BCNET

Shared IT Services for Higher Education & Research

Conference 2018

BCNET Shared CISO

Wency Lum, Farooq Naiyer and Ivor MacKay

Speakers:

Wency Lum	CIO University of Victoria, Chair of the Cybersecurity and Identity Management Services Committee
Farooq Naiyer	Shared CISO at ORION, Ontario's Research and Education Network Organization.
Ivor MacKay	Manager, Information Technology

Agenda

- CISO
- Executive Summary
- Purpose of the shared CISO
- Expectations
  - Shared CISO
  - BC Post Secondary Institutions
- The Numbers
- ORION's Shared CISO
- Q & A

A Chief Information Security Officer

- A CISO (Chief Information Security Officer) is responsible for developing and implementing security programs designated to protect enterprise communications, systems and assets from both internal and external threats.

  Source: http://searchsecurity.techtarget.com/definition/CISO-chief-information-security-officer

Executive Summary - Purpose of the shared CISO

Executive Summary – Shared CISO

Cybersecurity and Identity Management Services Committee (CSIMSC) is proposing a Shared Chief Information Security Officer (CISO) to:

- Assist 5-8 members
- 2 year commitment

Responsibilities include:

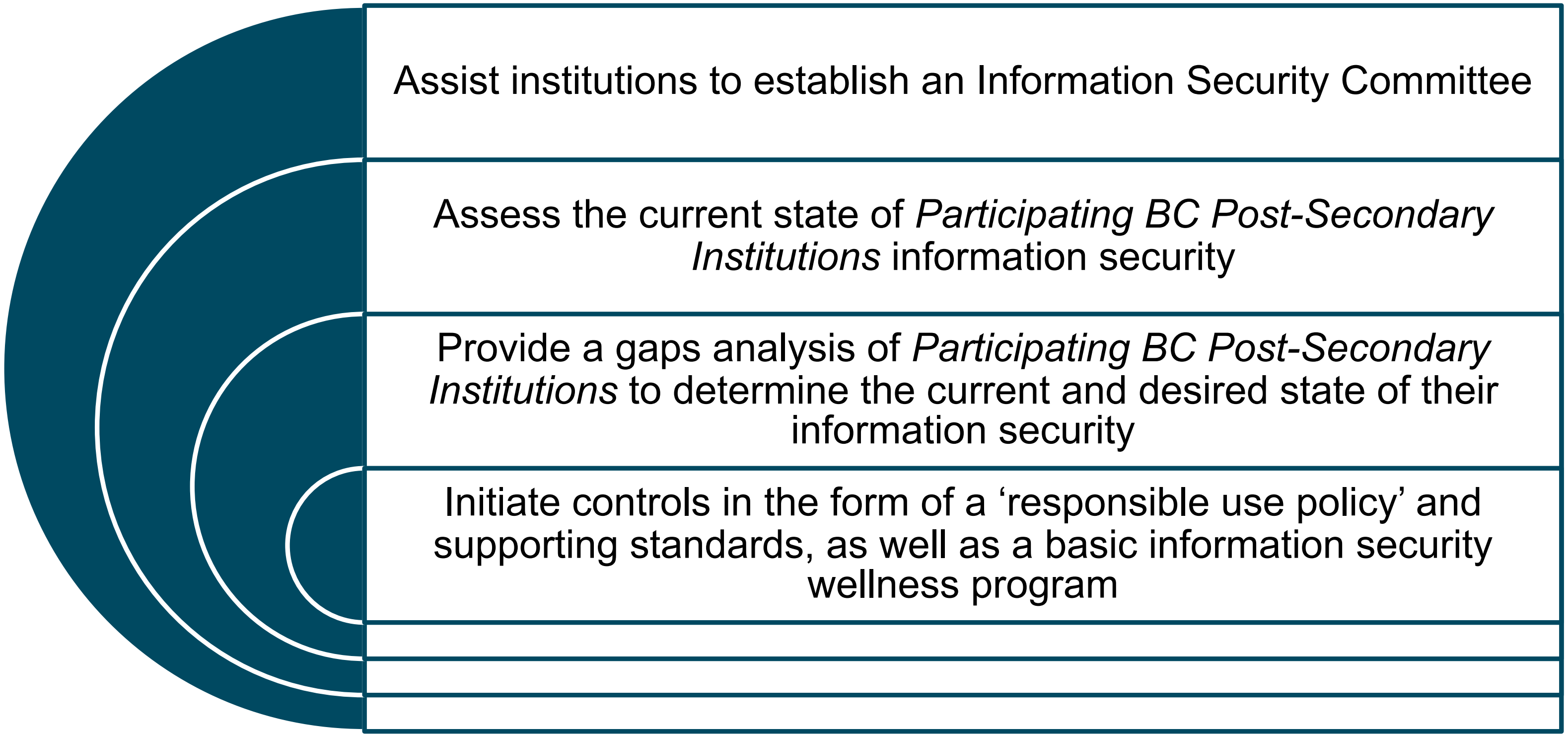
- Recommending guidelines and best practices to ensure a secure IT environment
- Identifying gaps, including information assets
- Recommending policies, processes and technologies to address those gaps
- Initiating a strategic plan and incidence response program.

