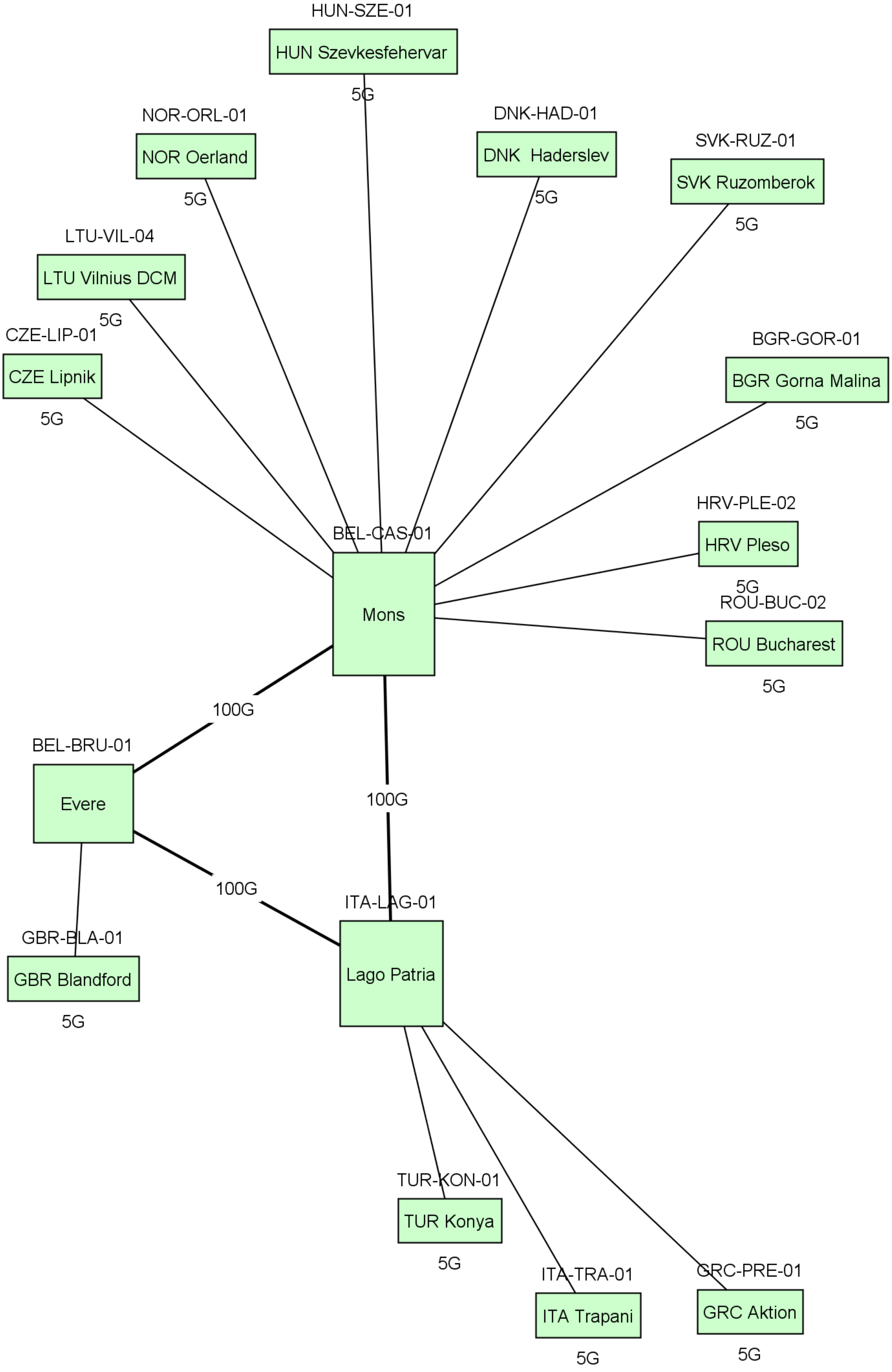


Figure 3-17 Remote Node network topology – Transport Topology Perspective

3.3.3. Infrastructure Node Network Infrastructure

he diagram below introduces the part of the overall context that is most relevant for the network infrastructure perspective documented herein.

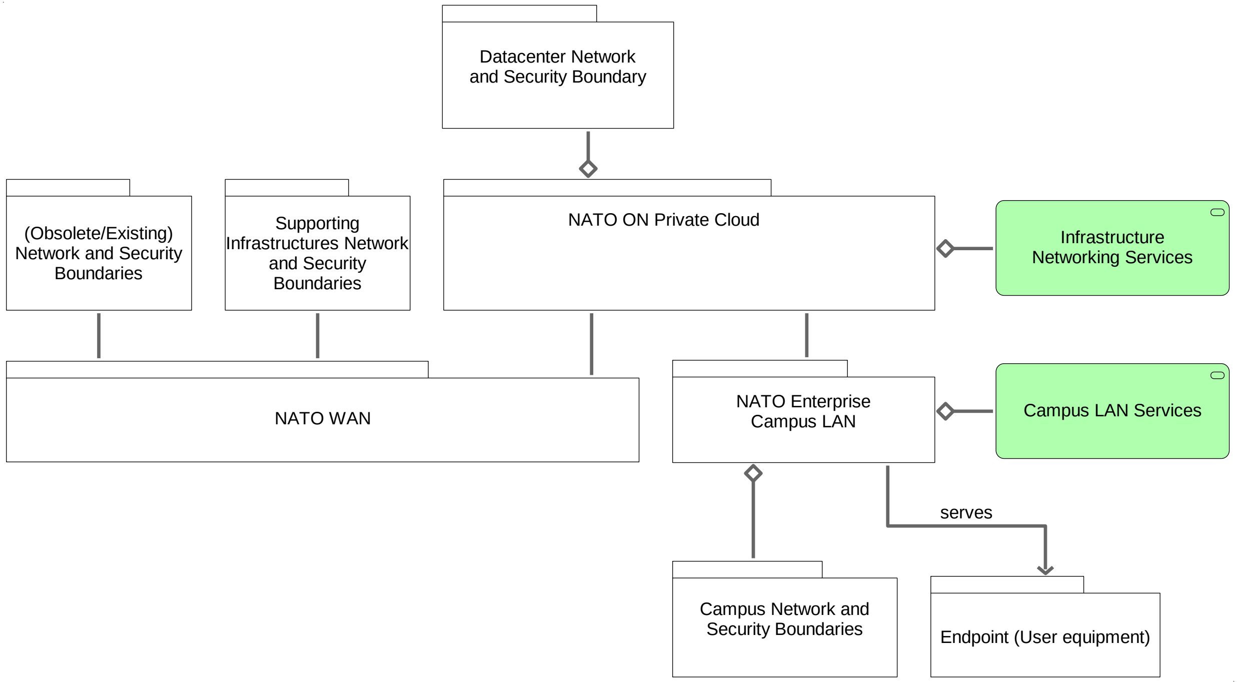

Datacenter Network and Security Boundary
(Obsolete/Existing) Network and Security Boundaries
Supporting Infrastructures Network and Security Boundaries
NATO ON Private Cloud
Infrastructure Networking Services
NATO WAN
NATO Enterprise Campus LAN
Campus LAN Services
serves
Campus Network and Security Boundaries
Endpoint (User equipment)

Figure 3-18 Network Infrastructure Context

This view depicts the network architecture for the NATO ON. This view identifies the network infrastructure building blocks present in the Data Centres, Enhanced Nodes or Standard Nodes, and Remote Nodes, with the interfaces to three distinct Coloured Clouds providing transport: NCI Coloured Cloud NS on the right, the NC V2 Coloured Cloud on the left and the DCI network (supported by the High Speed Core, HSC, as introduced in § 3.3.2) show top right, with the corresponding CCA-NS Router, the NS V2 Router and the DCI Switch.

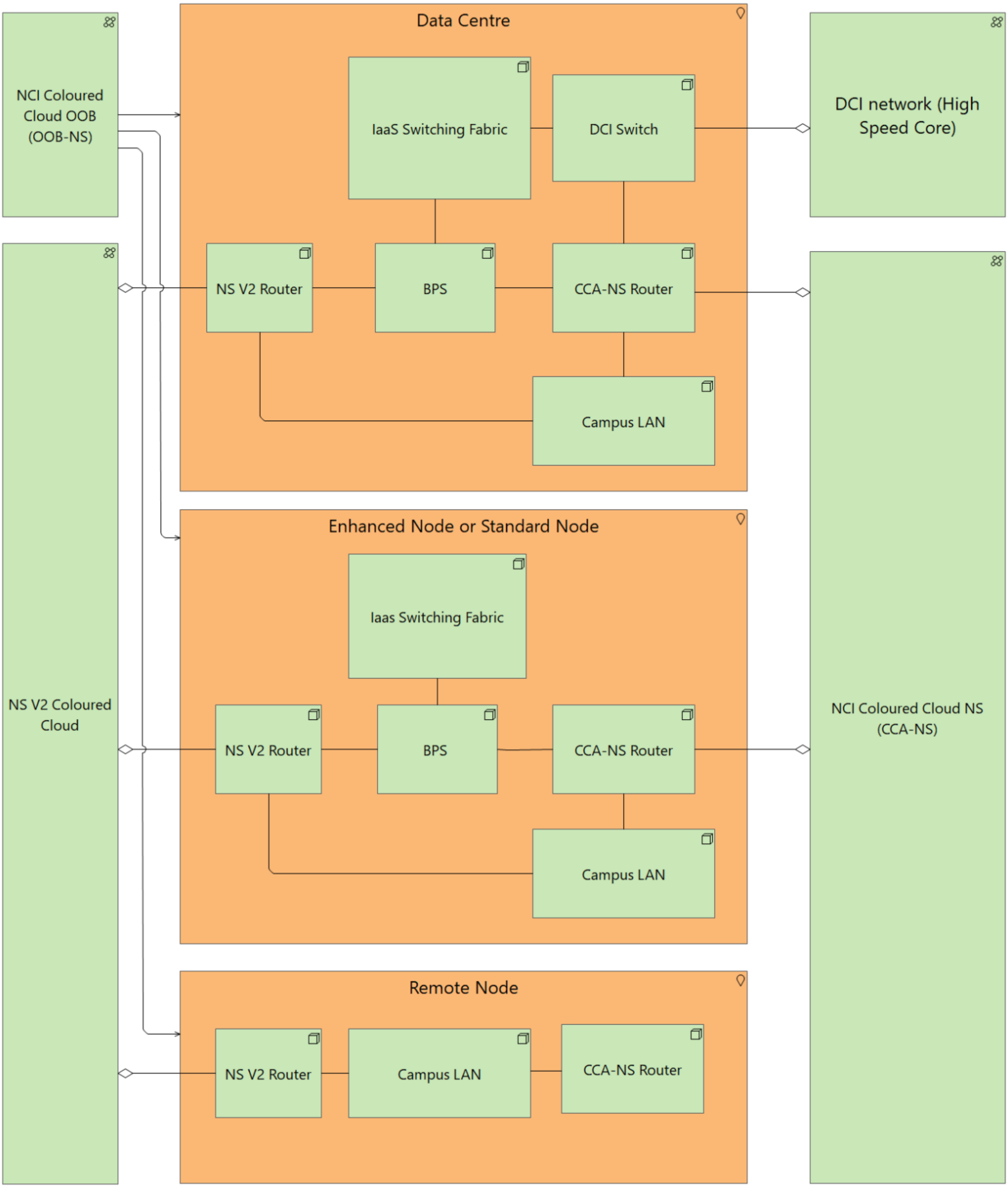


Figure 3-19 Networking Architecture of the NATO ON

The network infrastructure, identified in Figure 3-19 above, specific to NATO ON is limited to the IaaS Switching Fabric, the Client LAN infrastructure, and the BPS that provides connectivity to the Coloured Clouds supporting the WAN.

The Client LAN is another term used for the Campus LAN. It connects the user equipment (or user appliances) such as computers, VDI terminals, printers, telephones, etc.

The IaaS Switching Fabric, the Client LAN and the BPS are represented in Figure 3-20 below and further decomposed. The view in Figure 3-20, uses the perspective of the BPS, depicted at the centre of the diagram, as the "hub" that connects other building blocks and provides boundary protection appropriate for the interconnection.

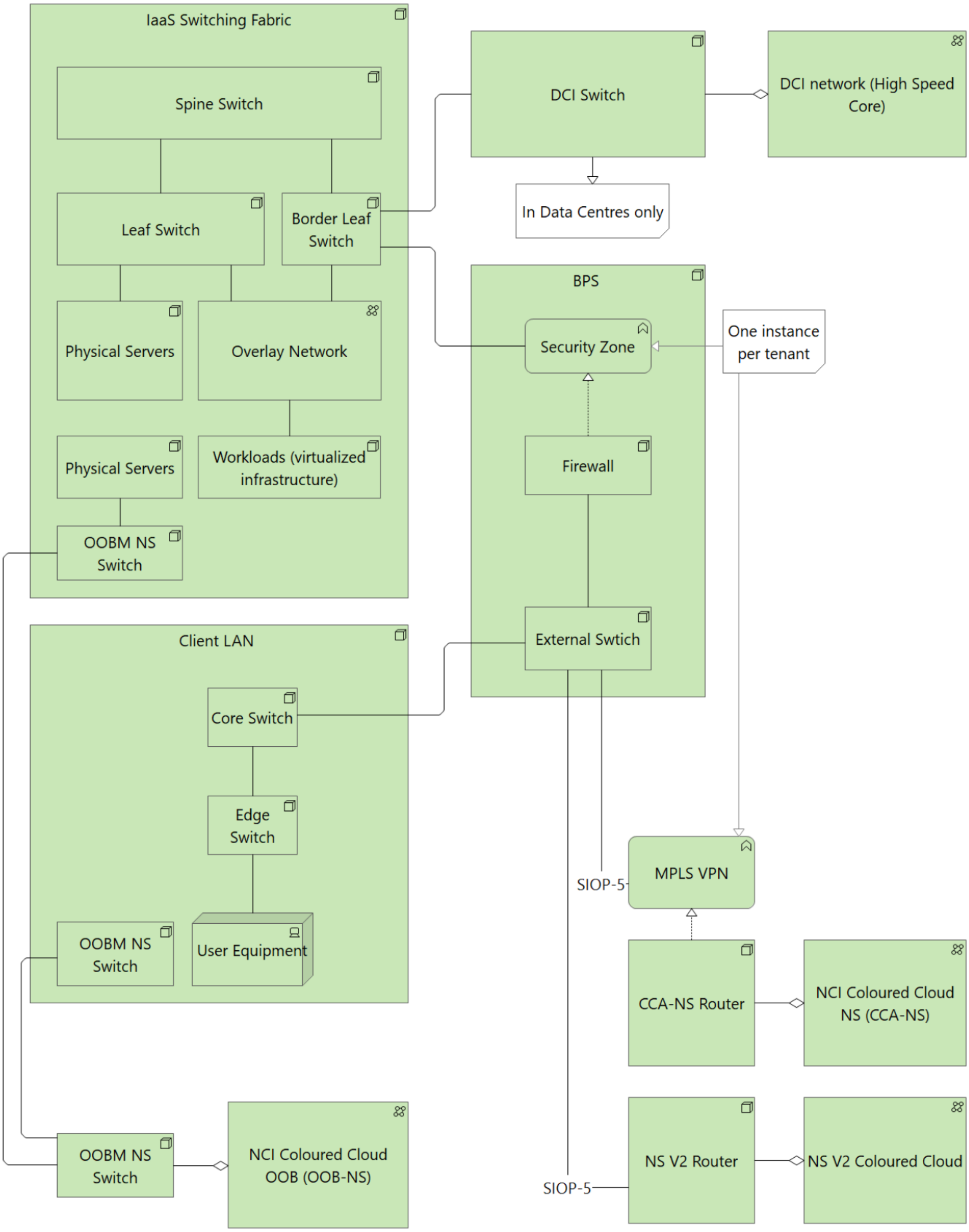


Figure 3-20 Network building blocks and their components

Figure 3-21 below provides another view if the interconnection function implemented by the BPS, and by the External Switch component in particular. The view introduces the high-level mapping between:

1) the Virtual Routing Functions (VRF) implemented on the NCI Coloured Cloud NS (using MPLS VPN)
2) the Security Zones implemented in the firewall element of the BPS building bloc
3) The Tenant Resource Clusters implemented in the IaaS, and connected through the IaaS Switching fabric (Spine/Leaf architecture).

This mapping can be further extended to different Client Virtual LANs (VLANs), implemented on the Core and Edge Switches of the Client LAN (also known as Campus LAN).

This mapping is essential to understand the cross security zone networking architecture, described under para. 3.3.3.4.

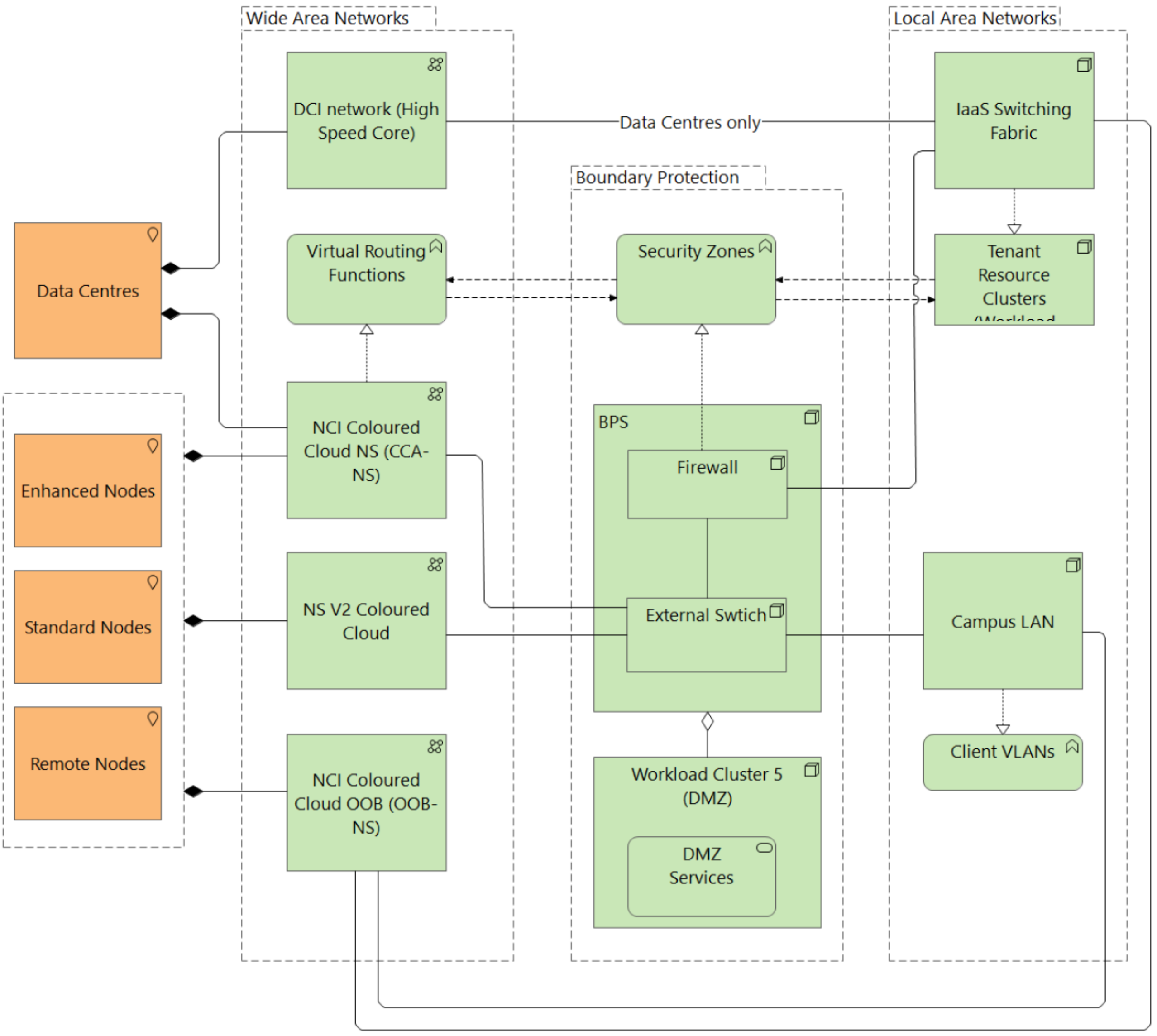


Figure 3-21 BPS in context

The following paragraphs describe each of the three buildings blocks of the NATO ON Network Infrastructure, introducing their components, interfaces, and the different logical instances implemented within.

3.3.3.1. IaaS Switching Fabric

The figure below depicts the components that make the IaaS Switching Fabric building blocks. The IaaS Switching Fabric exists at the DC, the EN and the SN, at different scales and levels of resiliency.

The IaaS Switching Fabric provides the network connectivity to the multiple clusters existing within the IaaS (Tenant Resource Clusters in the diagram). It further provides connectivity to the Data Centre Interconnection, and to the WAN with all its Coloured Clouds, via the BPS.

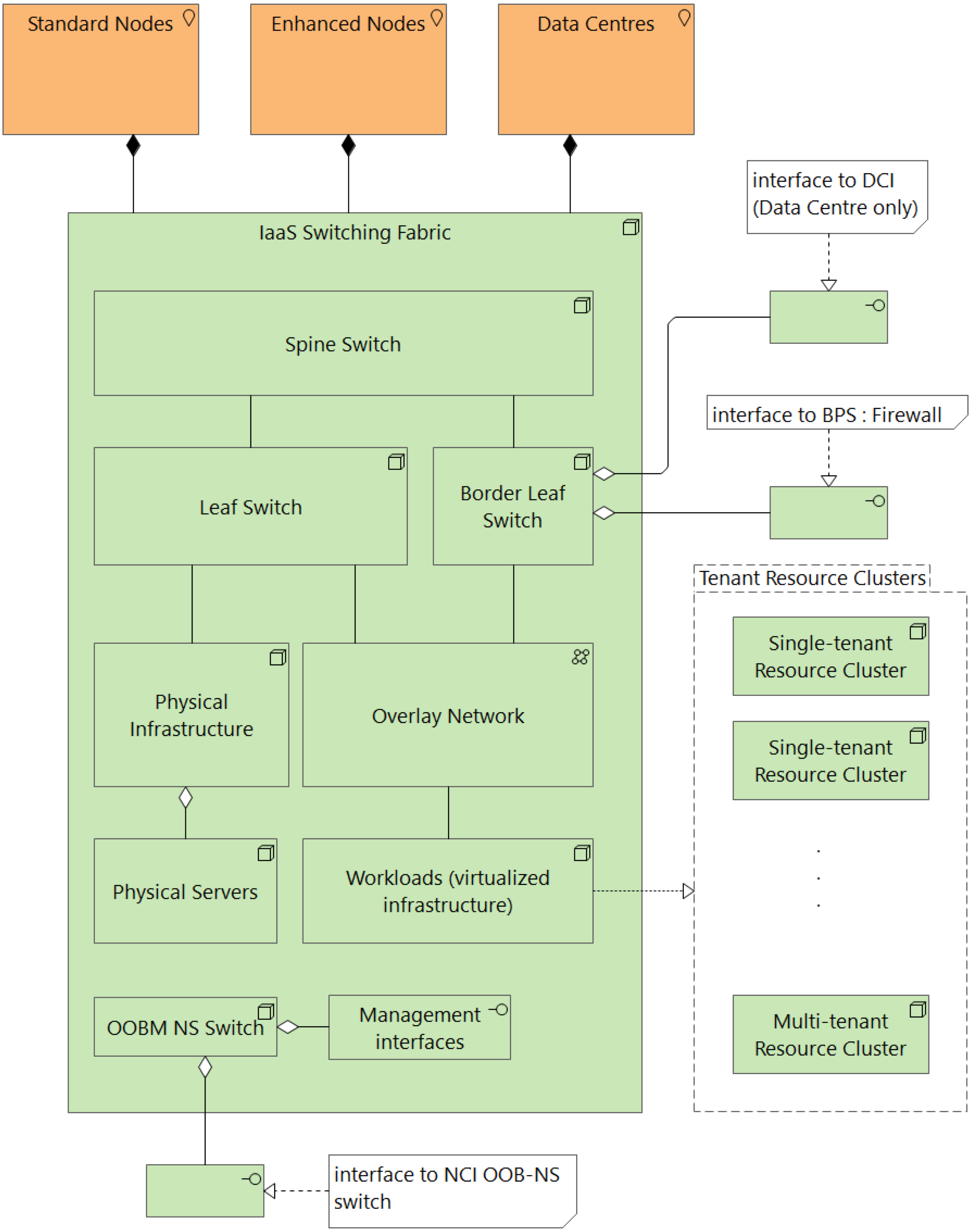

Standard Nodes
Enhanced Nodes
Data Centres
interface to DCI (Data Centre only)
IaaS Switching Fabric
Spine Switch
interface to BPS : Firewall
Leaf Switch
Border Leaf Switch
Tenant Resource Clusters
Single-tenant Resource Cluster
Single-tenant Resource Cluster
Physical Infrastructure
Overlay Network
Physical Servers
Workloads (virtualized infrastructure)
Multi-tenant Resource Cluster
OOBM NS Switch
Management interfaces
interface to NCI OOB-NS switch

Figure 3-22 IaaS Switching Fabric

3.3.3.2. Boundary Protection Services

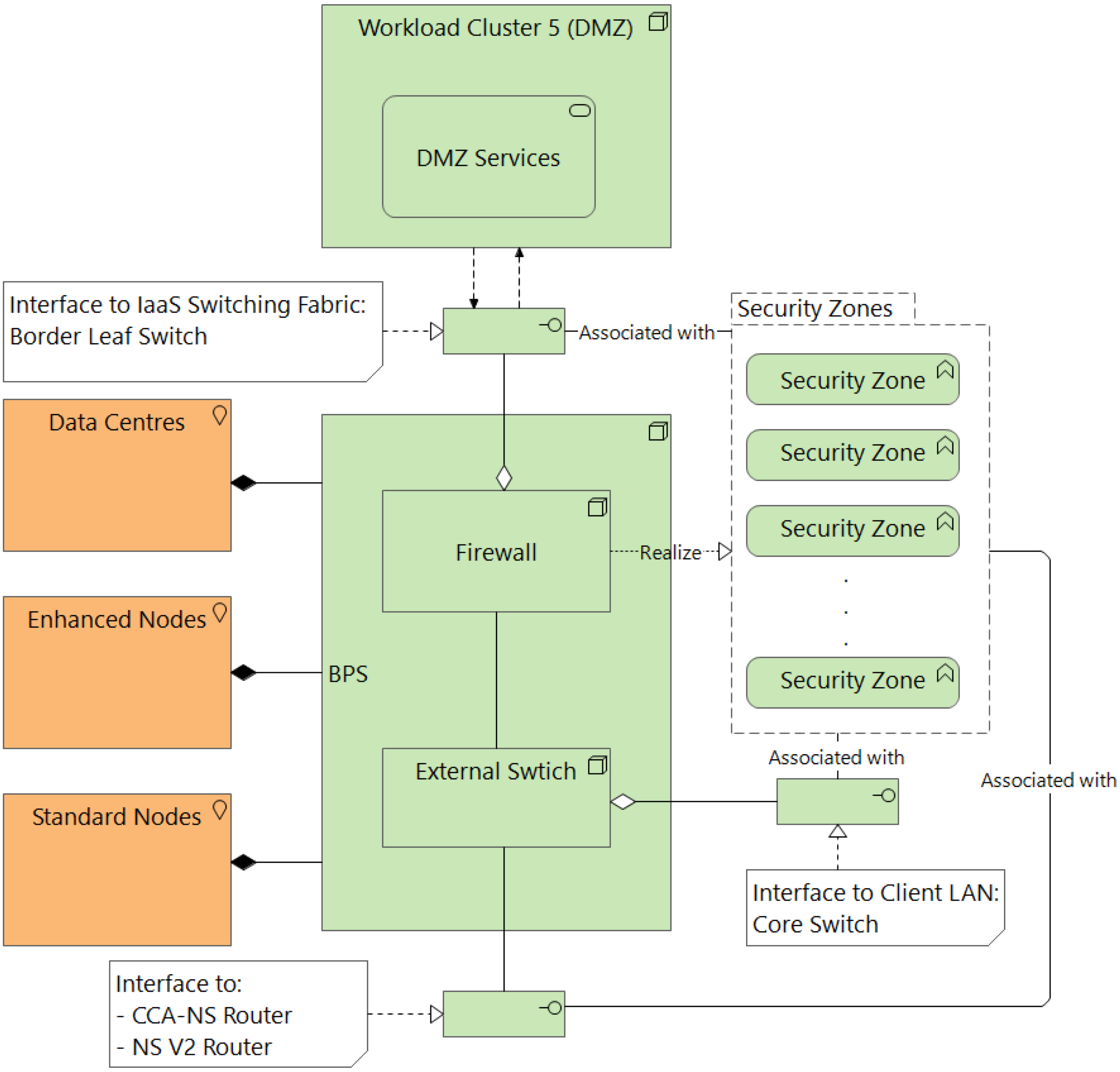


Figure 3-23 Boundary Protection Services

This view (Figure 3-24 below) describes the BPS-1; this view decomposes the BPS-1 node, into a Firewall node and External Switch. This view shows a Workload Cluster realizing the DMZ Services, and describes how the BPS-1 realizes the various security zones at the DC, EN and SN; and how these are interconnected through the BPS-1. The BPS-1 realizes security zones across / between the IaaS Switching Fabric, Workload Cluster 5 (DMZ), across the LAN and Across the CCA-NS Router and NS V2 Router.

