Defensible Security "DefSec" 101

Security Day

November 2017

Information Security Branch

Paul Falohun Senior Security Analyst
Dan Lathigee Senior Project Manager

BRITISH COLUMBIA

OCIO
Office of the Chief Information Officer

Content

Meet the team

Paul Falohun, B.Engr(Hon.), MBA

- Senior Security Analyst, Information Security Branch, OCIO
- Assisting with the implementation of DefSec
- Experience in consulting (worked with 2 big 4 professional services firm)
- Bachelor's Degree in Computer and Network Systems Engineering
- Master's in Business Administration
- Certificates:
  - COBIT 5
  - ITIL-F
  - CSX-F
  - CISM
  - Among others…
- Languages: English and Russian
- On the board of ISACA Victoria Local Chapter

Meet the team –Continued

Dan Lathigee

- Senior Project Manager, Information Security Branch, OCIO
- Currently managing the implementation of DefSec
- 23 years of leadership experience
- 16 years of IT management experience, including assisting businesses in identifying and managing their security posture
- Diplomas (with honours) in IT and Network Management, with a specialization in network security and design
- Certificates:
  - Business Analysis
  - IT Project Management
  - COBIT 5
  - ITIL
  - VMware Certified Professional
  - Microsoft Certified Systems Engineer
  - Among others…

Data Breach Statistics

EVERY DAY

5,146,763

Records

EVERY HOUR

214,448

Records

EVERY MINUTE

3,574

Records

EVERY SECOND

60

Records

Source: http://breachlevelindex.com/

Defensible Security helps organizations know what they need to be doing at a minimum to achieve a security posture that is defensible. It also helps them understand how to do it in a very iterative, pragmatic way.

-Gary Perkins
Chief Information Security Officer (CISO)
Executive Director, Information Security Branch
Government of British Columbia

What is DefSec?

Vision: To raise the water level of security across the public sector

DefSec as an Initiative:

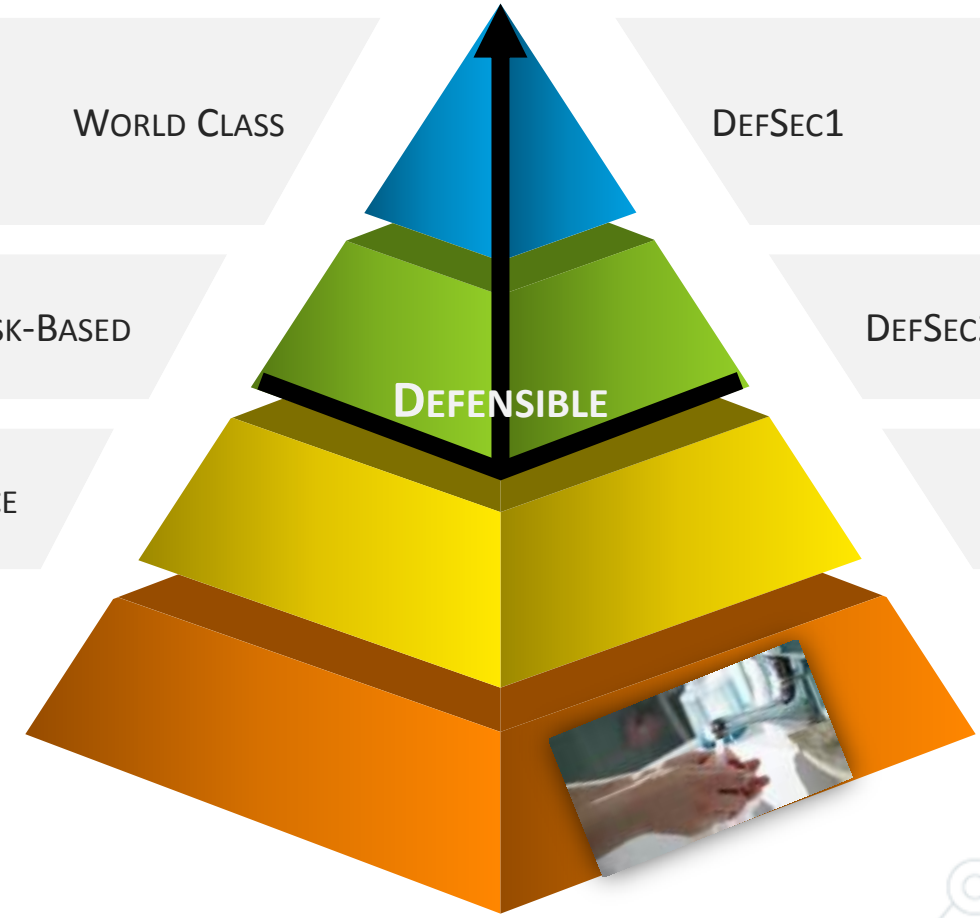
- A smoothie of international standards and best practices (ISO, NIST..)
- Digestible to the general public
- Improve security posture from hygiene to world-class

DefSec as a Project:

Assess and support core government, health authorities, crown corporations, municipalities, school districts, and advanced education

Phase 1: Core Government
Phase 2: Broader Public Sector & Crown Corps.
Phase 3: Municipalities and Education

DefSec for Public Sector Organizations



DefSec Manual

Defensible Security for Public Sector Organizations

Cybersecurity has never been as imperative as it is today. Most organizations have failed to invest at a rate that has sustained previously achieved capability levels. Others have never reached a level of security maturity adequate to mitigate risks to an acceptable level. Organizations must target a level at or above risk-based security. It is critical to ensure hygiene and compliance level controls are in effect. Public sector organizations have a responsibility to apply appropriate safeguards and maintain a defensible level of security.

