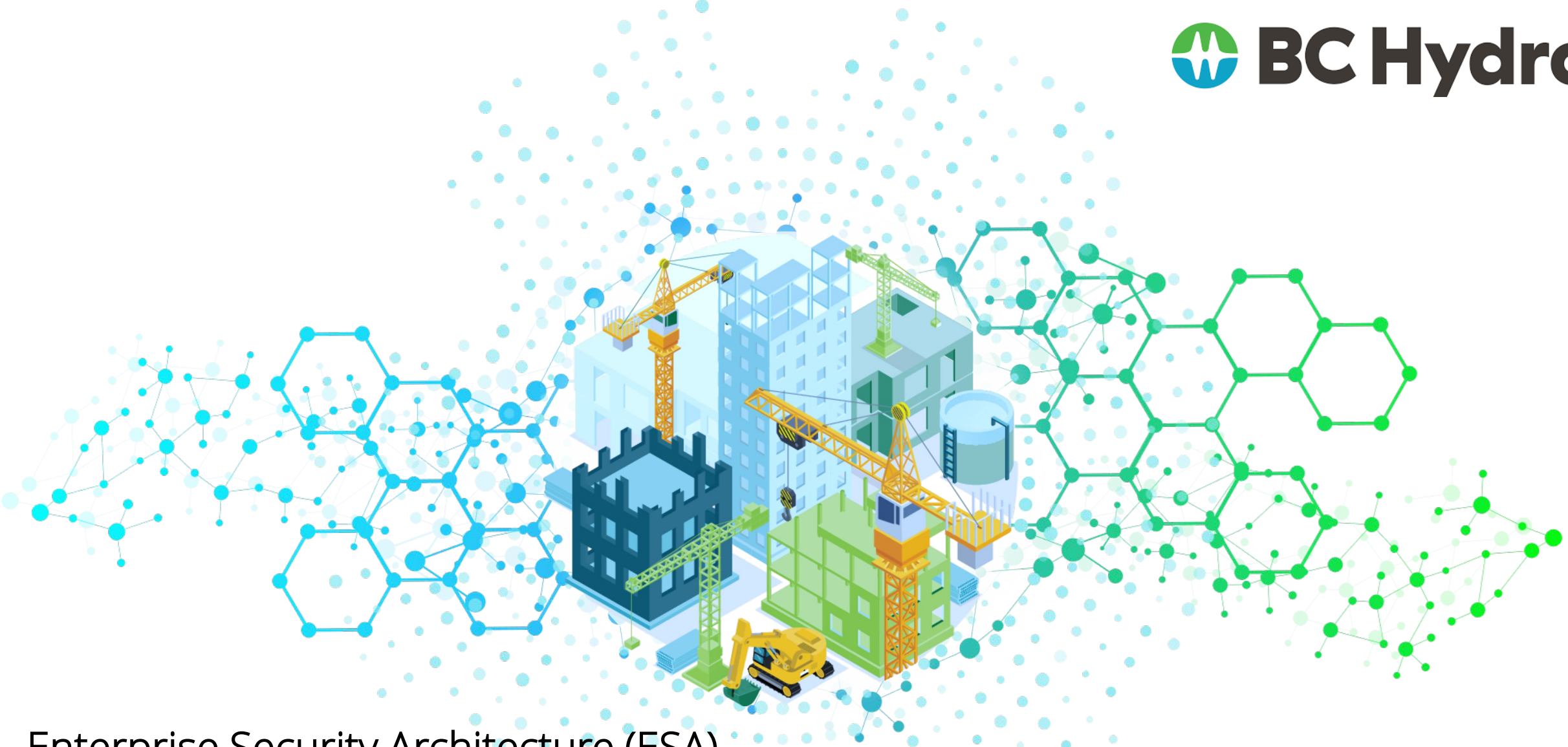


Enterprise Security Architecture (ESA)

Prioritized Roadmap – FULL VERSION

BC Hydro - December 2023 v1.0 | FINAL

Contents

Enterprise Security Architecture

Executive Summary

Enterprise Security Architecture Overview

The Enterprise Security Architecture (ESA) assists in providing answers to "What, Where, and How" BC Hydro's IT and OT systems deliver the cyber security outcomes required to manage cyber threats.

Background

- In July 2022, BC Hydro approved a Cyber Security Plan (CSP) that set out 10 planned initiatives which incorporated TRA recommendations identified as part of Directive 8.
- The Enterprise Security Architecture (ESA) is a foundation initiative of the CSP and is an important input to guide the implementation of the CSP.

What is the ESA?

- The ESA is a set of guidelines, strategies and governance statements that provides a comprehensive approach to maintain strong IT and OT cybersecurity controls.
- It provides a roadmap* to the desired future structure of BC Hydro's cyber security processes, systems, and personnel.
- The ESA was developed in alignment with recognized industry architecture frameworks as well as NIST**.
- The ESA considered BC Hydro's business and technology strategies as well as IT and OT constraints.

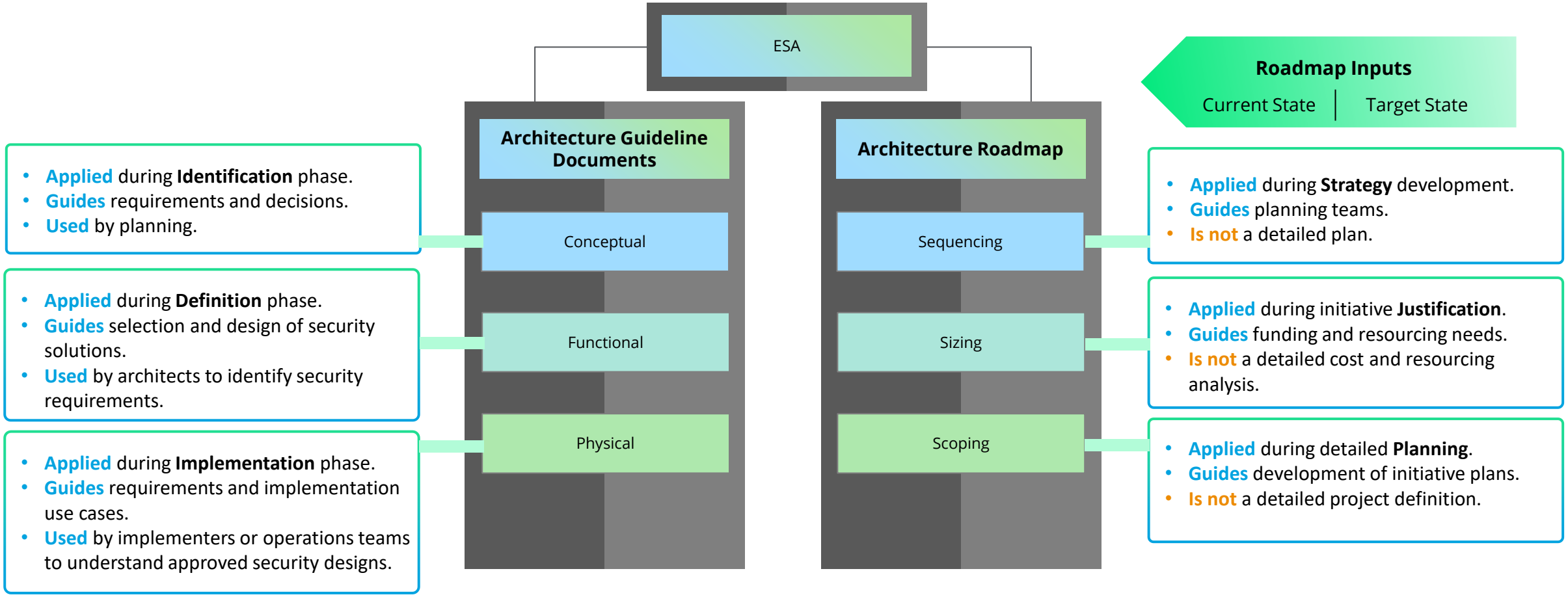
* The ESA roadmap is not an implementation plan, but represents a high-level strategy and sequencing of activities to achieve the desired target cybersecurity architecture capabilities

** BC Hydro is participating in a pilot of NIST under the BCUC Order G-126-23 (June 2023).

Structure and Use of the ESA

Using the ESA, Enterprise Architects can guide the requirements and design approaches for cyber initiatives and investments* across IT and OT.

ESA also provides guidance to Solution Architects to ensure use of repeatable approaches towards achieving desired outcomes.

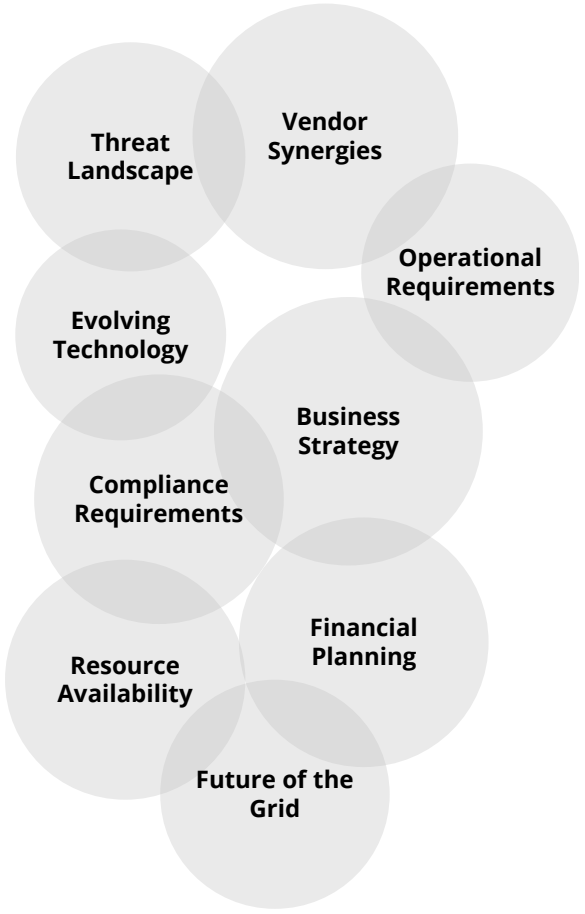


* The ESA applies to Cloud and on premise IT and OT architecture.

Sustainment of the ESA

The ESA is considered a **living document** that must be maintained based on input, direction and consideration of BC Hydro's needs and is influenced by the organization.

Ongoing Considerations



Use and Sustainment Roles

EA*	Cybersecurity	IT and OT Teams	Compliance	Procurement

The ESA should be maintained in order to guide design decisions, requirements and implementation planning.

Enterprise Architecture (EA)	The ESA should be referenced as part of strategic planning to ensure alignment with BC Hydro security objectives.
Cybersecurity	The BC Hydro Security Strategy drives new security requirements and serve as a key input for the development and maintenance of the Enterprise Security Architecture (ESA).
IT and OT Teams**	Solution designers should consult the ESA's reusable Patterns when developing solutions to ensure standardization for deployment of technologies and solutions.
Compliance	The ESA should be maintained in alignment with BC Hydro's overall risk landscape and compliance imperatives
Procurement	The ESA should be consulted in order to evaluate the planned technology solutions and designs in order to meet the principles and trust model requirements.

* Enterprise Architecture will hold primary responsibility to maintain the ESA, working with key business functions
** Sustainment of capability would be addressed within operating models. Links into the op model has been identified. The operational teams will need to consider the sustainment requirements as part of implementation planning.

Roadmap Approach

- The Roadmap has been developed based on extensive consultation with IT and OT architects and security leaders.
- The Roadmap is directional in nature and does not replace more detailed roadmaps such as the Identity and Access Management and Cloud roadmaps.
- Roadmap items serve as input to guide the development and implementation planning of cybersecurity and technology initiatives within BC Hydro's IT and OT.

Address BC Hydro's Cybersecurity Threats

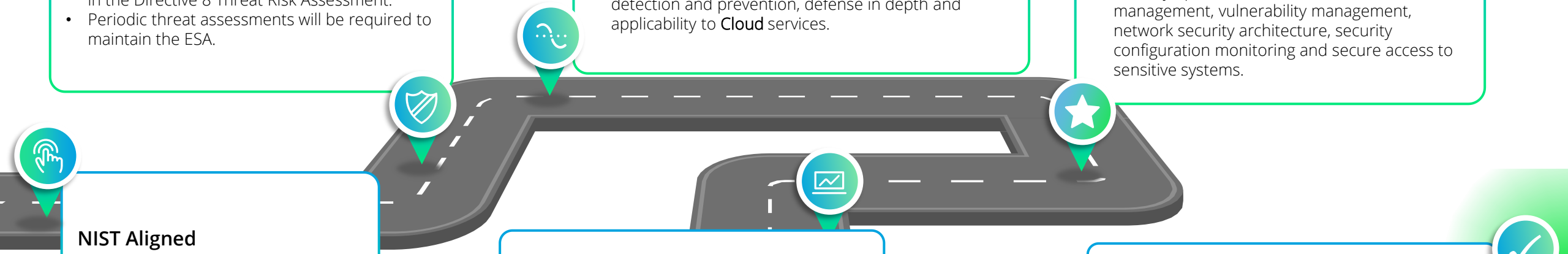
- This roadmap considered the threats identified in the Directive 8 Threat Risk Assessment.
- Periodic threat assessments will be required to maintain the ESA.

Apply the ESA Principles

- The roadmap encompasses the ESA principles related to zero trust, adapting to the threat landscape, use of proven standards and technologies, prioritizing both detection and prevention, defense in depth and applicability to Cloud services.

Implement Directive 8 Recommendations

- Addresses Directive 8 TRA recommendations and encompasses the CSP initiatives related to security operations, enhanced detection, access management, vulnerability management, network security architecture, security configuration monitoring and secure access to sensitive systems.



NIST Aligned

- The ESA was developed based on recognized EA standards and links to NIST CSF through its Functional capability model.

Prioritize delivering benefits early

- Represent actionable steps to implement Functional Architecture capabilities
- Provides a staged approach to address risks and gaps.

Provide Cyber Strategy Planning Direction

- A prioritized roadmap of required capabilities to serve as cybersecurity strategy and plan input
- A path to achieve desired target states for IT and OT

* The scope of the SOW for the development of the ESA set out to develop only a high-level roadmap to achieve the ESA target state.

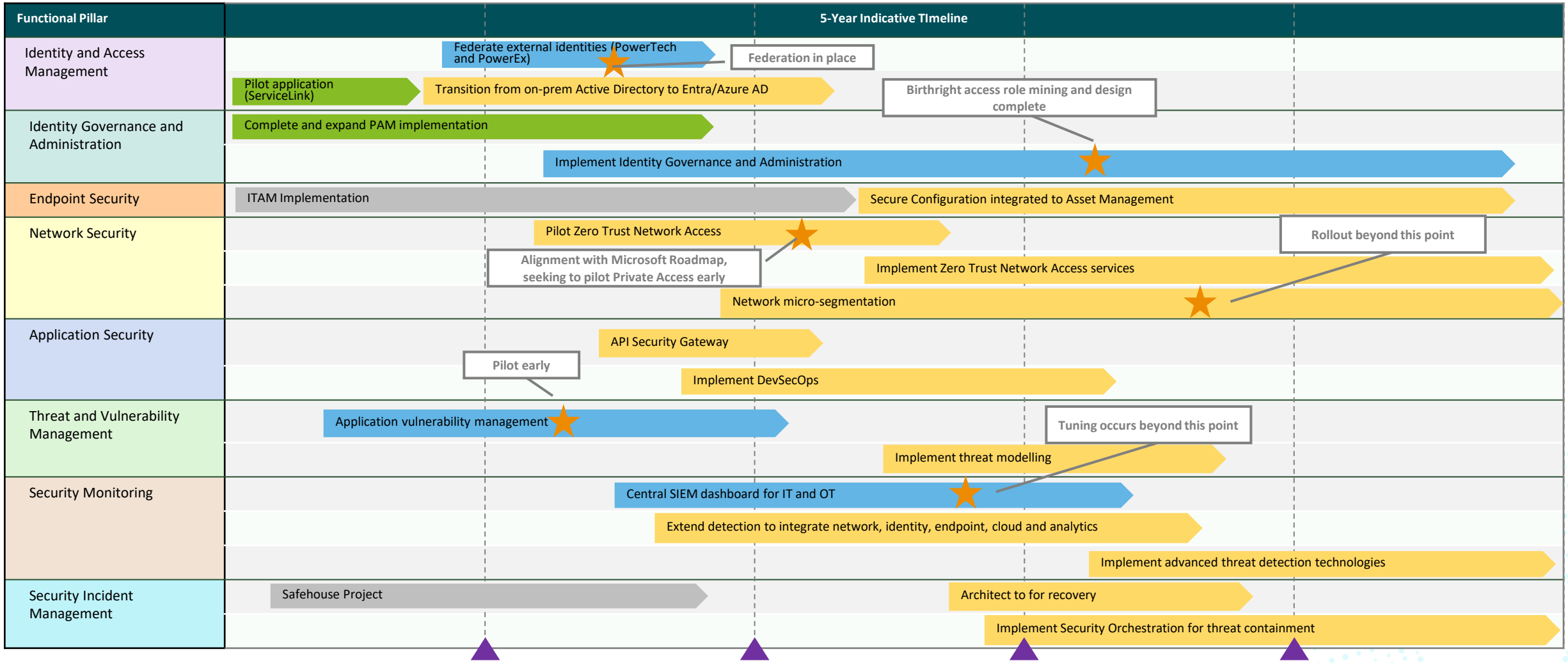
Corporate IT: ESA Roadmap Focus Areas

The IT roadmap addresses key gaps identified as part of the current and target state analysis, which are outlined below:

1. **Access Management** – leverage Microsoft Entra to support advanced authentication features
2. **Identity Governance** - automate provisioning and recertification.
3. **Privileged Access Management** - PAM implementation completion and expansion.
4. **Endpoint Security Baseline Enforcement** – addressing both on-prem and Cloud IaaS (includes Infrastructure as Code).
5. **Network Security Zero Trust Access Model** - a move towards zero-trust access models will require software-based micro-segmentation approaches, beyond traditional network segmentation.
6. **Application Security Secure Software Development** - extension of security in software development processes, including code developed, is required.
7. **Threat and Vulnerability Management** - extension of vulnerability management into applications, IoT and Cloud services is integral towards enabling zero-trust access models.
8. **Security Monitoring** - current SIEM is not yet platformed for all required features and does not yet ingest all log sources to enable full visibility of threats.
9. **Security Incident Management** - while host-based containment capabilities are in place, network level containment options and the automation of key containment actions are limited.

Corporate IT: Highlevel ESA Prioritized Roadmap

The IT roadmap below represents an unconstrained view of timelines for establishment of Enterprise Architecture's desired capability over a 5-year period



Active Project * | Planned Project * | Proposed | Dependency | ESA update, integrated with annual NIST Maturity Assessment

Consolidated OT Approach

- A consolidated approach has been taken to develop the OT roadmap from cyber risks (i.e. beyond compliance) point of view. It considered all of BC Hydro OT, including NERC and non-NERC.
- Although each OT area's unique needs and current states were considered, the target architecture has been developed to apply broadly for a desired outcome that will be based on a risk-based and fit-for-purpose approach.
- This consolidated view does not indicate that all architecture patterns and outcomes will be applied without due consideration of the operational and risk-based impacts on each OT area.
- The roadmap is not designed to address all OT environments but instead on creating capabilities to better manage cyber risks over time.