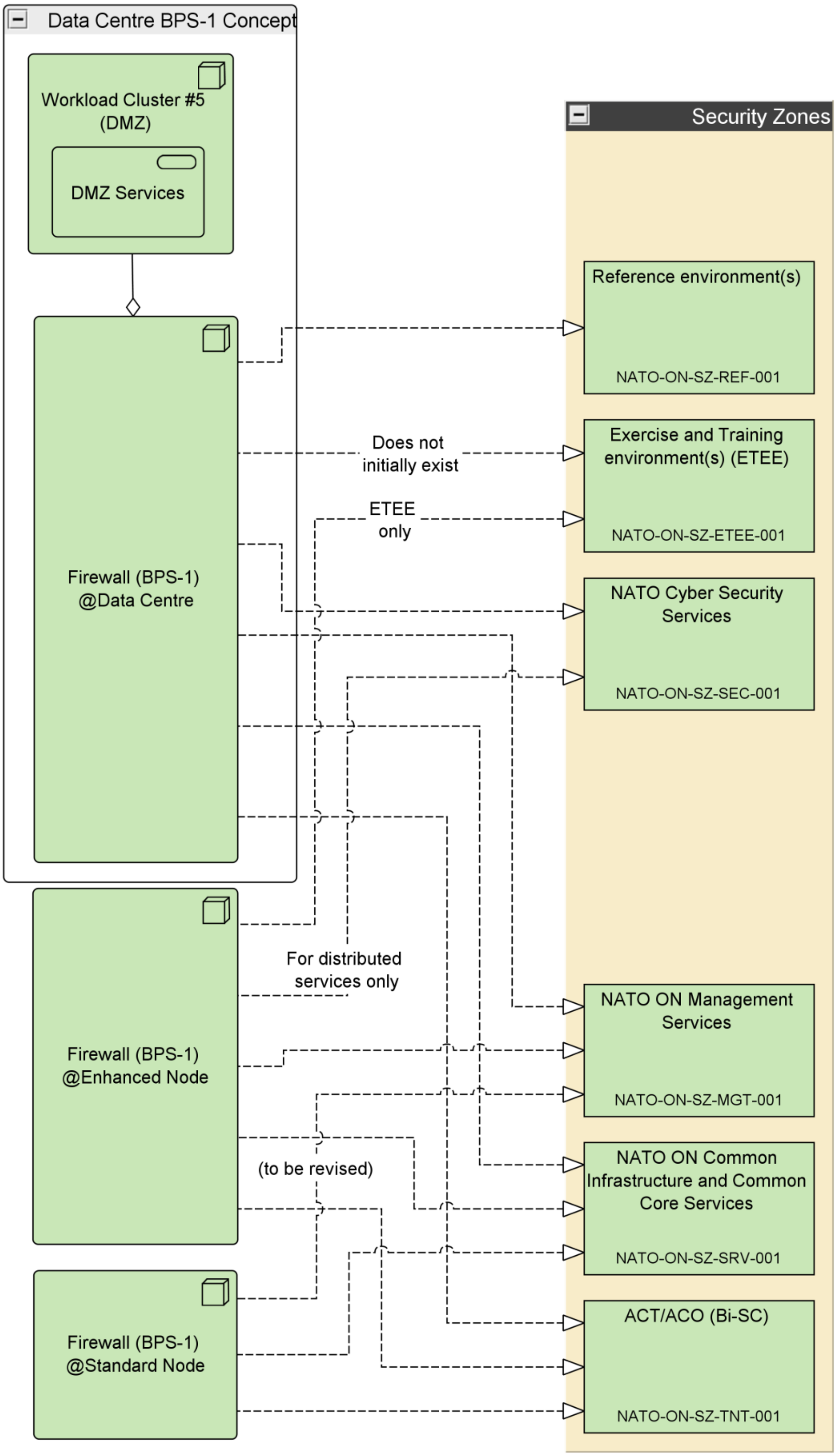

Data Centre BPS-1 Concept
Workload Cluster #5 (DMZ)
DMZ Services
Firewall (BPS-1) @Data Centre
Firewall (BPS-1) @Enhanced Node
Firewall (BPS-1) @Standard Node
Does not initially exist
ETEE only
For distributed services only
(to be revised)
Security Zones
Reference environment(s)
NATO-ON-SZ-REF-001
Exercise and Training environment(s) (ETEE)
NATO-ON-SZ-ETEE-001
NATO Cyber Security Services
NATO-ON-SZ-SEC-001
NATO ON Management Services
NATO-ON-SZ-MGT-001
NATO ON Common Infrastructure and Common Core Services
NATO-ON-SZ-SRV-001
ACT/ACO (Bi-SC)
NATO-ON-SZ-TNT-001

Figure 3-24 BPS-1 realizing and interconnecting security zones

The DMZ, which is implemented through Workload Cluster 5, is further described in Figure 3-25 below. The DMZ has common components that are present in every security zone and includes a number of specific components for specific security zones.

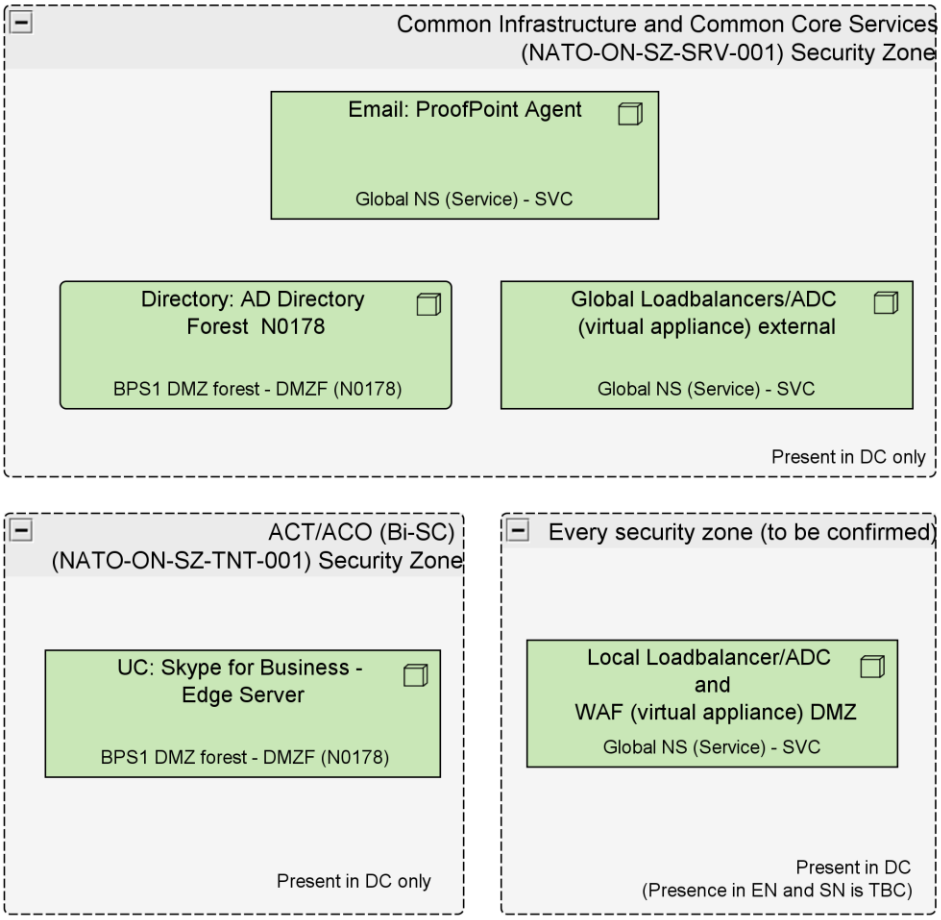

Common Infrastructure and Common Core Services
(NATO-ON-SZ-SRV-001) Security Zone
Email: ProofPoint Agent
Global NS (Service) - SVC
Directory: AD Directory Forest N0178
BPS1 DMZ forest - DMZF (N0178)
Global Loadbalancers/ADC (virtual appliance) external
Global NS (Service) - SVC
Present in DC only
ACT/ACO (Bi-SC)
(NATO-ON-SZ-TNT-001) Security Zone
UC: Skype for Business - Edge Server
BPS1 DMZ forest - DMZF (N0178)
Present in DC only
Every security zone (to be confirmed)
Local Loadbalancer/ADC and WAF (virtual appliance) DMZ
Global NS (Service) - SVC
Present in DC
(Presence in EN and SN is TBC)

Figure 3-25 DMZ (Workload Cluster 5) Components and their Security Zones

3.3.3.3. Campus LAN

This view in Figure 3-26 shows the Campus LAN, or the Client LAN components and interfaces. Less differences in scaling, capacity and resiliency, this architecture building block exists at the DC, the EN, the SN and RN Nodes.

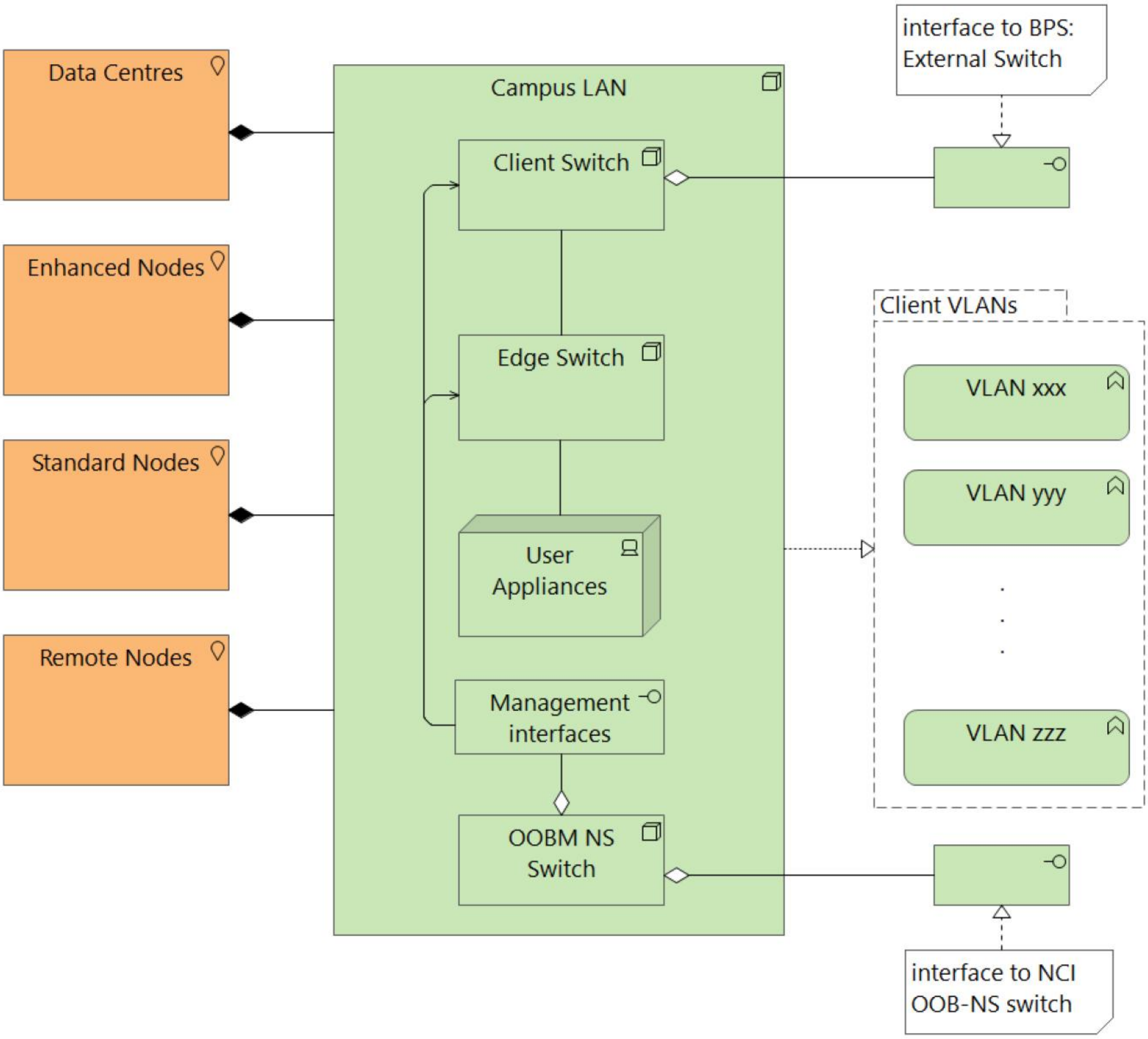


Figure 3-26 Client LAN components and interfaces

3.3.3.4. Cross Security Zone Networking

This view describes the CIS Segment networking architecture. In this context, a CIS Segment is equal to a Security Zone, including all systems within it. This view shows the routing and network-level boundary protection between CIS Segments, resource clusters, tenants and Coloured Clouds (CC), all at NS level. Figure 3-27 takes a high-level viewpoint while Figure 3-28 considers end-to-end networking.

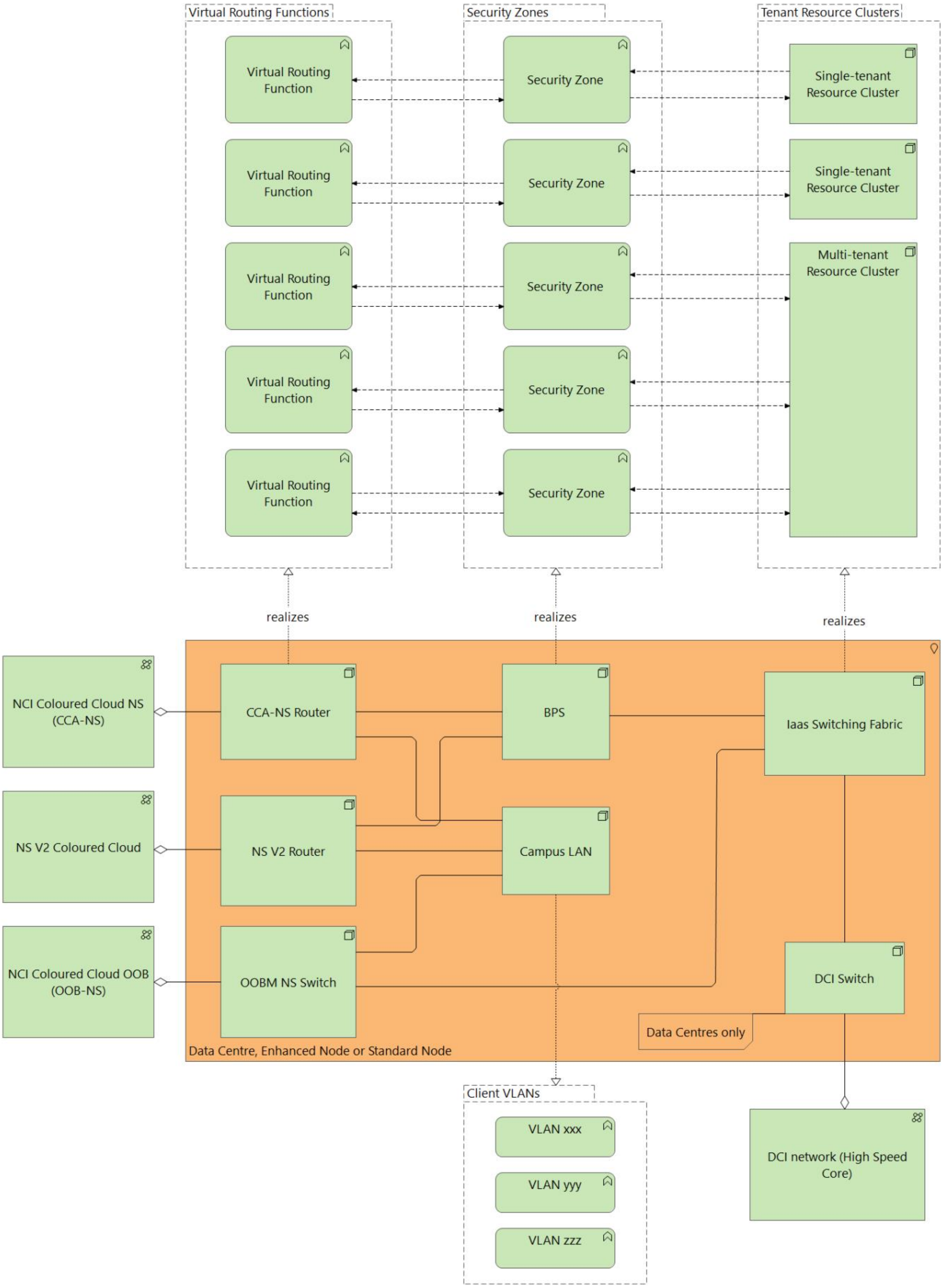


Figure 3-27 High-level NS cross security zone networking architecture

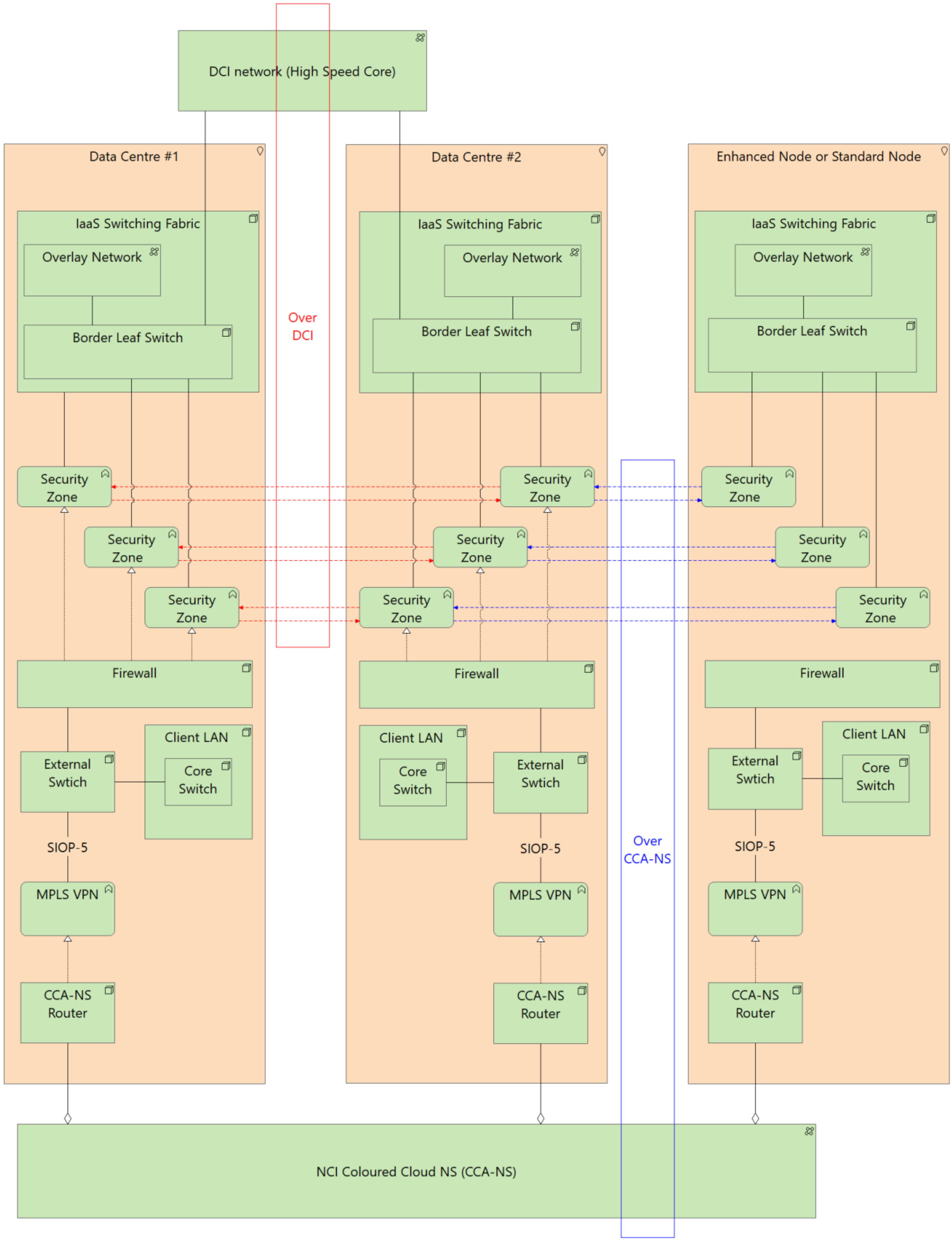


Figure 3-28 End-to-end networking diagram

3.3.3.5. Routing

The view below describes the routing between the EN and SN on one side and the DC on the other.

Note the SIOP5, which is the interface between the NCI (NATO Communications Access Node) on one side and the Enhanced Node, Standard Node and Data Centre (the various User Nodes and Infrastructure Nodes) on the other side. In other words, SIOP5 represents the interface to the WAN edge.