Costing will be based on the core service cost recovery model approved by the BCNET board last year (discussed on a later slide)

The Shared CISO Role

The Shared CISO Objectives

In the First Year



Assist institutions to establish an Information Security Committee

Assess the current state of *Participating BC Post-Secondary Institutions* information security

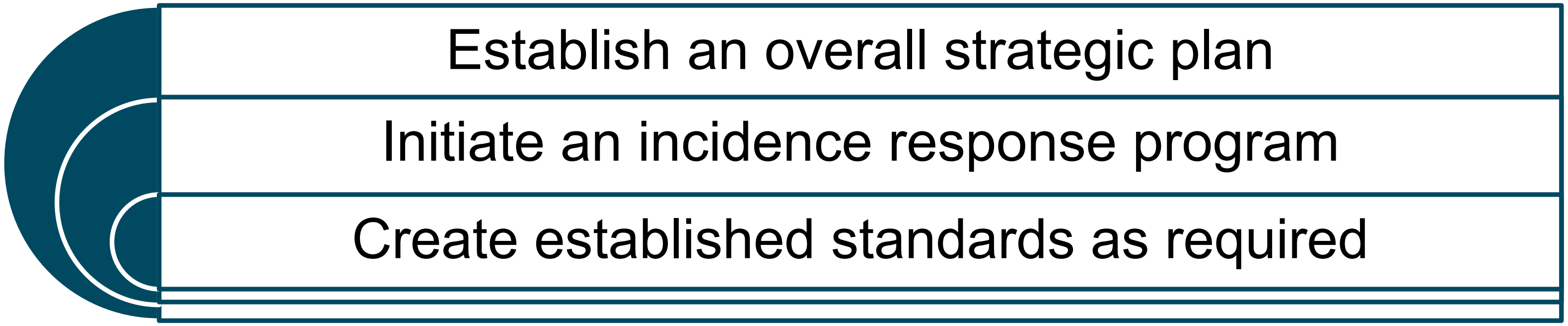
Provide a gaps analysis of *Participating BC Post-Secondary Institutions* to determine the current and desired state of their information security

Initiate controls in the form of a ‘responsible use policy’ and supporting standards, as well as a basic information security wellness program

The Shared CISO Role

The Shared CISO Objectives

In the Second Year,



Establish an overall strategic plan

Initiate an incidence response program

Create established standards as required

It is expected that each *Participating BC PSI* will assign a dedicated resource to their information security program

The Shared CISO Role

The Shared CISO Objectives cont'd

2. Deliver:
   a. A threat and risk assessment framework for *Participating BC Post-Secondary Institutions*
   b. A step-by-step action plan for *Participating BC Post-Secondary Institutions*

3. Recommend actions from the threat and risk assessment framework based on priorities identified by *Participating BC Post-Secondary Institutions*