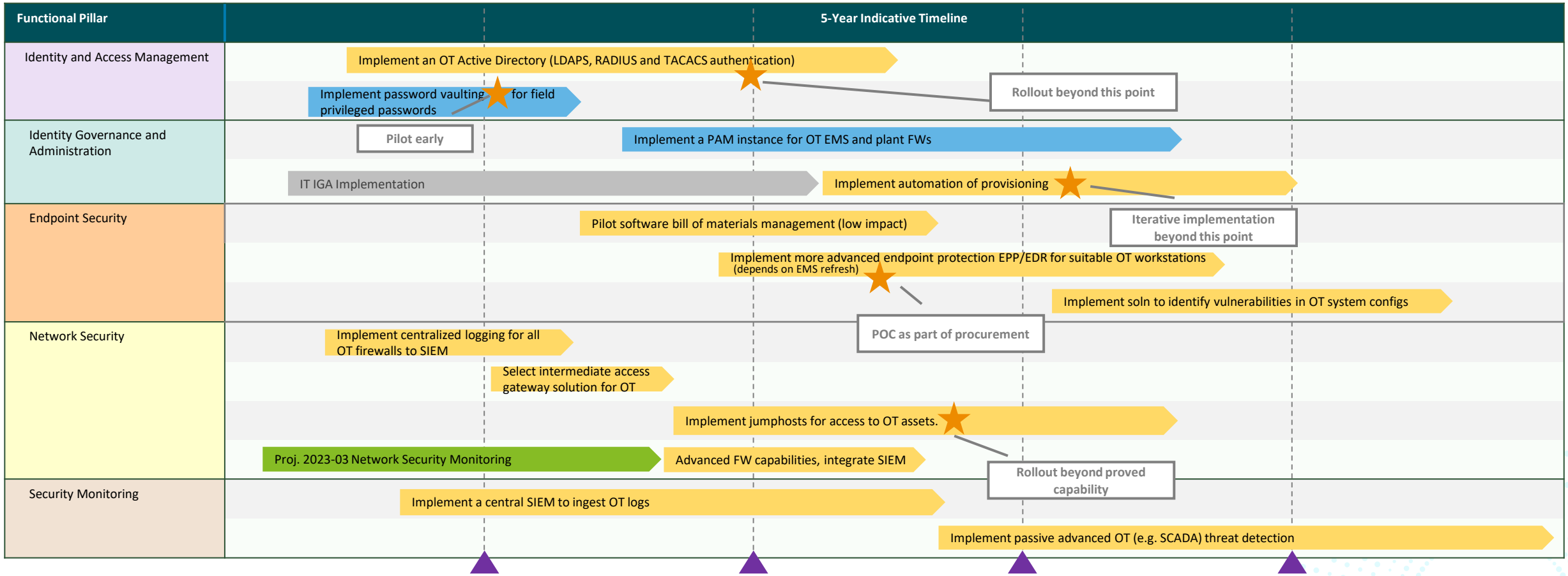
Consolidated OT: ESA Roadmap Focus Areas

The OT roadmap addresses key gaps identified as part of the current and target state analysis, which are outlined below:

1. **Access Management** – implement an Active Directory to support transition from local accounts to managed accounts.
2. **Privileged Access Management** – initially manage privileged passwords in an offline usable password vault. Later transition to use of common PAM implementation.
3. **Identity Governance** – leverage implemented IT IGA solution to automate provisioning and recertification of access.
4. **Network Security** – select a consistent intermediated secure network access gateway access model and design for use across all of OT.
5. **Security Monitoring** – implement a central SIEM suitable for ingesting OT logs (starting with firewalls).
6. **Software Security** – pilot the use of software bill of materials security solution for low impact sites.
7. **Network Security** – enable the advanced next-gen firewall features of OT firewalls.
8. **Endpoint Security** – implement more advanced endpoint detection and response solution for suitable OT workstations (EDR vs traditional signature-based antivirus).
9. **Secure Baseline Enforcement** – implement solution able to identify configuration weaknesses in OT devices (beyond TripWire).
10. **Threat Management** – implement passive threat detection technology for suitable OT environments.

Consolidated OT: Highlevel ESA Prioritized Roadmap

The OT roadmap below represents an unconstrained view of timelines for establishment of Enterprise Architecture's desired capability over a 5-year period



Active Project * | Planned Project * | Proposed | Dependency | ESA update, integrated with annual NIST Maturity Assessment

Next Steps

- The ESA Guideline documents (Conceptual, Functional, Physical patterns) and are being applied in IT and OT projects. This needs to be maintained.
- The ESA Roadmap will guide investment planning.
- The focus of the roadmap is to establish key capabilities that can be leveraged.
- Use of the ESA Guidelines, and execution of the roadmap will mature cyber capability over time across BC Hydro's IT and OT.

Roadmap Overview and Approach

Introduction to the approach taken in the development of the ESA roadmap

Enterprise Security Architecture Roadmap Objectives

- The Enterprise Security Architecture (ESA) Roadmap sets out the envisioned high-level timelines, interdependencies and phasing for establishment of capabilities needed in order to support the requirements and desired outcomes of the ESA.
- The ESA Roadmap is directional in nature and as such considers and complements more detailed roadmaps such as the Identity and Access Management and Cloud roadmaps.
- The roadmap serves as an input to guide the development and planning of cybersecurity initiatives and does not replace the need for detailed implementation planning*.
- The Roadmap should be considered a living document and should be updated on an ongoing basis to reflect the current threat landscape.

Address BC Hydro's Cybersecurity Threats

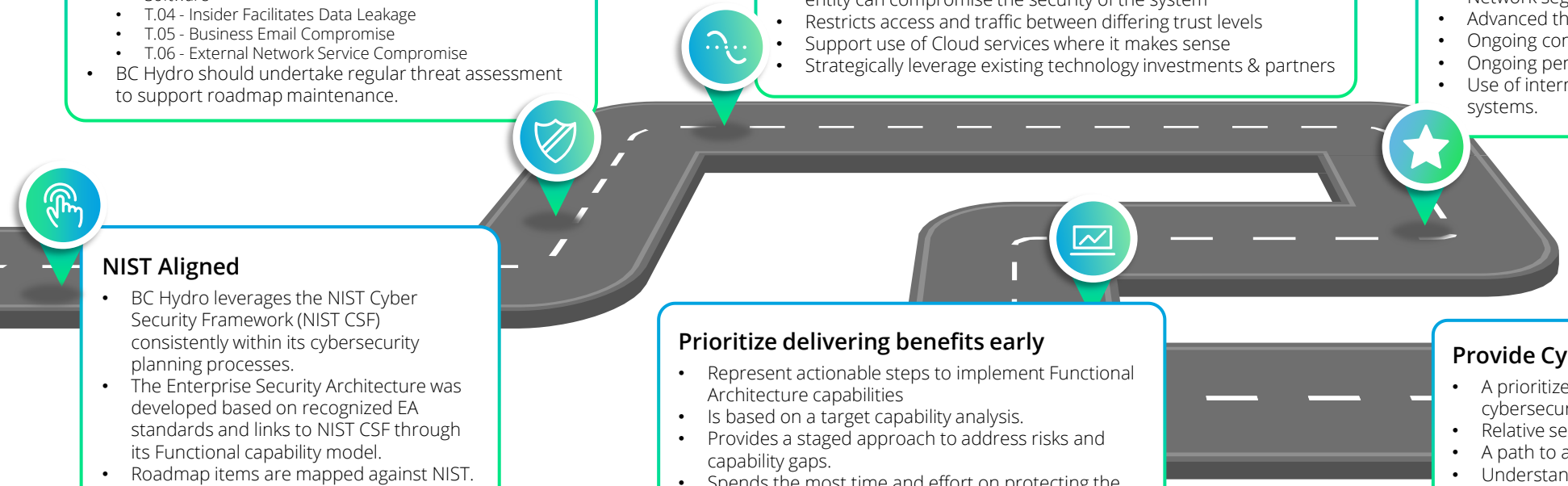
- This roadmap considered the threats identified in the Directive 8 Threat Risk Assessment, namely:
  - T.01 – Major Ransomware Outbreak
  - T.02 - Espionage by Advanced Persistent Threat (APT)
  - T.03 - Supply Chain Attack Introduces Compromised Software
  - T.04 - Insider Facilitates Data Leakage
  - T.05 - Business Email Compromise
  - T.06 - External Network Service Compromise
- BC Hydro should undertake regular threat assessment to support roadmap maintenance.

Apply the ESA Principles

- Design for zero trust
- Is adaptable to changes in the threat landscape
- Implements proven standards and technologies
- Prioritizes both detection and prevention
- Leverages segregation and isolation to ensures that no single entity can compromise the security of the system
- Restricts access and traffic between differing trust levels
- Support use of Cloud services where it makes sense
- Strategically leverage existing technology investments & partners

Implement Directive 8 Recommendations

- Security operations response capability expansion.
- SIEM consolidation and centralization.
- Enhanced detection within OT environments.
- Privileged Access Management implementation.
- Vulnerability management rigor and scope expansion.
- Network segmentation driving towards zero trust.
- Advanced threat detection across both IT and OT.
- Ongoing configuration monitoring.
- Ongoing penetration testing capability.
- Use of intermediated access for connections to sensitive systems.



NIST Aligned

- BC Hydro leverages the NIST Cyber Security Framework (NIST CSF) consistently within its cybersecurity planning processes.
- The Enterprise Security Architecture was developed based on recognized EA standards and links to NIST CSF through its Functional capability model.
- Roadmap items are mapped against NIST.

Prioritize delivering benefits early

- Represent actionable steps to implement Functional Architecture capabilities
- Is based on a target capability analysis.
- Provides a staged approach to address risks and capability gaps.
- Spends the most time and effort on protecting the things that are most important.

Provide Cyber Strategy Planning Direction

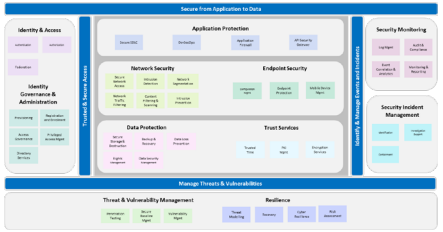
- A prioritized roadmap of required capabilities to serve as cybersecurity strategy and plan input
- Relative sequencing and timeline overview
- A path to achieve desired target states for IT and OT
- Understanding of how the roadmap addresses cybersecurity risks from Directive 8

* The scope of the SOW for the development of the ESA set out to develop only a high-level roadmap to achieve the ESA target state.

Approach Followed in the Development of the Roadmap

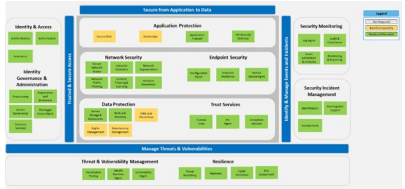
- The Roadmap has been developed based on extensive consultation with IT and OT architects and security leaders.
- The Roadmap is directional in nature, and as such considers but does not replace more detailed roadmaps such as the Identity and Access Management (IAM) and Cloud roadmaps. Roadmap items will require further detailed planning.
- Roadmap items serve as input to guide the development and implementation planning of cybersecurity and technology initiatives within BC Hydro's IT and OT teams.

1) Current State Capability Snapshot



A rapid assessment was conducted with key stakeholders of capabilities across BC Hydro that support the Functional Architecture, based on a structured "House View" of service capabilities.

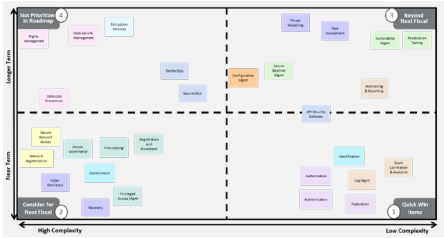
2) Target State Definition



A desired target state for each capability was determined across IT and OT (consolidated), based on architectural fit, risk mitigation, standards alignment, solution maturity and desired benefits realization.

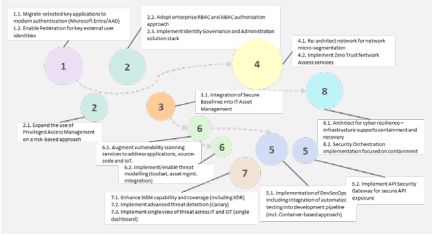
4-Phased Approach

3) Prioritization Heatmap



Capability gaps were prioritized based on a consideration of relative complexity to implement, urgency of capability need and fiscal planning considerations.

4) Sequence and Dependency Mapping



Roadmap items were defined at a thematic level, based on objective outcomes, and sequenced on a broad timeline based on dependency and priority.

Note: While technology environmental constraints and regulatory considerations have been considered as part of the development of this roadmap, the Roadmap represents an unconstrained view that has not considered available resourcing, funding, conflicting priorities and does not factor in consultation, setup and socialization timelines associated with initiatives.

Key Outcomes and Next Steps

The ESA Roadmap positions BC Hydro to understand the actions required to implement reusable and secure functional components, in alignment with the objectives of the Enterprise Security Architecture. However, it is a point-in-time view that will require regular updates and maintenance.

- The ESA roadmap sets out a sequenced and notionally sized set of actions to assist BC Hydro in implementing capabilities that will allow for the objectives of the ESA to be met.
- The roadmap reflects planned, in-flight and proposed activities that were identified during its development.
- The roadmap aims to address more than 50% of the recommendations made within Directive 8's Threat Risk Assessment.
- The Roadmap should serve as a key input to BC Hydro's IT and Cybersecurity planning processes.

Roadmaps are living documents

- The roadmap should feed directly into a more detailed implementation planning process.
- The roadmap should be reviewed and updated regularly, given that both BC Hydro's needs as well as market capabilities will change.
- The ESA itself, and consequently this roadmap, must evolve as the cyber threat landscape changes.
- BC Hydro should undertake an assessment of its Crown Jewel assets, and the roadmap should be revisited to ensure it represents the most important actions to protect the things that are most important.
- While the Directive 8 Threat Risk Assessment served as a good baseline of threats, there is a need a refreshed risk assessment that considers current threats and changes within BC Hydro, mapped against the outcomes to the ESA, and to revisit the ESA where required as a result.

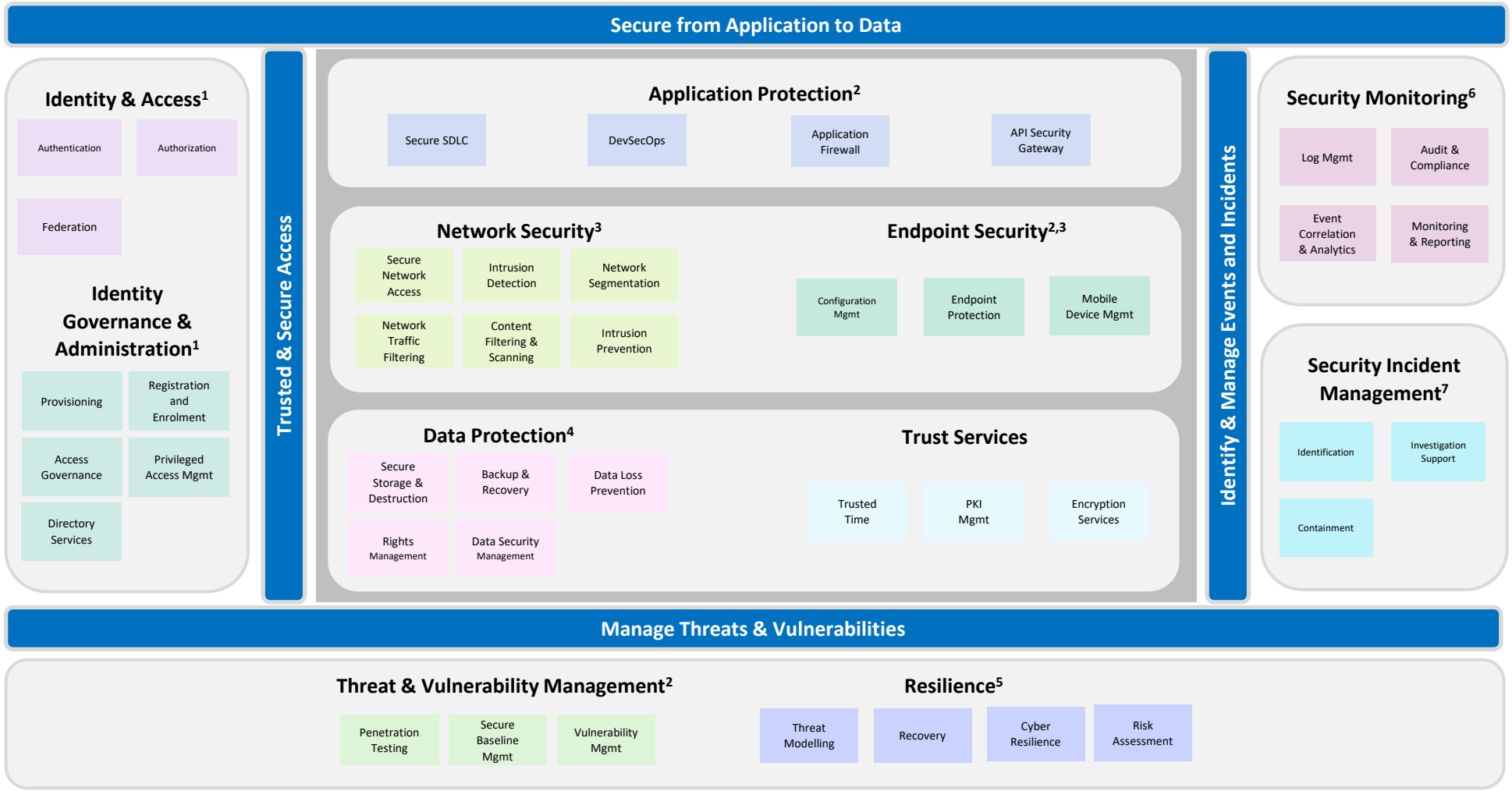
Current State Analysis Methodology

The ESA current state capability analysis focused on assessing functional architecture capability level based on interviews with BC Hydro subject matter experts for each area assessed and was designed to identify functional gaps that may hinder the ability of BC Hydro to achieve its Enterprise Security Architecture objectives and target state. This analysis is used to prioritize actions and estimate the relative effort required to address gaps towards a complete baseline ESA across IT and OT environments. The Functional "House View" of the Enterprise Security Architecture, together with the sub-function descriptions and functional requirements defined in the ESA, were used to assess capability level according to the following categorization model:

	RATING DESCRIPTION	ROADMAP CONSIDERATIONS
Not Applicable	• This rating indicates that no capability is required due to the scope of operations or the nature of the IT and OT cyber assets managed by the relevant team.	• The Target State for such ratings should match the Not Applicable rating, indicating no Roadmap item is required.
Missing	• This rating indicates that the Function is not yet in place.	• If the Target State for this capability indicates any level of requirement, this is a higher-priority roadmap item, as in order to introduce any level of Functional capability there is likely a need for investment.
Not Yet Mature	• This rating indicates that the Function exists, but is not yet mature or aligned with requirements, making it not suitable for re-use until further investment or implementation is completed.	• If the Target State indicates a requirements for this capability to be readily available and mature, there may be a need to prioritize efforts related to maturing this Function or a need to complete a planned in-flight initiative before the Function can be fully utilized in architecture designs.
Limited Deployment	• This rating indicates that a Function is deployed, however it is limited to specific BC Hydro environments and as a result not available as a reusable capability.	• If the Target State indicates a need for a mature and reusable capability, the Roadmap should consider how best to expand the availability of this Function more broadly across the BC Hydro environment in scope.
Ready and Reusable	• This rating indicates that the Function is deployed in such a way that it can be reused within architecture designs for the particular area of BC Hydro, and potentially more broadly, as it is a mature and readily available capability.	• Any Function that is rated mature and reusable is well suited for use within architecture designs. Within the Roadmap, such capabilities will not be considered for actions given their capability level.