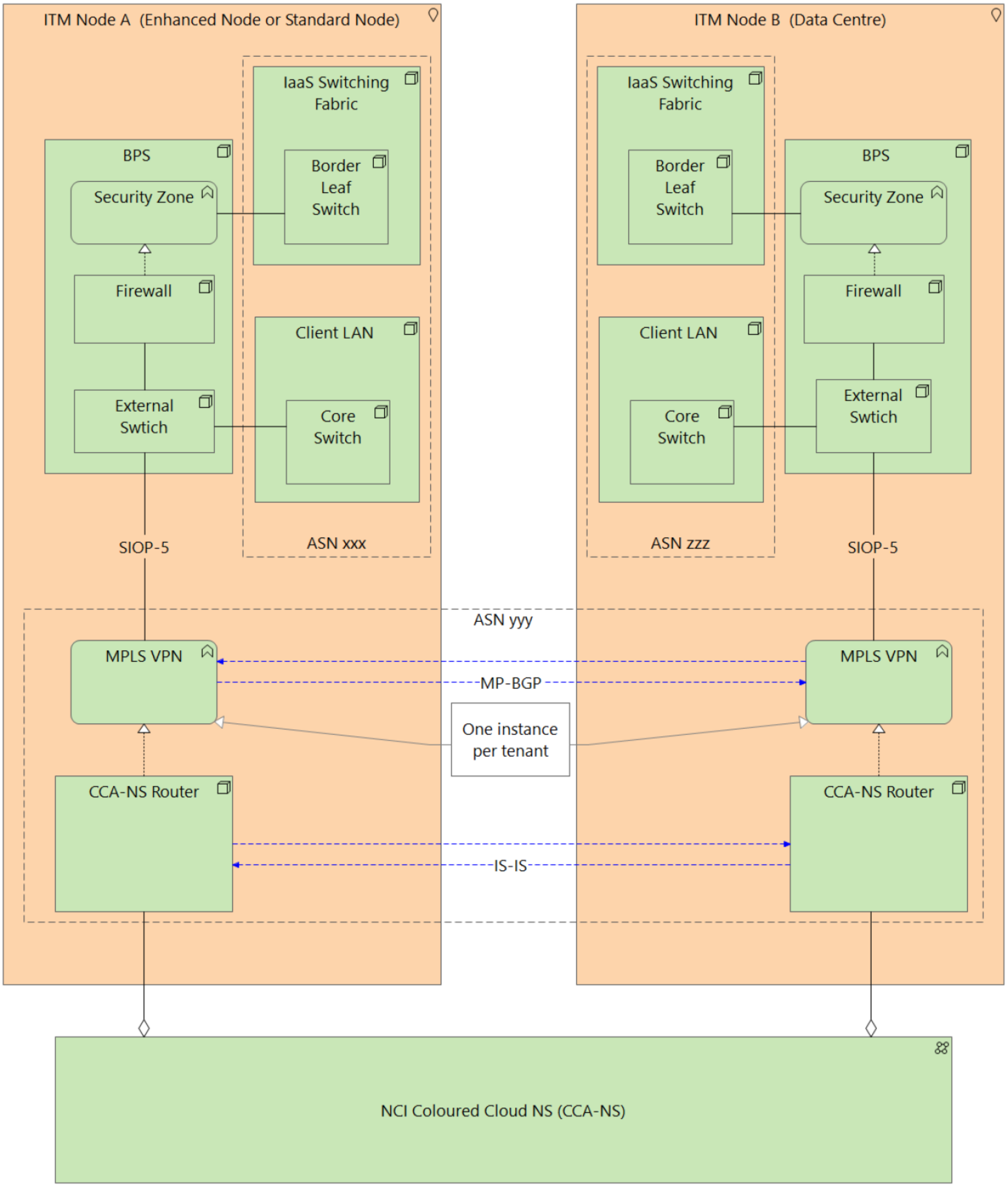


Figure 3-29 EN/SN – DC routing

The view in Figure 3-30 below describes the end-to-end networking between both DC and between the DC and an EN, RN or SN.

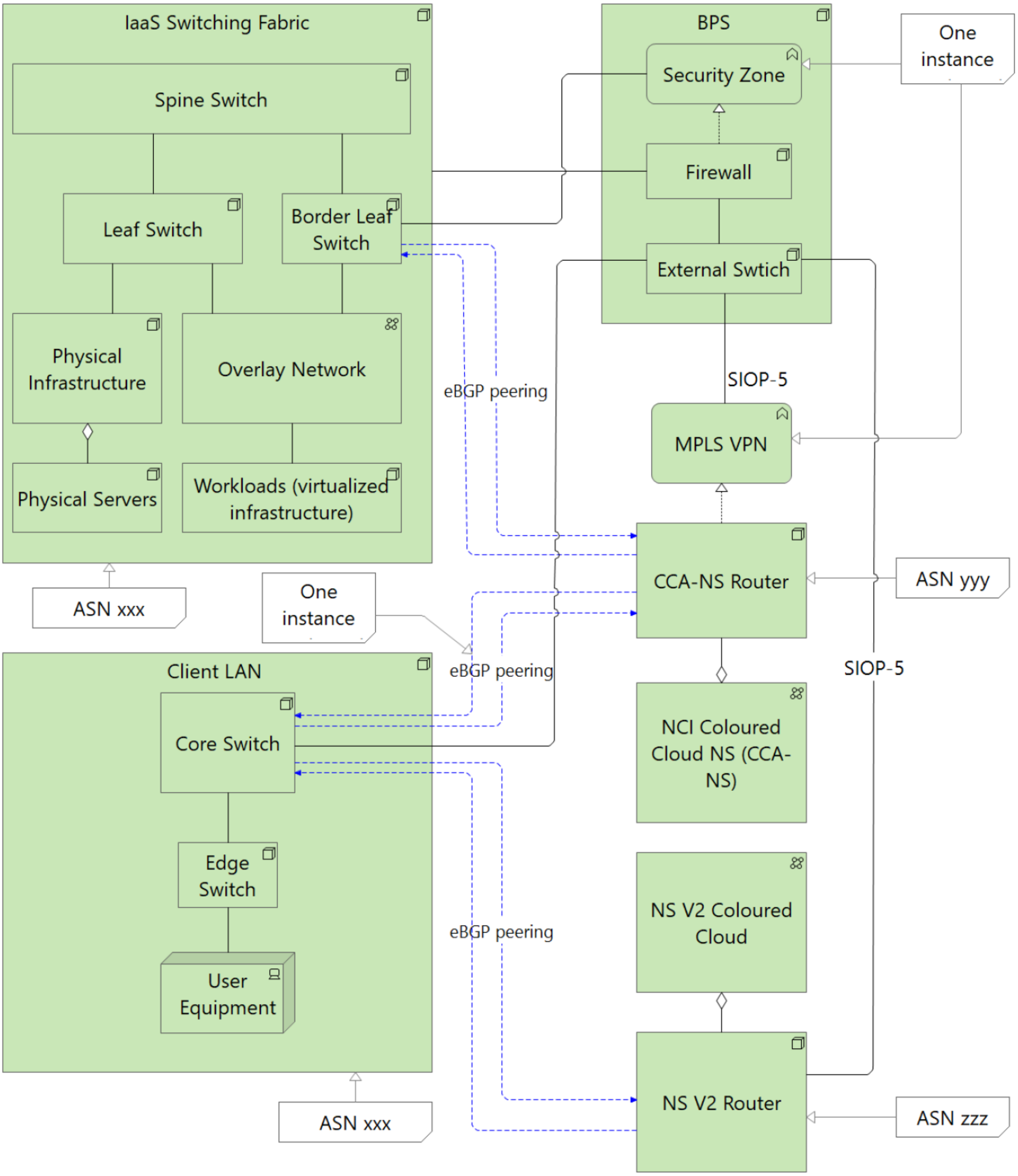


Figure 3-30 WAN-facing routing architecture

The view in Figure 3-31 describes the high-level NS cross-domain networking architecture from the IP routing perspective at a NATO CIS Node. Note the iBGP peering between the IaaS Switching Fabric and the Client LAN Core and note the routing exchange between the IaaS Switching Fabric and the BPS and the between Client LAN and the BPS (OSPF).

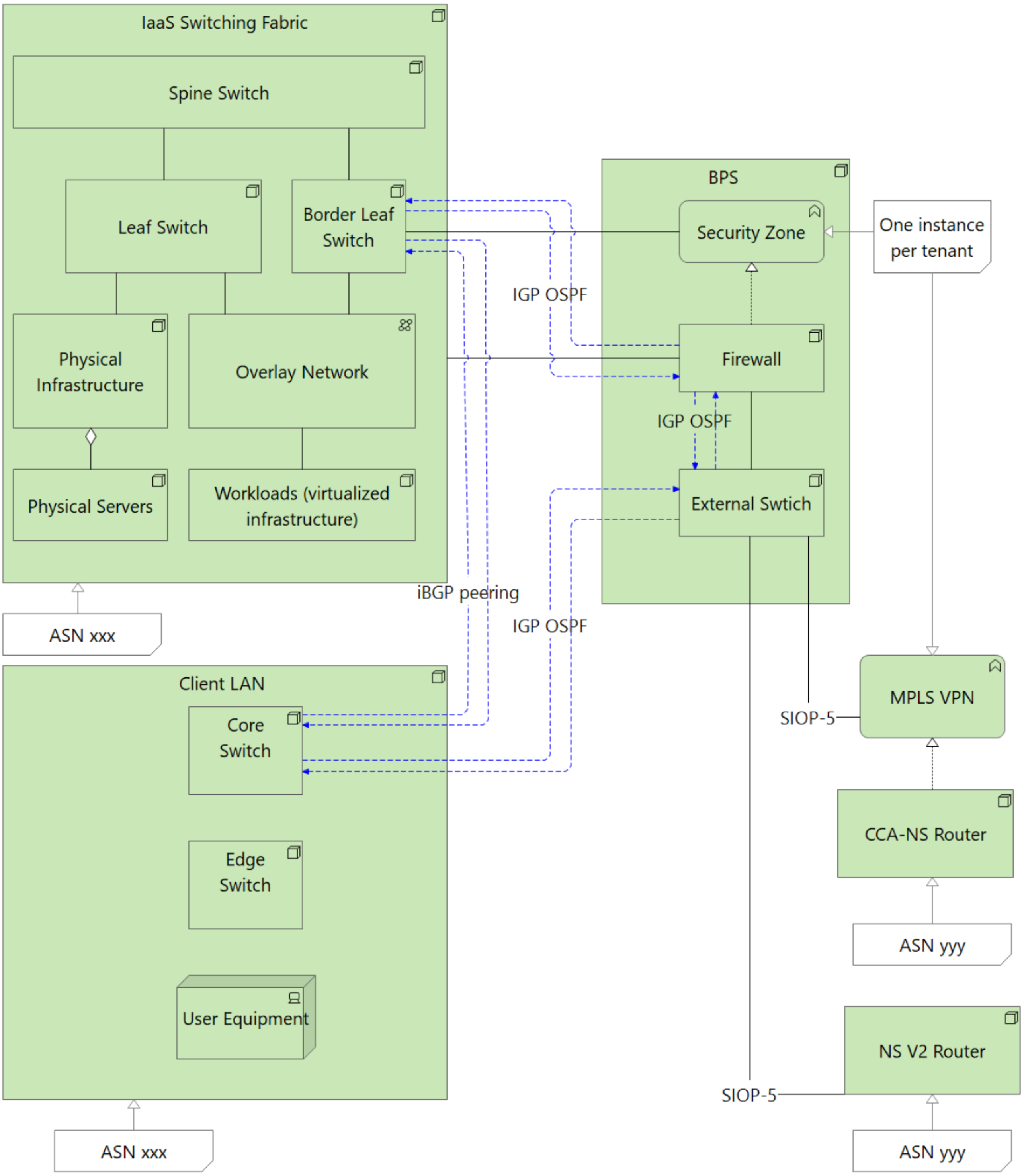


Figure 3-31 Routing architecture within a generic NATO CIS Node

3.3.4. IT Infrastructure

Paragraph 3.1 introduces the overall context in which the IT infrastructure features. The diagram below introduces the part of the overall context that is most relevant for the IT Infrastructure perspective documented herein.

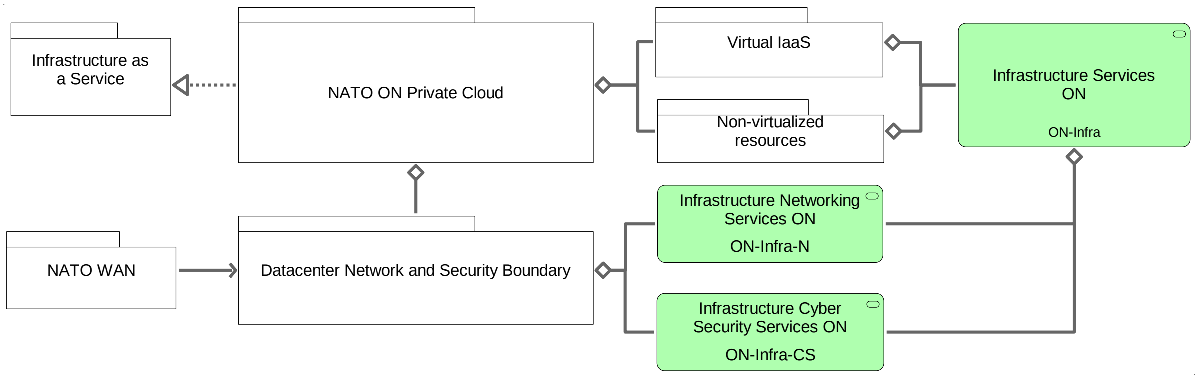

Infrastructure as a Service
NATO ON Private Cloud
Virtual IaaS
Non-virtualized resources
Infrastructure Services ON
ON-Infra
NATO WAN
Datacenter Network and Security Boundary
Infrastructure Networking Services ON
ON-Infra-N
Infrastructure Cyber Security Services ON
ON-Infra-CS

Figure 3-32 IT Infrastructure Context

This view describes the NATO Infrastructure Node, as introduced in the nodal decomposition (§ 3.3.1). Figure 3-33 identifies the IT Infrastructure components in context of the IaaS Switching Fabric as introduced earlier in the Network Infrastructure views (specifically § 3.3.3.1). The IT Infrastructure components are highlighted in darker green.

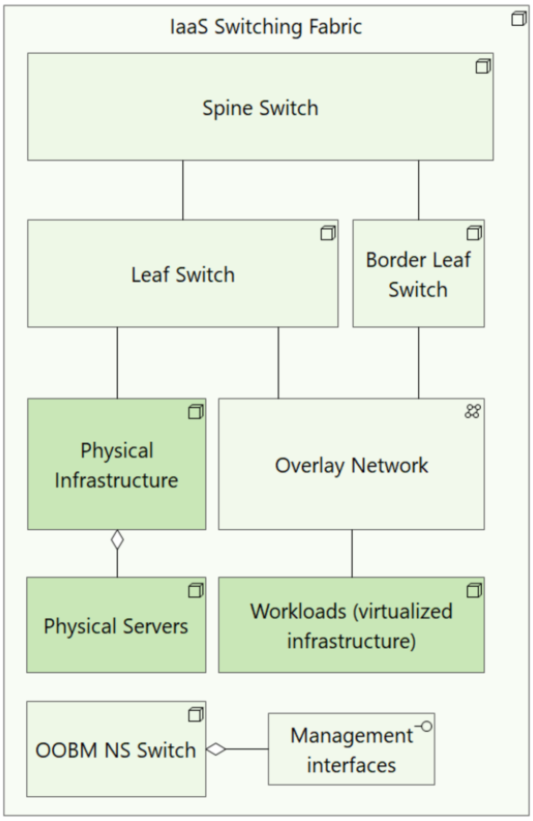


Figure 3-33 IT infrastructure decomposed and in context

The virtualized and the physical infrastructure are further described in the views below.

3.3.4.1. Virtualized Infrastructure

This view describes the virtualized IT infrastructure.

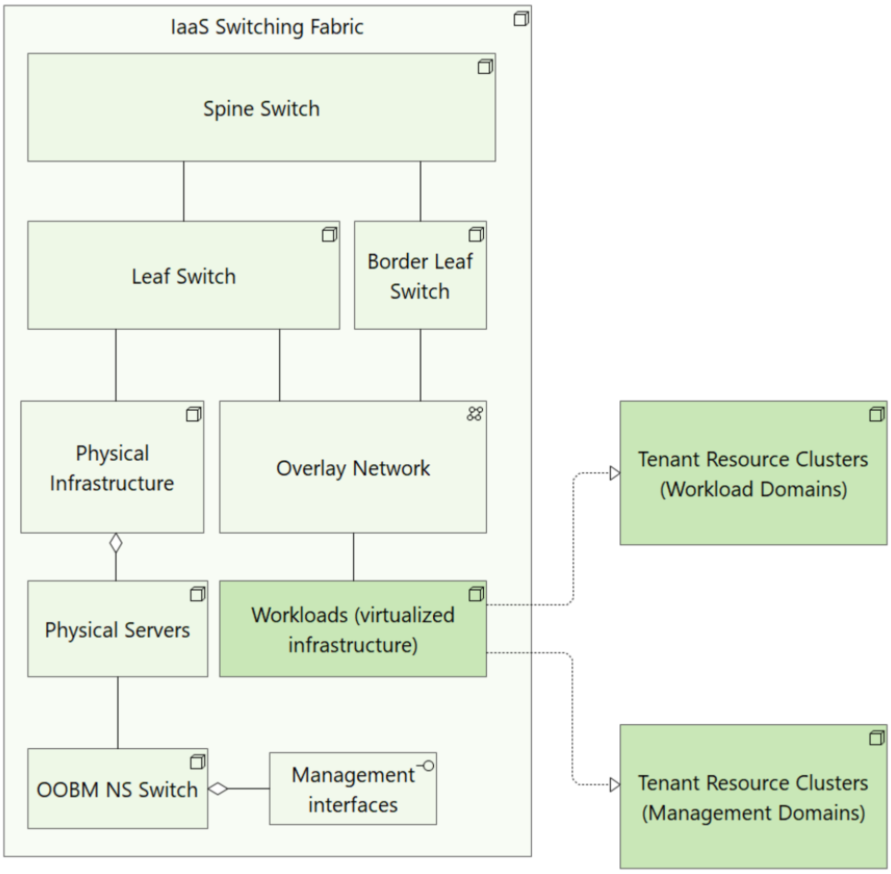


Figure 3-34 Virtualized infrastructure realizing Tenant Resource Clusters

The views below describe the IaaS Switching Fabric realizing the tenant resource clusters at the DC (Figure 3-35), the EN (Figure 3-36) and the SN (Figure 3-37). The workload domain depict an example set of workload clusters. Decisions about separating or clustering of workloads are determined by (non-exhaustive list):

- Service delineation scope (area of responsibility – service provider arguments);
- Cost and efficiencies;
- Cyber Security
- Governance arguments such as data protection, laws, etc.
- Enterprise and Domain SMC arguments on structuring services.

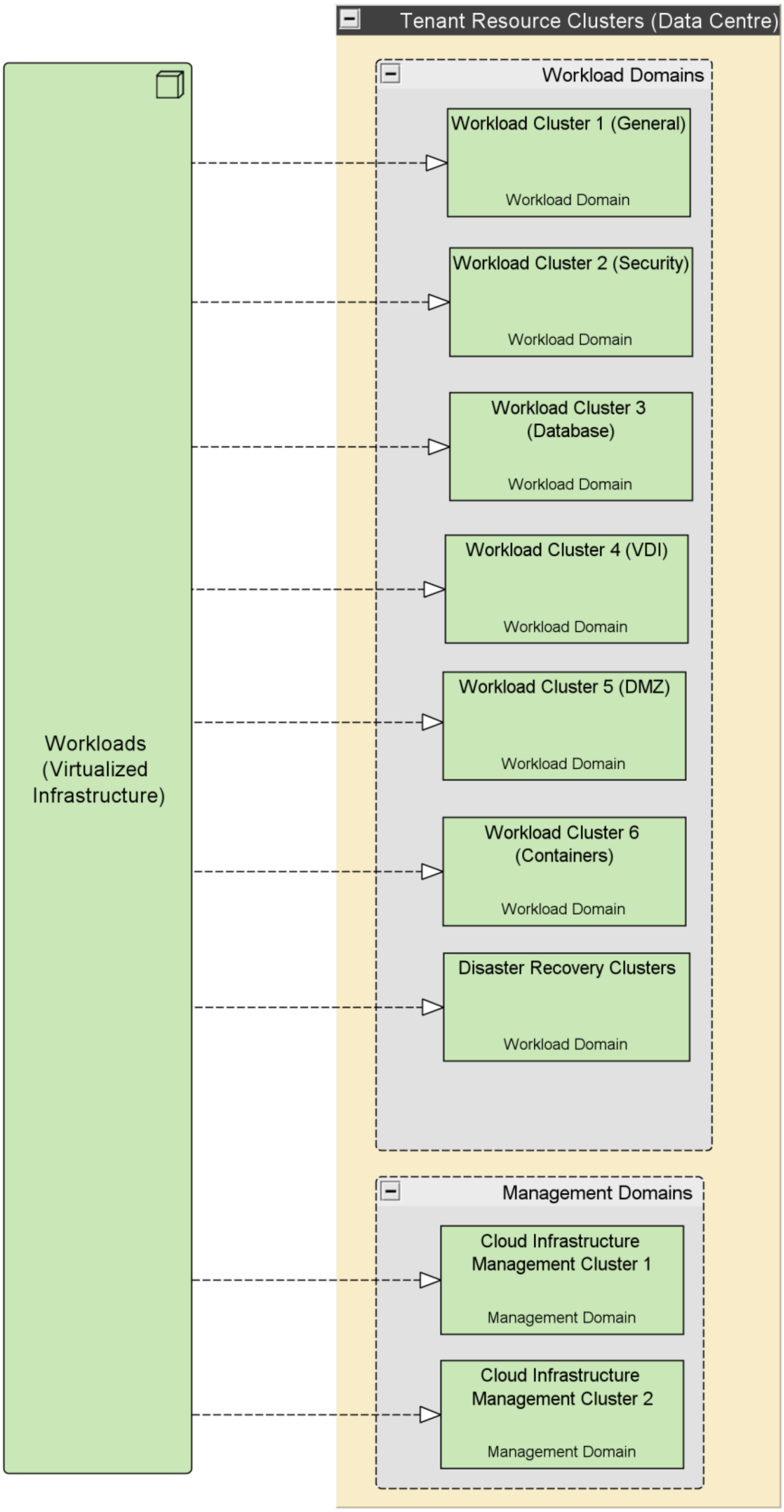

Tenant Resource Clusters (Data Centre)
Workload Domains
Workload Cluster 1 (General)
Workload Domain
Workload Cluster 2 (Security)
Workload Domain
Workload Cluster 3 (Database)
Workload Domain
Workload Cluster 4 (VDI)
Workload Domain
Workload Cluster 5 (DMZ)
Workload Domain
Workload Cluster 6 (Containers)
Workload Domain
Disaster Recovery Clusters
Workload Domain
Management Domains
Cloud Infrastructure Management Cluster 1
Management Domain
Cloud Infrastructure Management Cluster 2
Management Domain
Workloads (Virtualized Infrastructure)

Figure 3-35 DC virtualized infrastructure realizing workload and management domains

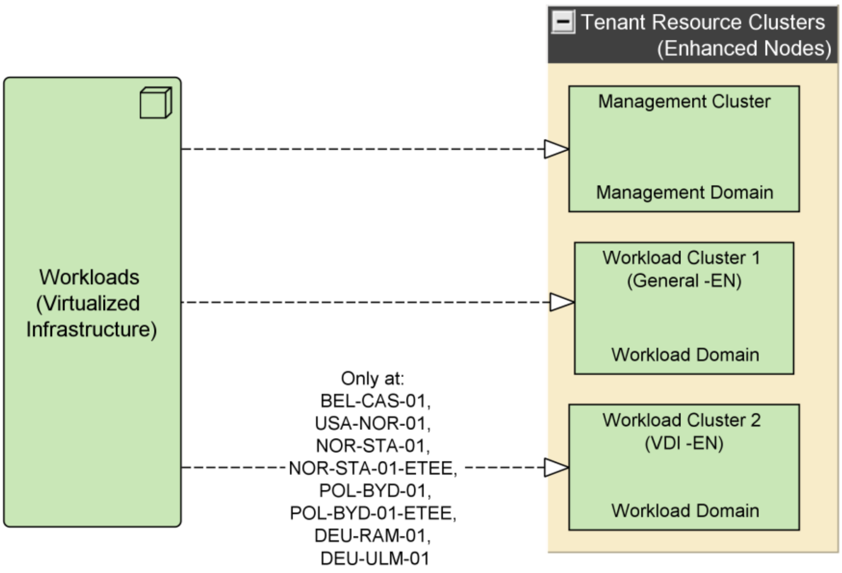

Tenant Resource Clusters (Enhanced Nodes)
Management Cluster
Management Domain
Workload Cluster 1 (General -EN)
Workload Domain
Workload Cluster 2 (VDI -EN)
Workload Domain
Workloads (Virtualized Infrastructure)
Only at: BEL-CAS-01, USA-NOR-01, NOR-STA-01, NOR-STA-01-ETEE, POL-BYD-01, POL-BYD-01-ETEE, DEU-RAM-01, DEU-ULM-01

Figure 3-36 EN virtualized infrastructure realizing tenant resource clusters

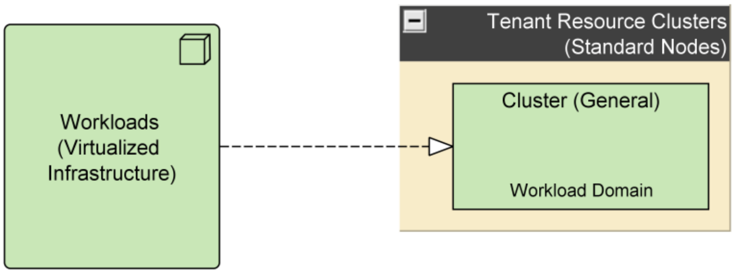

Tenant Resource Clusters (Standard Nodes)
Cluster (General)
Workload Domain
Workloads (Virtualized Infrastructure)

Figure 3-37 SN virtualized infrastructure realizing tenant resource clusters

3.3.4.2. Physical Infrastructure

A number of NATO ON services is realized with physical infrastructure, dedicated to the specific service. Reasons are widespread including aspects such as license cost optimization, performance and conformance with vendor reference implementations.

Figure 3-38 identifies the services that are realized through the physical infrastructure.