The Shared CISO Role

The Shared CISO Objectives cont'd

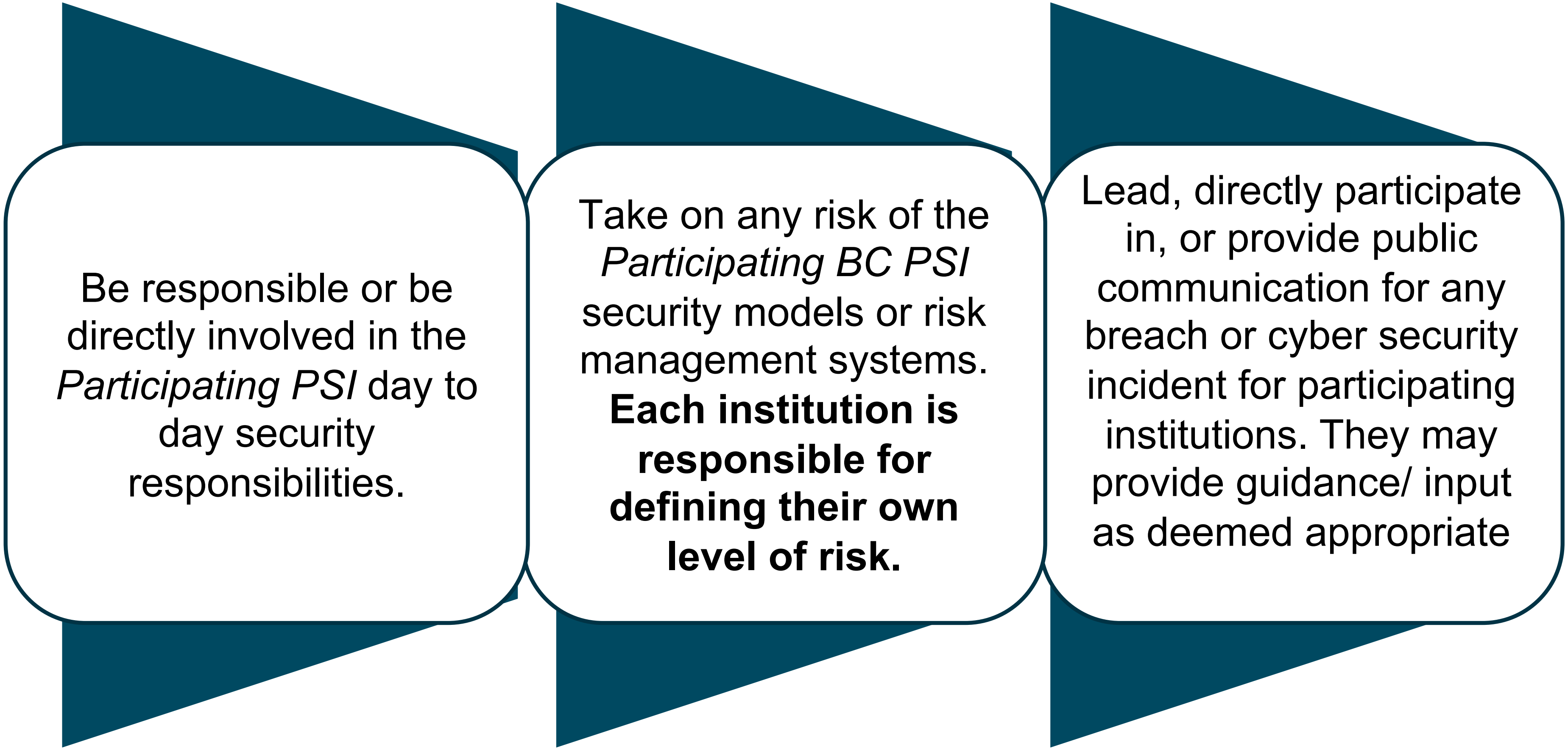
Evaluation of the Shared CISO program will be done by:

- Using feedback from the *Participating BC Post-Secondary Institutions*
- Using feedback received from the Cyber Security and Identity Management Committee (CSIMSC), which will be responsible for reviewing the performance and effectiveness of the program
- Through Shared CISO participation, reporting to the CSIMSC committee
- Using feedback from the BCNET Account Managers of the *Participating BC Post-Secondary Institutions*

The program will be reviewed on an annual basis.