Functional Architecture "House View"

The Functional Architecture "House View" was utilized in the assessment of current and desired capability. The requirements for each function, as defined in the Functional Architecture, were used as part of this assessment process.



The "House View" aligns broadly to NIST CSF Categories and Sub-Categories (see footnote numbered referenced) and serves as a means of grouping ESA capabilities into logical and actionable focus areas of capability.

NIST Category Reference:
1. PR.AC, 2. PR.IP, 3. PR.PT, 4. PR.DS, 5. RC.RP, 6. DE.AE & DE.CM, 7. RS.RP

Desired Target State Selection Criteria

The following were considered when identifying the Desired Target State within the ESA across IT and OT:

Architectural fit

- Alignment with areas within the ESA that required new or enhanced functionally and coverage.
- Alignment within BC Hydro's technology environment (private cloud, public cloud, on premise)
- Ability to address current architectural complexity
- Suitability for implementation in a phased approach

Maturity of solution

- Ability to deliver incremental maturity change
- Availability within the market, and emerging / innovative new approaches (including Cloud service models)
- Deployment within the power and utilities sector
- Delivery and support options available (local availability, support and functional understanding)

Industry alignment & references

- Peers within the sector that have also deployed the solution
- Solutions that have an industry aligned engagement model and reference architecture
- Solution footprint in Canada and North America (localization)

Benefits realization

- Degree of fit with BC Hydro priority requirements
- Delivery of benefits (according to market references)
- Support and enablement of other BC Hydro innovations and business strategic direction.
- Ability to maximize value from strategic vendor investments and relationships.

Risk mitigation

- Ability to address threat scenarios defined within the Directive 8 Threat Risk Assessment (TRA)
- Alignment with recommendations from the Directive 8 TRA
- Controls delivered against popular threat models (incl. STRIDE-LM).

Corporate IT

Capability Assessment and Roadmap Prioritization

Corporate IT: Current State Analysis

Identity & Access

- Authentication
- Authorization
- Federation

Identity Governance & Administration

- Provisioning
- Registration and Enrolment
- Access Governance
- Privileged Access Mgmt
- Directory Services

Trusted & Secure Access

Secure from Application to Data

Application Protection

- Secure SDLC
- DevSecOps
- Application Firewall
- API Security Gateway

Network Security

- Secure Network Access
- Intrusion Detection
- Network Segmentation
- Network Traffic Filtering
- Content Filtering & Scanning
- Intrusion Prevention

Endpoint Security

- Configuration Mgmt
- Endpoint Protection
- Mobile Device Mgmt

Data Protection

- Secure Storage & Destruction
- Backup & Recovery
- Data Loss Prevention
- Rights Management
- Data Security Management

Trust Services

- Trusted Time
- PKI Mgmt
- Encryption Services

Identify & Manage Events and Incidents

Security Monitoring

- Log Mgmt
- Audit & Compliance
- Event Correlation & Analytics
- Monitoring & Reporting

Security Incident Management

- Identification
- Investigation Support
- Containment

Manage Threats & Vulnerabilities

Threat & Vulnerability Management

- Penetration Testing
- Secure Baseline Mgmt
- Vulnerability Mgmt

Resilience

- Threat Modelling
- Recovery
- Cyber Resilience
- Risk Assessment

Legend

- Missing
- Not Yet Mature
- Limited Deployment
- Ready & Reusable

Corporate IT: Desired Target State

Secure from Application to Data

Identity & Access
- Authentication
- Authorization
- Federation

Identity Governance & Administration
- Provisioning
- Registration and Enrolment
- Access Governance
- Privileged Access Mgmt
- Directory Services

Trusted & Secure Access

Application Protection
- Secure SDLC
- DevSecOps
- Application Firewall
- API Security Gateway

Network Security
- Secure Network Access
- Intrusion Detection
- Network Segmentation
- Network Traffic Filtering
- Content Filtering & Scanning
- Intrusion Prevention

Endpoint Security
- Configuration Mgmt
- Endpoint Protection
- Mobile Device Mgmt

Data Protection
- Secure Storage & Destruction
- Backup & Recovery
- Data Loss Prevention
- Rights Management
- Data Security Management

Trust Services
- Trusted Time
- PKI Mgmt
- Encryption Services

Identify & Manage Events and Incidents

Security Monitoring
- Log Mgmt
- Audit & Compliance
- Event Correlation & Analytics
- Monitoring & Reporting

Security Incident Management
- Identification
- Investigation Support
- Containment

Legend
- Baseline Capability
- Ready and Reusable

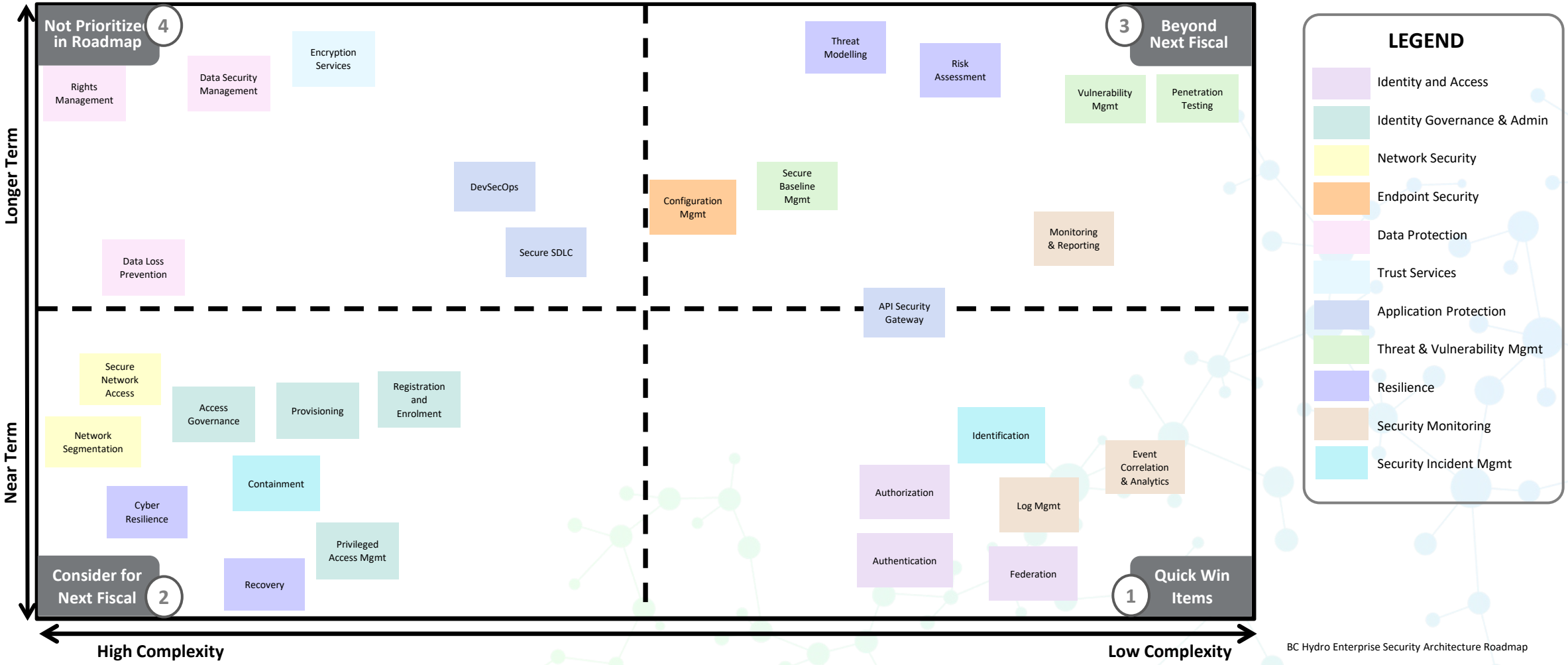
Manage Threats & Vulnerabilities

Threat & Vulnerability Management
- Penetration Testing
- Secure Baseline Mgmt
- Vulnerability Mgmt

Resilience
- Threat Modelling
- Recovery
- Cyber Resilience
- Risk Assessment

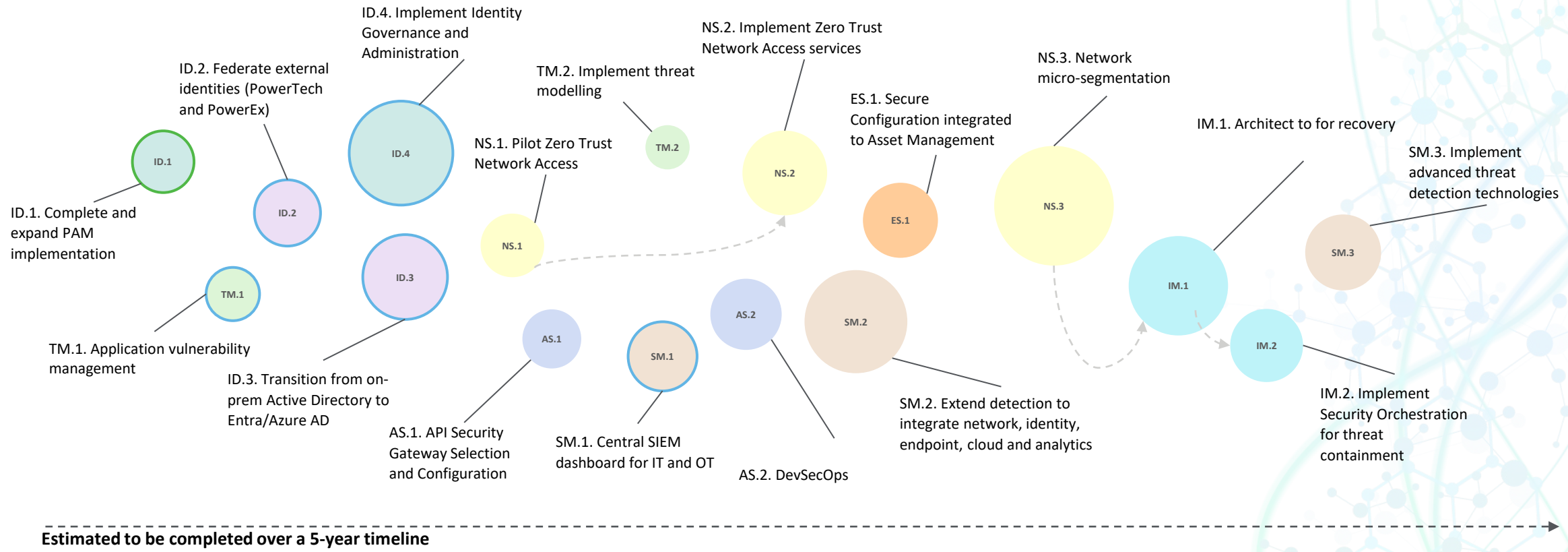
Corporate IT: Prioritized Capability Gap Heatmap

The heatmap below illustrates a consolidated view of the placement of functions relative to the current and target Functional capability. The bottom right quadrant indicates where gaps are most extreme based on the current state and desired target state and provides a means of prioritizing Functions that require most investment or operationalization to ensure that BC Hydro is able to meet its cybersecurity objectives encapsulated within the Enterprise Security Architecture and the Cyber Security Plan (CSP).



Corporate IT: ESA Roadmap Item Sequencing

The diagram below indicates the roadmap items in a timeline sequence that also reflects broad sizing, interdependencies and a clear mapping to the "House View" capability models.



Corporate IT: ESA Prioritized Roadmap

The roadmap below represents an unconstrained view of timelines for establishment of Enterprise Architecture's desired capability over a 5-year period

Functional Pillar	Roadmap Item	
Identity and Access Management	IT.ID.2. Federate external identities for key subsidiaries (PowerTech and Powerex)	IAM Federated Access**
	IT.ID.3. Transition from on-prem Active Directory to Entra/Azure AD for candidate applications to benefit from modern auth features.	Complete pilot application (ServiceLink); IAM Enable Azure seamless SSO & Passwordless; IAM Expand SSO capabilities
Identity Governance and Administration	IT.ID.1. Complete PAM implementation and expand use on a risk-based approach***	PAM implementation, IAM # 4, #9**
	IT.ID.4. Implement Identity Governance and Administration solution stack	IAM Roadmap Vendor Alignment & selection; IAM Roadmap RBAC discovery & role mining; IAM Roadmap RBAC ABAC & Access certification (IGA platform –IT)
Endpoint Security	IT.ES.1. Integrate Secure Configuration Baselines into IT Asset Management toolsets	ITAM Implementation; Requirements; Design; Integration of VM/CPM to ITAM
Network Security	IT.NS.1. Pilot implementation of Zero Trust Network Access services	Rqmnts & Design; Eval & select; Pilot rollout
	IT.NS.2. Implement Zero Trust Network Access Services	Design; Procure; Deploy and Configure; Discovery; Staged rollout
	IT.NS.3. Implement network micro-segmentation (leveraging investments in software defined networking and ensure extension to Cloud)***	Rqmnts & Design; Select & Pilot; Infra Deploy; Rollout
Application Security	IT.AS.1. Implement/enable API Security Gateway feature of MuleSoft and SAP BTP, and evaluate API gateway solutions for secure API exposure	Configure existing API services; Eval API Gateway Solutions; Pilot API Gateway
	IT.AS.2. Implement integrated and automated security testing of application and platform security configuration (DevSecOps)	Rqmnt & Design; Procure; CI/CD Integration; IaC/Container Integration
Threat and Vulnerability Management	IT.TM.1. Implement vulnerability scanning of applications and application source code	Scope & eval; Select, pilot, procure; Implement & integrate
	IT.TM.2. Implement/enable threat modelling toolset	Rqmnts; Eval & Procure; Implement & integrate
Security Monitoring	IT.SM.1. Implement central SIEM dashboard that monitors IT and OT	Use case design; Data sourcing; Log onboarding and integration
	IT.SM.2. Extend detection and response to integrate network, identity, endpoint, cloud and analytics (journey to XDR)***	SIEM Re-platform and SOC Transformation*; Rqmnts; Soln Eval; Procure (& PoC); Deploy; Tune
	IT.SM.3. Implement advanced threat detection technologies	Scope & Design; Eval; PoC & Procure; Implement
Security Incident Management	IT.IM.1. Architect to recover all critical business functions within business-defined thresholds***	Safehouse Project; Architecture study; Architecture design
	IT.IM.2. Implement Security Orchestration to automate threat containment across both on-premise and cloud workloads***	Scope & Design; Toolset Eval; Procure; Implement

* Refer to Cybersecurity Plan F24-F26 in Appendix B
** Refer to IAM Roadmap Appendix C
*** This action should address both on-premise and Cloud environments

Active Project * | Planned Project * | Proposed | Dependency | Multi-year iterative rollout

Corporate IT: Directive 8 Recommendations Addressed by the Roadmap Items (13/40)

The roadmap aims to address a number of recommendations made within the Directive 8 Threat Risk Assessment. While not all recommendations related to architecture enhancements, this roadmap is able to significantly address the recommendations.

Functional Pillar	Roadmap Item	Directive 8 Recommendations Addressed
Identity & Access	IT.ID.3. Transition from on-prem Active Directory to Entra/Azure AD for candidate applications to benefit from modern auth features.	• REC-CORP-05 [HIGH]: Continue AD hardening: Continue AD hardening initiatives identified in Mandiant Ransomware Assessment.
Identity Governance and Administration	IT.ID.1. Complete PAM implementation and expand use on a risk-based approach	• REC-GEN-06 [MEDIUM]: Expand and consolidate PAM: Consider consolidation of PAM program across BC Hydro environments (i.e. corporate IT and OT) with vaulting solution segmentation in critical environments (MRS OT).
Network Security	IT.NS.3. Implement network micro-segmentation (leveraging investments in software defined networking and ensure extension to Cloud)	• REC-CORP-06 [HIGH]: Expand network security towards zero trust: Continue software defined network architecture initiative to implement more robust corporate network segmentation; consider designs which would position the organization for future implementation of zero trust architectures .
Endpoint Security	IT.ES.1. Implement Secure Configuration Baselines management (incl IT Asset Management integration)	• REC-GEN-03 [HIGH]: Continue asset management formalization: Continue implementing asset management solutions (i.e. ServiceNow) and work towards harmonization of process and toolset across environments (where not restricted due to NERC CIP confidentiality requirements - MRS OT asset management may be better served by a dedicated OT asset database complying with NERC CIP requirements)
Threat and Vulnerability Management	IT.TM.1. Implement vulnerability scanning of applications and application source code	• REC-CORP-03 [HIGH]: Continue vulnerability management expansion: Continue to expand scope and rigor of vulnerability management program; continue Tenable implementation. • REC-CORP-09 [MEDIUM]: Execute penetration testing strategy: Implement penetration testing program per defined strategy
Security Monitoring	IT.SM.2. Extend detection and response to integrate network, identity, endpoint, cloud and analytics (journey to XDR)	• REC-CORP-01 [HIGH]: Expand logs to SIEM: Continue to expand log feeds integrated into Splunk SIEM environment. • REC-CORP-14 [LOW]: Continue to enhance user anomaly detection: Complete implementation of Splunk Enterprise Security and enable UEBA and advanced analytics capability. • REC-GEN-05 [MEDIUM]: Consolidate SIEM: Consider consolidation of SIEM infrastructure, resourcing, and operations to a single enterprise program.
	IT.SM.3. Implement advanced threat detection technologies (Canary)	• REC-CORP-13 [LOW]: Implement deceptive detection tactics: Implementation of deceptive threat detection techniques and honey pots such as decoy device, files, systems, accounts, etc. • REC-GEN-08 [MEDIUM]: Expand threat hunting: Augment and expand existing threat hunting capability to deliver broader enterprise capability using threat-driven approaches to search for exposure to threat-relevant TTPs and indicators of compromise (IOCs) • REC-GEN-09 [MEDIUM]: Implement network anomaly analysis: Ensure expansion of Netflow log collection from network devices from all environments, and implement NetFlow analysis capability, to perform in-depth monitoring and understanding of network traffic data.
Security Incident Management	IT.IM.1. Architect to recover all critical business functions within business-defined thresholds	• REC-CORP-02 [HIGH]: Continue securing backups: Complete the project to implement technical controls to secure backups and backup systems, including segmentation and encryption

Corporate IT: ESA Roadmap Addressed Identified Capability Gaps

The roadmap addressed key gaps identified as part of the current and target state analysis, which are outlined below:

1. Access management to many applications remains based on legacy technologies. To support advanced authentication features, including adaptive authentication, a movement towards use of Microsoft Entra is required. This should also extend to support external user groups through federation.
2. Increasing complexity and risks related to access management require managed and governed access, enabled by a solution that provides automation of provisioning and recertification. The highest risk relates to privileged users, for which the PAM implementation completion and expansion is a key capability.
3. Moves towards use of Cloud IaaS and Infrastructure as Code will demand the ability to systematically enforce secure baselines.
4. A move towards zero-trust access models will require support for software-based micro-segmentation approaches beyond traditional network segmentation based on traditional network zones.
5. Extension of security in development processes, including code developed to manage infrastructure, is required to address cyber risk in software.
6. Extension of vulnerability management into applications, IoT and Cloud services is an integral capability to enable zero-trust access models.
7. Current SIEM platform is not yet platformed for all required features and does not yet ingest all log sources to enable full visibility of cyber threats.
8. While host-based containment capabilities are in place, network level containment options and the automation of key network containment actions are limited.