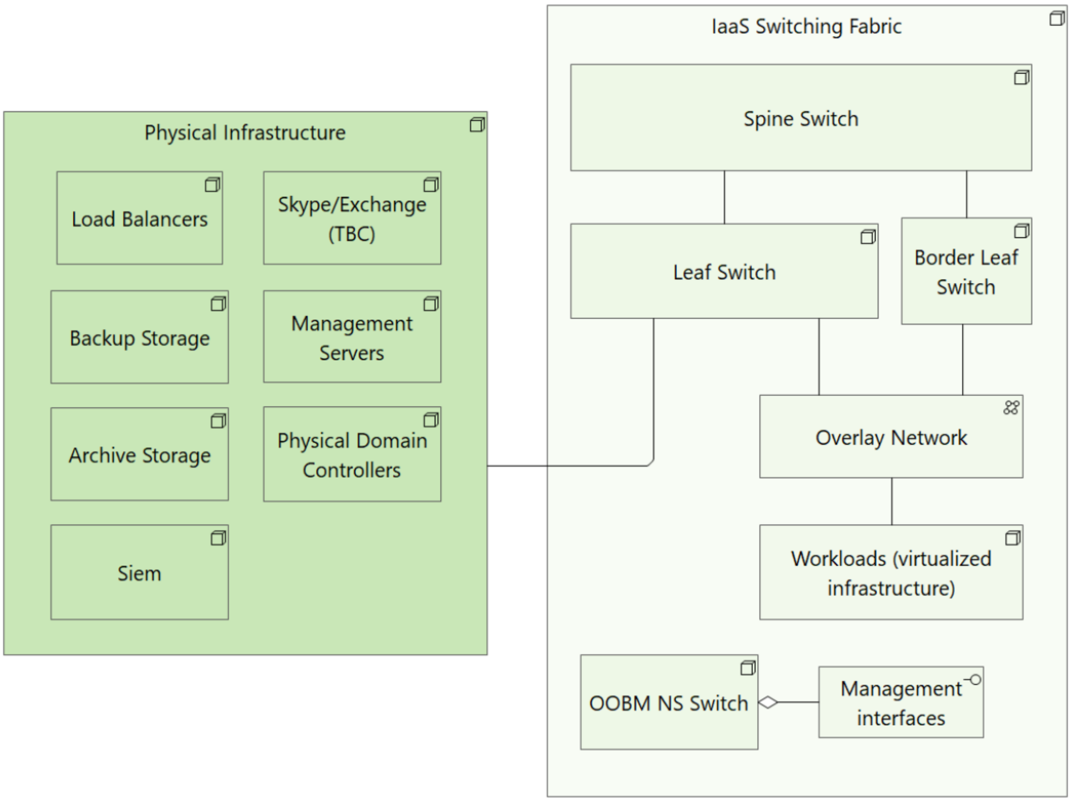


Figure 3-38 Physical infrastructure in support of selected services

3.4. Service Management and Control Perspective

The diagram below introduces the part of the overall context that is relevant for the SMC perspective documented herein.

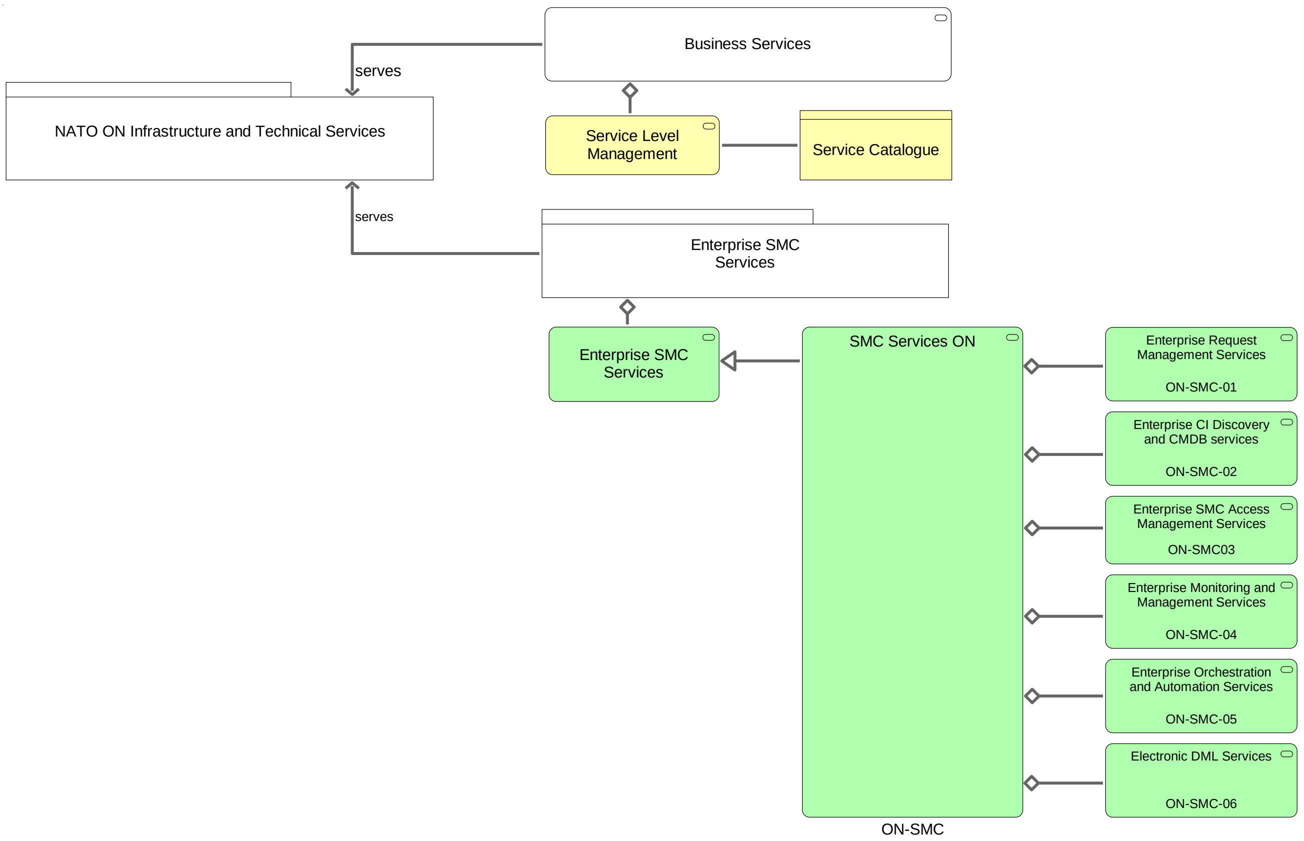

Business Services
serves
NATO ON Infrastructure and Technical Services
Service Level Management
Service Catalogue
serves
Enterprise SMC Services
Enterprise SMC Services
SMC Services ON
ON-SMC
Enterprise Request Management Services
ON-SMC-01
Enterprise CI Discovery and CMDB services
ON-SMC-02
Enterprise SMC Access Management Services
ON-SMC03
Enterprise Monitoring and Management Services
ON-SMC-04
Enterprise Orchestration and Automation Services
ON-SMC-05
Electronic DML Services
ON-SMC-06

Figure 3-39 Service Management and Control context

The paragraphs below provide further detail relevant to the SMC perspective. The paragraphs below do not necessary address specific aspects identified in the diagram above but affect SMC for NATO ON services, as realized by ITM, as a whole.

3.4.1. SMC by Design

SMC by Design is intended to automate the fulfilment of Service Management requirements across CIS services.

The objective is to standardize the SMC requirements to facilitate future integrations and reporting.

3.4.1.1. SMC functions

SMC Functions are building blocks that address specific Service Management and Control (SMC) needs and requirements. These building blocks are defining foundation requirements supported by the implementation of SMC capabilities.

The Service Management & Control main functions are:

1. Service infrastructure / Configuration management

2. Service Modelling
3. System Monitoring
4. Reactive SMC Configuration
5. Proactive SMC Configuration
6. SMC Monitoring, analysis and report

There are dependencies between functions, and it is possible to define a different implementation strategy based on the business requirements.

3.4.1.2. Function 1: Infrastructure / Configuration Management

This function consists in the creation of a database (CMDB) containing the list of infrastructure nodes supporting the services (servers, software, routers, firewalls…). It is sometimes possible to configure an automated discovery solution to collect these inventory data, configuration information and relationships between configuration items. It is also possible to load manually infrastructure data in the CMDB.

3.4.1.3. Function 2: Service Modelling

This function consists in the creation of service trees in the CMDB. These service trees, also named service models, are used to assess the importance of a configuration item via the relationship of this CI with business services. The service modelling consists in the creation of relationships between all business services and supporting configuration items, creating an interconnected forest where configuration items have an operational role. The function 1 - Infrastructure is an enabler for this function.

3.4.1.4. Function 3: System Monitoring

This function consists in the implementation of the system monitoring for IT infrastructure. Monitoring solutions are responsible for controlling infrastructure (hardware, networks, communications, operating systems and applications) in order to analyse the performance and to detect and alert about possible errors. It is possible to configure monitoring solutions to raise events when certain thresholds are reached. Thresholds are defined as the high and low resource utilization values for resources consumed by infrastructure. Thresholds are usually defined for CPU, memory, storage.

Multiple monitoring solutions exist. The choice of the most appropriate monitoring solution and technology is part of this component implementation.

3.4.1.5. Function 4: Reactive SMC Configuration

This function is supporting the implementation of Request Fulfilment, Incident Management, Change Management and Service Level Management.

- Request fulfilment

The first objective of request fulfilment is to provide a channel for customers to require and receive standard services. This objective is implemented via a self-service interface.

The second objective is to support the implementation of these standard services.

The last key objective is to provide information to customers about the availability of services and the procedures for obtaining them.

- Incident Management

The purpose of incident management is to restore normal service operation as quickly as possible and minimize impact on business operations.

Incidents are often related to Configuration Items present in the Configuration database. The function 1 - Infrastructure is an optional predecessor for Incident Management.

Service impact can be extrapolated from the relationship between the configuration item and the services. The function 2 – Service Modelling is an optional predecessor for Incident Management.

- Change Management

The purpose of change management is to guide, prepare and help organizations during the roll out of change requests. It helps to control risk and keep disruptions to services to a minimum.

Changes are often related to Configuration Items present in the Configuration database. The function 1 - Infrastructure is an optional predecessor for Change Management.

Service impact can be extrapolated from the relationship between the configuration item and the services. The function 2 – Service Modelling is an optional predecessor for Change Management.

- Service Level Management

The purpose of service level management is to give the assurance to the service consumer that the level of service provided by the Organization is in line with the Service Level Agreement contract. Service Level Management is measuring the performance of each service request, change request and incident. It reports on the quality of service and can escalate when the service targets are not respected.

The SLA component is directly depending on the implementation of the other components of the reactive SMC (Request Fulfilment – Change Management and Incident Management), and is adding a performance assessment dimension to these implementations.

3.4.1.6. Function 5: Proactive SMC Configuration

Service Monitoring is a service oriented monitoring technique, where an event bus is integrated in the solution architecture. The monitoring toolset will now simply send the collected events to the event bus. The event bus will then correlate all events. The correlation aligns all system events collected on the service core components everywhere to define the final impact on the service availability. When the correlation is complete, the event bus can optionally generate an intelligent incident providing the root cause, the list of impacted services, the incident support group and the correct service level target.

Service Availability: The passive method is measuring service availability via the KPIs extracted from Service Monitoring technique. The service is down when errors are detected by the monitoring environment.

The Active method is based on a probe consuming the service and actively reporting if the service is available. The service is down when the probe is reporting that the service is down. This method can also be used to measure performance for degraded services.

Service Capacity is another dimension of service monitoring. The objective is to configure the high and low resource utilization thresholds values for critical resources across the service infrastructure. Thresholds are usually defined for CPU, memory, storage, etc. When a capacity threshold is met, an event is sent to the event bus for correlation.

- The function 2 – Service Modelling is an enabler for this function.
- The function 3 – System Monitoring is an enabler for this function.

3.4.1.7. Function 6: SMC Monitoring, analysis and report

This function is intended to provide reporting capability about service usage, request consumption and service performance.

3.4.2. SMC Capability Mapping

3.4.2.1. Enterprise, Domain and Element SMC

SMC is made of three implementation layers: Enterprise SMC, Domain SMC and Element SMC. Figure 3-40 below provides an illustration.

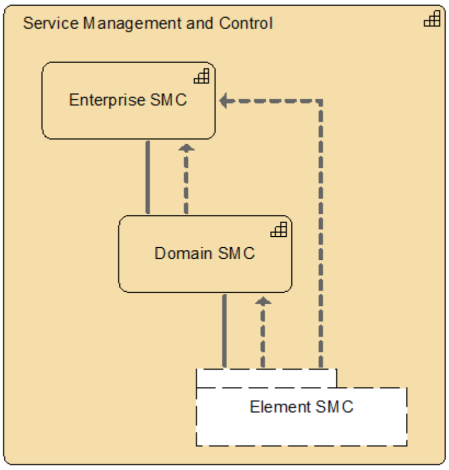


Figure 3-40 SMC layering

The following paragraphs further elaborate the Enterprise SMC, Domain SMC and Element SMC layers, as introduced in the view in Figure 3-40 above.

3.4.2.2. Enterprise SMC

The architecture of the Enterprise SMC capability follows the logic of a Service Oriented Architecture; a central element of this architecture is the Service Management and Control Enterprise Service Bus. Following SOA approach, this enterprise SMC service bus provides common Service Management motivation models, strategy models, business models, process models, software models, system models and data models to all enterprise SMC consumers.

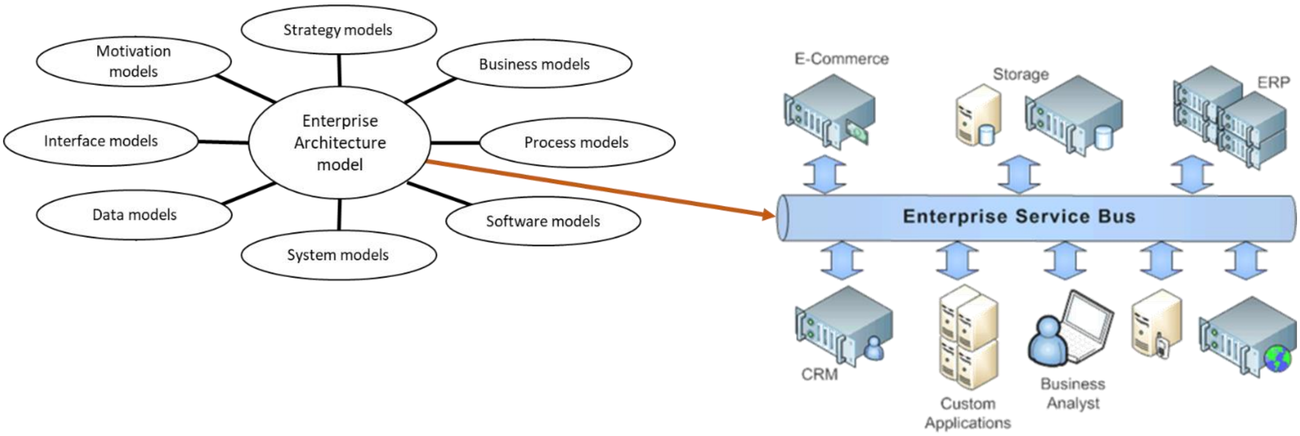


Figure 3-41 Enterprise SMC Service Bus

The Enterprise SMC Service bus is the core environment where service-oriented business models are applied to the way the organization works with the purpose of improving performance, efficiency, and service delivery. Enterprise SMC models are applied to the whole organization by default.

3.4.2.3. Domain SMC

Domain SMC is still consuming enterprise models, but is also deploying specific SMC domain models to support specific business needs.

Examples of Service Domain present in the NCI Agency:

1. Communications Services, this domain is supporting three specific sub domains:
   a. Access Services (relevant for the NATO ON, the Campus LAN)
   b. Transport Services (relevant for the NATO ON, the NCI)
   c. Transmission Services (wired and wireless transmission, wired typically outsourced)
2. COI Services and User Applications (Application Monitoring, Development)
3. Enterprise Core Services (Infrastructure as a Service, Platform as a Service)
4. NATO Digital Workplace Services; End User Services (User Applications, User Equipment); Unified Communication and Collaboration Services; Information Management Services.
5. Cyber Security Services[5] and Cyber Security Applications[6]
6. Non CIS Services (Logistics, Facilities)

Figure 3-42 decomposes the Domain SMC layer further and identifies strong ties and overlap with the Element SMC.

[5] The C3 Taxonomy revers to Cyber Security Services as CIS Security Services

[6] The C3 Taxonomy groups Cyber Security Applications under CIS Applications, which covers design, plan, deliver, protect, operate and control information and communication technology services

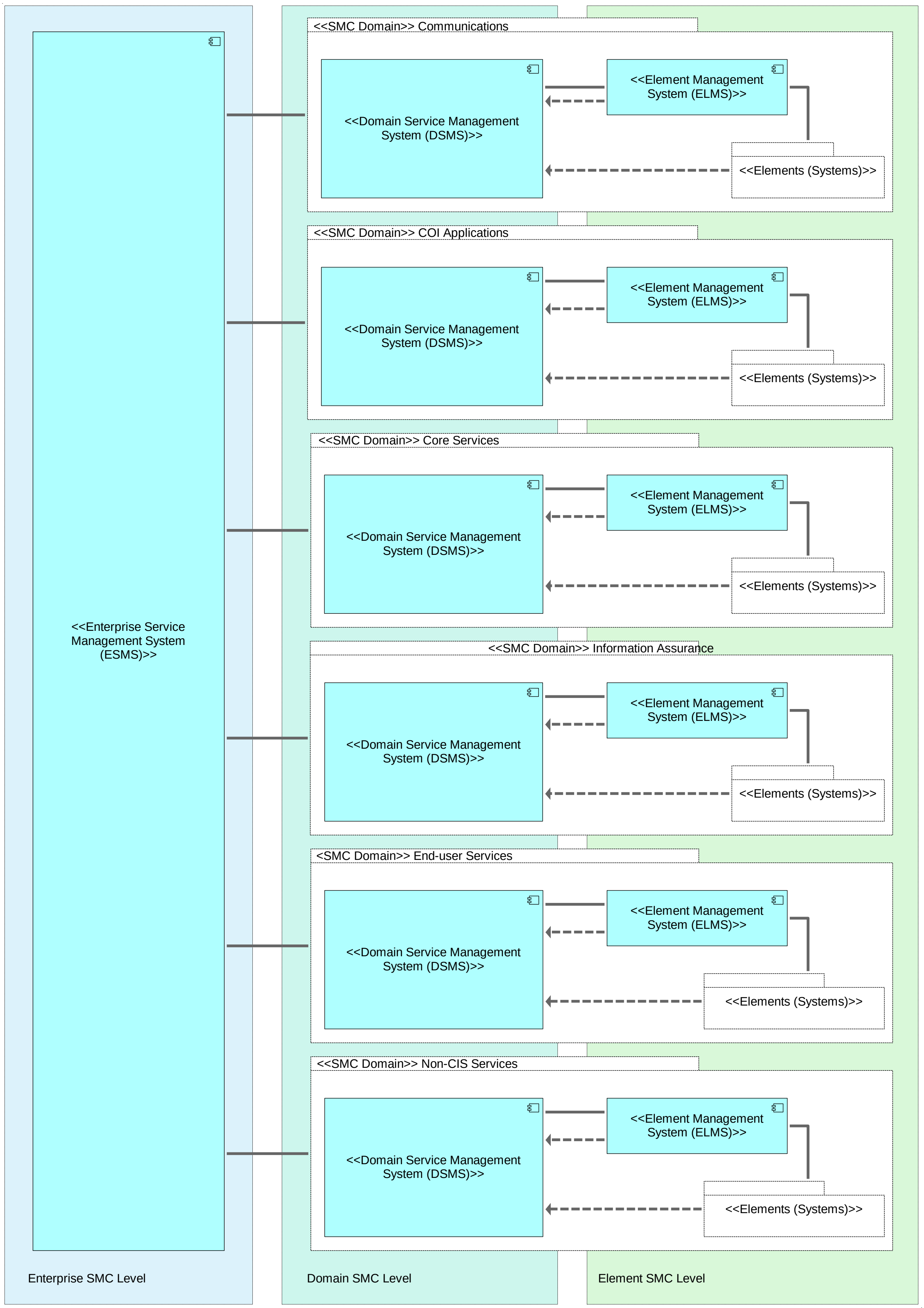

<<SMC Domain>> Communications
<<Domain Service Management System (DSMS)>>
<<Element Management System (ELMS)>>
<<Elements (Systems)>>
<<SMC Domain>> COI Applications
<<Domain Service Management System (DSMS)>>
<<Element Management System (ELMS)>>
<<Elements (Systems)>>
<<SMC Domain>> Core Services
<<Domain Service Management System (DSMS)>>
<<Element Management System (ELMS)>>
<<Elements (Systems)>>
<<Enterprise Service Management System (ESMS)>>
<<SMC Domain>> Information Assurance
<<Domain Service Management System (DSMS)>>
<<Element Management System (ELMS)>>
<<Elements (Systems)>>
<SMC Domain>> End-user Services
<<Domain Service Management System (DSMS)>>
<<Element Management System (ELMS)>>
<<Elements (Systems)>>
<<SMC Domain>> Non-CIS Services
<<Domain Service Management System (DSMS)>>
<<Element Management System (ELMS)>>
<<Elements (Systems)>>
Enterprise SMC Level
Domain SMC Level
Element SMC Level

Figure 3-42 Domain and Element SMC further decomposed

3.4.2.4. Element SMC

Element SMC is supporting a specific technology providing a set of capabilities to Domain SMC or Enterprise SMC. It includes the tools/mechanisms capable of monitoring/configuring/changing specific service elements or specific hardware/software components and features in support of the higher layer domain or enterprise SMC services.

Element SMC is deploying specific capabilities to support specific business needs.

3.4.3. SMC Capabilities

SMC Core capabilities can be defined as follows:

- **Request management capability**: service request lifecycle and interactions between service provider and users.
- **ICT asset management capability**: tracking and manage asset life cycle, from purchasing till decommissioning. Focus on price, provider, warranty…
- **Configuration management capability**: manage the configuration of services, including relationships between services and service components or resources.
- **Service provisioning capability**: supply or removal of a service
- **CI discovery and relationship mapping**: automatic finding, identification and relationship mapping of network connected service components.
- **Service monitoring capability**: hardware or software component used to monitor system resources and performance, collect system errors and route alerts. System monitoring is providing a valid perspective on service availability via the monitoring data collected on all configuration items supporting the service.
- **Service capacity management capability**: hardware or software component used to monitor service capacity thresholds. Alerts are generated when service thresholds are breached. This can be used to forecast demand and reserve resources.
- **Log management capability**: record activities or events in files for later analysis or reporting.
- **Cross security domain data federation**: bi-directional exchange of service data across protected network boundary.
- **Cross network data federation capability**: bi-directional exchange of service data between need-to-know participants.
- **Reporting capability**: consume raw data and provide business intelligence capability to produce detailed output and service reports. Reporting to external Agency customers is an Enterprise SMC capability.
- **Automation capability**: automatic task executed without human intervention.
- **Orchestration capability**: automatic multi-system task executed without human intervention.

The view in Figure 3-43 below represents the SMC Capability Realization view. It describes how the SMC capability is realized through software.

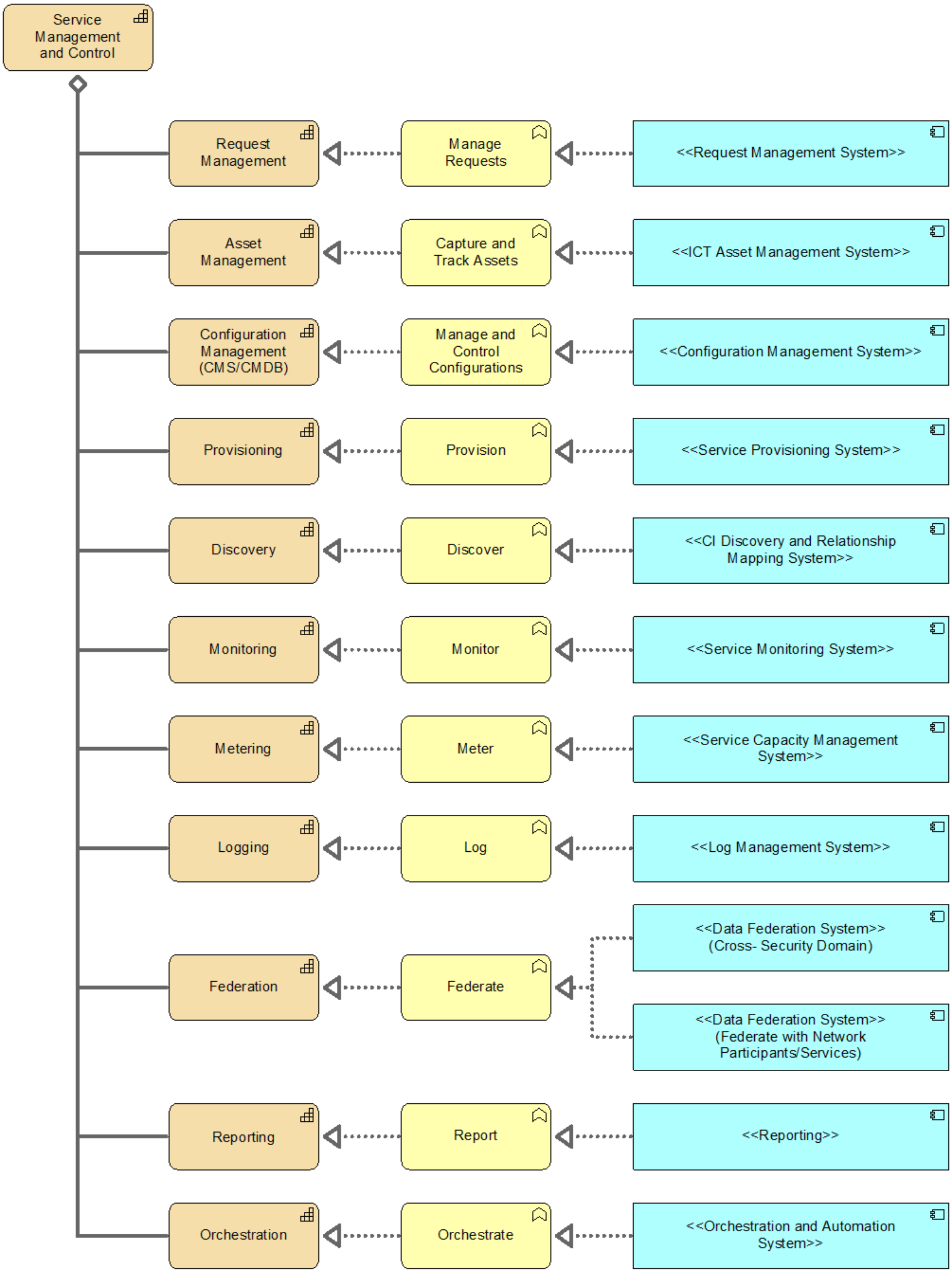

Service Management and Control
Request Management
Manage Requests
<<Request Management System>>
Asset Management
Capture and Track Assets
<<ICT Asset Management System>>
Configuration Management (CMS/CMDB)
Manage and Control Configurations
<<Configuration Management System>>
Provisioning
Provision
<<Service Provisioning System>>
Discovery
Discover
<<CI Discovery and Relationship Mapping System>>
Monitoring
Monitor
<<Service Monitoring System>>
Metering
Meter
<<Service Capacity Management System>>
Logging
Log
<<Log Management System>>
<<Data Federation System>> (Cross- Security Domain)
Federation
Federate
<<Data Federation System>> (Federate with Network Participants/Services)
Reporting
Report
<<Reporting>>
Orchestration
Orchestrate
<<Orchestration and Automation System>>

Figure 3-43 SMC Capability Realization View

All these capabilities can be provided by the Enterprise SMC.