The Shared CISO Role

The Shared CISO will not:



Be responsible or be directly involved in the *Participating PSI* day to day security responsibilities.

Take on any risk of the *Participating BC PSI* security models or risk management systems. **Each institution is responsible for defining their own level of risk.**

Lead, directly participate in, or provide public communication for any breach or cyber security incident for participating institutions. They may provide guidance/ input as deemed appropriate

Expectation of BC Post-Secondary Institutions

- Each *Participating BC Post-Secondary Institution* will pay an ***annual fee***
- *Participating BC Post-Secondary Institutions* will commit on a 2-year basis, renewable every 2nd year
- The first 2-year term will be a trial period with explicit objectives. There is no termination process for the first two years of this service
- After the first 2-year term, any termination of agreement by any of the *Participating BC Post-Secondary Institutions* will require **60 days notice***.* *BCNET* will not refund the termination as the fee would be charge on an annual basis
- The entire program terminates if there are less than the minimum number of five institutions required
- In the case of termination of this MOU, *BCNET* will not assume any financial responsibilities for the CISO, and the Shared CISO Program may be concluded

The Numbers

The Shared CISO Cost:

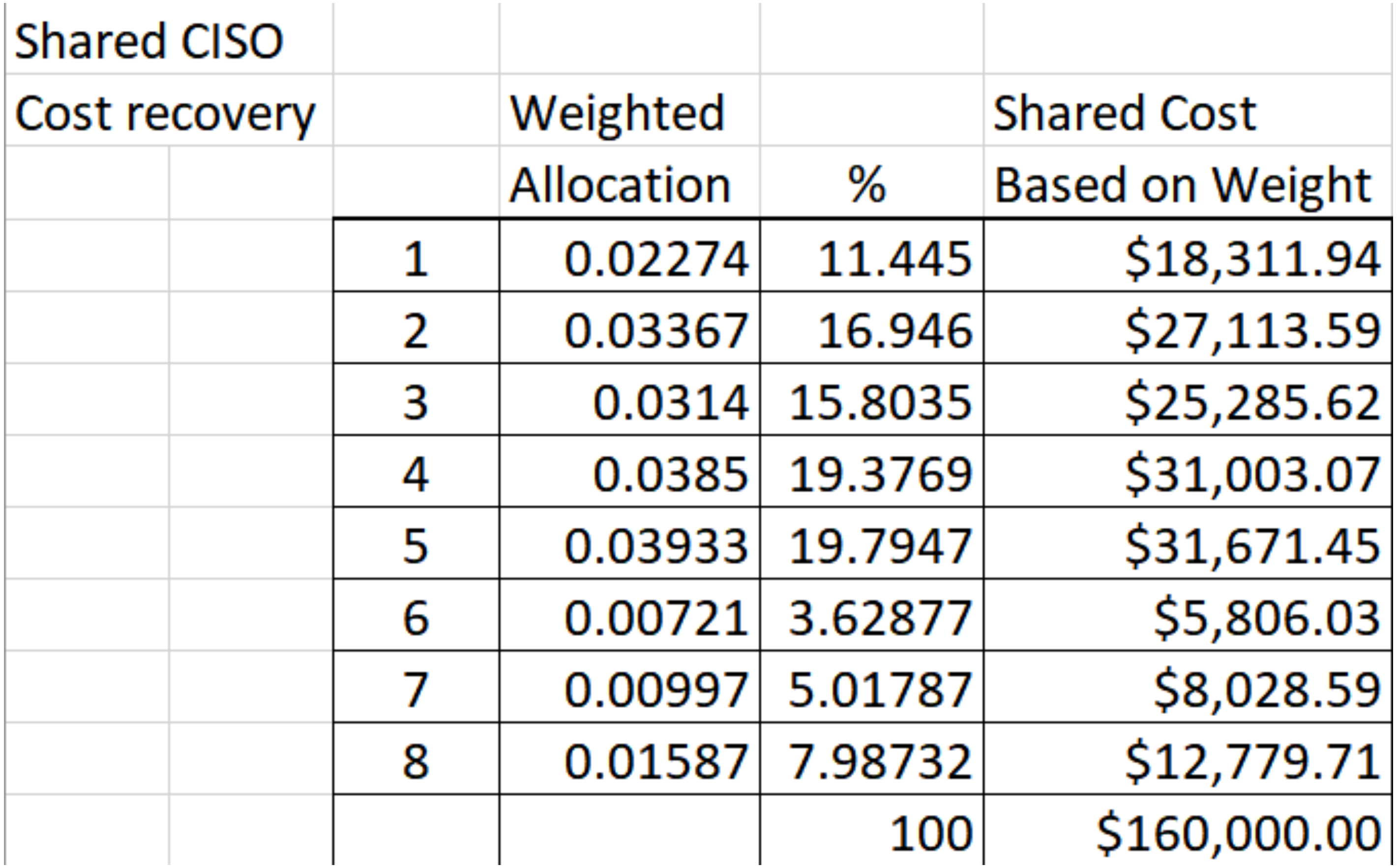
Total cost of Shared CISO would be $160,000. This includes travel and benefits