Roadmap Item: IT.ID.1. Complete PAM implementation and expand use on a risk-based approach

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Identity Governance and Administration	PAM implementation, IAM # 4, #9					Tactical	• Identity Management Lead

Roadmap Item Detail

Sub-function Capability	Privileged Access Mgmt
Approximate start	Year 1
Estimated Duration	8-12 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$600,000 - $1m
Directive 8 Recommendation(s) Addressed	• REC-GEN-06 [MEDIUM]: Expand and consolidate PAM: Consider consolidation of PAM program across BC Hydro environments (i.e. corporate IT and OT) with vaulting solution segmentation in critical environments (MRS OT).
Example vendor technologies	Azure PIM, CyberArk
Dependencies / Considerations for Approach	• IAM Roadmap #4 - Privileged Access Management (Procurement, Design, Build) -OT • IAM Roadmap #9 - PAM improvements & CyberArk enhancements –IT

Roadmap Item Description

- This roadmap item focuses on expanding the use of PAM across user accounts and systems within BC Hydro.

Roadmap Item Objective(s)

- A Privileged Access Management (PAM) solution delivers a comprehensive set of tools and capabilities that enable organizations to manage, control, and monitor privileged access to critical systems, applications, and data.

Roadmap Item Activities

- Finalize implementation architecture as well as system requirements, including identifying the use cases. Ensure suitability for use both on-prem and in cloud.
- Complete procurement (part of current IAM roadmap, item #4).
- Develop prioritized account onboarding requirements
- Expand the use of CyberArk to onboard infrastructure & app-level privilege accounts (IAM roadmap #9)
- Training users

Outcomes/Deliverables

- Enhanced security: Provides a centralized and secure way of managing privileged access to critical systems and data, reducing the risk of unauthorized access and human error.
- Improved compliance: Provides audit trails and reporting capabilities that help demonstrate compliance.
- Better visibility: Provide visibility into privileged access across the organization.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: IT.ID.2. Federate external identities for key subsidiaries (PowerTech and Powerex)

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Identity and Access Management	IAM # 12 – Federated Access					Tactical	• Identity Management Lead

Roadmap Item Detail

Sub-function Capability	Authentication
Approximate start	Year 1
Estimated Duration	4 – 10 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$350k - $600k
Directive 8 Recommendation(s) Addressed	• N/A
Example vendor technologies	Microsoft Entra, Okta
Dependencies / Considerations for Approach	• External federated AAD capability • IAM Roadmap 12

Roadmap Item Description

- The roadmap item is represented in the existing IAM roadmap, and will implement federated access to BC Hydro applications for users from BC Hydro subsidiaries; Powerex and PowerTech.

Roadmap Item Objective(s)

- Enabling federation for external users (particularly for entities such as Powerex and PowerTech) to access BC Hydro applications involves setting up a secure capability and processes using identity federation protocols for users from other organizations to authenticate and access BC Hydro applications.
- Federation removes the requirement to provision and manage user accounts within BC Hydro's own directories and can assist in both reducing risk as well as easing administration.

Roadmap Item Activities

- Complete development of architecture and solution design.
- IAM roadmap item #12 - Develop migration strategy, design and plan for moving Powerex users from BC Hydro Active Directory to the new dedicated Active Directory solution
- Configure federated access through trust between BC Hydro Azure AD and Azure AD instances of Powerex and PowerTech and configure selected BC Hydro applications to accept authentication tokens or assertions from the IdP (via application delivery platform for access to BC Hydro applications, e.g., Citrix)
- Migrate users, while addressing identity security in the process.

Outcomes/Deliverables

- Reduced risk of provisioned external users, while still enabling an SSO experience for users.
- Reduced password and account management risks.
- Enforcement of Multi-Factor Authentication (MFA)

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: IT.ID.3. Transition from on-prem Active Directory to Entra/Azure AD for candidate applications to benefit from modern auth features

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Identity and Access Management	Complete pilot application (ServiceLink) → IAM Enable Azure seamless SSO & Passwordless	IAM Expand SSO capabilities				Tactical	• Identity Management Lead

Roadmap Item Detail

Sub-function Capability	Authentication
Approximate start	Year 1
Estimated Duration	10 – 16 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$500k - $800k
Directive 8 Recommendation(s) Addressed	• REC-CORP-05 [HIGH]: Continue AD hardening: Continue AD hardening initiatives identified in Mandiant Ransomware Assessment.
Example vendor technologies	Microsoft Entra, Microsoft ADFS, Okta
Dependencies / Considerations for Approach	• IAM Roadmap 22, 14, 16

Roadmap Item Description

- This initiative is focused on migrating authentication for candidate applications to leverage Microsoft Entra. This will include migration of the authentication stack for the applications away from traditional Kerberos authentication towards SAML/OIDC auth.

Roadmap Item Objective(s)

- Migrate to the use of modern authentication protocols using Microsoft Entra (OIDC, SAML) to allow BC Hydro to leverage modern authentication security and service features and apply a single set of access controls and policies across BC Hydro's on-premises and cloud environments. This includes the use of authentication security capabilities including adaptive authentication and conditional access policies.

Roadmap Item Activities

- Identification (via discovery study and technical analysis) of candidate systems for migration to use of Entra authentication, prioritized based on value and risk.
- Architect approach (based on approach applied in pilot application ServiceLink) for transition of authentication to Entra.
- Phased migration of applications to Azure AD/Entra - configure / update authentication stack for applications from legacy (Kerberos/SMB) to a SAML or OpenID Connect to leverage Entra.
- Migrate users, while addressing identity security in the process.

Outcomes/Deliverables

- Uplifts in security posture of users and authentication security
- Enhanced audit and security insights of the migrated applications.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: IT.ID.4. Implement Identity Governance and Administration solution stack

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Identity Governance & Administration	IAM Roadmap Vendor Alignment & selection	IAM Roadmap RBAC discovery & role mining	IAM Roadmap RBAC ABAC & Access certification (IGA platform –IT)			Tactical	• Identity Management Lead

Roadmap Item Detail

Sub-function Capability	Access Governance & Provisioning
Approximate start	Year 1/2
Estimated Duration	18-24 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$1.7m-$2.5m
Directive 8 Recommendation(s) Addressed	• N/A
Example vendor technologies	Microsoft Entra, Okta
Dependencies / Considerations for Approach	• IAM Roadmap item 23 (requirements) • Addresses access to birth-right entitlements (LAN ID, AD, Internet access) only. • IAM Roadmap 19, 18, 1

Roadmap Item Description

- This initiative, which forms part of the IAM roadmap, will implement identity governance and administration services (IGA) for foundational roles and access to birth-right entitlements (LAN ID, AD, Internet access).

Roadmap Item Objective(s)

- Automating access provisioning using an Identity Governance and Administration (IGA) system can help organizations streamline the process of granting and revoking access to resources.
- Role-Based Access Control (RBAC) is a security model that is used to restrict access to resources based on the roles and responsibilities of users within an organization.

Roadmap Item Activities

- Gather IGA requirements (identity lifecycle management across IT, OT, and PACS).
- Perform a market scan of vendors with capabilities to meet requirements.
- Complete session to assess the vendor capability
- Complete vendor selection & procurement *see appendix E
- Perform role discovery
- Implement and configure the IGA solution based on role-based access model

Outcomes/Deliverables

- Improving security: ensure that only authorized users have access to sensitive data and systems.
- Enhancing compliance: ensure strong identity and access management controls.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: IT.ES.1. Integrate Secure Configuration Baselines into IT Asset Management toolsets

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Threat & Vulnerability Management	ITAM Implementation		Rqmnts → Design	Integration of VM/CPM to ITAM		Tactical	• Vulnerability and Threat Manager

Roadmap Item Detail

Sub-function Capability	Secure Baseline Mgmt
Approximate start	Year 3
Estimated Duration	18-24 Months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$900k - $1.6m
Directive 8 Recommendation(s) Addressed	• REC-GEN-03 [HIGH]: Continue asset management formalization: Continue implementing asset management solutions (i.e. ServiceNow) and work towards harmonization of process and toolset across environments (where not restricted due to NERC CIP confidentiality requirements - MRS OT asset management may be better served by a dedicated OT asset database complying with NERC CIP requirements)
Example vendor technologies	ServiceNow, SolarWinds, Tenable, AlienVault, ManageEngine, PatchMyPC
Dependencies / Considerations for Approach	• Key dependency on a robust ITAM capability and CMDB to drive System of Record • Selection of any related uplift in scanning technologies (currently Tenable)

Roadmap Item Description

- Integrate automated vulnerability scanning and asset discovery with a system of record.

Roadmap Item Objective(s)

- Integrating security standards assessment into IT asset management (ITAM) systems to establish a system of record that ensures that the organization's assets are secure and protected against potential threats.

Roadmap Item Activities

- Gap analysis of existing vulnerability management and asset management processes
- Define requirements for security asset management and vulnerability management
- Document the design and technical specifications
- Design integration architecture to System of Record ITAM solution
- Procure any missing technical services
- Develop secure system image specifications for IT asset classes
- Integrate automated vulnerability scanning and asset discovery with SOR

Outcomes/Deliverables

- Improved asset discovery leveraging existing security scanners, and integrate the results with the CMDB solution
- ITSM will use the vulnerability information from Tenable to create incidents and open tickets for mitigation plans, relate with asset information in CMDB and assess the risk score

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: IT.NS.1. Pilot implementation of Zero Trust Network Access (ZTNA) services

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Network Security		Rqmnts & Design → Eval & select	→ Pilot rollout			Tactical	• Cybersecurity Infrastructure Manager

Roadmap Item Detail

Sub-function Capability	Secure Network Access
Approximate start	Year 2
Estimated Duration	10-14 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$400k - $650k
Directive 8 Recommendation(s) Addressed	• REC-CORP-06 [HIGH]: Expand network security towards zero trust: Continue software defined network architecture initiative to implement more robust corporate network segmentation; consider designs which would position the organization for future implementation of zero trust architectures .
Example vendor technologies	Microsoft Entra Private Access (currently in Private Beta), Zscaler ZPA
Dependencies / Considerations for Approach	• Consider requirements for CASB/DLP, and potentially pilot concurrently as often offered as part of same solution set.

Roadmap Item Description

- Pilot of a Zero Trust Network Access service for a select user group.

Roadmap Item Objective(s)

- Zero Trust Network Access (ZTNA) is a security framework that focuses on providing secure access to resources based on the user's identity and context, rather than the location of the user or the resource.
- ZTNA enables a security model that requires all users and devices to be verified and authenticated before they are granted access to network resources.
- Modern solutions offer a cloud-based security platform that can be used to implement ZTNA.

Roadmap Item Activities

- Requirements gathering (discovery for applications, data, and services).
- Develop architecture design based on requirements.
- Select technology for pilot – engage vendor for pilot.
- Pilot with a selected user group - configure the selected solution, deploying agents, on-prem and Cloud services to enable.
- Conduct extensive testing of access to different applications and services to ensure that the ZTNA policies are being enforced correctly.

Outcomes/Deliverables

- Enhanced security by providing a granular level of control over access to resources.
- ZTNA can simplify access management by providing a centralized platform for managing access policies and user identities.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: IT.NS.2. Implement Zero Trust Network Access (ZTNA) Services

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Network Security			Design, Procure	Deploy and Configure, Discovery	Staged rollout	Tactical	• Cybersecurity Infrastructure Manager

Roadmap Item Detail

Sub-function Capability	Secure Network Access
Approximate start	Year 3
Estimated Duration	18-24 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$2m – $3m (full 6000+ user count Private Access – no DLP/CASB)
Directive 8 Recommendation(s) Addressed	• REC-CORP-06 [HIGH]: Expand network security towards zero trust: Continue software defined network architecture initiative to implement more robust corporate network segmentation; consider designs which would position the organization for future implementation of zero trust architectures .
Example vendor technologies	Microsoft Entra Private Access (currently in Private Beta), Zscaler ZPA
Dependencies / Considerations for Approach	• Operational team must be established to maintain access policies, as well as create new policy for new applications and user groups. • Consideration has been given to the network access services, but service can be extended to support in-line DLP and off-network managed internet access (CASB and DLP).

Roadmap Item Description

- Implement the selected Zero Trust Network Access service based on the outcomes of the pilot.

Roadmap Item Objective(s)

- Zero Trust Network Access (ZTNA) is a security framework that focuses on providing secure access to resources based on the user's identity and context, rather than the location of the user or the resource.
- ZTNA enables a security model that requires all users and devices to be verified and authenticated before they are granted access to network resources.
- Modern solutions offer a cloud-based security platform that can be used to implement ZTNA.

Roadmap Item Activities

- Agree on design and architecture, including traffic forward method selection
- Discovery - detailed application and network analysis
- Infrastructure deployment – connectors and traffic forwarding
- Agent deployment
- Policy configuration
- Test site (opportunity to leverage pilot) and staged deployment

Outcomes/Deliverables

- Enhanced security by providing a granular level of control over access to resources.
- ZTNA can simplify access management by providing a centralized platform for managing access policies and user identities.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: IT.NS.3. Implement network micro-segmentation (leveraging investments in software defined networking and ensure extension to Cloud)

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic
Network Security			Rqmnts & Design → PoC & Select	Infra Deploy	Rollout	Strategic

Related Cyber Op Model Roles

- Cybersecurity Infrastructure Manager

Roadmap Item Detail

Sub-function Capability	Secure Network Access
Approximate start	Year 3
Estimated Duration	24-36 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$1.6m - $3m (hardware replacement costs to be considered, incl. firewalls and switches)
Directive 8 Recommendation(s) Addressed	• REC-CORP-06 [HIGH]: Expand network security towards zero trust: Continue software defined network architecture initiative to implement more robust corporate network segmentation; consider designs which would position the organization for future implementation of zero trust architectures .
Example vendor technologies	Guardicore, Illumio, (extending upon Cisco SD-WAN and Cisco SDA)
Dependencies / Considerations for Approach	• Note that Cisco ACI has been evaluated and found to be unsuitable for BC Hydro • This project should leverage existing investments in SDA and SD-WAN • Sustainment requiring dedicated onboarding and ops team. • Roadmap item has a particular emphasis on data center / cloud where critical apps are hosted. • Must ensure alignment with Zero Trust outcomes (e.g. SASE architecture) and linked projects (e.g. ZTNA, segmentation)

Roadmap Item Description

- Implement micro-segmentation across BC Hydro networks, extending beyond current SDA and SD-WAN capabilities and achieving a target network zoning and segmentation model for the end-to-end network landscape (data center, office, cloud, SaaS).

Roadmap Item Objective(s)

- Leverage software-defined networking to segment the network in a manner that reduces the attack surface and isolates workload, devices (servers and desktops) and application elements, ensuring that all traffic between segments/boundaries is inspected, managed by policy and access controlled. Focus initially would be on broad policy approach addressing major risk areas. Phased approach starting with environment, then legacy isolation, then application.

Roadmap Item Activities

- Scoping - identify key assets for protection and identify use cases to be applied to the in-scope systems.
- Agree solution design, scope of systems and uses cases. Develop segmentation strategy (application, environment, user, workload).
- Select solution to meet strategy and procure. Conduct pilot for monitoring and enforcement to develop application dependency map, how applications connect and communicate to each other, and visualize attack path mapping to determine weak points and vulnerable attack paths. Test and prove segmentation policies and approach.
- Phased deployment based on asset risk and operational impact. Create monitoring/alert rules, based on the observed network traffic to confirm confidence of coverage, then transition to enforcement rules – Develop onboarding schedule. Deploy infrastructure and agents, coordinate with vendor and platform support teams. Implement and zone – phase application onboarding based on agreed upon use cases.

Outcomes/Deliverables

- Segmentation strategy and requirements, together with segmentation architecture and technology selection
- Solution procurement, implementation plan and phased rollout

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: IT.AS.1. Implement/enable API Security Gateway feature of MuleSoft and SAP BTP, and evaluate API gateway solutions for secure API exposure

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Application Protection		Configure existing API services – MuleSoft, SAP BTP; Eval API Gateway Solutions	Pilot API Gateway			Tactical	• Application Security Program Lead

Roadmap Item Detail

Sub-function Capability	API Security
Approximate start	Year 2
Estimated Duration	9 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$100k - $300k implementation services (Configure) (assumption is that Anypoint is licensed as part of BC Hydro's existing SKU for MuleSoft) TBD – Gateway solution costs
Directive 8 Recommendation(s) Addressed	• N/A
Example vendor technologies	MuleSoft, F5, CloudFlare, SAP BTP
Dependencies / Considerations for Approach	• Existing MuleSoft Anypoint licensing

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item Description

- Begin by implementing security features of existing API services, including implementing governed security features of the Mulesoft Anypoint platform and SAP BTP (SAP API Management).
- Evaluate, select and pilot an API Gateway that addresses other APIs (so-called "shadow APIs"), mitigates OWASP API Top Ten attacks, DDoS and volumetric attacks and provides real-time monitoring.

Roadmap Item Objective(s)

- Secure and govern API security across developed and third party APIs while leveraging an API gateway to safeguard API and data at the network edge.
- Establish capability to create new APIs and integrations from prebuilt API security fragments, access patterns, and policies vetted by security experts.

Roadmap Item Activities

- MuleSoft Anypoint and SAP API Manager/Cloud Foundry:
  - Implement centralized authentication for APIs (App and User) - AD, app secrets, SAML/JSON, federation.
  - API policy design and implementation (identity, throttling, JSON/XML threat protection, content validation, usage restrictions)
  - Configure API governance – API security standards conformance
  - Native (MuleSoft and SAP) API gateway configuration for protection (DDoS, IP allow, WAF)
- Evaluate broader API Gateway Solutions (policy-driven perimeter gateway)
- Select and pilot dedicated API gateway solution

Outcomes/Deliverables

- API inspection and security enforcement.

Roadmap Item: IT. AS.2. Implement integrated and automated security testing of application and platform security configuration

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Application Protection			Rqmnt & Design → Procure → CI/CD Integration, IaC/Container Integration			Tactical	• Application Security Program Lead

Roadmap Item Detail

Sub-function Capability	DevSecOps
Approximate start	Year 3
Estimated Duration	9-12 months (including procurement) Note: If using existing platforms (Tenable) procurement window can reduce.
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$250k - $400k (licensing, based on code repo count 1-2) $120k - $300k implementation
Directive 8 Recommendation(s) Addressed	• N/A
Example vendor technologies	Tenable, Qualys, Aqua, Sonar, GitHub Security, ThreadFix, Microsoft Defender for Containers
Dependencies / Considerations for Approach	• IT.TM.1 • Consideration of existing Tenable toolset

Roadmap Item Description

- Integrate security checks and testing into the development and release cycles for applications and changes, to ensure that security vulnerabilities and misconfigurations are not introduced into BC Hydro's production environments.