Domain SMC capabilities are leveraged for:

- Configuration management capability
- Service provisioning capability
- CI discovery and relationship mapping capability
- Service monitoring capability
- Reporting capability
- Automation capability
- Orchestration capability

Element SMC capabilities are leveraged for:

- Configuration management capability
- Service provisioning capability
- Service monitoring capability
- Reporting capability
- Automation capability
- Orchestration capability

The view in Figure 3-44 introduces the software components used in support of the enterprise, domain and element SMC capabilities listed above.

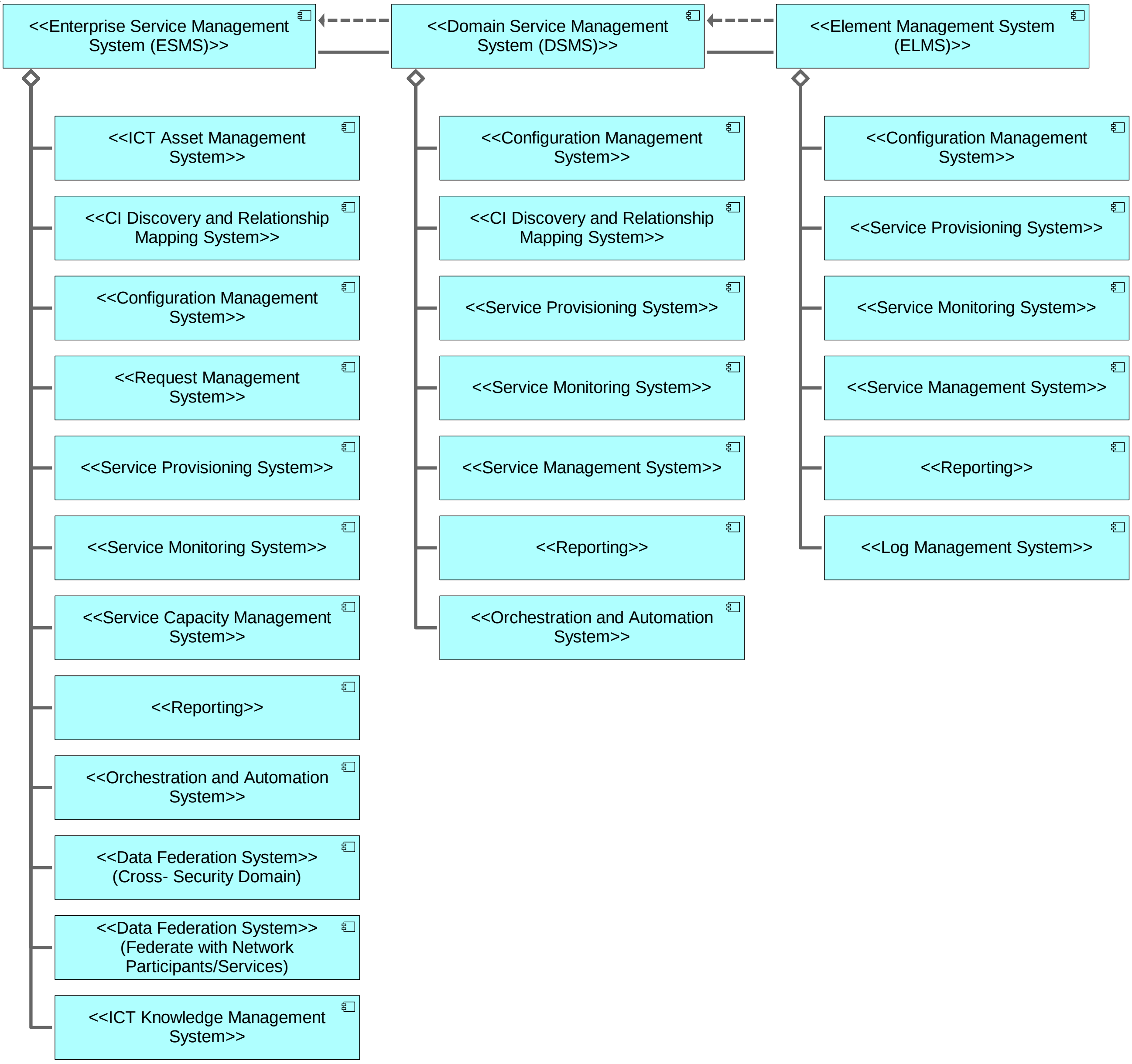

<<Enterprise Service Management System (ESMS)>>
<<Domain Service Management System (DSMS)>>
<<Element Management System (ELMS)>>
<<ICT Asset Management System>>
<<CI Discovery and Relationship Mapping System>>
<<Configuration Management System>>
<<Request Management System>>
<<Service Provisioning System>>
<<Service Monitoring System>>
<<Service Capacity Management System>>
<<Reporting>>
<<Orchestration and Automation System>>
<<Data Federation System>> (Cross- Security Domain)
<<Data Federation System>> (Federate with Network Participants/Services)
<<ICT Knowledge Management System>>
<<Configuration Management System>>
<<CI Discovery and Relationship Mapping System>>
<<Service Provisioning System>>
<<Service Monitoring System>>
<<Service Management System>>
<<Reporting>>
<<Orchestration and Automation System>>
<<Configuration Management System>>
<<Service Provisioning System>>
<<Service Monitoring System>>
<<Service Management System>>
<<Reporting>>
<<Log Management System>>

Figure 3-44 SMC Capabilities – Software components

3.4.4. ACPV Configuration Management enablers

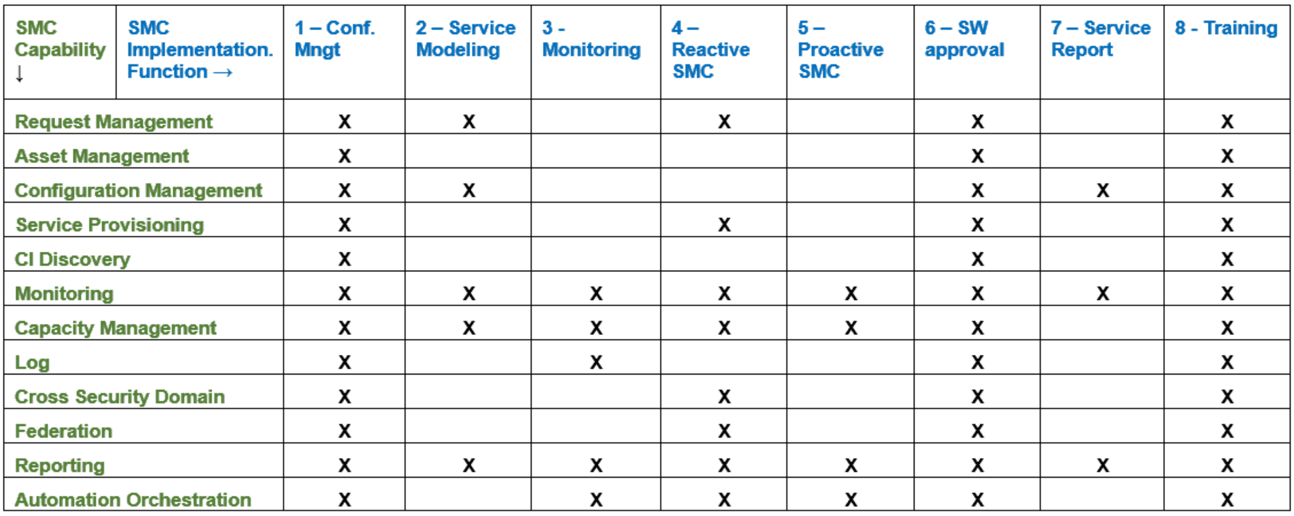
- **Request management capability**: service request lifecycle and interactions between service provider and users. Impact on service configuration is maintained in the enterprise SMC environment.
- **CI discovery and relationship mapping**: automatic finding, identification and relationship mapping of network connected service components.
- **Configuration management capability**: manage the configuration of services, including relationships between services and service components or resources. Creation of service and configuration items data models and storage of configuration information. “Request management capability” and “CI Discovery” are critical feeder of this core capability, used to provide normalized information feeding the ACPV Configuration Strategic Tier-1 level

- **Orchestration capability**: automatic multi-system task executed without human intervention. Orchestration will be a critical success factor when the integration and coordination with ACPV Strategic Tier-1 level will be deployed. The NATO ON, realized by ITM Recovery Increment 1, is an enabler of the enterprise SMC side of this connector.

3.4.5. SMC Capabilities and functions

The Table 3-1 below identifies the SCM capabilities and maps these capabilities to the relevant functions.

Table 3-1 Mapping of SMC Capabilities to Functions



SMC Capability ↓	SMC Implementation. Function →	1 – Conf. Mngt	2 – Service Modeling	3 - Monitoring	4 – Reactive SMC	5 – Proactive SMC	6 – SW approval	7 – Service Report	8 - Training
Request Management		X	X		X		X		X
Asset Management		X					X		X
Configuration Management		X	X				X	X	X
Service Provisioning		X			X		X		X
CI Discovery		X					X		X
Monitoring		X	X	X	X	X	X	X	X
Capacity Management		X	X	X	X	X	X		X
Log		X		X			X		X
Cross Security Domain		X			X		X		X
Federation		X			X		X		X
Reporting		X	X	X	X	X	X	X	X
Automation Orchestration		X		X	X	X	X		X

3.4.6. SMC Interface description methodology

For each of the interfaces, the SMC functions which need to be configured / implemented are documented and the interfaces are added to the traceable matrix to ensure that all SMC interfaces supported by ITM Recovery Increment 1 are identified and that the related requirements are incorporated.

Enterprise / Domain SMC components 2.0 document (reference [21]) is a core element of this documentation and is considered as an annex to this ADP document. The list of interfaces in scope are identified in the Interface Definition Document Table (reference [50]).

3.5. Cyber Security Perspective

The diagram below introduces the part of the overall context that is most relevant for the Cyber Security perspective documented herein. This section provides an overview of the Cyber Security context for the NATO ON.

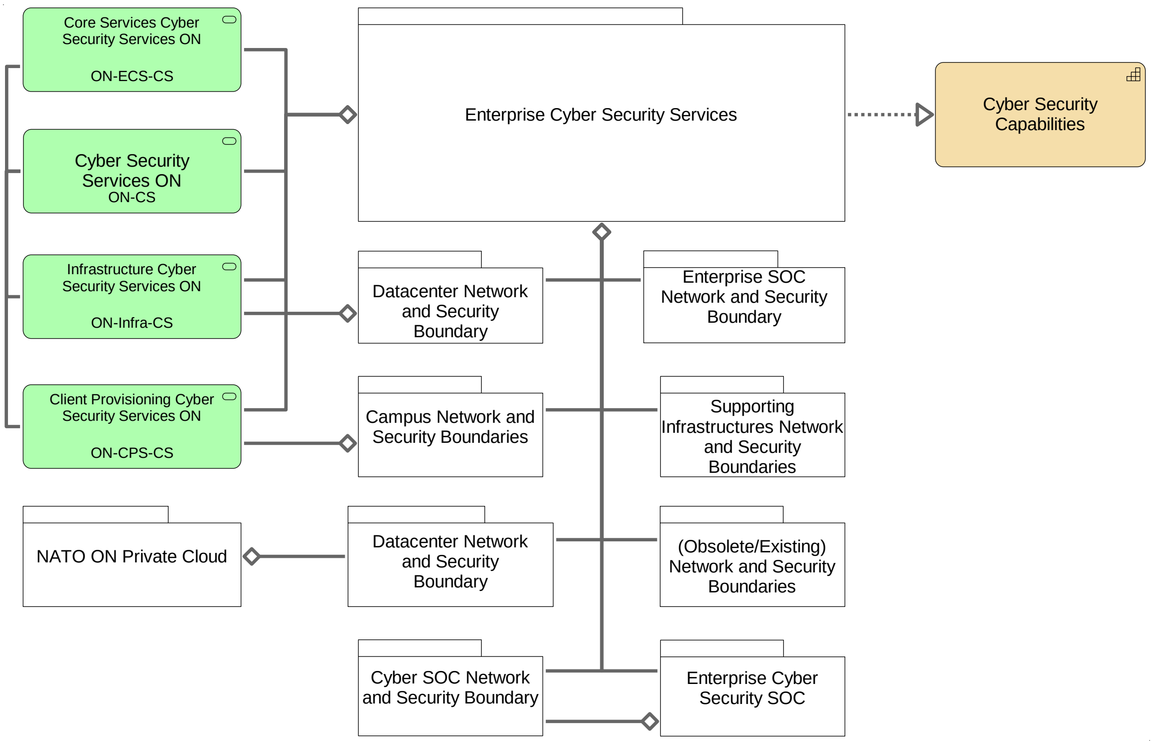

Core Services Cyber Security Services ON
ON-ECS-CS
Cyber Security Services ON
ON-CS
Infrastructure Cyber Security Services ON
ON-Infra-CS
Client Provisioning Cyber Security Services ON
ON-CPS-CS
NATO ON Private Cloud
Enterprise Cyber Security Services
Cyber Security Capabilities
Datacenter Network and Security Boundary
Enterprise SOC Network and Security Boundary
Campus Network and Security Boundaries
Supporting Infrastructures Network and Security Boundaries
Datacenter Network and Security Boundary
(Obsolete/Existing) Network and Security Boundaries
Cyber SOC Network and Security Boundary
Enterprise Cyber Security SOC

Figure 3-45 Cyber Security Context

3.5.1. Cyber Security by Design

Cyber Security is an important aspect of any CIS and is achieved by designing and implementing a wide range of Cyber Security Functions (CSFs). The determination of the CSFs is based on a number of considerations, see Section 3.5.3. The CSFs are provided by cyber security capabilities (see 3.5.2) and are made available to the environment as cyber security services (which may be implemented as an integral part of a dependant service in some cases as described in 3.5.5).

3.5.2. Cyber Security functions and capabilities

The set of Cyber Security capabilities that can provide CSFs are divided into groups as shown in Figure 3-46. (The set of Cyber Security capabilities is equal to the set of CIS Security capabilities as described in reference [31] which is referred to as the ‘CIS Security Capability Breakdown’. For the purpose of this document the term ‘CIS Security’ is interchangeable with ‘Cyber security’.) For each capability group, there are many CSFs that could be implemented, both technical and non-technical. The main groups are described below.

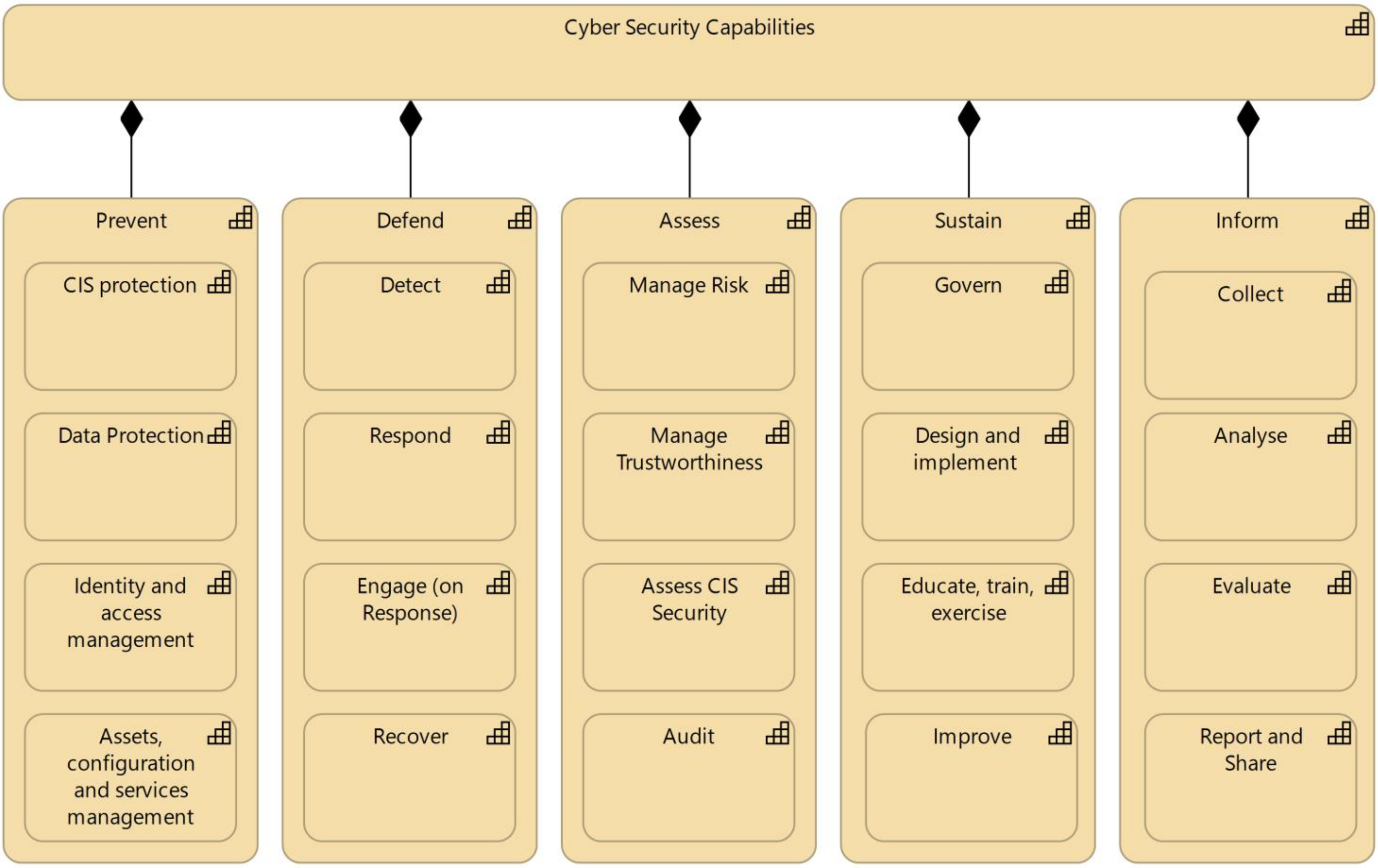


Figure 3-46 Cyber Security Capabilities

3.5.2.1. Cyber Security Prevent Capability

The Prevent capability ensures that cyber security functions are applied for both the CIS and the data processed by the CIS. Continual updates of the configuration of CIS components are needed as either the systems changes, the environment changes, or the usage changes. The capability includes updates of hardware and software components as needed, configuration control and management, updates to identities as personnel changes and their roles change, as well as updating measures to ensure data is properly protected such as ensuring data is handled according to its classification level.

3.5.2.2. Cyber Security Defend Capability

The Defend capability ensures a detection and response capability for any incidents that occur, as a result of mistakes or attacks. This includes the ability to monitor systems, detect security events (whether intentional or unintentional), respond to such events in a timely manner, and recover from security events by restoring services.

3.5.2.3. Cyber Security Assess Capability

The Assess capability ensures that CIS Security is analysed and evaluated on a continual basis in order to reach the appropriate level of security and that the residual risk is understood. The capability includes the management of risk, the management of trust in both CIS components and other entities, the assessment of how effective and efficient CIS Security is, and the auditing of CIS in order to achieve accountability of CIS Security provision.

3.5.2.4. Cyber Security Sustain Capability

The Sustain capability ensures that CIS Security can be provided at the appropriate level over long periods of time. This includes the governance which sets strategic objectives and direction, the design and implementation of new systems and improvements to the existing systems, the ability to educate, train, and exercise personnel in order to reach the right level of skill and practice, and the ability to identify improvements to CIS Security to be able to better deal with current attacks, as well as being able counter new and changing attacks.

3.5.2.5. Cyber Security Inform Capability

CIS Security information includes a wide range of information such as methodologies and best practices, information about the security of CIS components and their vendors, as well as threat, vulnerability, incident information, CIS assets and dependencies, and CIS assets operational values. The capability to manage CIS Security information is referred to as the Inform capability and includes the organization of its management, which will identify information requirements, roles and responsibilities, as well as how information will be collected, analysed, evaluated, reported, and shared.

3.5.3. Determination and Implementation of the Cyber Security Functions

The determination of the CSFs to be implemented and the strength of each CSF is an integral part of the solution and needs to be considered from the very beginning of a project and updated and maintained throughout the entire project lifecycle.

The CSFs are determined based on three considerations that are visualized in Figure 3-47:

- The CSFs are required to fulfil the user (operational) requirements;
- The CSFs are required to comply with NATO Security Policy;
- The CSFs are required to comply with NCI Agency architectures and standards.

In Figure 3-47 the vertical axis ensures that the user (operational) requirements for cyber security are captured and understood, and that the resulting services are delivered at a security level appropriate for the users (NATO Bodies). The horizontal axis ensures that the solution complies with NCI Agency architectures and standards, and is compliant with NATO Policy which identifies a set of CSFs that is expected to be implemented. The compliance with policy is validated through the accreditation process.

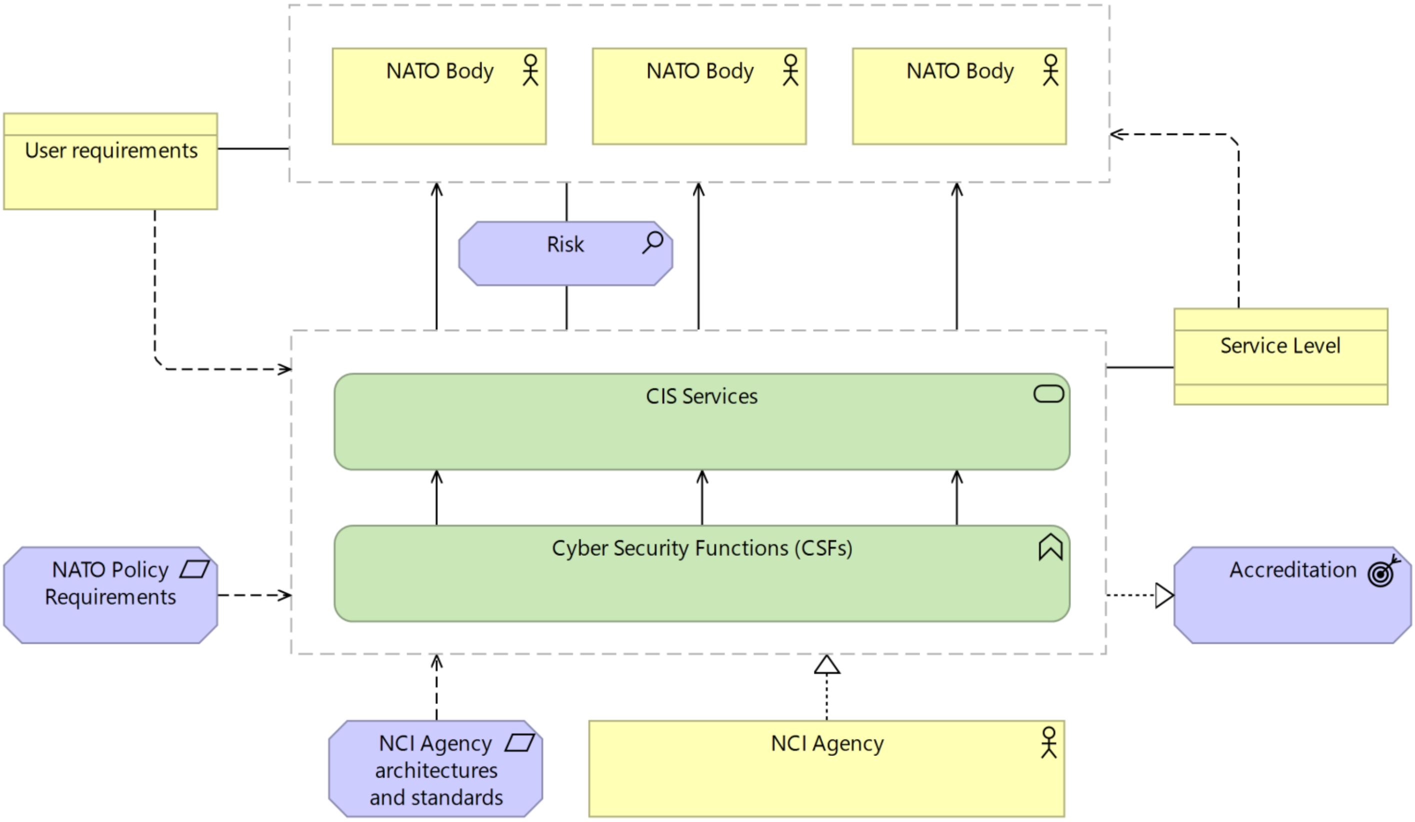


Figure 3-47 Cyber Security dimensions (vertical and horizontal)

3.5.4. NATO Security Policy Compliancy

NATO Security policy directs the implementation of CISs handling NATO Information, and includes a significant number of security requirements that are expected to be implemented, in particular those captured in the Technical and Implementation Directive on CIS Security (reference [30], [34]).

The full set of NATO Security policy requirements to comply with will need to be addressed by the NATO ON services, realized by the various work packages in ITM Recovery Increment 1. In order to make explicit which work packages are involved in addressing the policy requirements - and in what Responsibility Accountability Consult Inform (RACI) role - a RACI matrix has been provided in [18] (noting that responsibilities may have to shift during execution).