A breakdown of hours would be roughly 1 day/week per institution if there are 5 *Participating BC Post-Secondary Institutions;* 2/3 of a day/week per institution if there are 8 *Participating BC Post-Secondary* Institutions, and based on a 7-hour day.

DEVICES
PVS
DISCOVER VULNERABILITIES IN MOBILE DEVICES AND VIRTUAL INFRASTRUCTURE
IDENTIFY SENSITIVE DATA IN MOTION
UNCOVER SUSPICIOUS CONNECTIONS

The Numbers

The Shared CISO Cost:



Shared CISO				
Cost recovery		Weighted		Shared Cost
		Allocation	%	Based on Weight
	1	0.02274	11.445	$18,311.94
	2	0.03367	16.946	$27,113.59
	3	0.0314	15.8035	$25,285.62
	4	0.0385	19.3769	$31,003.07
	5	0.03933	19.7947	$31,671.45
	6	0.00721	3.62877	$5,806.03
	7	0.00997	5.01787	$8,028.59
	8	0.01587	7.98732	$12,779.71
			100	$160,000.00

BCNET

Shared IT Services for Higher Education & Research

Conference 2018

Welcome Farooq Naiyer

Shared CISO Project at ORION

ORION Empowering Innovation

Why shared CISO for Ontario's Higher Ed?