Roadmap Item Objective(s)

- Deploy integrated security testing capabilities within BC Hydro's key development and change release pipelines and processes.

Roadmap Item Activities

- Requirements gathering and solution design
- Toolset evaluation
- Procurement *see appendix E
- Integration with existing CI/CD pipeline and code repos (git/jira/bitbucket).
- Workflow implementation and integration.
- Training.

Outcomes/Deliverables

- Integration of code-security checks and remediation into development lifecycles.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: IT.TM.1. Implement vulnerability scanning of applications and application source code

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Threat and Vulnerability Management	Scope & eval → Select, pilot, procure	→ Implement & integrate				Tactical	• Vulnerability and Threat Manager

Roadmap Item Detail

Sub-function Capability	Vulnerability Mgmt
Approximate start	Year 1
Estimated Duration	3-9 months select and procure, 3-6 months implement
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	Solution: $100k-$150k for 10 URLs and 6 code repos Implementation: $100k - $200k
Directive 8 Recommendation(s) Addressed	• REC-CORP-03 [HIGH]: Continue vulnerability management expansion: Continue to expand scope and rigor of vulnerability management program; continue Tenable implementation. • REC-CORP-09 [MEDIUM]: Execute penetration testing strategy: Implement penetration testing program per defined strategy
Example vendor technologies	Veracode, Fortify, Sonarqube
Dependencies / Considerations for Approach	• Leverage of existing Tenable implementation, extension of licensing

Roadmap Item Description

- This roadmap item implements vulnerability scanning of applications and application source code in an on-demand or manually operated manner (i.e. not integrated into development pipelines).

Roadmap Item Objective(s)

- To identify vulnerabilities beyond infrastructure (operating system and system services).

Roadmap Item Activities

- Confirm requirements
- Evaluate toolset
- Procure licensing (existing product) or conduct PoC and move to procure (new product) *see appendix E
- Configure access to permit scanning
- Integrate into vulnerability tracking.
- Establish reporting mechanisms and processes

Outcomes/Deliverables

- Visibility into application level vulnerabilities across BC Hydro's applications based on systemic and ongoing scanning of applications and code bases.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: IT.TM.2. Implement/enable threat modelling toolset

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Resilience			Rqmnts → Eval & Procure → Implement & integrate			Strategic	• Vulnerability and Threat Manager

Roadmap Item Detail

Sub-function Capability	Threat Modelling
Approximate start	Year 3
Estimated Duration	4-9 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$100k - $200k (solution licensing) $100k - $160k deployment
Directive 8 Recommendation(s) Addressed	• N/A
Example vendor technologies	Tenable.ep Exposure Management (Tenable One)
Dependencies / Considerations for Approach	• Consideration of existing Tenable licensing

Roadmap Item Description

- This roadmap item seeks to implement tooling to support a threat modelling and exposure management approach is taken to address BC Hydro's attack surface and model threats comprehensively based on visibility across the IT and OT estate.

Roadmap Item Objective(s)

- Ability to model threats and exposures across BC Hydro assets based on actionable information. Model exposure across the attack surface, applying technical and business context to identify and communicate cyber risk.

Roadmap Item Activities

- Solution requirements gathering and design
- Toolset evaluation
- Procurement (including PoC where required) *see appendix E
- Connection of toolset to data sources including vulnerability information, web app information, cloud resources and other IT resources (like firewalls, IDS/IPS, NGFW's). Determine gaps in coverage or integration.
- Build dashboards and information that to provide technical information into actionable exposure management information

Outcomes/Deliverables

- Leverage an integrated platform to apply context to anticipate threats.
- Assists BC Hydro's security practitioners in prioritizing efforts in remediating cyber risks such as software vulnerabilities, misconfigurations and identity and access management weaknesses.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: IT.SM.1. Implement central SIEM dashboard that monitors IT and OT

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Security Monitoring			Use case design; Data sourcing; Log onboarding and integration			Strategic	• Manager, Cybersecurity Operations

Roadmap Item Detail

Sub-function Capability	Event Correlation & Analytics
Approximate start	Year 3
Estimated Duration	12-18 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	Ingestion cost – per GB based on current SIEM licensing $250k - $400k - Implementation effort
Directive 8 Recommendation(s) Addressed	• REC-GEN-05 [MEDIUM]: Consolidate SIEM: Consider consolidation of SIEM infrastructure, resourcing, and operations to a single enterprise program.
Example vendor technologies	Splunk, MS Sentinel
Dependencies / Considerations for Approach	• OT.SM.1. Architect and implement a central SIEM that is able to ingest OT logs. Once completed, integrate OT logs into central SIEM to allow CSO proactive monitoring

Roadmap Item Description

- This roadmap item involves the establishment of a cross-IT-and-OT SIEM capability through extension of OT logs into a common SIEM and the development of centralized capability (and use cases) to monitor for OT threats and cross-estate threat.

Roadmap Item Objective(s)

- Establish a cross-organizational view of threats across IT and OT, within s single monitoring and response capability that has the data and skills to response to threats.

Roadmap Item Activities

- Use case definition (based on OT use cases).
- Log data sourcing and planning
- Log data onboarding – including deployment of forwarders where required and any required data transformation for compliance purposes.
- Integration to SIEM, including skills training, use case enablement and tuning..
- Training and onboarding of resources and teams

Outcomes/Deliverables

- An integrated view of cyber threats and events across IT and OT.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: IT.SM.2. Extend detection and response to integrate network, identity, endpoint, cloud and analytics

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Security Monitoring	SIEM Re-platform and SOC Transformation*	Rqmnts, Soln Eval, Procure (& PoC)	Deploy, Tune			Tactical	• Manager, Cybersecurity Operations

Roadmap Item Detail

Sub-function Capability	Event Correlation & Analytics
Approximate start	Year 2/3 (Year 2 start of SIEM replatform)
Estimated Duration	18-24 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	Cost-per-GB ingested: $1 - $6 (solution dependent) Solution licensing: $500k - $1.2m (solution dependent) Deployment: $150k - $350k Infrastructure: unknown, requires assessment
Directive 8 Recommendation(s) Addressed	• REC-CORP-01 [HIGH]: Expand logs to SIEM: Continue to expand log feeds integrated into Splunk SIEM environment. • REC-CORP-14 [LOW]: Continue to enhance user anomaly detection: Complete implementation of Splunk Enterprise Security and enable UEBA and advanced analytics capability. • REC-GEN-05 [MEDIUM]: Consolidate SIEM: Consider consolidation of SIEM infrastructure, resourcing, and operations to a single enterprise program.
Example vendor technologies	Palo Alto XSIAM, InSightIDR, Microsoft Sentinel
Dependencies / Considerations for Approach	• SIEM Re-platform and SOC Transformation (part of Cyber Security Plan) • Direct links to orchestration and automation (IT.IM.2)

Roadmap Item Description

- Extend the current SOC and detection capabilities to provide end-to-end-management of threats across both cloud and enterprise security operations and to address identity, network and endpoint threat information.

Roadmap Item Objective(s)

- Implement advanced Threat Detection and Response capabilities that integrate identity (IDR), network (NTA), Threat intel (TIP) and endpoint (EPP) threat vectors across on-premise and Cloud (CDR) environments to automate and orchestrate response (SOAR).

Roadmap Item Activities

- Identify data sources to support requirements – network, identity, endpoint and cloud, including log data from containers, commercial off-the-shelf software (COTS) and non-COTS applications.
- Evaluate solutions, considering agent deployment, architecture and operational considerations.
- Architect and design solution.
- Procure (with PoC as part of procurement) solution. *see appendix E
- Deploy/install solution and host agents (where required)
- Modify firewall rules to accommodate solution connectivity
- Onboard data sources
- Review the data ingested and develop playbooks for automated system generated events
- Review and tune security events generated

Outcomes/Deliverables

- Faster decisions with enhanced cross-organization view of threats.
- Reduced SIEM false positives
- Gain forensic-level visibility into all asset groups and threat types.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: IT.SM.3. Implement advanced threat detection technologies

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Security Monitoring				Scope & Design → Eval → PoC & Procure	Implement	Tactical	• Manager, Cybersecurity Operations

Roadmap Item Detail

Sub-function Capability	Event Correlation & Analytics
Approximate start	Year 4
Estimated Duration	3 months eval, 6 months procure, 6-12 months implement
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$200k – $300k solution $300k-$500k implement
Directive 8 Recommendation(s) Addressed	• REC-CORP-13 [LOW]: Implement deceptive detection tactics: Implementation of deceptive threat detection techniques and honey pots such as decoy device, files, systems, accounts, etc. • REC-GEN-08 [MEDIUM]: Expand threat hunting: Augment and expand existing threat hunting capability to deliver broader enterprise capability using threat-driven approaches to search for exposure to threat-relevant TTPs and indicators of compromise (IOCs) • REC-GEN-09 [MEDIUM]: Implement network anomaly analysis: Ensure expansion of Netflow log collection from network devices from all environments, and implement NetFlow analysis capability, to perform in-depth monitoring and understanding of network traffic data.
Example vendor technologies	Vectra (IT), Tenable (OT), Claroty

Roadmap Item Description

- Implement advanced threat detection technologies capable of detecting advanced threats both passively (taps) and actively.

Roadmap Item Objective(s)

- Implement advanced threat detection technologies to augment ability to detect threats within system logs and analytics.

Roadmap Item Activities

- Scoping - solution requirements and design, including network architecture assessment (suitability)
- Solution evaluation
- Procurement (including PoC) *see appendix E
- Network updates or implementation (incl. network taps)
- Pilot deployment and data ingestion testing
- Full deployment and integration

Outcomes/Deliverables

- Advanced threat detection capabilities integrated within current SIEM and response operations.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: IT.IM.1. Architect to recover all critical business functions within business-defined thresholds

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Resilience	Safehouse Project			Architecture study Architecture design		Strategic	• Chief Enterprise Architect

Roadmap Item Detail

Sub-function Capability	Recovery
Approximate start	Year 4
Estimated Duration	12 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$200k-300k (assessment and design)
Directive 8 Recommendation(s) Addressed	• REC-CORP-02 [HIGH]: Continue securing backups: Complete the project to implement technical controls to secure backups and backup systems, including segmentation and encryption
Example vendor technologies	N/A
Dependencies / Considerations for Approach	• Safehouse Project • Dependent on broader BC Hydro initiatives on recovery of business functions in the event of a disaster, including disaster recovery, business continuity and crisis management.

Roadmap Item Description

- This roadmap item addresses the need to review and update BC Hydro's overall network and backup architecture to ensure it is resilient against cyber attacks and that BC Hydro is able to recover from modern cyber threats such as ransomware.

Roadmap Item Objective(s)

- To review and update BC Hydro's network, backup and security services architecture based on an assessment of resilience and recovery capabilities. This addresses ability to recover and continue operations while cyber threat containment activities are ongoing.

Roadmap Item Activities

- Ransomware readiness assessment – assess architecture for ability to resist and recover from a ransomware attack as a primary example of cyber threats to develop recovery capability against. Current state -> Gaps -> Simulation.
- Harden perimeter – resilience of key services; remote services and perimeter access; media and device security; monitoring and response toolset resilience.
- Limit the blast radius – identity and access management; network segmentation; firewalls and traffic filtering; Active Directory security and recoverability; credential protection; endpoint isolation.
- Establish recovery building blocks – data protection controls (including resilient and immutable storage); backup integrity and testing; recovery execution.

Outcomes/Deliverables

- Updated architecture to ensure that business operations can be recovered in the event of a cyber breach.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: IT.IM.2. Implement Security Orchestration to automate threat containment across both on-premise and cloud workloads

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Security Incident Management				Scope & Design → Toolset Eval → Procure	Implement	Tactical	• Manager, Cybersecurity Operations.

Roadmap Item Detail

Sub-function Capability	Containment
Approximate start	Year 4
Estimated Duration	18-24 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$350k - $550k (solution) $220k-$450k implementation
Directive 8 Recommendation(s) Addressed	• N/A
Example vendor technologies	Palo Alto XSIAM
Dependencies / Considerations for Approach	• IT.SM.2. Extend detection and response to integrate network, identity, endpoint, cloud and analytics • If XSOAR licensing is already in place (even quick-start) this should be considered and has not been accounted for.

Roadmap Item Description

- This roadmap item seeks to implement an integrated orchestration solution that can allow for automated and managed containment, triage and remediation of a cyber threat..

Roadmap Item Objective(s)

- Leverage security orchestration and automation, integrated with detection and prevention controls within endpoint, network and Cloud workload, to automate containment of cyber threats across on-premise and Cloud-based workloads.

Roadmap Item Activities

- Requirements gathering and high-level architecture design
- Analysis – assess suitability of existing perimeter, network, endpoint and Cloud workload technologies
- Evaluate and select SOAR solution: Select a SOAR platform that is able to meet BC Hydro's requirements and architecture.
- Procurement - After evaluation of requirements move to conduct a PoC of a SOAR solution that aligns with BC Hydro's technology requirements. If successful, move to procurement.
- Implement and integrate: Implement the selected SOAR solution. Integrate the security tools that are required for the containment process, including tools such as firewalls, intrusion detection systems, and endpoint protection solutions.

Outcomes/Deliverables

- Faster threat detection and response: A SOAR solution can automate the process of threat detection and response, significantly reducing the time it takes to identify and contain threats.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Consolidated OT

Capability Assessment and Roadmap Prioritization

Consolidated OT: Current State Analysis

Secure from Application to Data

Identity & Access
- Authentication
- Authorization
- Federation

Identity Governance & Administration
- Provisioning
- Registration and Enrolment
- Access Governance
- Privileged Access Mgmt
- Directory Services

Trusted & Secure Access

Application Protection
- Secure SDLC
- DevSecOps
- Application Firewall
- API Security Gateway

Network Security
- Secure Network Access
- Intrusion Detection
- Network Segmentation
- Network Traffic Filtering
- Content Filtering & Scanning
- Intrusion Prevention

Endpoint Security
- Configuration Mgmt
- Endpoint Protection
- Mobile Device Mgmt

Data Protection
- Secure Storage & Destruction
- Backup & Recovery
- Data Loss Prevention
- Rights Management
- Data Security Management

Trust Services
- Trusted Time
- PKI Mgmt
- Encryption Services

Identify & Manage Events and Incidents

Security Monitoring
- Log Mgmt
- Audit & Compliance
- Event Correlation & Analytics
- Monitoring & Reporting

Security Incident Management
- Identification
- Investigation Support
- Containment

Legend
- Not Required
- Missing
- Not Yet Mature
- Limited Deployment
- Ready & Reusable

Manage Threats & Vulnerabilities

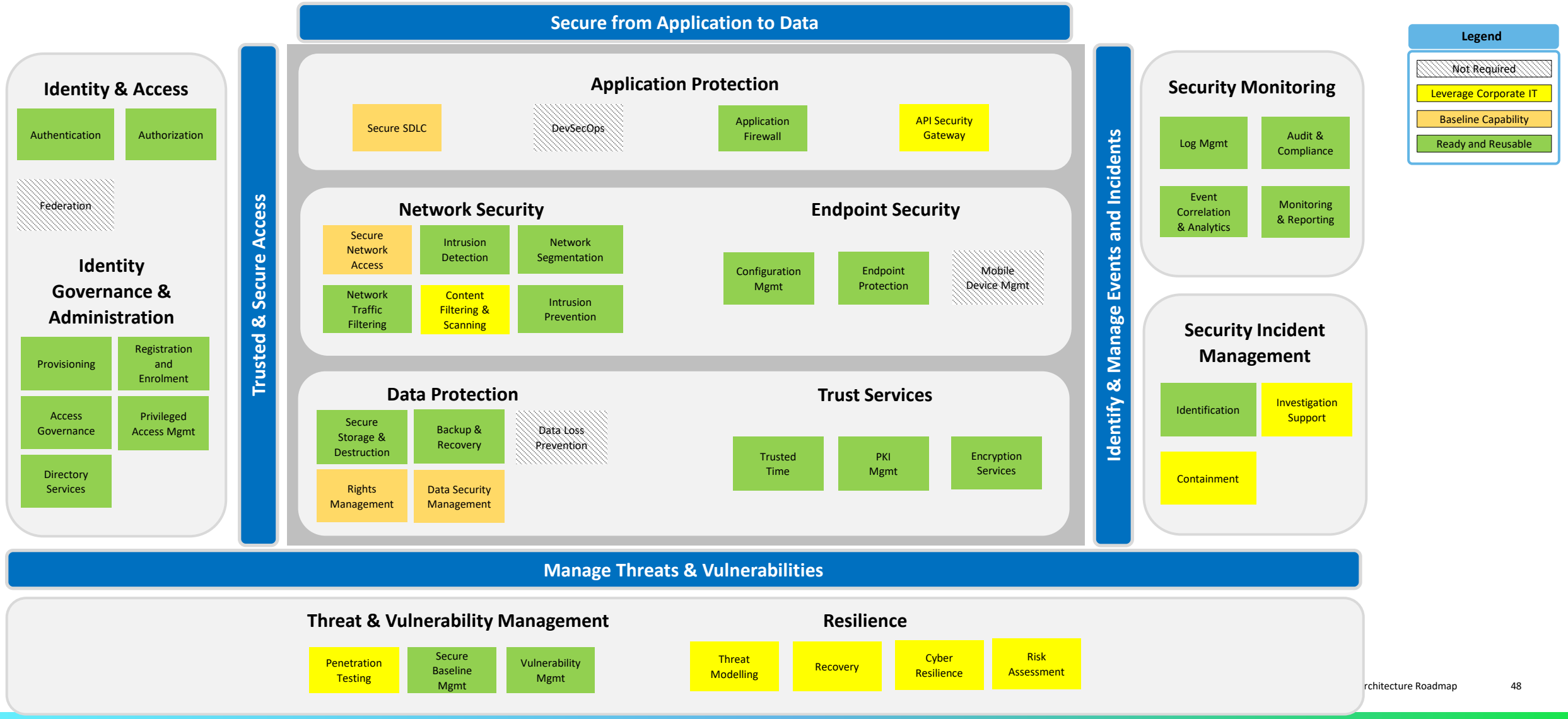
Threat & Vulnerability Management
- Penetration Testing
- Secure Baseline Mgmt
- Vulnerability Mgmt

Resilience
- Threat Modelling
- Recovery
- Cyber Resilience
- Risk Assessment

Refer to Appendix A for individual OT teams current state assessments

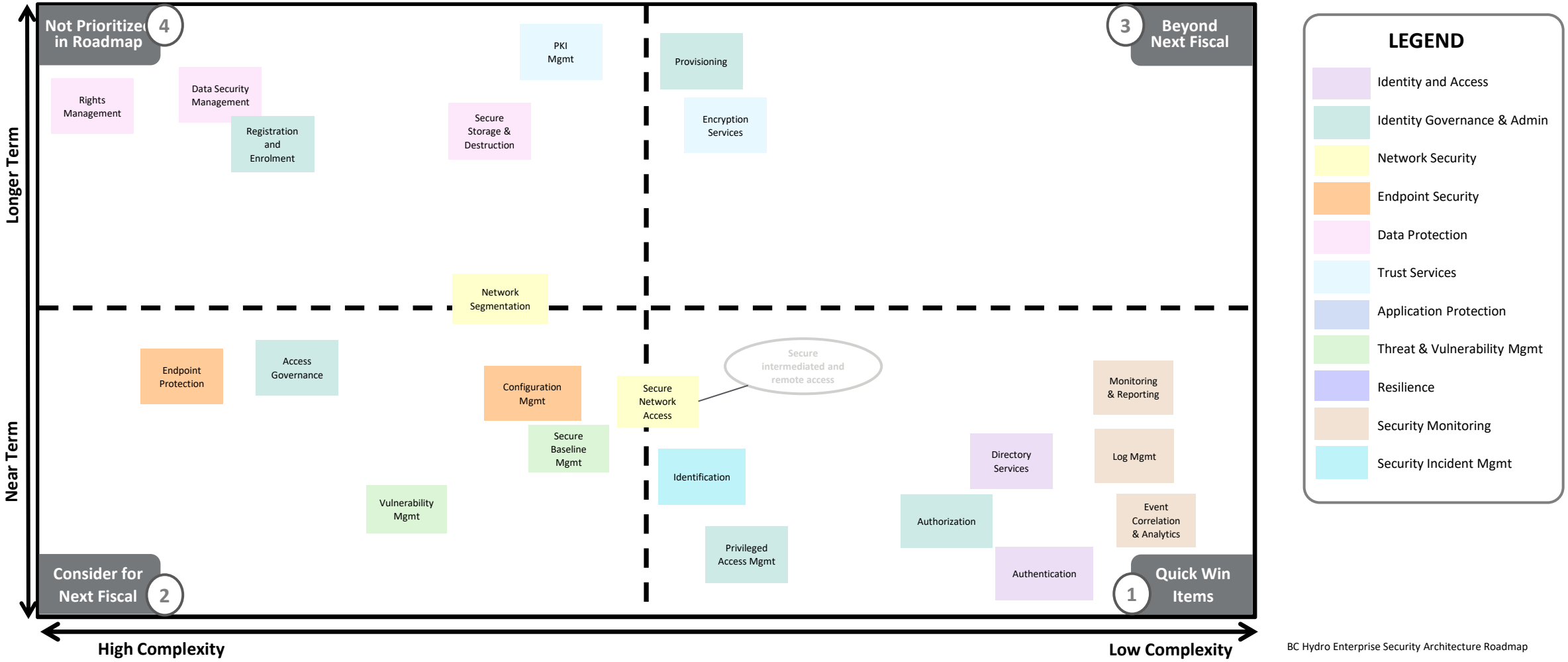
Consolidated OT: Desired Target State

Note: The desired target state has been defined using an unconstrained view and assumes security architecture capability establishment in environments that can support the capability requirements.