3.5.5. Cyber Security Integration Architecture

3.5.5.1. Cyber Security Functions and Services

Many of the CSFs that will be implemented in the ON will be managed and monitored by the NCI Agency Cyber Security Operations Centre (CSOC), a part of the NATO Cyber Security Centre (NCSC). The implementation therefore needs to be fully integrated with the CSOC, leading to specific choices for some functions:

- Some of the new CSFs introduced with the ON will be made available to the environment as cyber security services under Infrastructure as a Service (ON-Infra-CS), Client Provisioning Services (ON-CPS-CS), and Enterprise Core Services (ON-ECS-CS). (These cyber security

services will not provide many interfaces but mainly depend on interfaces from the aforementioned services for integration.) These CSFs are (see Figure 3-49):
  - Segmentation / Zoning;
  - DNS Security (DNSSEC);
  - Endpoint Security (addition of application control);
  - Data Loss Prevention (DLP) Discovery;
  - Email (server) security.
- Other new CSFs will need to be made available to the environment as specific Cyber Security Services in the ON – listed below - and fully integrated into the overall solution.
  - The Enterprise Logging service (ON-CS-EL) will provide log collection, retention, and analysis for all systems in the ON. The main interface is the submission of logs;
  - The Privileged Access Management (PAM) service (ON-CS-PAM) provides control of administration rights for the ON systems, ensuring that administrators do not have standing admin rights but are assigned rights when needed for the time needed. Administrator actions are also logged/recorded to ensure the ability to audit administrator actions;
  - The User and Device Credentials service (ON-CS-UDC; see [32]) provides the ability to issue and manage cryptographic credentials for users and devices. The credentials are used to authenticate to various systems and services. The key interface is the issuance of credentials. Note that subsequent use of credentials for authentication does not involve this service but uses the Enterprise-Wide Security Certificate Service [SEC015] for validation;
  - The service ‘Gateway to external CIS’ (ON-CS-GW) provides security functions that enables information flows between the ON and any external network necessary, including the legacy systems;
  - The service ‘Data Diode as a service’, also referred to as ‘Data Diode service’ or simply ‘data diode’ (ON-CS-DD), enables one-way transfer of data from low to high, in this case from the Internet, NU, or NR into the ON at NS level. The service can support email, file transfer, as well as other data.

Figure 3-48 illustrates the orchestration of CSFs and Cyber Security Services and also shows the Cyber Security Monitoring service for the ON (ON-CS-M). This is not a new service, but it will uplift existing monitoring where necessary, either from a functional or capacity point of view. The service will ensure new components and approaches (e.g. the Software Defined Data Centre approach and the use of virtualization and automation) are properly monitored, performing any required analysis to understand attack/misuse scenario and required information to detect such cases.

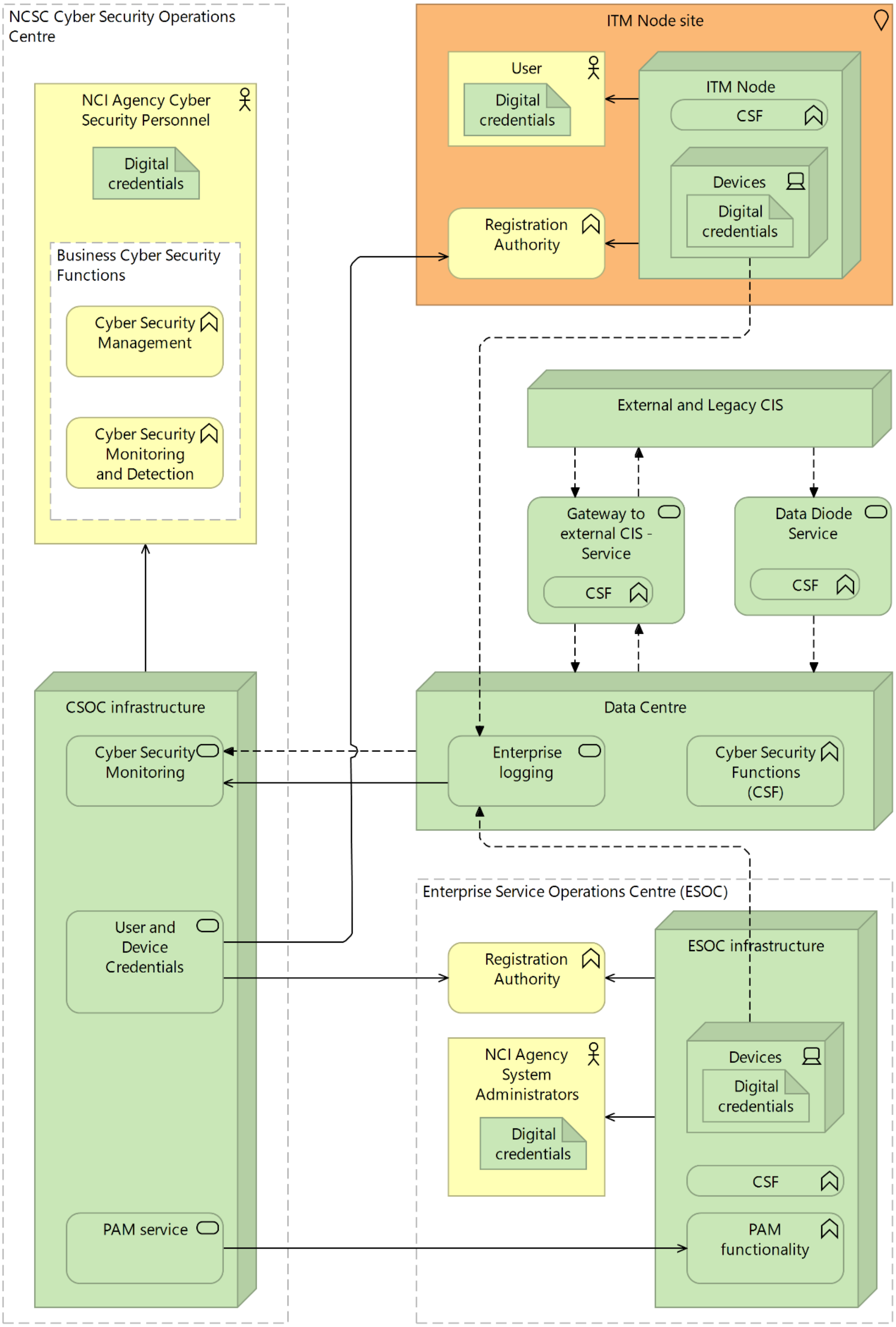

NCSC Cyber Security Operations Centre
NCI Agency Cyber Security Personnel
Digital credentials
Business Cyber Security Functions
Cyber Security Management
Cyber Security Monitoring and Detection
CSOC infrastructure
Cyber Security Monitoring
User and Device Credentials
PAM service
ITM Node site
User
Digital credentials
ITM Node
CSF
Devices
Digital credentials
Registration Authority
External and Legacy CIS
Gateway to external CIS - Service
CSF
Data Diode Service
CSF
Data Centre
Enterprise logging
Cyber Security Functions (CSF)
Enterprise Service Operations Centre (ESOC)
Registration Authority
NCI Agency System Administrators
Digital credentials
ESOC infrastructure
Devices
Digital credentials
CSF
PAM functionality

Figure 3-48 Overview of Cyber Security Functions and Services

Figure 3-49 provides an overview of NATO ON Cyber Security Services. In addition to those services realized by ITM Recovery Increment 1, the figure also shows the following enterprise-wide NCI Agency catalogue Cyber Security Services with which interaction is expected and that are not significantly changed by ITM Recovery Increment 1:

- Gateway Security Services (SEC011): provides global management of gateways and firewalls. Configuration and maintenance of firewalls will be through SEC011;
- The Crypto Management and Logistics Support Service (SEC014): provides management and keying of high-assurance cryptographic devices. Any high assurance crypto device deployed will be managed through SEC014;
- The Security Certificate Services (SEC015): provides the NATO PKI services including certificate validation. In the NATO ON, most credentials are managed through the UDC service, which in turn uses SEC015. However, any authentication will require SEC015 validation.

The Cyber Security Services and their interaction with the other ON services are further defined in the IDDs and are all listed per service in the Interface Definition Document Table (reference [50]).

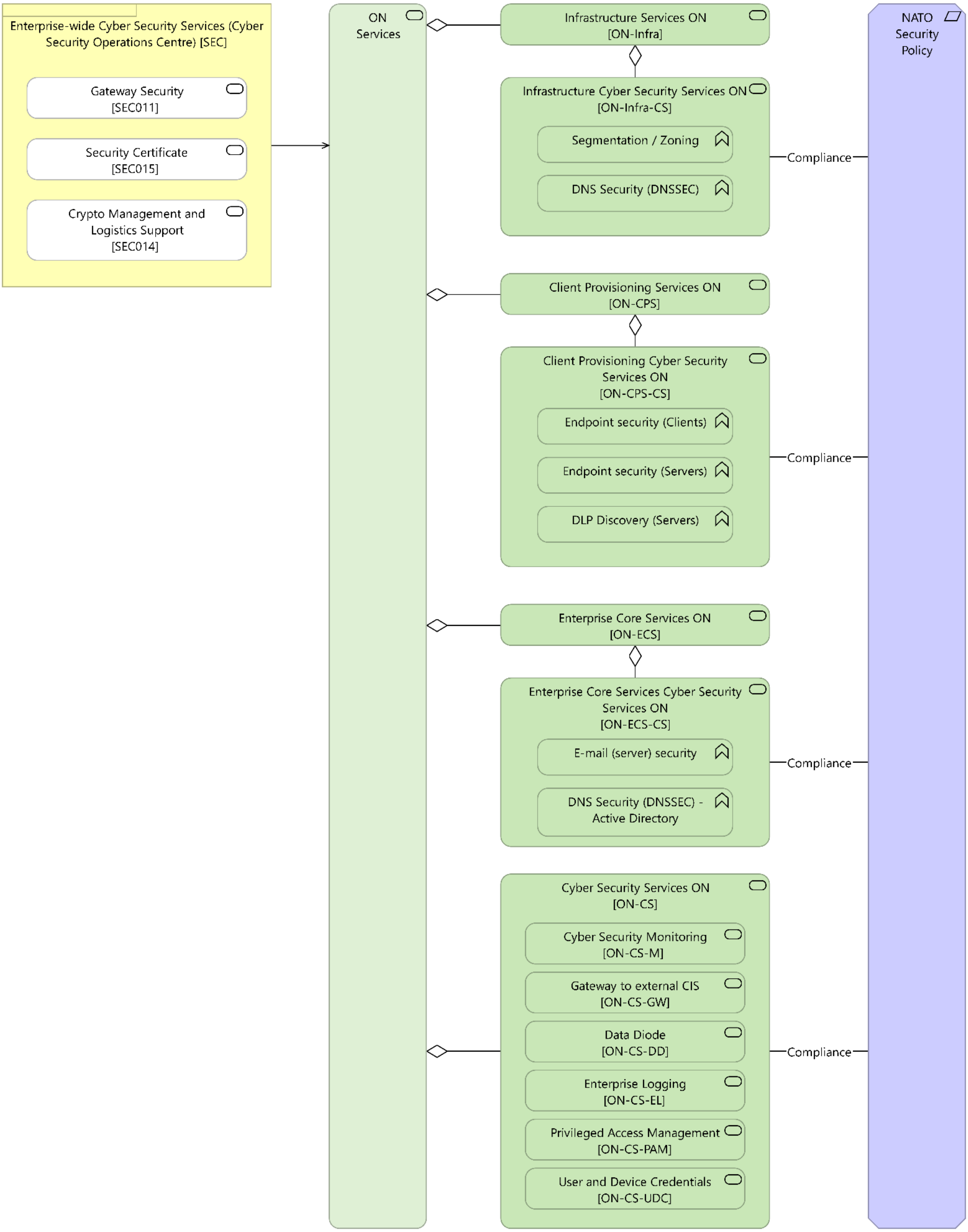

Enterprise-wide Cyber Security Services (Cyber Security Operations Centre) [SEC]
Gateway Security [SEC011]
Security Certificate [SEC015]
Crypto Management and Logistics Support [SEC014]
ON Services
Infrastructure Services ON [ON-Infra]
Infrastructure Cyber Security Services ON [ON-Infra-CS]
Segmentation / Zoning
DNS Security (DNSSEC)
Client Provisioning Services ON [ON-CPS]
Client Provisioning Cyber Security Services ON [ON-CPS-CS]
Endpoint security (Clients)
Endpoint security (Servers)
DLP Discovery (Servers)
Enterprise Core Services ON [ON-ECS]
Enterprise Core Services Cyber Security Services ON [ON-ECS-CS]
E-mail (server) security
DNS Security (DNSSEC) - Active Directory
Cyber Security Services ON [ON-CS]
Cyber Security Monitoring [ON-CS-M]
Gateway to external CIS [ON-CS-GW]
Data Diode [ON-CS-DD]
Enterprise Logging [ON-CS-EL]
Privileged Access Management [ON-CS-PAM]
User and Device Credentials [ON-CS-UDC]
Compliance
Compliance
Compliance
Compliance
NATO Security Policy

Figure 3-49 NATO ON Cyber Security Services

3.5.5.2. Data Loss Prevention Architecture

Data Loss Prevention functionality will be provided in the ON by Enterprise Core Services Cyber Security Services (ON-ECS-CS) and Client Provisioning Cyber Security Services (ON-CPS-CS). Data Loss Prevention functionality breaks down into three categories:

- DLP for data in use ("DLP Endpoint") – DLP for data in use is part of Endpoint Security and is implemented at both clients and servers.
- DLP for data at rest ("DLP Discovery") – DLP for data at rest can be implemented for clients and servers, however in ITM Recovery Increment 1 this will be implemented for servers only as clients will not store data locally. A high-level DLP Discovery architecture overview is provided in the IDD for DLP Discovery (reference [33]).
- DLP for data in transit ("E-mail DLP") – DLP for data in transit is generally implemented as part of boundary protection services, however in ITM Recovery Increment 1, this is limited to external e-mail traffic.

All categories of DLP are dependent on data object classification and labelling functionality that will be implemented at clients. This functionality allows users to label files and e-mail messages with data classification metadata. Based on this metadata, a DLP security policy can be enforced by DLP Endpoint, DLP Discovery, and E-mail DLP.

An integration effort is required to ensure that a centrally managed DLP security policy is enforced coherently by DLP Endpoint, DLP Discovery, and E-mail DLP. This also requires a standardized and supported set of data classification metadata in line with NATO Security Policy.

Figure 3-50 depicts the DLP architecture and shows:

- The categorization of DLP functionality;
- DLP functionality that will be covered by ON-ECS-CS;
- DLP functionality that will be covered by ON-CPS-CS; and
- The dependency on data object classification and labelling functionality, to be covered by CPS.

Note that although the enforcement of 'DLP for data at rest' and 'DLP for data in use' on servers would architecturally fit under ON-ECS-CS, both clients and servers will be covered by ON-CPS-CS. This architecture calls for an implementation where clients and servers are covered by the same vendor and product suites.

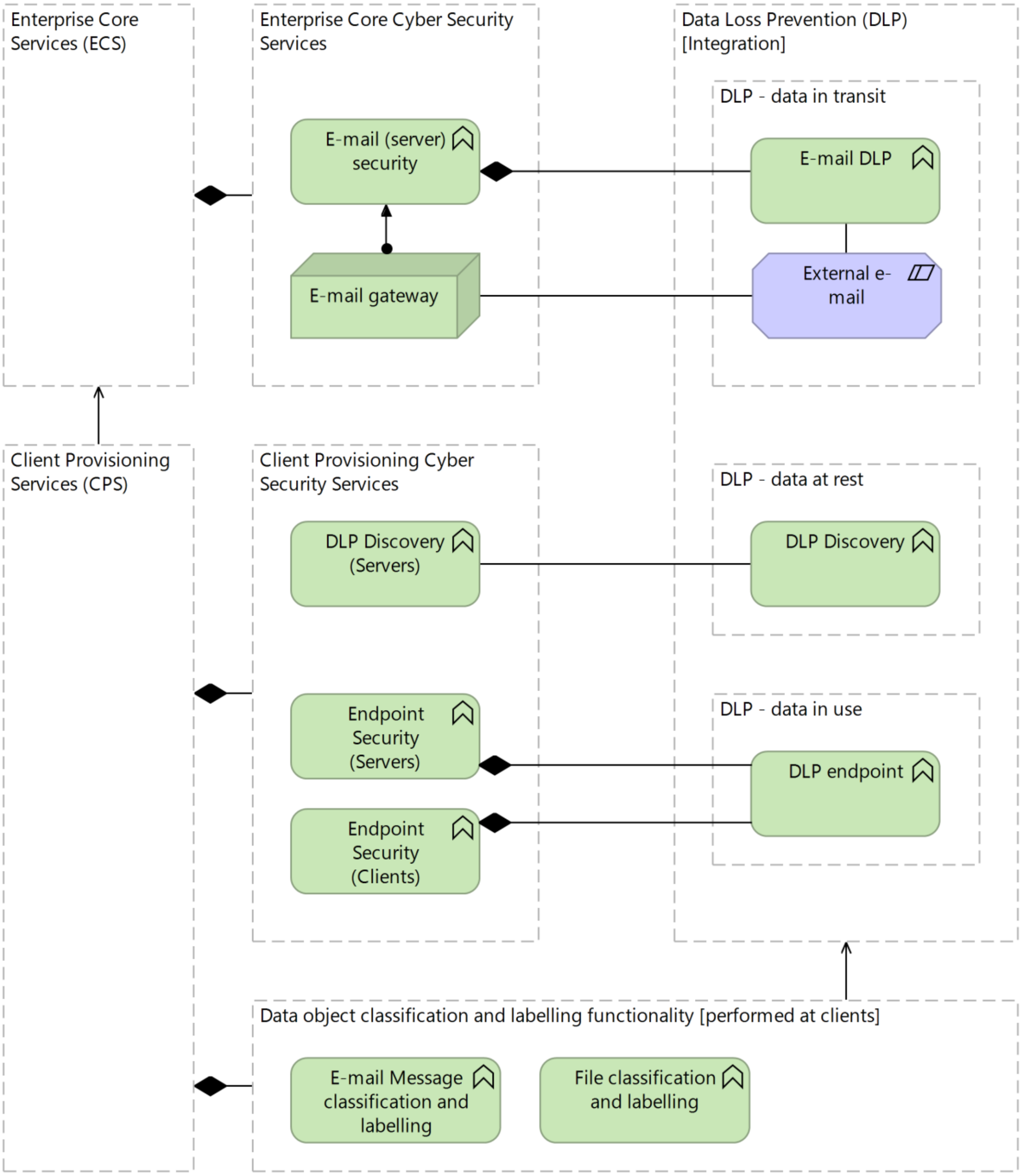

Enterprise Core Services (ECS)
Enterprise Core Cyber Security Services
Data Loss Prevention (DLP) [Integration]
DLP - data in transit
E-mail (server) security
E-mail DLP
E-mail gateway
External e-mail
Client Provisioning Services (CPS)
Client Provisioning Cyber Security Services
DLP - data at rest
DLP Discovery (Servers)
DLP Discovery
DLP - data in use
Endpoint Security (Servers)
DLP endpoint
Endpoint Security (Clients)
Data object classification and labelling functionality [performed at clients]
E-mail Message classification and labelling
File classification and labelling

Figure 3-50 DLP architecture

3.6. Lifecycle Management of ITM based Software

3.6.1. Introduction of the Key lifecycle stages and release pipeline

For the ITM based software, which is mainly COTS software with Software Based automation and orchestration artefacts, the NATO software policy guidance (reference [7]) is followed and the lifecycle phases as depicted in Figure 3-51 are applicable.

Following the guidance of the NATO Software Policy (see reference [7]), ITM is following a lifecycle based approach and will adopt a scheme of evolutionary and continual development, where software based development/configuration is applicable. The lifecycle concept for the release and deployment of software defined artefacts, defining NATO ON services, is depicted in Figure 3-51 below. The granularity of these artefacts range from a configuration update, a software patch, a virtual machine, a container, up to and including a full application suite/package. Such an artefact may include a day one realization or day 2 update of virtual machine and network aspects. Critical in this process are the release and change management authorities.

Fundamentally, the NATO ON services release pipeline covers four major lifecycle stages that engage various environments:

1. **Development and Integration**: Focus on development of the various SW elements and internal integration testing. On top of that the integration engineering and testing of external interfaces and end-2-end services effects and performance is executed in this stage. These activities are executed on in a Development and Integration Environment, which is out of scope of ITM Recover Incr1 implementation. In case Hardware based engineering aspects are relevant those may be included in this environment but main intent is to have a virtualised/simulated instance of the target environment platform.
2. **Formal release testing**: The formal release testing involves assessing the so-called “Release Candidate” and potentially achieving deployment authorization. This environment allows one to test SW features on the target production platform baseline.
3. **Deployment to the Production Environment**: final installation (test) and (performance) calibration procedures supported by the option of a utilising a staging environment and/or pre-production environment.
4. **Production and identification of changes.** Operated and monitored in the production environment that health and proper functioning of the software is maintained.

In case of issues remedial actions/or, at any of the stages in the lifecycle, changes may be necessary that will require issuing change requests that loop-back to the previous stages and possibly to the development stage causing a potential (new) release pipeline.

Figure 3-51 below illustrates the above mentioned release pipeline and environments engaged.

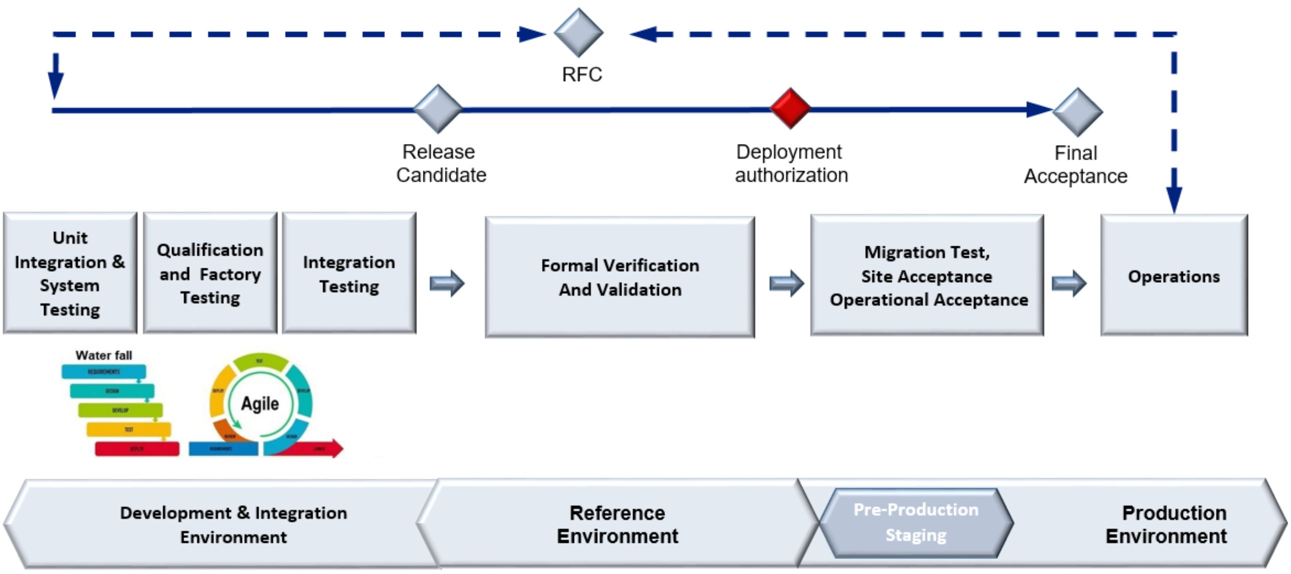

RFC
Release Candidate
Deployment authorization
Final Acceptance
Unit Integration & System Testing
Qualification and Factory Testing
Integration Testing
Formal Verification And Validation
Migration Test, Site Acceptance Operational Acceptance
Operations
Water fall
Agile
Development & Integration Environment
Reference Environment
Pre-Production Staging
Production Environment

Figure 3-51 Generic Release Pipeline

The agility of the Engineering and Integration Environment and the Reference Environment must support those of the Production Environment, the rate of initial CIS services deployment and the rate of configuration changes during operations.

3.6.2. Mapping to Environments

Figure 3-52 shows the logical environments and SW-artefacts information flow supporting the release pipeline introduced in the previous view (§ 3.6.1).