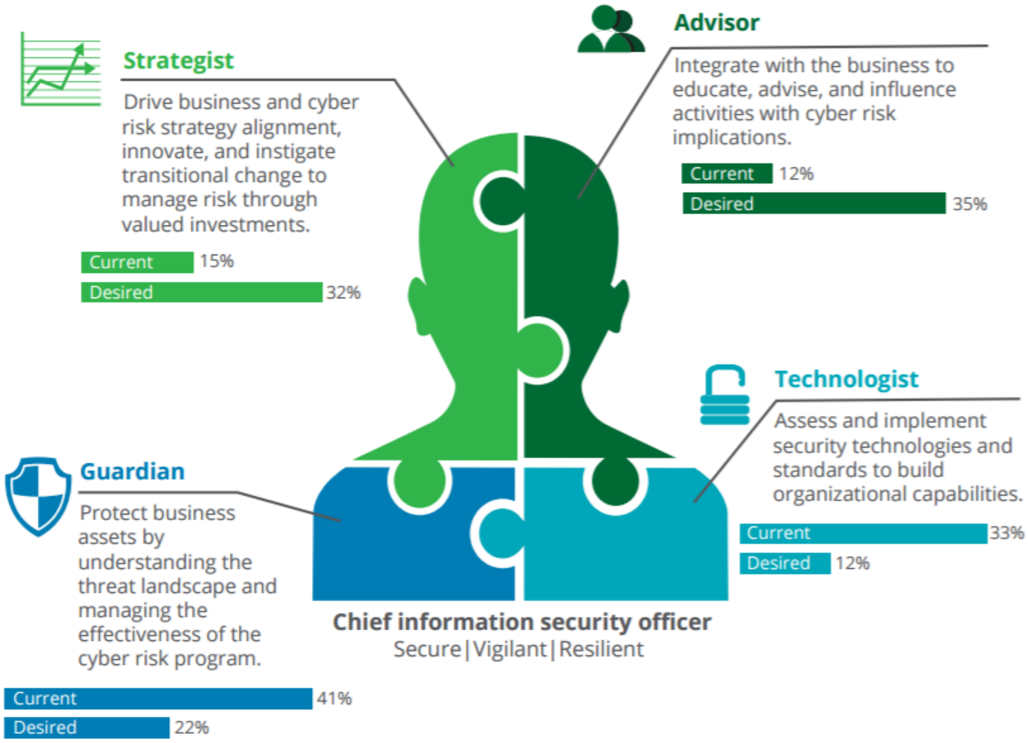
- IT budgets stretched; Limited funding
- Cyber threats evolving faster than ability to keep up
- Lacking time and expertise for mitigation framework for cyber security risks
- Shared security services optimize costs and increase efficiency

Ontario’s G8 Institutions

ORION
Empowering Innovation
WILFRID LAURIER UNIVERSITY
LAURIER
Inspiring Lives.
Brock University
OCAD UNIVERSITY
O C
A D
U
Queen's UNIVERSITY
LaurentianUniversity
UniversitéLaurentienne
St. Lawrence College
HUMBER
nc
Niagara College Canada
APPLIED DREAMS.

Four Faces of the CISO Role

Figure 2. The four faces of the CISO



Strategist

Drive business and cyber risk strategy alignment, innovate, and instigate transitional change to manage risk through valued investments.

Advisor

Integrate with the business to educate, advise, and influence activities with cyber risk implications.

Technologist

Assess and implement security technologies and standards to build organizational capabilities.

Guardian

Protect business assets by understanding the threat landscape and managing the effectiveness of the cyber risk program.

Chief information security officer

Secure|Vigilant|Resilient

Source: Research from Deloitte's CISO Transition Labs.

Graphic: Deloitte University Press | DUPress.com

Overview of the shared CISO role

- Two-year shared CISO initiative
- Develop a governance model
- Develop and deliver federated cyber security/information security framework
  - G8
  - ORION
- Deliver threat and risk assessment framework and action plan
- Propose and develop shared security services for the G8

Governance Structure: Steering Committee

- One from each institution, plus two from ORION
- Provides guidance on the proposed integrated security framework, recommend new initiatives and prioritization, and assist in their development
- Provides input and recommendations in identifying practical strategies and solutions for ensuring the security and privacy of data

The Opportunity

- Information sharing and collaboration
- Identification of common issues and challenges
- Understanding of risks and implications
- Creates a commitment for change
- Establish/Improve security governance
- Develop methodologies to tackle shared problems
- Guidance on building a security framework, leveraging provided security standards

The Challenges

- Managing different levels of expectations and understanding
- Complex topic
- Varying levels of information security maturity
- Resource availability, especially for working-groups
- Competing and conflicting deadlines and priorities
- Potential for scope creep
- Project management

Year One Achievements

- Security Gap Assessment
- Three project streams based on the security assessment and G8 priorities
- Threat Risk Assessment Workshop (working group)
- CND workshop (working group)
- Workshop on security governance (for ISSC)
- Initial input for technical requirements for a shared SIEM
- Workshop on PCI-DSS compliance

Plans for Year 2

- Workshops for the Steering Committee and working group aligned with the proposed roadmap and security baseline
- Develop a shared security framework
- Conduct POC (proof of concept) for potential shared security services

Q & A