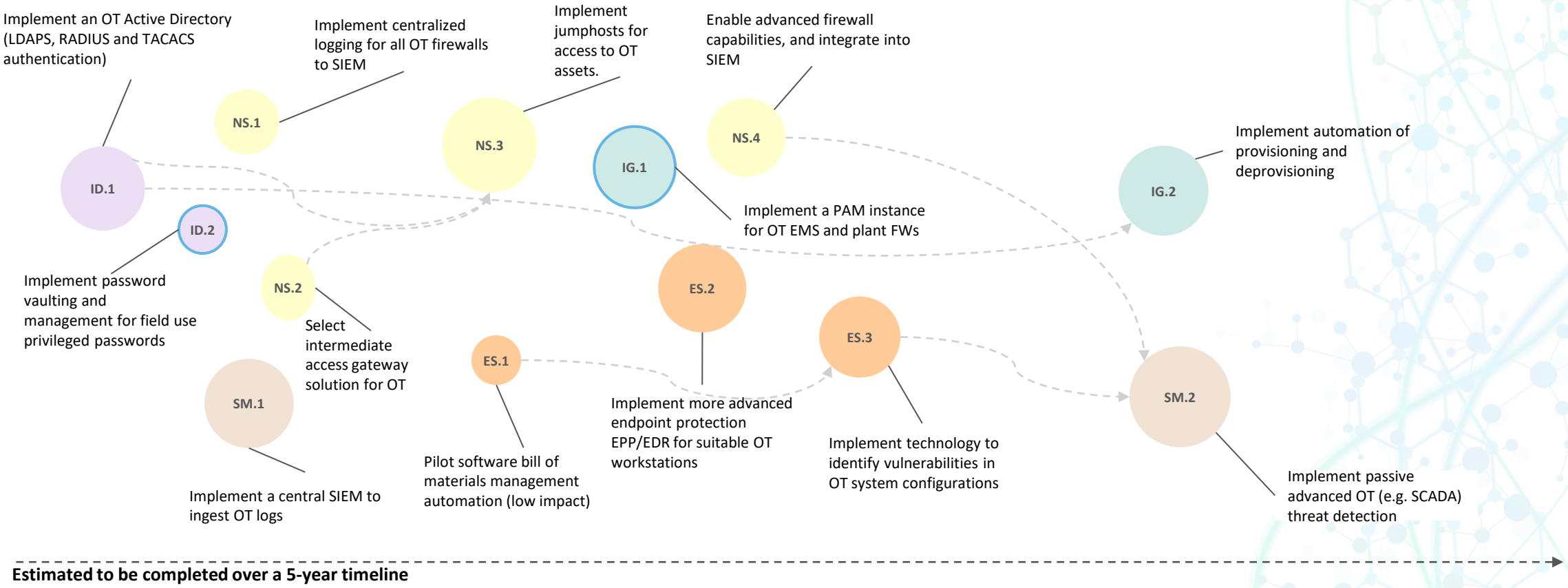
Consolidated OT: Prioritized Capability Gap Heatmap

The heatmap below illustrates a consolidated view of the placement of functions relative to the current and target Functional capability. The bottom right quadrant indicates where gaps are most extreme based on the current state and desired target state and provides a means of prioritizing Functions that require most investment or operationalization to ensure that BC Hydro is able to meet its cybersecurity objectives encapsulated within the Enterprise Security Architecture and the Cyber Security Plan (CSP).

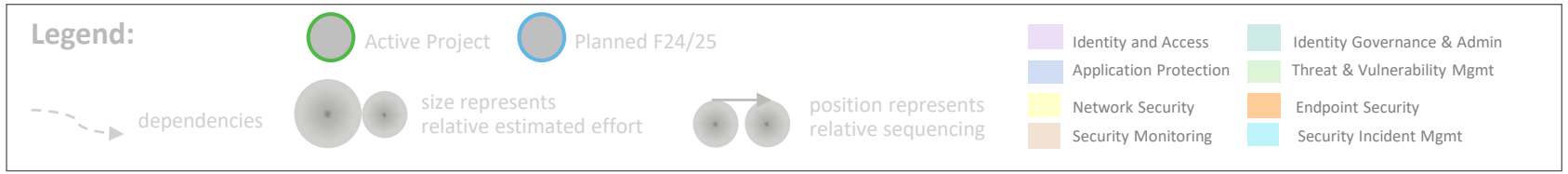


Consolidated OT: ESA Roadmap Item Sequencing

The diagram below indicates the roadmap items in a timeline sequence that also reflects broad sizing, interdependencies and a clear mapping to the “House View” capability models.



Estimated to be completed over a 5-year timeline



Consolidated OT: ESA Prioritized Roadmap

The roadmap below represents an unconstrained view of timelines for establishment of Enterprise Architecture's desired capability over a 5-year period

Functional Pillar	Roadmap Item	
Identity and Access Management	OT.ID.1. Replace use of local accounts for OT networking and server systems by implementing an OT Active Directory and leveraging AD, LDAPS, RADIUS and TACACS authentication services	IAM Roadmap # 26 (OT credential mgmt); Design; Pilot; Migrate Systems
	OT.ID.2. Implement password vaulting and management solution for field use privileged passwords.	Design; Pilot; Migrate Accounts
Identity Governance and Administration	OT.IG.1. Implement a PAM instance for OT EMS and plant FWs to manage privileged accounts for compliance.	IAM Roadmap # 4 (PAM for OT); Rollout
	OT.ID.2. Implement automation of provisioning and deprovisioning leveraging IGA solution selected for IT, replacing use of SureSight.	IT IGA Implementation (appendix C); Design; Pilot; Implement
Endpoint Security	OT.ES.1. Pilot software bill of materials management automation for low impact sites	Scope; Eval; PoC & Procure; Implmnt
	OT.ES.2. Implement more advanced endpoint protection EPP/EDR for suitable OT workstations (Control Centre)	EMS Refresh; Scope; Design and eval; PoC & Procure; Implement
	OT.ES.3. Implement technology to identify vulnerabilities in OT system configurations (beyond TDSO Tripwire) and integrate to asset database technology	Design; PoC & Procure; Implement
Network Security	OT.NS.1. Implement centralized logging for all OT firewalls to SIEM for visibility.	Assess; Implement
	OT.NS.2. Conduct a study of intermediated access gateway product for OT	Study
	OT.NS.3. Implement jumphosts for all access to OT assets.	Assess; Implement; Migrate access (rollout)
	OT.NS.4. Enable advanced firewall capabilities, and integrate into central monitoring	Proj. 2023-03 Network Security Monitoring; Pilot; Implnt; SIEM integ
Security Monitoring	OT.SM.1. Architect and implement a central SIEM that is able to ingest OT logs. Once completed, integrate OT logs into central SIEM to allow CSO proactive monitoring	Design; Implement; Use Case Activation
	OT.SM.2. Implement passive advanced OT (e.g. SCADA) threat detection based on analysis of network traffic.	Plan; Procure & POC; Pilot Sites; Phased implement

Active Project * | Planned Project * | Proposed | Dependency | Multi-year iterative rollout

* Refer to Cybersecurity Plan F24-F26 in Appendix B

Consolidated OT: Directive 8 Recommendations Addressed by the Roadmap Items (16/40)

The roadmap aims to address a number of recommendations made within the Directive 8 Threat Risk Assessment. While not all recommendations related to architecture enhancements, this roadmap is able to significantly address the recommendations.

Functional Pillar	Roadmap Item	Directive 8 Recommendations Addressed
Identity Governance and Administration	IG.1. Implement a PAM instance for OT EMS and plant FWs to manage privileged accounts for compliance.	• REC-GEN-06 [MEDIUM]: Expand and consolidate PAM: Consider consolidation of PAM program across BC Hydro environments (i.e. corporate IT and OT) with vaulting solution segmentation in critical environments (MRS OT). • REC-REG-03 [MEDIUM]: Implement consolidated PAM: Consider integration with consolidated PAM program, and implementation of dedicated OT environment PAM solution instance (related to recommendation REC-GEN-06). • REC-NONREG-05 [MEDIUM]: Implement consolidated PAM: Consider integration with consolidated PAM program, alignment to BC Hydro's access management/control policies and standards, and implementation of dedicated non-MRS OT environment PAM solution instance (related to recommendation REC-GEN-06)
Network Security	NS.3. Implement jumphosts for all access to OT assets.	• REC-NONREG-07 [MEDIUM]: Expand use of jump hosts: Expand the use jump hosts for connections to provide access control layers to remote connected systems • REC-REG-05 [MEDIUM[: Restrict authorized connections: Implement restriction of remote access (dialup) connections to specified numbers
	NS.4. Enable advanced firewall capabilities, and integrate into central monitoring	• REC-NONREG-08 [LOW]: Implement process for reviewing firewalls: Conduct regular firewall ruleset reviews to review, identify, and remediate changes or drifts from hardened firewall security configurations (could leverage corporate processes).
Endpoint Security	ES.3. Implement technology to identify vulnerabilities in OT system configurations (beyond TDSO Tripwire) and integrate to asset database technology	• REC-GEN-03 [HIGH]: Continue asset management formalization: Continue implementing asset management solutions (i.e. ServiceNow) and work towards harmonization of process and toolset across environments (where not restricted due to NERC CIP confidentiality requirements - MRS OT asset management may be better served by a dedicated OT asset database complying with NERC CIP requirements) • REC-NONREG-02 [HIGH]: Implement configuration monitoring: Document and define hardened configuration standards for non-MRS systems, and implement processes and tools for ongoing configuration monitoring to detect unauthorized changes to systems
Threat and Vulnerability Management	ES.3. Implement technology to identify vulnerabilities in OT system configurations (beyond TDSO Tripwire) and integrate to asset database technology	• REC-NONREG-04 [HIGH]: Implement the planned vulnerability scanning and penetration testing program: Implement process for ongoing vulnerability scanning and penetration testing to identify and remediate system vulnerabilities
Security Monitoring	SM.1. Architect and implement a central SIEM that is able to ingest OT logs. Once completed, integrate OT logs into central SIEM to allow CSO proactive monitoring	• REC-GEN-05 [MEDIUM]: Consolidate SIEM: Consider consolidation of SIEM infrastructure, resourcing, and operations to a single enterprise program. • REC-REG-01 [HIGH]: Expand logs to SIEM: Expand ingestion of log information from MRS OT systems and network devices (i.e. NetFlow logs) in alignment with BC Hydro's log management standard, where technically feasible. • REC-NONREG-06 [MEDIUM]: Adopt consolidated SIEM: Consider adoption of enterprise SIEM program and expand resources to accommodate integrate log feeds to a SIEM environment where technically feasible and monitoring/response resources (related to recommendation item REC-GEN 05)
	SM.2. Implement passive advanced OT (e.g. SCADA) threat detection based on analysis of network traffic.	• REC-REG-02 [HIGH]: Implement ICS specialized detection: Implement dedicated ICS threat identification platform (e.g. Dragos), to provide robust threat detection, visualization, and response capabilities. • REC-NONREG-09 [LOW]: Implement ICS specialized detection: Implement dedicated ICS threat identification platform (e.g. Dragos) where feasible to provide robust threat detection, visualization, and response capabilities.

Roadmap Item: OT.ID.1. Replace use of local accounts for OT networking and server systems by implementing an OT Active Directory and leveraging AD, LDAPS, RADIUS and TACACS authentication services

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Identity & Access Management	IAM Roadmap # 26 (OT credential mgmt) Design → Pilot	Migrate Systems				Tactical	• IT Identity Management Lead • OT Identity Advisor

Roadmap Item Detail

Sub-function Capability	Authentication
Approximate start	Year 1
Estimated Duration	12-24 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$280k - $550k (services) AD pricing is dependent on BC Hydro licensing agreement
Directive 8 Recommendation(s) Addressed	• N/A
Example vendor technologies	Microsoft Active Directory
Dependencies / Considerations for Approach	• Compatibility of OT devices • Risk-based planning • RADIUS server

Roadmap Item Description

- This roadmap item is focused on implementing an Active Directory environment to support .

Roadmap Item Objective(s)

- Establish separate Azure AD tenants for IT and OT where each Active Directory Forest is connected to the relevant Azure AD tenant and custom domains are configured.

Roadmap Item Activities

- Identifying AD DS design and deployment requirements
- Develop AD DS deployment strategy, including design of logical and site topology for AD DS
- Deploy AD
- Deploy RADIUS server, and integrate with AD
- Provision required accounts for OT users
- Pilot configuration of select OT assets to authenticate via RADIUS, TACACS+, LDAPS and native AD (where possible)
- Continue deployment across OT assets on a risk-based approach

Outcomes/Deliverables

- AD environment to support OT authentication and authorization.
- No impact to OT environments from IT security vulnerabilities.
- An OT operational directory that aligns with the Purdue model.
- Makes separation/divestment operations easier as there are no dependencies with the IT tenant..

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: OT.ID.2. Implement password vaulting and management solution for field use privileged passwords

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Identity & Access Management	Design	Pilot, Migrate Accounts				Tactical	• IT Identity Management Lead • OT Identity Advisor

Roadmap Item Detail

Sub-function Capability	Privileged Access Management
Approximate start	Year 1
Estimated Duration	6-9 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$100k-$500k (solutions vary significantly)
Directive 8 Recommendation(s) Addressed	• N/A
Example vendor technologies	ManageEngine, CyberArk
Dependencies / Considerations for Approach	• Alignment with broader PAM, and leverage of existing licensing (CyberArk)

Roadmap Item Description

- This roadmap item aims to implement a solution to vault privileged passwords used in the field within a secure vault, that can be leveraged by field workers through offline caching, but which has a “phone home” capability.

Roadmap Item Objective(s)

- To secure privilege access secrets (passwords, PINS) and allow users in the field to access these via a secure cache on a mobile app. The service should support synchronization of these when connectivity is available.

Roadmap Item Activities

- Define requirements, including discovery of accounts in use and evaluation of suitability for vaulting.
- Conduct a market-scan for leading credential management tools - evaluate solution suitability.
- Engage vendor to conduct pilot implementation (using existing solution footprint if possible).
- Develop a migration plan for account to move into vault.
- Implement and roll-out the selected tool to all OT users - deploy application.
- Train users
- Migrate accounts.

Outcomes/Deliverables

- Integration into broader PAM can eliminate the use of hard-coded secrets by securely storing and rotating application credentials based on policy.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: OT.IG.1. Implement a PAM instance for OT EMS and plant FWs to manage privileged accounts for compliance

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Identity Governance		IAM Roadmap # 4 (PAM for OT)	Rollout			Tactical	• IT Identity Management Lead • OT Identity Advisor

Roadmap Item Detail

Sub-function Capability	Privileged Access Management
Approximate start	Year 2/3
Estimated Duration	6-12 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$300k - $550k project cost
Directive 8 Recommendation(s) Addressed	• REC-GEN-06 [MEDIUM]: Expand and consolidate PAM: Consider consolidation of PAM program across BC Hydro environments (i.e. corporate IT and OT) with vaulting solution segmentation in critical environments (MRS OT). • REC-REG-03 and EC-NONREG-05 [MEDIUM]: Implement consolidated PAM: Consider integration with consolidated PAM program, and implementation of dedicated OT environment PAM solution instance (related to recommendation REC-GEN-06).
Example vendor technologies	CyberArk
Dependencies / Considerations for Approach	• IAM Roadmap for PAM implementation, and IAM roadmap for OT PAM

Roadmap Item Description

- There are no Privileged Access Management (PAM) capabilities for the OT network. This roadmap item aims to expand PAM for securing OT privileged access..

Roadmap Item Objective(s)

- To extend PAM capabilities to OT through a dedicated PAM solution and thereby reducing risk of misuse and exposure of privileged accounts.

Roadmap Item Activities

- Business analysis for establishing a standard process for justifying the need for creation and management of a privileged account
- Define PAM policies and operating model
- Complete solution design for privilege account creation, secure access, management and expiry including automated provisioning and de-provisioning of these accounts
- Implement the foundation capability for priority accounts and an end-to-end lifecycle management process

Outcomes/Deliverables

- PAM capabilities extended to OT.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: OT.IG.2. Implement automation of provisioning and deprovisioning (ensure that the IGA solution selected for IT is scalable for OT requirements, incl replacement of SureSIght).

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Identity Governance	IT IGA Implementation (appendix C)		Design, Pilot	Implement		Tactical	• IT Identity Management Lead • OT Identity Advisor

Roadmap Item Detail

Sub-function Capability	Access Governance
Approximate start	Year 3
Estimated Duration	10-12 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$400k - $800k project cost
Directive 8 Recommendation(s) Addressed	• N/A
Example vendor technologies	SailPoint, Saviynt, AlertEnterprise
Dependencies / Considerations for Approach	• IAM Roadmap IT IGA implementation

Roadmap Item Description

- Implement automated access governance capability, extending IT identity governance administration (IGA) toolset to OT.