As part of the NATO Software Factory, the following elements can be identified:

- For a NU based release pipeline
    - NU level Development and Integration environments:
        - IREEN ON @NU as part of NSF CIS(Public Cloud and on premise equipment)
    - NU Integration Environment:
        - IREEN ON @NU as part of NSF CIS (Public Cloud and on premise equipment)
        - (fading) AIS reference (on premise)
- For a NS based release pipeline
    - NS level Development and Integration environment:
    - through NSF NU (public cloud) and (future) NSF NS (Azure stack)
    - NS level Reference Environment
    - (optional)National Software Factories, connected through Coalition Battle Lab Services
    - Pre-Production Environment (Service Staging)
    - ON Production Environment

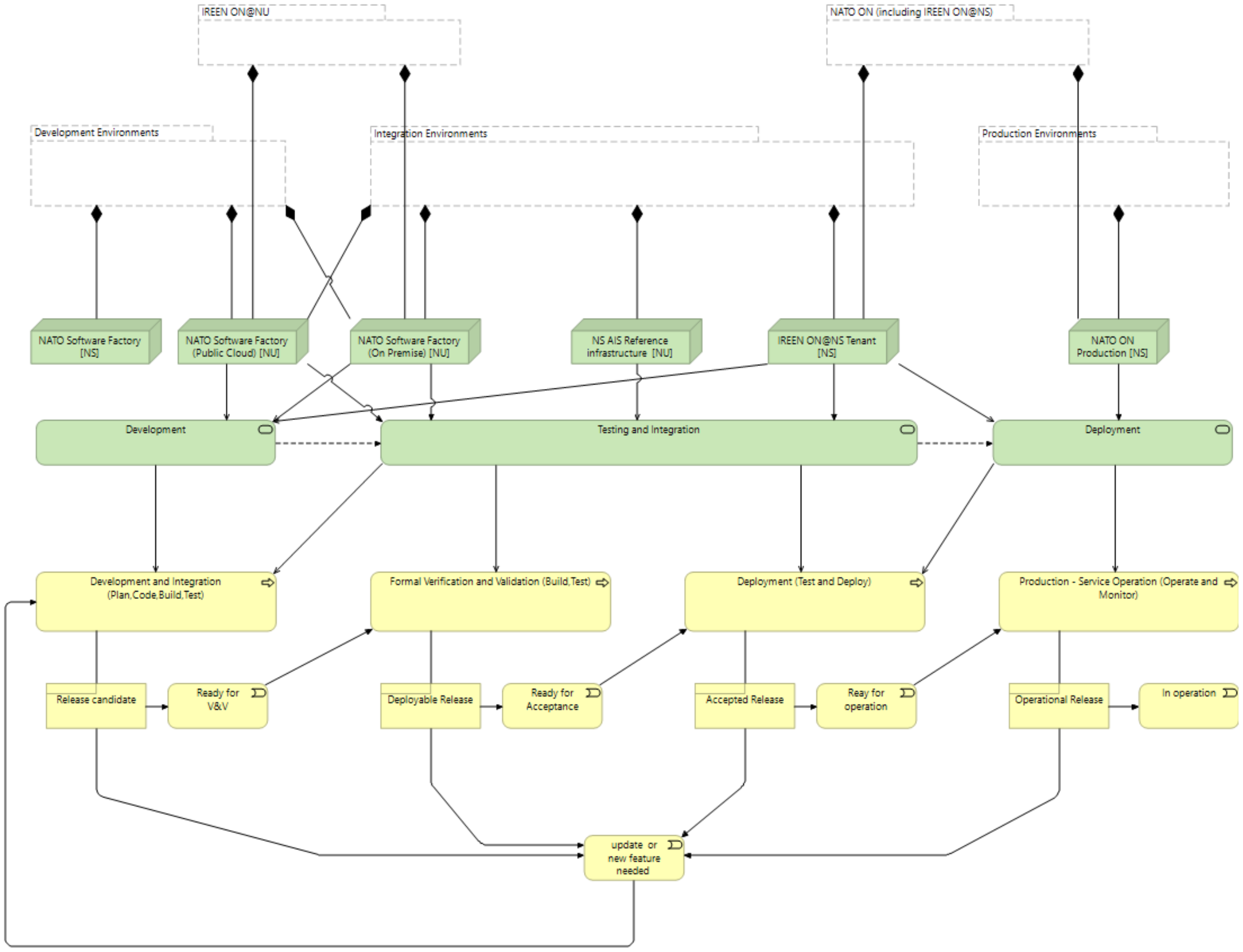

IREEN ON@NU
NATO ON (including IREEN ON@NS)
Development Environments
Integration Environments
Production Environments
NATO Software Factory [NS]
NATO Software Factory (Public Cloud) [NU]
NATO Software Factory (On Premise) [NU]
NS AIS Reference infrastructure [NU]
IREEN ON@NS Tenant [NS]
NATO ON Production [NS]
Development
Testing and Integration
Deployment
Development and Integration (Plan,Code,Build,Test)
Formal Verification and Validation (Build,Test)
Deployment (Test and Deploy)
Production - Service Operation (Operate and Monitor)
Release candidate
Ready for V&V
Deployable Release
Ready for Acceptance
Accepted Release
Reay for operation
Operational Release
In operation
update or new feature needed

Figure 3-52 ITM Services DevSecOps lifecycle mapping

For the transfer of SW artefacts from the one CIS Segment to another, the following boundary protection/gateways are required on the ITM side to support the flows identified:

- BPS 4: diode from NU to NS
- BPS 1: protect the ON environment
- IREEN BPS: both at NU and NS level: protect the IREEN environment from external interconnections.

3.6.3. Applicability of DevSecOps for ITM

During the design and implementation of the NATO ON, the intent is to leverage a DevSecOps approach from the start for the ITM software defined areas where this makes sense (most likely in the area of IaaS automation/orchestration – Infrastructure as a Code, Cyber Security and IDAM and SMC), to prepare all aspects (people, process, technology) and ensure the NATO ON can be changed and adapted based on the evolving NATO business requirements. For this the ITM capability will rely on extant NCIA processes and services that support this area. The services that ITM will rely upon are:

- PLT008: DevSecOps Services, provided through the NATO Software Factory (NSF) capability.
- PLT009: Enterprise Definitive Media Library (formal repository for publication of NATO SW artefacts)

4. Interface Definition Methodology

The NATO ON services and sub-services are identified in the service tree, documented in paragraph 3.2. For ease of reference, the technical CIS services, as far as relevant for ITM Recovery Increment 1, are summarized in paragraph4.1.2.

This paragraph describes the modelling of the service interfaces, relevant for ITM Recovery Increment 1, into a listing of interfaces. This artefact is referred to as the Interface Definition Document.

The actual Interface Definition Table, identifying for each relevant service the service interfaces and input/output relationships is included in the Interface Definition Document Table (reference [50]). This ADP, however, does not provide technical detail nor references to standards nor protocols for these interfaces; such detail is provided in the respective Interface Definition Documents (IDD) and Service Design Package (SDP) documents.

4.1. Interface Definition Model

This paragraph describes the modelling convention and the concepts used to model the exchange between services and to model the service interfaces.

- Paragraph 4.1.1 introduces the modelling concept
- Paragraph 4.1.2 summarizes the (technical) CIS services relevant for ITM Recovery Increment 1 for ease of reference
- Paragraph 4.1.3 summarizes the service access and provisioning concept for the various site types
- Paragraph 4.1.4 provides a reference to the IER definition for ease of reference
- Paragraph 4.1.5 identifies the high-level and aggregated service interface view to be further elaborated in the interface definition document.

4.1.1. Interface Definition Modelling Concept

This paragraph describes the high-level modelling concept. It introduces the concept of information exchange, provider and subscriber interfaces and the concept of provided and dependent services that the architects use throughout this architecture.

The list of interfaces across (sub) services is modelled through a concept of Information Exchange Requirements (IER) between (sub) services, served through an interface. In this context, “service” may refer to a technical service but may also refer to a business service (which in turn may be supported by underpinning technical services and human-executed processes).

The above mentioned interface, across which an IER is realized, is per definition provided by only one of the services that take part in this exchange. The provider service defines the detail of the interface such as interface profiles, standards, protocols, etc. This interface is referred to as the “provider interface”. The other side of the exchange is the subscriber. The subscriber may be a service itself, or the subscriber may be a user node. The subscriber uses the interface definition by the provider service and refers to the interface as a dependent interface.

Obviously the subscriber will have to realize the technical counterpart of the provider interface, the “subscriber interface” to reach the provider counterpart of the exchange. However, this architecture abstracts the subscriber interface and aggregates the subscriber and provider interface into a single object, which is defined and specified by the providing service. This modelling convention is further described in Figure 4 2 below.

As a real-life example of the concept described above, of the provider / subscriber concept, consider the following example. Consider a shop, a retail store. The provider service is represented by the shop. The provider interface is the person behind the counter. The subscriber is the person that is requesting a product or a service from the person behind the counter. I.e. the customer at the counter in this example is the subscriber; the counter represents technical means connecting the provider and the subscriber.

In this architecture, the concept of provider / subscriber is opaque to “push” or “pull” service provisioning. Hence, who is the provider and who is the subscriber is independent of who initiates the connection to exchange data. Referring back to the example of the shop, the architecture is agnostic if the provider delivers the service at home or that that the customer goes to the shop and if this is a subscription model or an on -demand request; from the perspective of the architecture the service and the interface is still what the service provider has defined.

The diagram below illustrates this service provider / subscriber concept and taxonomy.

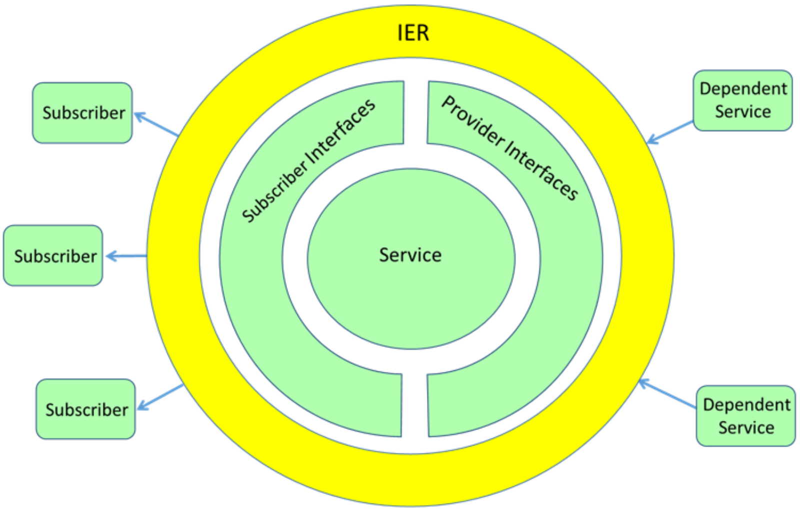


Figure 4-1 Service interface definition concept – NAFv4 S1

The concept of service provider / subscriber concept and taxonomy, introduced in Figure 4-1 above, is formalized through the “modelling of data exchange between services and the associated interfaces” view in Figure 4-2 below.

Figure 4-2 below shows a data exchange between CIS Service A and CIS Service B. This exchange is the basis of the interaction between two services. The exchange is served through the CIS Service B Interface and described through the CIS Data Exchange object. The latter is modelled in ArchiMate as an interaction, i.e. a collective behaviour (the exchange of data). In other words, the CIS Data Exchange is a technical representation of the IER.

Specifically, the view below describes the methodology for modelling the data exchange between services and modelling the associated interfaces. This methodology is based on ArchiMate 3.1 and, as modelled in Figure 4-2 below, describes an exchange between technology services (ICT services). However, the same methodology equally applies to the exchange between business services. Hence, the exchange between / with business services can be modelled the same way using business layer elements instead, including exchange between a technical and business service.

The exchange, the Information Exchange Requirement (IER) is modelled as the interaction describing the exchange, and a flow (of data) from one service to the other. These exchanges, modelled as an interaction, are unidirectional (ignoring any signalling, which may be bidirectional). That means that a bidirectional exchange, between services, is modelled through two interactions; one from A to B and one from B to A.

As a matter of principle, there is only one interface. It is the provider service that defines the interface as part of its service architecture building block (ABB), the consuming service is merely served through this provider interface. The consuming service's IDD and SDP refers to the provider's interface definition in the provider's IDD and SDP.

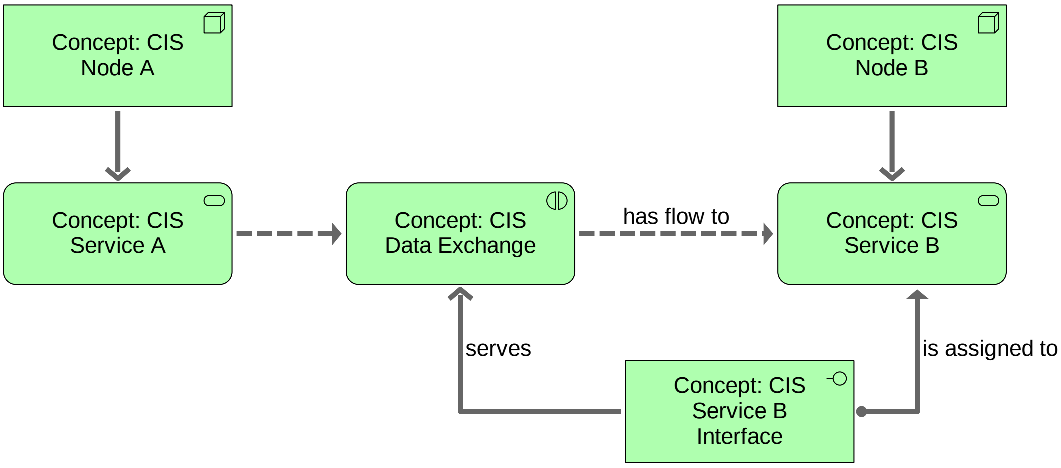


Figure 4-2 Modelling of data exchange between services and the associated interfaces

The naming convention for Interface IDs is as follows:

Interfaces are named from the perspective of the providing service, as illustrated above. That means that if, for example, the Enterprise Core Service (ECS) implements the interface, the interface is defined and named by ECS.

The generic structure of an Interface Name is as follows:

[Network] - [Service] - [Function] - [Logical/Physical] [sequence number]

Example: ON-CS-M-L04

Optional, interfaces may be referred to a specific instance through a suffix.

Example: ON-CS-M-L04-CPS

The "connecting service" suffix (in this example "-CPS") may only be used if it is necessary to refer a specific interface instance, i.e. between a pair of services or systems. When an interface (type) is used to serving multiple subscribers or subscribing services that are "connecting" to the same interface, one must not use the suffix.

For ITM Recovery Increment 1, the network is "ON". The service is an abbreviation of the service and defined in Figure 4 3 below. The Interface Definition Document Table (reference 50) identifies the relevant interfaces. The individual interfaces are detailed in the respective SDPs.

4.1.2. Services Overview

The starting point for documenting the service consumption and delivery model is the CIS service tree, which is introduced in the service tree documented in § 3.2.

For convenience, the diagram below takes the NATO ON CIS service tree and summarizes the (technical) CIS services that are relevant for ITM Recovery Increment 1. These CIS services are further linked to the so-called Service Access and Provisioning, identifying the entities that consume and provide services.

The following views will decompose these services as and where considered relevant.

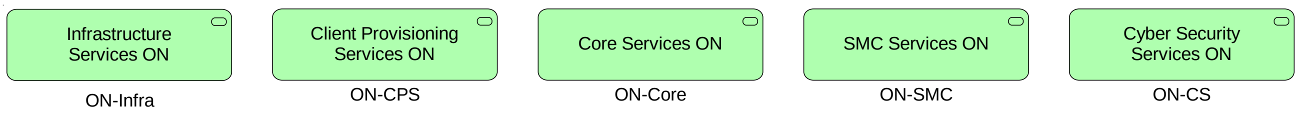

Infrastructure Services ON
ON-Infra
Client Provisioning Services ON
ON-CPS
Core Services ON
ON-Core
SMC Services ON
ON-SMC
Cyber Security Services ON
ON-CS

Figure 4-3 Most relevant technical services in scope this ADP

4.1.3. Service Access and Provisioning to/at NATO Enterprise Static Sites

This paragraph defines the provider / subscriber operational activity model, of which the concept is introduced in the description of the Interface Definition Model in § 4.1.1. This view considers the CIS services defined in § 3.2 and summarized in § 4.1.2 above.

The service access and provisioning is, from the perspective of the actors, differentiated in Static Users and Administrators.

Figure 4-4 below describes the high-level service delivery differentiated for Static Users and Administrators of the NATO ON, generalized for all NATO Enterprise Static Sites. (The NATO Enterprise Static Site types are identified in Figure 3-4.)

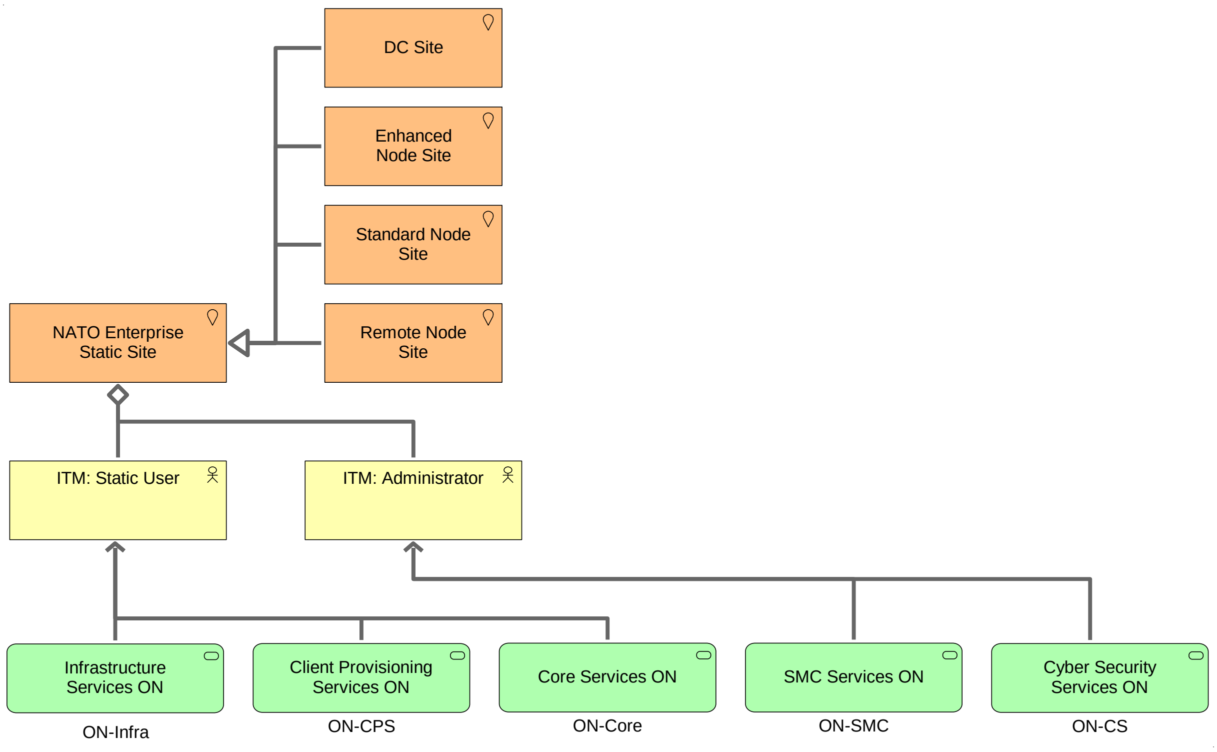


Figure 4-4 Services Accessible from Nodes by User Type

When considering both the "Service Hosting per Node Type" view, Figure 3-9 in paragraph 3.3.1, and the "Services Accessible from Nodes by User Type" view, in Figure 4-4 Figure 3-8above, service access is differentiated per type of site. That means that services are primarily served from the Data Centre. However, at the Enhanced Node includes local instances of essential Enterprise Core Services and local instances of Infrastructure Services to reduce the dependency on communications with the DC for local users. Furthermore, Standard Nodes include local instances of Infrastructure Services for local users. Remote Nodes have only the bare minimum to power the user equipment, all infrastructure, core and functional area services are served from the Data Centre.

The view in Figure 4-5 below defines the service provisioning from a Static User's viewpoint. The view in Figure 4-6 defines the service provisioning from an Administrator's[7] viewpoint. The Figure 4-7 lists the various administrator roles. Figure 4-6 is generally applicable for all so-called "ITM: Administrators" as listed in Figure 4-7. These administrators will be defined using the SFIA skills framework (reference [60]).

[7] More granular definition of user and admin types is required. Input process and workforce analysis will provide the required details. This is essential to provide the architecture guidance for effective identity and access management.

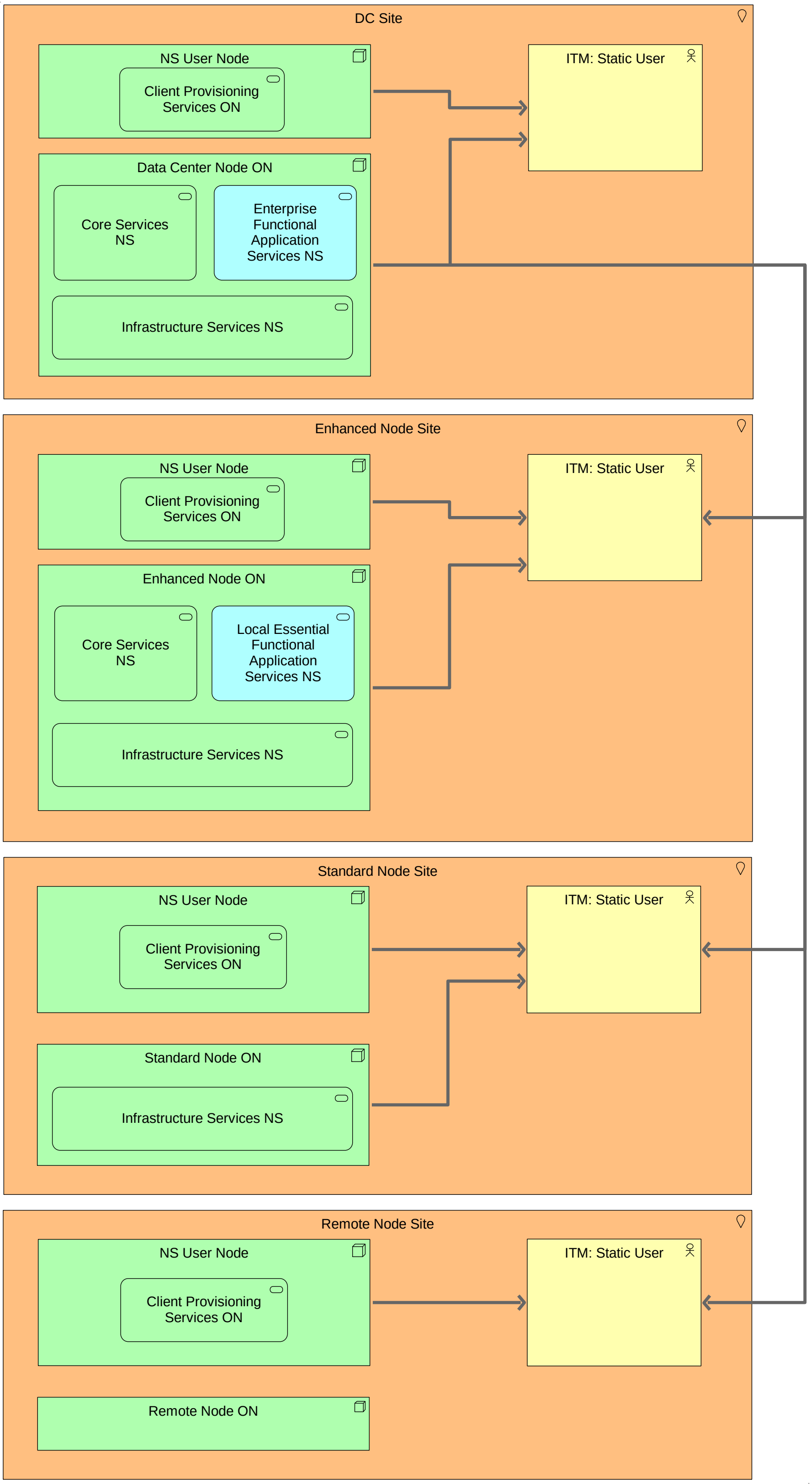

DC Site
NS User Node
Client Provisioning Services ON
ITM: Static User
Data Center Node ON
Core Services NS
Enterprise Functional Application Services NS
Infrastructure Services NS
Enhanced Node Site
NS User Node
Client Provisioning Services ON
ITM: Static User
Enhanced Node ON
Core Services NS
Local Essential Functional Application Services NS
Infrastructure Services NS
Standard Node Site
NS User Node
Client Provisioning Services ON
ITM: Static User
Standard Node ON
Infrastructure Services NS
Remote Node Site
NS User Node
Client Provisioning Services ON
ITM: Static User
Remote Node ON

Figure 4-5 Service Provisioning by Origin – Static User Viewpoint

Note in the view below the ESOC Site. The ESOC is not shown in the Static User's (U1) viewpoint. Needless to say that users in the ESOS Site also access specific Infrastructure, Core and Client Provisioning Services, but for clarity these are not included in the Administrator's viewpoint.