Roadmap Item Objective(s)

- To leverage IGA platform capabilities to perform regular and automated access certifications and thereby enhancing security and accountability, enabled by risk-based access granting with periodic certification.

Roadmap Item Activities

- Confirm design suitability for IT IGA and Pilot
- Document access certification roles and responsibilities
- Define access certification policy
- Configure IT IGA platform, define automated events and triggers for access review/certifications
- Automate access re-certification and rules for exception scenarios and delegation
- Configure access certification reports
- Implement capability for override
- Implement workflows for recertifying access for time bound roles (for example; contractors who may get extended)

Outcomes/Deliverables

- OT access certification automated through the new IGA platform.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: OT.ES.1. Pilot software bill of materials (SBOM) management automation for low impact sites

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Application Protection & Endpoint Security		Scope, Eval, PoC & Procure, Implmnt				Tactical	• Vulnerability and Threat Manager • Application Security Program Lead

Roadmap Item Detail

Sub-function Capability	DevSecOps & Configuration Management
Approximate start	Year 2
Estimated Duration	6-12 months (procurement accounted for)
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$75k - $150k deployment $50k - $120k licensing (annual)
Directive 8 Recommendation(s) Addressed	• N/A
Example vendor technologies	Tanium, WhiteSource, FOSSA, Vigilant
Dependencies / Considerations for Approach	• Dependent on asset management capabilities • Support for software ecosystem

Roadmap Item Description

- Deploy a software bill of materials management and assessment solution and assess against OT software and vendor solutions.

Roadmap Item Objective(s)

- Deploy capability to identify and manage vulnerabilities within OT software, including software supplied by vendors..

Roadmap Item Activities

- Scope and identify requirements for SBOM, including target software code bases
- Evaluate solutions available against the solutions
- Conduct a Proof of Concept with the vendor (see Appendix E). Available solutions offer PoC / Pilot options.
- Configure access to software / assets (incl. CICD), and deploy asset management agents where required
- Develop SBOM profiles, configure scanning and integrate into asset management processes
- Inventory libraries and vendors
- Develop reporting mechanisms
- Integrate to vulnerability management processes

Outcomes/Deliverables

- A detailed record of all components within a software application, including open-source libraries, third-party dependencies, licenses, and known vulnerabilities..

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: OT.ES.2. Implement more advanced endpoint protection EPP/EDR for suitable OT workstations (Control Centre)

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Endpoint Security	EMS Refresh	Scope; Design and eval	PoC & Procure	Implement		Tactical	• Cybersecurity Infrastructure Manager

Roadmap Item Detail

Sub-function Capability	Endpoint Protection
Approximate start	Year 2/3
Estimated Duration	18-24 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	Solution dependent, costs vary significantly Assumes 2,000 endpoints $1m – $2.5m
Directive 8 Recommendation(s) Addressed	• N/A
Example vendor technologies	Crowdstrike, Trend, Defender for IoT
Dependencies / Considerations for Approach	• Dependency on network capabilities to support • Selection of active vs passive detection capabilities • Focus is on Control Centre assets that can accommodate EPP

Roadmap Item Description

- To implement an endpoint protection solution for OT workstations (Control Center focus), provide modern endpoint protection capability (EDR and potentially XDR).

Roadmap Item Objective(s)

- Enable more advanced endpoint protection for capable OT systems within higher-risk environments with interactive workstations.

Roadmap Item Activities

- Scope - requirements gathering (incl. environment scan) and market scan
- Solution design and evaluation
- Procurement cycle (including PoC if possible to prove alignment and ensure impact understood)
- Implementation, including planning, network deployment (config and architect) and agent deployment (where possible)
- Train and transition to operations

Outcomes/Deliverables

- EDR deployed that integrates endpoint visibility and threat management into security operations.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: OT.ES.3. Implement technology to identify vulnerabilities in OT system configurations (beyond TDSO Tripwire) and integrate to asset database technology

Functional Domain	Y1	Y2	Y3	Y4	Y5
Endpoint Security; Threat & Vulnerability			Design → PoC & Procure →	Implement →	

Tactical/Strategic
Tactical

Related Cyber Op Model Roles
• Vulnerability and Threat Manager

Roadmap Item Detail

Sub-function Capability	Configuration Mgmt & Vulnerability Mgmt
Approximate start	Year 3
Estimated Duration	12-18 months (incl. procurement)
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	$300-$600k for solutions
Directive 8 Recommendation(s) Addressed	• REC-NONREG-04 [HIGH]: Implement the planned vulnerability scanning and penetration testing program: Implement process for ongoing vulnerability scanning and penetration testing to identify and remediate system vulnerabilities • REC-NONREG-08 [LOW]: Implement process for reviewing firewalls: Conduct regular firewall ruleset reviews to review, identify, and remediate changes or drifts from hardened firewall security configurations (could leverage corporate processes).
Example vendor technologies	Claroty, Tenable OT, TripWire, Radiflow, Tufin
Dependencies / Considerations for Approach	• Network dependencies exist • Site selection is a critical planning consideration • Requires quality in OT asset management data (incl. non-NERC)

Roadmap Item Description

- To implement threat/vulnerability detection for misconfiguration issues within OT that is linked to the assets criticality and risk.

Roadmap Item Objective(s)

- Implement a solution suitable for OT that is able to evaluate configurations on IT assets, monitor and audit to alert for configuration modifications or weaknesses that introduce vulnerability.

Roadmap Item Activities

- Design, scope and plan. Note, due to passive vulnerability scanning nature, will require careful planning
- As part of procurement, conduct a PoC at selected sites for asset configuration assessment.
    - Configure SPAN session or tap and media converters (for serial) where required.
    - Configure solution for analysis of potential threats, backdoors, exploits etc.
    - Integrate asset inventory data
    - Identify and tune for false positive detections.
- PoC a solution for network equipment assessment (including firewalls)
- Upon successful PoC, move to procurement
- Phased implementation, site by site.

Outcomes/Deliverables

- Inventory of vulnerabilities in OT environments and the ability to target the vulnerabilities that have exploits associated with them..

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: OT.NS.1. Implement centralized logging for all OT firewalls to SIEM for visibility.

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Security Monitoring	Assess → Implement					Tactical	• Manager, Cybersecurity Operations

Roadmap Item Detail

Sub-function Capability	Log Mgmt
Approximate start	Year 1
Estimated Duration	6-9 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	Internal effort
Directive 8 Recommendation(s) Addressed	• N/A
Example vendor technologies	N/A
Dependencies / Considerations for Approach	• Connectivity

Roadmap Item Description

- Ingest OT firewall logs into a central SIEM for logging and analytics to identify threats and anomalies within OT environments.

Roadmap Item Objective(s)

- Visibility of anomalies within OT.

Roadmap Item Activities

- Confirm assets in scope
- Confirm connectivity
- Confirm capacity and capability of assets
- Implement collectors / forwarders where required
- Ingest logs
- Develop use cases

Outcomes/Deliverables

- OT firewall logs ingested into SIEM to provide visibility of OT-related threats and events.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: OT.NS.2. Conduct a study to select intermediate access gateway solution for OT

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Network Security	Study					Strategic	• Cybersecurity Infrastructure Manager • OT Cybersecurity Program Lead/Manager

Roadmap Item Detail

Sub-function Capability	Secure Network Access
Approximate start	Year 1
Estimated Duration	4-6 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	Internal effort, $90k-$120k study
Directive 8 Recommendation(s) Addressed	• REC-NONREG-07 [MEDIUM]: Expand use of jump hosts: Expand the use jump hosts for connections to provide access control layers to remote connected systems • REC-REG-05 [MEDIUM[: Restrict authorized connections: Implement restriction of remote access (dialup) connections to specified numbers
Example vendor technologies	CyberArk Alero, BeyondTrust, Cisco CVD,
Dependencies / Considerations for Approach	

Roadmap Item Description

- Conduct an architecture study of solution and architecture options to manage and provide users access to OT assets (including remote).

Roadmap Item Objective(s)

- Adopt a Zero Trust architectures and enforce network segmentation (incl. protocol isolation) to limit risks involved in access to OT assets.
- Gain visibility and control by moderating and intermediating asset access and control.
- Provide a frictionless and secure solution for intermediate OT access.
- Implement controls over use of credentials.
- Implement network and access isolation and segmentation (incl. protocol isolation)
- Implement session analytics, and full system logging/monitoring with integration to SEIM.

Roadmap Item Activities

- Assess requirements
- Develop conceptual design
- Market scan and initial evaluation
- Develop recommended design and architecture

Outcomes/Deliverables

- Study, suitable to move to next phase of pilot or procurement.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: OT.NS.3. Implement jumphosts for all access to OT assets

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Network Security		Assess → Implmnt → Migrate all access				Tactical	• Cybersecurity Infrastructure Manager • OT Cybersecurity Program Lead/Manager

Roadmap Item Detail

Sub-function Capability	Secure Network Access
Approximate start	Year 1 / 2
Estimated Duration	12 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	Internal costs for VDI solutions
Directive 8 Recommendation(s) Addressed	• REC-NONREG-07 [MEDIUM]: Expand use of jump hosts: Expand the use jump hosts for connections to provide access control layers to remote connected systems • REC-REG-05 [MEDIUM[: Restrict authorized connections: Implement restriction of remote access (dialup) connections to specified numbers
Example vendor technologies	VDI technologies in use at BC Hydro
Dependencies / Considerations for Approach	• Ability to provision into intermediate zone • Alignment with OT asset access requirements

Roadmap Item Description

- To transition all access to OT assets to be via secured jumphosts (i.e. no direct through-firewall access to OT assets).

Roadmap Item Objective(s)

- Ensure that access to OT assets is via a managed and intermediated host that is able to provide visibility within the SIEM.

Roadmap Item Activities

- Identify current access models (incl. study of firewall log data to identify patterns in use)
- Implement managed jumphosts (virtual) within the intermediate zone.
- Configure jumphosts with required tooling and access.
- Integrate jumphosts into SIEM for monitoring.
- Train users.
- Transition access.

Outcomes/Deliverables

- Intermediated access and ability to monitor access and actions.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: OT.NS.4. Enable advanced firewall capabilities, and integrate into central monitoring

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Network Security	Proj. 2023-03 Network Security Monitoring	Pilot	Implnt	SIEM integ		Tactical	• Manager, Cybersecurity Operations

Roadmap Item Detail

Sub-function Capability	Content Filtering & Scanning; Intrusion Prevention
Approximate start	Year 2
Estimated Duration	9 – 12 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	Internal costs only, FW features assumed licensed
Directive 8 Recommendation(s) Addressed	• N/A
Example vendor technologies	Cisco, Palo Alto
Dependencies / Considerations for Approach	• FW features licensed • NGFW deployed

Roadmap Item Description

- Gain visibility into OT perimeter traffic and dedicated OT traffic through use of advanced firewall features.

Roadmap Item Objective(s)

- Activate NGFW capabilities within firewalls in OT, leveraging features to identify and alert to threats.

Roadmap Item Activities

- Develop phased implementation plan
- Pilot capability enablement
- Log ingestion and use case development

Outcomes/Deliverables

- Advanced capabilities implemented within OT firewalls.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: OT.SM.1. Architect and implement a central SIEM that is able to ingest OT logs. Once completed, integrate OT logs into central SIEM to allow CSO proactive monitoring

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Security Monitoring	Design	Implement	Use Case Activation			Strategic	• Manager, Cybersecurity Operations

Roadmap Item Detail

Sub-function Capability	Event Correlation & Analytics
Approximate start	Year 1 (design), Year 2 (implement)
Estimated Duration	12-18 months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	Dependent on whether procured as a managed service or leveraging an on-prem / CSP solution. Dependent on use of existing Splunk footprint.
Directive 8 Recommendation(s) Addressed	• REC-GEN-05 [MEDIUM]: Consolidate SIEM: Consider consolidation of SIEM infrastructure, resourcing, and operations to a single enterprise program. • REC-NONREG-06 [MEDIUM]: Adopt consolidated SIEM: Consider adoption of enterprise SIEM program and expand resources to accommodate integrate log feeds to a SIEM environment where technically feasible and monitoring/response resources (related to recommendation item REC-GEN 05)
Example vendor technologies	Splunk, Microsoft Sentinel
Dependencies / Considerations for Approach	• Alignment with future of SIEM within BC Hydro • Consideration of conversed and emerging workload footprint.

Roadmap Item Description

- This roadmap item aims to ingest and integrate OT log data into a consolidated SIEM that has use cases developed for both OT and cross-system threats and allows cybersecurity operations teams to identify and respond to threats both within IT and OT.

Roadmap Item Objective(s)

- Architecting a SIEM for OT requires a careful approach that takes into account the unique requirements of OT environments.

Roadmap Item Activities

- Gather requirements.
- Identify critical OT assets and associated logs
- Architect solution, with assurance over compliance obligations
- Evaluate SIEM solution suitability - Ensure SIEM is able to operate use cases:
- Deploy log forwarders and collectors
- Activate use cases for OT
- Escalation and reporting configuration
- Tune

Outcomes/Deliverables

- Improved visibility: An OT ready SIEM can provide improved visibility into OT systems by collecting and analyzing data from a variety of sources, including network traffic, system logs, and security devices. This can help identify potential security threats and vulnerabilities that may be missed by traditional security tools.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Roadmap Item: OT.SM.2. Implement passive advanced OT (e.g. SCADA) threat detection based on analysis of network traffic

Functional Domain	Y1	Y2	Y3	Y4	Y5	Tactical/Strategic	Related Cyber Op Model Roles
Security Monitoring			Plan	Procure & POC → Pilot Sites	Phased implement	Tactical	• Vulnerability and Threat Manager

Roadmap Item Detail

Sub-function Capability	Event Correlation & Analytics
Approximate start	Year 3
Estimated Duration	24+ months
Estimated Sizing* (implementation cost range high-level estimate based on industry average, excl. sustainment/ops)	Dependent on site and hardware selected, no current data available at the time of writing. Sizing should account for site count, device count and sizing, redundancy and implementation costs for configuration of network.
Directive 8 Recommendation(s) Addressed	• REC-GEN-08 [MEDIUM]: Expand threat hunting: Augment and expand existing threat hunting capability to deliver broader enterprise capability using threat-driven approaches to search for exposure to threat-relevant TTPs and indicators of compromise (IOCs) • REC-REG-02 [HIGH]: Implement ICS specialized detection: Implement dedicated ICS threat identification platform (e.g. Dragos), to provide robust threat detection, visualization, and response capabilities.
Example vendor technologies	Verve, Claroty, Dragos, RadiFlow
Dependencies / Considerations for Approach	• Routable connectivity to transfer alerts

Roadmap Item Description

- Implement OT visibility & anomaly detection to provide network visibility, threat detection, and alerting for OT devices and protocols to address and supplement monitoring where XDR coverage is not in place.

Roadmap Item Objective(s)

- Enable central monitoring at a security operations centre for to identify OT threats through a single dashboard.

Roadmap Item Activities

- Generate baseline for network and host behaviour
- Install or configure collectors at selected OT sites (incl configuring port mirroring).
- Integrate asset data.
- Configure non-intrusive analysis logic.
- Configure alerts and integrate to SIEM/SOC.
- Tune and monitor.

Outcomes/Deliverables

- Selected sites are assessed in real-time for anomalous and malicious activity, including within OT protocols.
- XDR provides the ability to monitor regular workloads, but is now augmented with passive and network-layer detection.
- Integration to SIEM provides more capability of supporting threat hunting and incident response.

* Estimates provided are based only on averages from similar implementations and publicly available information. No vendors have been engaged for cost estimates, and the estimates should be treated as initial estimates only. Detailed costing estimates and resource planning will be part of implementation planning..

Appendix A

Individual OT team current state assessments

OT Generation – Current State Analysis

Secure from Application to Data

Identity & Access
- Authentication
- Authorization
- Federation

Identity Governance & Administration
- Provisioning
- Registration and Enrolment
- Access Governance
- Privileged Access Mgmt
- Directory Services

Trusted & Secure Access

Application Protection
- Secure SDLC
- DevSecOps
- Application Firewall
- API Security Gateway

Network Security
- Secure Network Access
- Intrusion Detection
- Network Segmentation
- Network Traffic Filtering
- Content Filtering & Scanning
- Intrusion Prevention

Endpoint Security
- Configuration Mgmt
- Endpoint Protection
- Mobile Device Mgmt

Data Protection
- Secure Storage & Destruction
- Backup & Recovery
- Data Loss Prevention
- Rights Management
- Data Security Management

Trust Services
- Trusted Time
- PKI Mgmt
- Encryption Services

Identify & Manage Events and Incidents

Security Monitoring
- Log Mgmt
- Audit & Compliance
- Event Correlation & Analytics
- Monitoring & Reporting

Security Incident Management
- Identification
- Investigation Support
- Containment

Legend
- Not Required
- Missing
- Not Yet Mature
- Limited Deployment
- Ready & Reusable

Manage Threats & Vulnerabilities

Threat & Vulnerability Management
- Penetration Testing
- Secure Baseline Mgmt
- Vulnerability Mgmt

Resilience
- Threat Modelling
- Recovery
- Cyber Resilience
- Risk Assessment

OT TDSO – Current State Analysis

Secure from Application to Data

Identity & Access
- Authentication
- Authorization
- Federation

Identity Governance & Administration
- Provisioning
- Registration and Enrolment
- Access Governance
- Privileged Access Mgmt
- Directory Services

Trusted & Secure Access

Application Protection
- Secure SDLC
- DevSecOps
- Application Firewall
- API Security Gateway

Network Security
- Secure Network Access
- Intrusion Detection
- Network Segmentation
- Network Traffic Filtering
- Content Filtering & Scanning
- Intrusion Prevention

Endpoint Security
- Configuration Mgmt
- Endpoint Protection
- Mobile Device Mgmt

Data Protection
- Secure Storage & Destruction
- Backup & Recovery
- Data Loss Prevention
- Rights Management
- Data Security Management

Trust Services
- Trusted Time
- PKI Mgmt
- Encryption Services

Identify & Manage Events and Incidents

Security Monitoring
- Log Mgmt
- Audit & Compliance
- Event Correlation & Analytics
- Monitoring & Reporting

Security Incident Management
- Identification
- Investigation Support
- Containment

Manage Threats & Vulnerabilities

Threat & Vulnerability Management
- Penetration Testing
- Secure Baseline Mgmt
- Vulnerability Mgmt

Resilience
- Threat Modelling
- Recovery
- Cyber Resilience
- Risk Assessment

Legend
- Not Required
- Missing
- Not Yet Mature
- Limited Deployment
- Ready & Reusable

OT Telecoms – Current State Analysis

Secure from Application to Data

Identity & Access
- Authentication
- Authorization
- Federation

Identity Governance & Administration
- Provisioning
- Registration and Enrolment
- Access Governance
- Privileged Access Mgmt
- Directory Services

Trusted & Secure Access

Application Protection
- Secure SDLC
- DevSecOps
- Application Firewall
- API Security Gateway

Network Security
- Secure Network Access
- Intrusion Detection
- Network Segmentation
- Network Traffic Filtering
- Content Filtering & Scanning
- Intrusion Prevention

Endpoint Security
- Configuration Mgmt
- Endpoint Protection
- Mobile Device Mgmt

Data Protection
- Secure Storage & Destruction
- Backup & Recovery
- Data Loss Prevention
- Rights Management
- Data Security Management

Trust Services
- Trusted Time
- PKI Mgmt
- Encryption Services

Identify & Manage Events and Incidents

Security Monitoring
- Log Mgmt
- Audit & Compliance
- Event Correlation & Analytics
- Monitoring & Reporting

Security Incident Management
- Identification
- Investigation Support
- Containment

Legend
- Not Required
- Missing
- Not Yet Mature
- Limited Deployment
- Ready & Reusable

Manage Threats & Vulnerabilities

Threat & Vulnerability Management
- Penetration Testing
- Secure Baseline Mgmt
- Vulnerability Mgmt

Resilience
- Threat Modelling
- Recovery
- Cyber Resilience
- Risk Assessment

OT Integrated Planning – Current State Analysis

Secure from Application to Data

Identity & Access
- Authentication
- Authorization
- Federation

Identity Governance & Administration
- Provisioning
- Registration and Enrolment
- Access Governance
- Privileged Access Mgmt
- Directory Services

Trusted & Secure Access

Application Protection
- Secure SDLC
- DevSecOps
- Application Firewall
- API Security Gateway

Network Security
- Secure Network Access
- Intrusion Detection
- Network Segmentation
- Network Traffic Filtering
- Content Filtering & Scanning
- Intrusion Prevention

Endpoint Security
- Configuration Mgmt
- Endpoint Protection
- Mobile Device Mgmt

Data Protection
- Secure Storage & Destruction
- Backup & Recovery
- Data Loss Prevention
- Rights Management
- Data Security Management

Trust Services
- Trusted Time
- PKI Mgmt
- Encryption Services

Identify & Manage Events and Incidents

Security Monitoring
- Log Mgmt
- Audit & Compliance
- Event Correlation & Analytics
- Monitoring & Reporting

Security Incident Management
- Identification
- Investigation Support
- Containment

Legend
- Not Required
- Missing
- Not Yet Mature
- Limited Deployment
- Ready & Reusable

Manage Threats & Vulnerabilities

Threat & Vulnerability Management
- Penetration Testing
- Secure Baseline Mgmt
- Vulnerability Mgmt

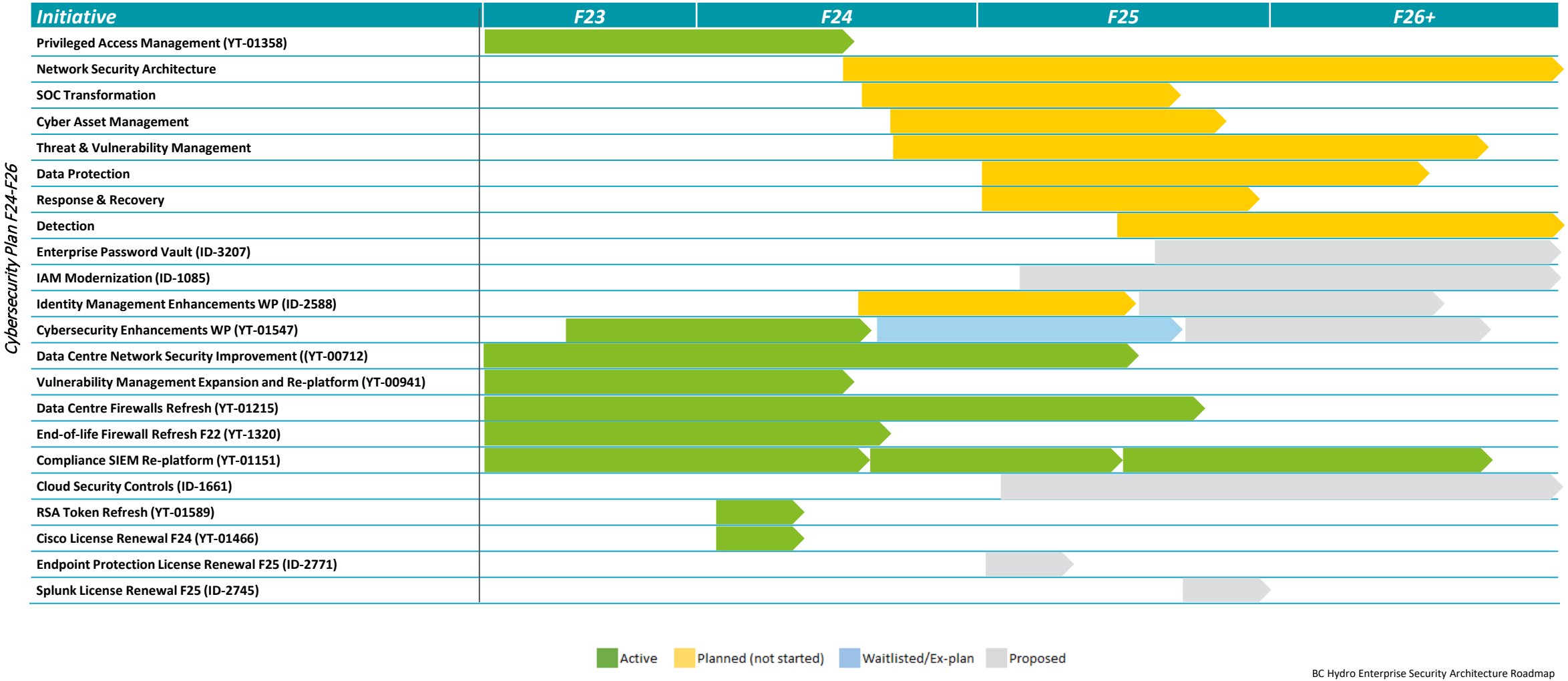
Resilience
- Threat Modelling
- Recovery
- Cyber Resilience
- Risk Assessment

Appendix B
BC Hydro Cybersecurity Plan F24-F26

Cybersecurity Plan F24-F26 Initiatives

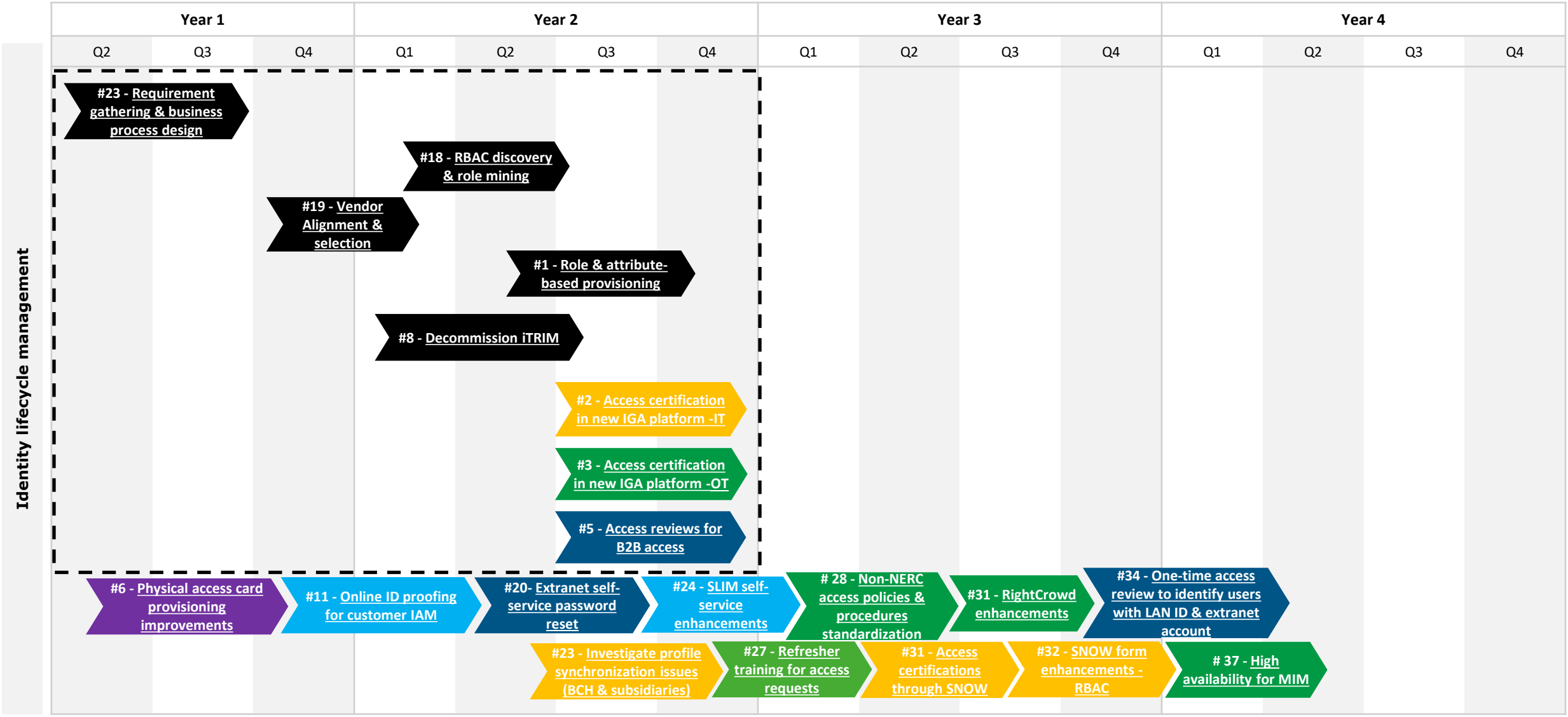
The following figure provides an overview of proposed, planned, waitlisted or active initiatives that will have a direct impact on the ESA Roadmap

The initiatives below should be considered as opportunities to address enterprise security architecture gaps, and as a result should be a focus within the EA team to ensure that the initiatives align with the ESA functional requirements and vision



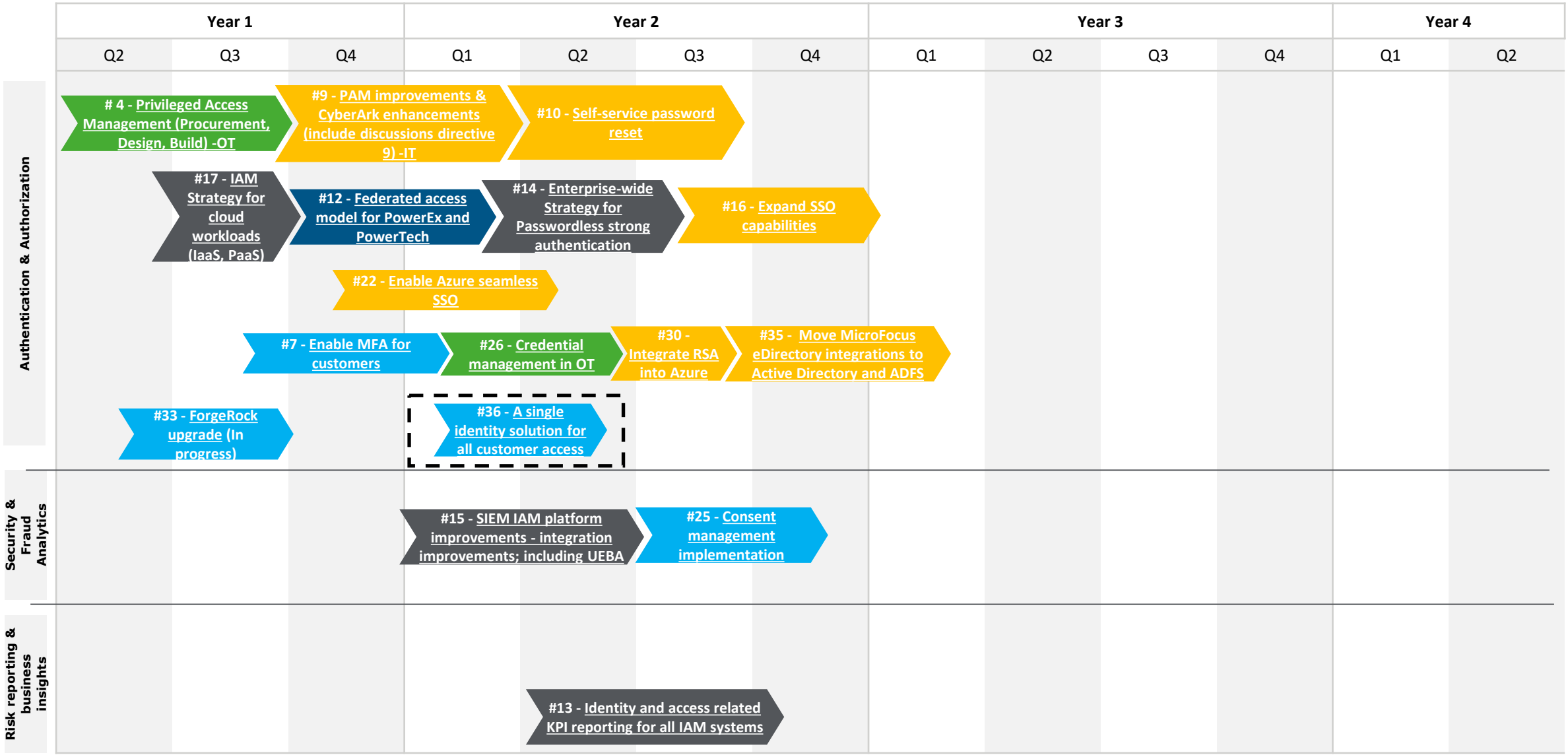
Appendix C
IAM Roadmap

Proposed IAM Roadmap (1/2)



Legend	IT	OT	IT & OT	PACS	Customer	B2B	Dependent Initiatives

Proposed IAM Roadmap (2/2)



Legend	IT	OT	IT & OT	B2B	Customer	PACS	All	Dependent on vendor alignment & selection

Appendix D
Roadmap Item Technology Landscape Map

Candidate Solution Offering Mapping

The chart below provides a mapping of solution offering market candidates against the identified roadmap items:

Functional Pillar	Roadmap Item	Candidate Solution Landscape
Identity & Access	IT. ID.3. Transition from on-prem Active Directory to Entra/Azure AD for candidate applications to benefit from modern auth features.	Azure AD (incl. Directory Services and Conditional Access), Azure PIM, Azure MFA,
	IT. ID.2. Federate external identities for key subsidiaries (PowerTech and PowerEx)	Okta, Microsoft/AAD, PingIdentity
	OT. ID.1. Replace use of local accounts for OT networking and server systems by implementing an OT Active Directory and leveraging AD, LDAPS, RADIUS and TACACS authentication services	MS Active Directory (on-premise)
Identity Governance and Administration	IT. ID.1. Complete PAM implementation and expand use on a risk-based approach	Azure PIM, CyberArk, BeyondTrust
	IT. ID.4. Implement Identity Governance and Administration solution stack	ForgeRock, Saviynt, Sailpoint, PingIdentity, Azure PIM, Azure Identity Protection, CyberArk
	OT. IG.1. Implement a PAM instance for OT EMS and plant FWs to manage privileged accounts for compliance. OT.ID.2. Implement password vaulting and management solution for field use privileged passwords. OT. ID.2. Implement automation of provisioning and deprovisioning leveraging IGA solution selected for IT, replacing use of SureSight.	CyberArk, BeyondTrust
Endpoint Security	IT. ES.1. Integrate Secure Configuration Baselines into IT Asset Management toolsets	ServiceNOW
	OT.ES.1. Pilot software bill of materials management automation for low impact sites	Cybellum, Fortress
	OT.ES.3. Implement technology to identify vulnerabilities in OT system configurations (beyond TDSO Tripwire) and integrate to asset database technology	Claroty, Tenable OT, TripWire, Verve
	OT.ES.2. Implement more advanced endpoint protection EPP/EDR for suitable OT workstations (Control Centre)	Crowdstrike, Claroty
Network Security	IT. NS.3. Implement network micro-segmentation (leveraging investments in software defined networking and ensure extension to Cloud)	Guardicore, Illumio
	IT. NS.1. Pilot implementation of Zero Trust Network Access services	Zscaler, Citrix, MS Entra Private Access
	IT. NS.2. Implement Zero Trust Network Access Services	Zscaler, Citrix, MS Entra Private Access
	OT.NS.2. Conduct a study of intermediated access gateway product for OT	Claroty, BeyondTrust
	OT.NS.1. Implement centralized logging for all OT firewalls to SIEM for visibility.	Splunk
	OT.NS.3. Implement jumphosts for all access to OT assets.	VMWare Horizon, Citrix Private Access
	OT.NS.4. Enable advanced firewall capabilities, and integrate into central monitoring	Palo Alto, Check Point
Application Security	IT. AS.2. Implement integrated and automated security testing of application and platform security configuration (DevSecOps)	Aqua, Sonar, GitHub Security, VeraCode, ThreadFix, Microsoft Defender for Containers
	IT. AS.1. Implement/enable API Security Gateway feature of MuleSoft for secure API exposure	Mulesoft, F5, Azure Front Door, Azure API Management, Azure Application Gateway, Azure Web Application Firewall
Threat and Vulnerability Management	IT. TM.1. Implement vulnerability scanning of applications and application source code	Tenable.io, Qualys
	IT. TM.2. Implement/enable threat modelling toolset	Atomic Red. Caldera, Infection Monkey
Security Monitoring	IT. SM.2. Extend detection and response to integrate network, identity, endpoint, cloud and analytics (journey to XDR)	Microsoft Sentinel, Microsoft Defender for Cloud, Splunk, Microsoft Defender for Identity
	IT. SM.3. Implement advanced threat detection technologies (Canary)	Palo Alto XIM, ExtraHop, Vectra
	IT. SM.1. Implement central SIEM dashboard that monitors IT and OT	Tenable
	OT. SM.1. Architect and implement a central SIEM that is able to ingest OT logs. Once completed, integrate OT logs into central SIEM to allow CSO proactive monitoring	Sentinel, Splunk
	OT. SM.2. Implement passive advanced OT (e.g. SCADA) threat detection based on analysis of network traffic.	Tenable.OT, Armis, Claroty
Security Incident Management	IT. IM.1. Architect to recover all critical business functions within business-defined thresholds	Azure Backup, Azure Confidential Computing, Key Vault Managed HSM, Azure Site Recovery
	IT. IM.2. Implement Security Orchestration to automate threat containment across both on-remise and cloud workloads	Palo Alto XIM, Extrahop, Vectra

Appendix E
Roadmap Recommended PoC Approach

Recommended Evaluation, Selection and Proof of Concept (PoC) Approach

The diagram below represents the recommended approach for further planning, design, evaluation and selection of solutions within the roadmap, and is commonly adopted by vendors to conduct PoCs.

Vendor Benchmarking

- Vendor identification
- Definition of objective & functionalities to be evaluated
- Vendor contact for PoC
- Vendor selection for PoC

Scope definition

- Scope definition for the PoC execution
- Deployment activities definition
- Economic estimation for licensing based on the overall scope

PoC Implementation

- Architecture design (i.e., environment, integration with other tools, etc.)
- Initial configuration
- Functionality testing
- Demo with key personnel

POC Results

- Evaluation of results
- Reports:
  - Executive report
  - Technical report
- Deployment plan
- Economic estimation of the implementation phase

Deliverables

- Theorical benchmark report that includes the coverage for the requirements defined.

- Use Cases definition for PoC
- Economic estimation

- Technical details of the tests performed

- Technical report of the tests
- Executive report
- Deployment plan
- Adjustment to economic estimate