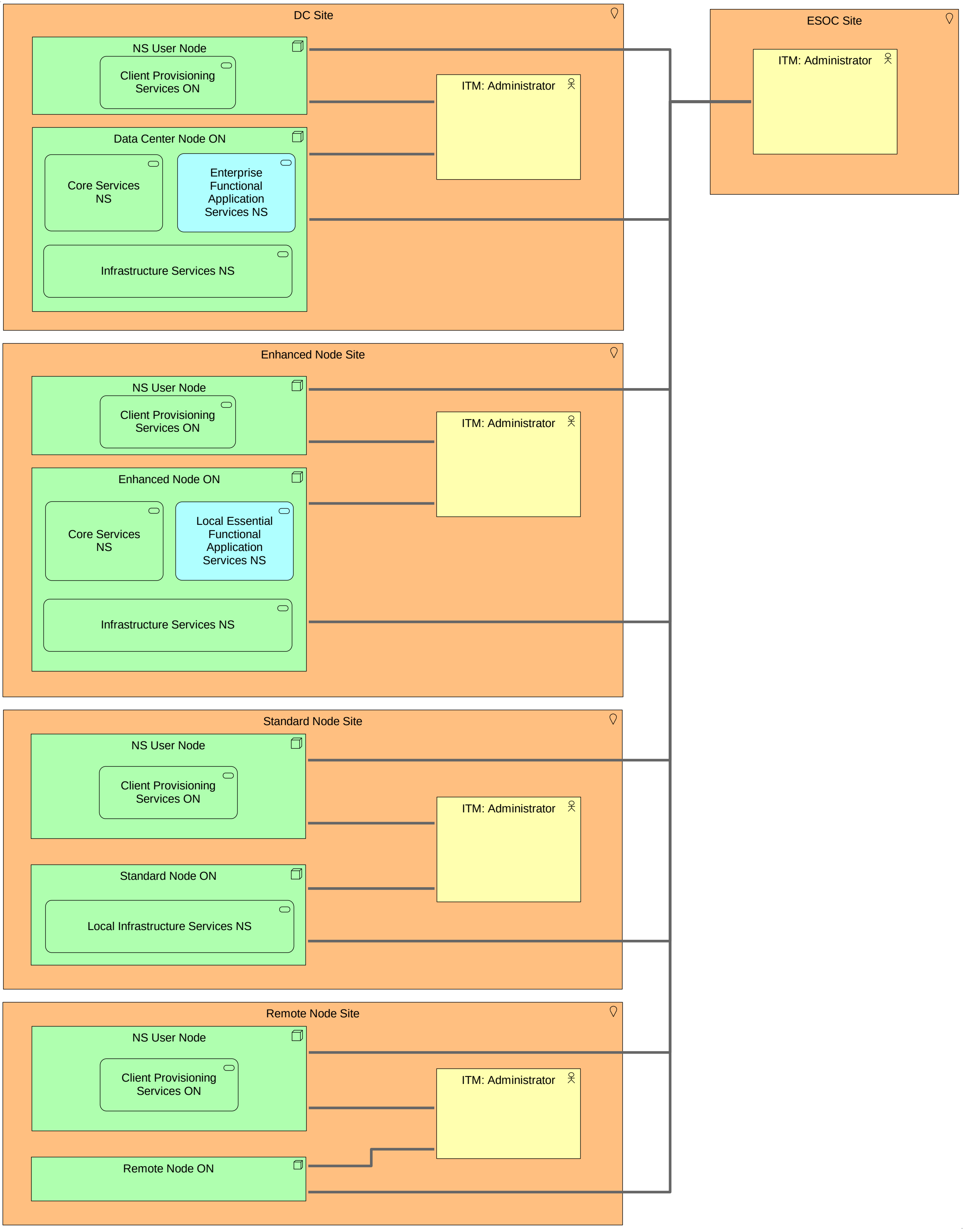

DC Site
NS User Node
Client Provisioning Services ON
Data Center Node ON
Core Services NS
Enterprise Functional Application Services NS
Infrastructure Services NS
ITM: Administrator
ESOC Site
ITM: Administrator
Enhanced Node Site
NS User Node
Client Provisioning Services ON
Enhanced Node ON
Core Services NS
Local Essential Functional Application Services NS
Infrastructure Services NS
ITM: Administrator
Standard Node Site
NS User Node
Client Provisioning Services ON
Standard Node ON
Local Infrastructure Services NS
ITM: Administrator
Remote Node Site
NS User Node
Client Provisioning Services ON
Remote Node ON
ITM: Administrator

Figure 4-6 Service Provisioning by Origin – Administrator Viewpoint

The "ITM Administrator", identified in Figure 4-6, represents administrators assigned to any of the roles introduced in the view in Figure 4-7 below.

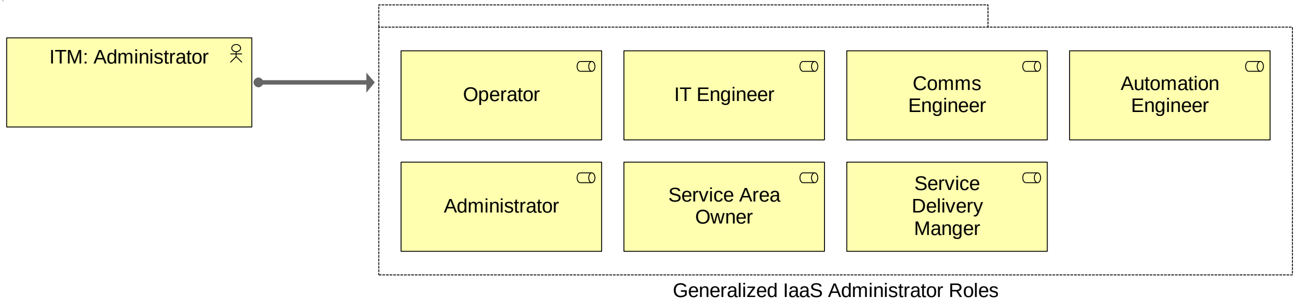


Figure 4-7 Generalized set of Identified Administrator Roles

Note that the generalized set of Identified Administrator Roles, introduced in Figure 4-7, will be further developed in due course.

4.1.4. Information Exchange Requirements

NATO CIS Nodes, across the NATO ON, interact with each other, with users and administrators (both modelled as actors) and with external entities. The interactions, or needlines, represent a need or requirement to exchange information or communicate. The IDD Table (reference [50]) addresses the (technical) exchange between CIS services.

4.1.5. Interfaces

This Service Interfaces View, in Figure 4-8 below, identifies the high-level NATO ON services and associated interfaces, as far as relevant for ITM Recovery Increment 1. In this view we aggregate all interfaces per high-level service.

The Interface Definition Document Table (reference [50]) provides a list per service, which decomposes these interfaces, per service, in provided and consumed interfaces (dependent interfaces).

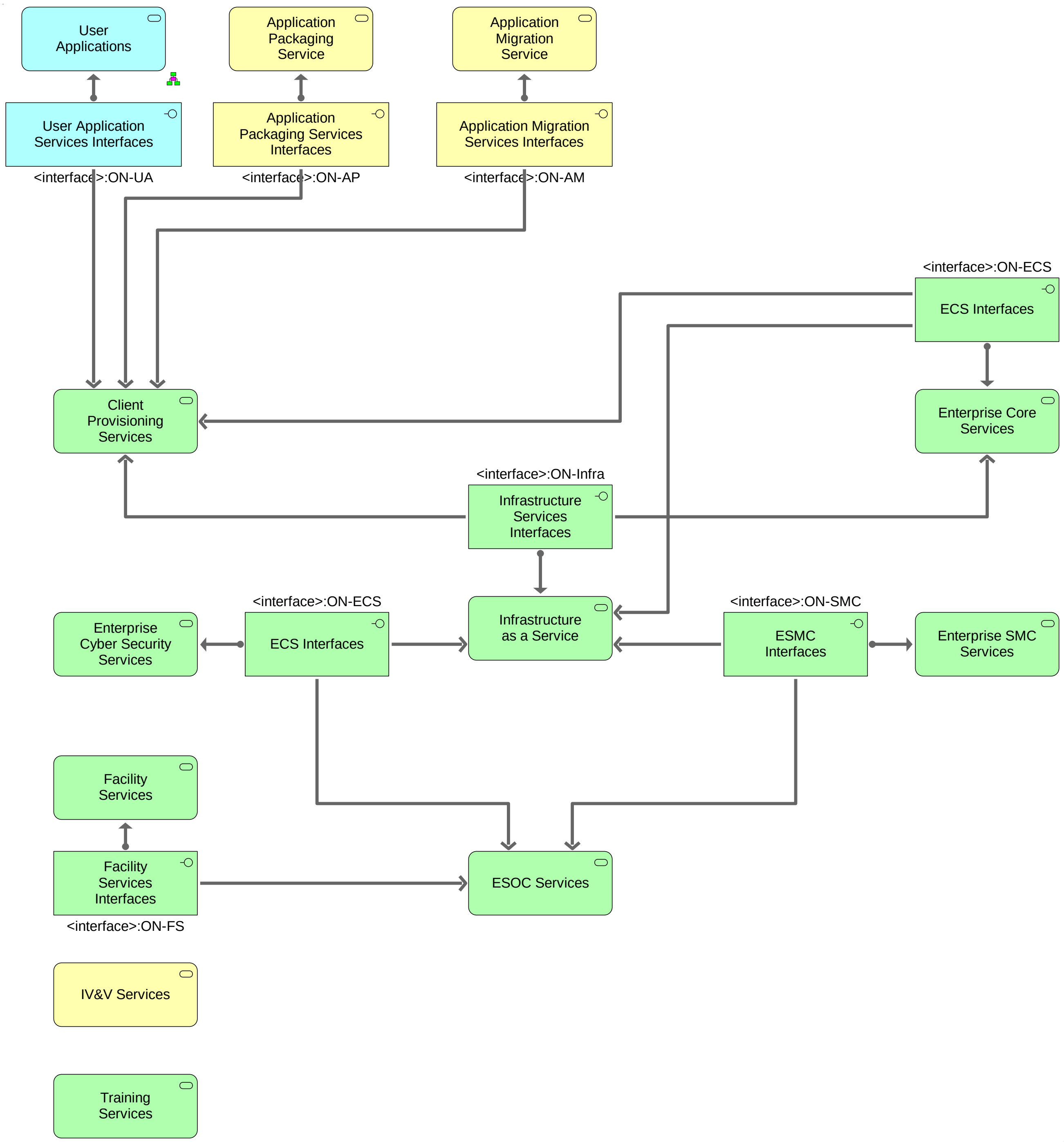

User Applications
Application Packaging Service
Application Migration Service
User Application Services Interfaces
Application Packaging Services Interfaces
Application Migration Services Interfaces
<interface>:ON-UA
<interface>:ON-AP
<interface>:ON-AM
<interface>:ON-ECS
ECS Interfaces
Client Provisioning Services
Enterprise Core Services
<interface>:ON-Infra
Infrastructure Services Interfaces
<interface>:ON-ECS
<interface>:ON-SMC
Enterprise Cyber Security Services
ECS Interfaces
Infrastructure as a Service
ESMC Interfaces
Enterprise SMC Services
Facility Services
Facility Services Interfaces
ESOC Services
<interface>:ON-FS
IV&V Services
Training Services

Figure 4-8 High-level interface graph (as relevant for ITM Recovery Increment 1) – NAFv4 S3

4.2. Interface Definition elements

This paragraph introduces the taxonomy of the so-called Interface Definition Document, or IDD for short. The Interface Definition Document identifies per service the provided and dependent (subscribing) interfaces.

The Interface Definition Document (IDD) builds on and combines the following concepts:

- Services Overview
- Service Access and Provisioning at NATO Enterprise Static Sites

- Information Exchange Requirements
- Service Interfaces

These concepts are introduced in the paragraphs 4.1.1- 4.1.5 above.

The interface document identifies:

- **Interface ID**: The unique Interface Identifier, using the naming structure as introduced in the IDD in paragraph 4.1.1.
  - The unique interface identifier.
  - Each interface is uniquely named, defined by the providing service and re-used by services that depend on this service by referring to the Interface Instance ID.
- **Service Description**: Reference to the service function that this interface relates to.
  - Refers to "Concept: CIS Service" and specifically the service function realizing the CIS service.
  - Refers to the (sub) service as introduced in NATO ON service tree, in Figure 3-2, and summarized (aggregated) in Figure 4-3.
- **Interface Instance Description**: A high-level reference to the technical exchange between CIS services across a specific interface instance.
  - Refers to "Concept: CIS Data Exchange" in Figure 4-2.
  - The Interface Instance Description is a brief description of the usage of this interface instance.
- **Level of Detail**: The required level of detail that the SDP and IDD shall provide.
  - Guidance to SDP and IDD.
  - Options: High/Low level.
  - Where interfaces are actually well known and well understood industry standard interfaces that require little detailing for a 3rd party to realize in such a way that services that depend on this service can utilise it, the required level of detail is low.
  - If the interface is bespoke, requires NATO specific tailoring or is inadequately standardized or universal, the required level of detail is high.

The identification of relevant services interfaces is provided in the Interface Definition Document Table (reference [50]). Detail is provided in the respective SDP and IDD.

5. Availability and IT Continuity of Services Model

5.1. Introduction

The NATO ON services availability and IT continuity of service model applies for IaaS, SMC, ECS and CPS alike. The following paragraphs contain a definition of the model, provide the minimum-level scenarios for IT continuity of service and provides information about SMC KPI driven aspects.

Herein the focus is on the technical aspects, as an enabler for a holistic approach (including people and process) for availability and IT continuity of services, including:

- Achievement of the relevant people and processes as part of the ESOC, Enterprise SMC and Service Integration efforts;
- Achievement of logistics functions.

The availability and IT continuity of services are addressed in the Domain and Element SMC functions that support the automation of planning, management, control and administration in support of availability and disaster recovery. These Domain and Element SMC functions integrate through the interfaces at business and technical level) with the ESOC and Enterprise SMC. The interface dependencies are identified in the Interface Definition Document Table (reference [50]).

The final part of this chapter is addressing the implementation aspects (strategy) that will be followed to achieve the required service availability and IT continuity of service levels.

5.1.1. Generic Availability and IT continuity of Service Model

Figure 5-1 introduces the basics, considering the dimension of time, of the ITM availability and IT continuity of service modelling:

- Normal service operation can be interrupted, reported as an incident, in two ways:
    1. A (normal) service interruption
    2. A recognised disaster.
- These incidents are followed up in two different ways:
    1. A normal service interruption is resolved via a service restoration sequence.
    2. A disaster is followed up by a sequence of disaster response and disaster recovery activities.
- In section 5.2, the ITM service availability model and service levels will be introduced; this section will deal normal service interruption situations.
- In section 5.3, the ITM IT continuity of service model will be introduced; this section will deal with disaster response and recovery situations.

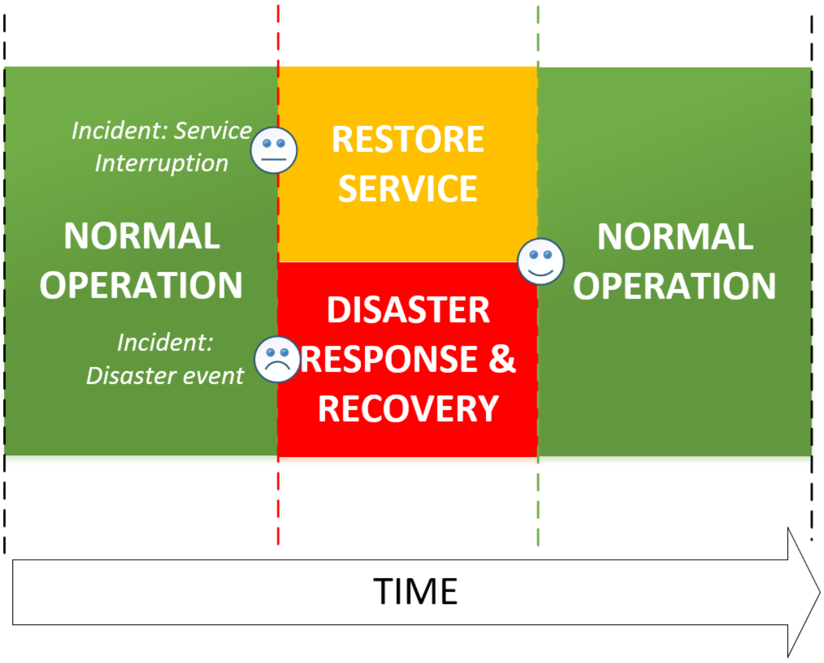


Figure 5-1. Basic Model for Service Availability and IT Continuity of Service

5.2. ITM Service Availability Model and Service Levels

Before zooming in at the non-functional requirements (NFR) required level of availability, capacity and maintainability it is worthwhile to provide some more background on availability theory and terms and definitions.

First of all it is useful to explain the relationship between the terms availability, reliability and maintainability:

- Availability is defined as the probability that the system is operating properly when it is requested for use.
- Reliability represents the probability of systems to perform their required functions for a desired period of time without failure. Reliability, does not account for any repair actions that may take place.
- Maintainability is a characteristic of design and installation, expressed as the probability that a system will be restored to a specified condition within a given period of time. The ease with which maintenance of a functional unit can be performed in accordance with prescribed requirements.

Bottom line: maintainability is the main factor for downtime duration of a system/service. The relationships of the terms as identified above are depicted in Figure 5-2. The diagram above should be read as follows: from left to right, if the reliability stays the same (yellow horizontal arrow), and the maintainability reduces (red down arrow), the availability goes down. Etc… (Backtracking from right to left, if the availability goes down, the reliability or the maintainability (or both) must have gone down.)

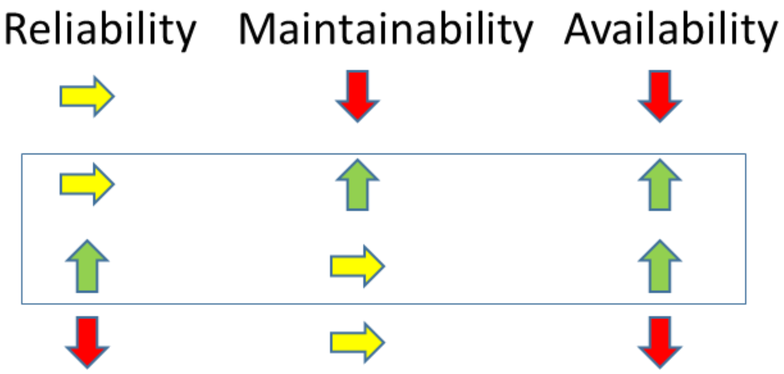


Figure 5-2. Availability-Reliability-Maintainability relationships

The NATO ON implementation shall focus, from a technical perspective, on:

- Intrinsic availability of the end-to-end services build from the (hardware/software) components.
- Defining KPIs, defining metrics that are captures that help to calculate the Achieved and Operational Availability.

Taking the theory forward the following Availability definitions are included to manage and control the ITM Recovery Increment 1 Services Implementation, based on the NATO ON design (e.g. SDPs), address the fulfilment of the required IaaS/ECS/CPS/ESCM service levels:

Intrinsic availability is the theoretical availability of the system. This is based on the Mean-Time Before Failure (MTBF) and the Mean-Time To Repair (MTTR). It is assumed that the necessary support is in place (spares, support, test equipment, and personnel). Intrinsic availability is expressed as a percentage per year, using the following formula:

Ai = 100 x (MTBF / (MTBF + MTTR)); and

Operational availability takes all aspects of the achieved availability into account and will be monitored end-to-end. This includes all components that are a part of the end-to-end service, even those that are not under the responsibility of the ITM Recovery Increment 1 Project such as the WAN equipment, application availability and the operational support services. Operational Availability is expressed in a percentage per month, using the following formula:

Ao = 100 x (uptime – downtime)/uptime*.*

The focus for the NATO ON availability design will be to work-out the (system) availability design based on the intrinsic availability definition. The Operational availability definition is relevant for the SMC services in support of Service Level Management, IT Service Continuity Management and Availability Management, including support to end-to-end monitoring/reporting functions.

The technical design, however, shall work towards achieving IaaS Service Levels used for in-service operations and handling incidents are based on 4 service levels, which are introduced in the SOR/MER (reference [2]). These 4 service levels are referred herein as so-called “L-levels” (not to be confused with Service Restoration Priority Levels (P-levels) for systems support as in used for the CSLA). The Key Performance Indicators (KPI), which define these 4 L-levels for ITM Recovery

Increment 1, are outlined in Table 5-1 below. It shall be noted that the required 99.99% availability (L1) is only applicable for services accessed at and from the DC location. The L-levels shall be considered as Operational Availability requirements for the IaaS services.

Table 5-1. NATO ON infrastructure availability Levels

L-level	Availability (%)	System Minimum MTBF (hours)	System Max Allowable MTTR (hours)	Access Location
L1	99.99	10000	1	DC-only
L2	99.9	1500	2	All Node Types
L3	99	350	4	All Node Types
L4	98	300	7	All Node Types

The availability percentages for the above introduced L-Levels, L1…L4, specified in Table 5-1 above, are defined in the SOR/MER 21 (reference [2]). The System MTBF and MTTR are not explicitly specified in the SOR/MER 21, but are based on technical analysis stemming from the original ITM design. Note that in contrast to the typical service level agreement, the MTBF and MTTR herein are not monthly averages but absolute numbers. That means that these System MTBF and MTTR, as defined in in Table 5-1, must be understood as a maximum of [MTTR hours] service unavailability, once per [MTBF hours]. I.e. for example, L1 Availability = 100% - 1/10000 x100% = 99.99%.

Based on technical analysis stemming from the original ITM design, for specific ECS, for SMC and for CPS Services, specific (operational) service availability levels and system MTBF and MTTR are required. These service levels are specified in Table 5-2.

Table 5-2. ECS, SMC and CPS availability Levels

ECS/CPS service	Availability (%)	System MTBF (hours)	System MTTR (hours)
ECS: Email	99	350	4
ECS: Portal	99	350	4
ECS: SfB	99	350	4
SMC	99,9	1500	2
CPS Client Application Provisioning Service	99.9	1500	2

5.2.1. Availability Automation Enabled by SMC Functions

Availability planning, management, control and administration are enabled and automated through SMC services at the enterprise, domain, and element levels. Table 5-3 below identifies the SMC functions at each of these levels that support availability requirements.

Table 5-3. Availability Automation Enabled by SMC Functions

Availability Support Area	SMC Function	SMC Level		
		Enterprise	Domain	Element
Planning	Capacity optimisation monitors and optimises resource use, scheduling and spare information to achieve required service levels	●	●	

Management	Manage configurations to achieve required availability	●	●	●
Control	Collection, review, and alert triggering based on health, performance, availability and capacity information	●	●	●
Administration	Operations management and site recovery management automates failover to support availability requirements	●	●	

5.3. ITM Continuity of Service Model and Service Levels

First we consider the terminology that is used for identifying NATO ON related “disaster events” to be covered in the IaaS design.

Disaster: The NATO ON does not operate as planned due to a major event that leads to a significant impact on the ability of the organisation to conduct its business. The processes to recover from this state are defined by continuity management, which include:

- **Disaster Recovery (DR)** to restore the service,
- and **Disaster Response** that defines the critical minimum degraded service levels, based on business priorities and the identified disaster scenarios.

In defining service level for IT continuity of service the following service levels are used:

- **Recovery Time Objective** The Recovery Time Objective (RTO) is the targeted duration of time and a service level within which a business process must be restored after a disruption in order to avoid a break in business continuity.
- **Recovery Point Objective** A Recovery Point Objective (RPO) is the maximum acceptable interval during which transactional data is lost from an IT service.

Compared to a “normal” service interruption which is expected to be resolved within the SLA availability target and maximum time to restore a services the disaster recovery measures in its Recovery Time Objective (RTO) the time it takes to recover from a disaster event.

The disaster scenarios are identified as a part of the Business Impact Assessment and risk assessment.

For the purpose of initial NATO ON services planning, a disaster can be defined as an event leading to any of the following effects:

- losing WAN communication from any of the Data Centres, nodes or client-only sites;
- destruction of any site;
- disabling more than 30% of back-end IaaS components
- disabling more than 30% of client components
- unavailability of any service (hosted on IaaS) of Business Criticality 1 for more than 24h

NATO ON services will have to fulfil the following Disaster Recovery related Service Levels for IaaS and ECS/CPS/SMC, shown in Table 5-4 and Table 5-5 respectively, as originally derived from the SOR2019 and related to the L-levels introduced in paragraph 5.2.

Table 5-4. IaaS Disaster Recovery Service Levels

Level	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)
L1	N/A	N/A[8]
L2	4 hrs	8 hrs
L3	12 hrs	24 hrs
L4	48 hrs	48 hrs

Table 5-5. ECS/CPS/SMC Disaster Recovery Service Levels

	RTO	RPO
ECS: Email	4 hrs	8 hrs
ECS: Portal	4 hrs	8 hrs
ECS: Skype for Business	4 hrs	8 hrs
Application Provisioning Service	4 hrs	8 hrs
SMC	N/A	N/A

5.3.1. Disaster Recovery Automation Enabled by SMC Functions

The required service levels are achieved by a combination of technologies, people, processes and procedures as outlined in Table 5-6below.

Table 5-6. Disaster Recovery Automation Enabled by SMC Functions

Availability Support Area	SMC Function	SMC Level		
		Enterprise	Domain	Element
Planning	Provides visibility into capacity use and collects and analyses resource utilisation, schedule and system spare information to support capability planning to ensure availability.	●	●	
Management	Monitors events, health status, capacity and availability of resources for replications and backups.	●	●	●
Control	Sets data replication policies for of block level and NAS/file level storage replication to support identify application recovery level. Schedules data backup replication activities and backup archival activities.	●	●	●
Administration	Operations and site recovery management automates disaster recovery processes to meet requirements.	●	●	

[8] NCIA has identified that zero RTO/RPO with non-synch connected DCs and ENs is technically/theoretically not feasible. The understanding is that L1 data services will be backed up in a way that the RPO will be minimized. Further analysis is needed during the DC/EN failover scenario testing.

5.4. KPIs

The NATO ON Service Levels can proactively be managed through monitoring of IaaS/ECS/CPS SMC domain and element level KPI parameters and potentially combined with automation and orchestration triggered thresholds set. Also, through the either the Domain and/or Enterprise SMC tools KPI related metrics shall be recorded across well determined time windows in support of the various Enterprise SMC processes (e.g. service (level) management, reporting, planning, problem management, etc.).

The IaaS/ECS/CPS SDPs shall include KPI tables as part of the SDP SMC-KPI sections, but in summary for the service areas:

- IaaS KPIs, among others, include a series of subcomponent utilization and performance KPI's with set thresholds. For the IaaS BPS and Networking services the throughput and events such as package loss and blocked URLs are identified.
- ECS KPIs, among others, include KPI's that measure end-2-end performance and delivery of ECS services and measuring capacity and scale of usages (measure against set thresholds such as maximum number of participants in a skype conference).
- CPS KPI, among others, include KPIs that measure end user client platform and client application performance from a user perspective. The supporting infrastructure is monitored on capacity thresholds (such as maximum number of concurrent VDI instances supported via the VDI backend).

5.5. NATO ON Availability Implementation Strategy

As ITM Recovery Increment 1 is implementing an infrastructure based on a single availability zone within a single region per Data Centre, it is understood that the required L-level 99.99 cannot be achieved at the infrastructure level (e.g. IaaS). Therefore, for the ITM Recovery Increment 1, timeframe the goals and objectives in this area are:

- Achieve the infrastructure Availability level for infrastructure that can be achieved with the single availability zone per region architecture;
- Define the KPI's and collect statistical evidence on the achieve availability levels.
- Ensure the IaaS architecture can be enhanced in future to achieve and measure the availability service levels.
- Considering FAS/Application Measured and Achieved Availability Levels (via the available QSLRs and as reflected in the CSLA) to validate the IaaS can support the same or better availability level for the applications. In case of consistent underperformance redesign of either the FAS or supporting IaaS services may be required.