Defensible security is at or above hygiene + compliance:

The following are pre-requisites to success for security:

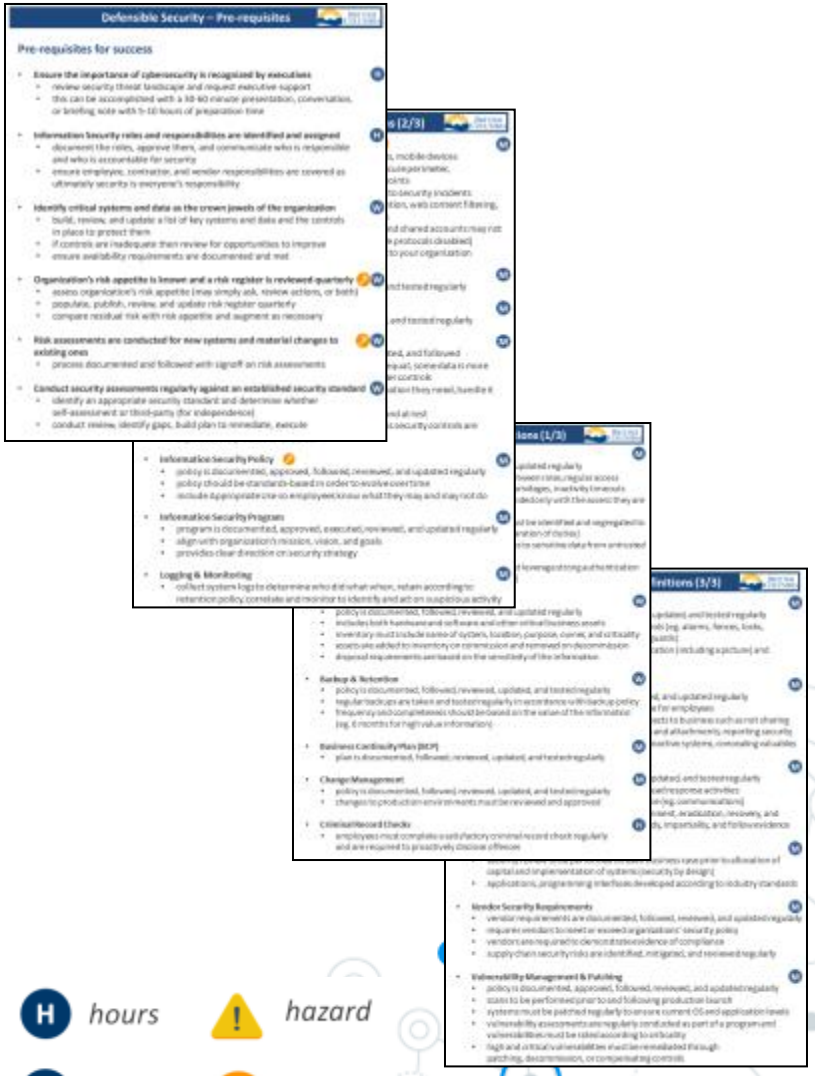
- ❑ Ensure the importance of cybersecurity is recognized by executives
- ❑ Information Security roles and responsibilities are identified and assigned
- ❑ Identify critical systems and data as the crown jewels of the organization
- ❑ Organization's risk appetite is known and a risk register is reviewed quarterly
- ❑ Risk assessments are conducted for new systems and material changes to existing ones
- ❑ Conduct security assessments regularly against an established security standard

Organizations must have documented, followed, reviewed, updated, and tested:

- ❑ Asset Management & Disposal
- ❑ Change Management
- ❑ Incident Management
- ❑ Business Continuity Plan (BCP)
- ❑ Disaster Recovery Plan (DRP)
- ❑ Backup & Retention
- ❑ Logging & Monitoring
- ❑ Physical Security & Visible Identification
- ❑ Security Incident Response
- ❑ Information Security Policy
- ❑ Information Security Program
- ❑ Information Security Classification
- ❑ Criminal Record Checks
- ❑ Security Awareness Program & Course
- ❑ Vendor Security Requirements

The following practices must be in effect:

- ❑ Access Control
- ❑ Defence in Depth for Endpoints and Networks
- ❑ Security Governance
- ❑ Vulnerability Management & Patching



"Organizations will continue to be at risk for cyber-attacks and breaches, but the solution is not rocket science; it's basic cyber hygiene like patching and scanning"

-Tony Sager
Senior V.P. and Chief Evangelist for the Center for Internet Security (CIS) Controls.

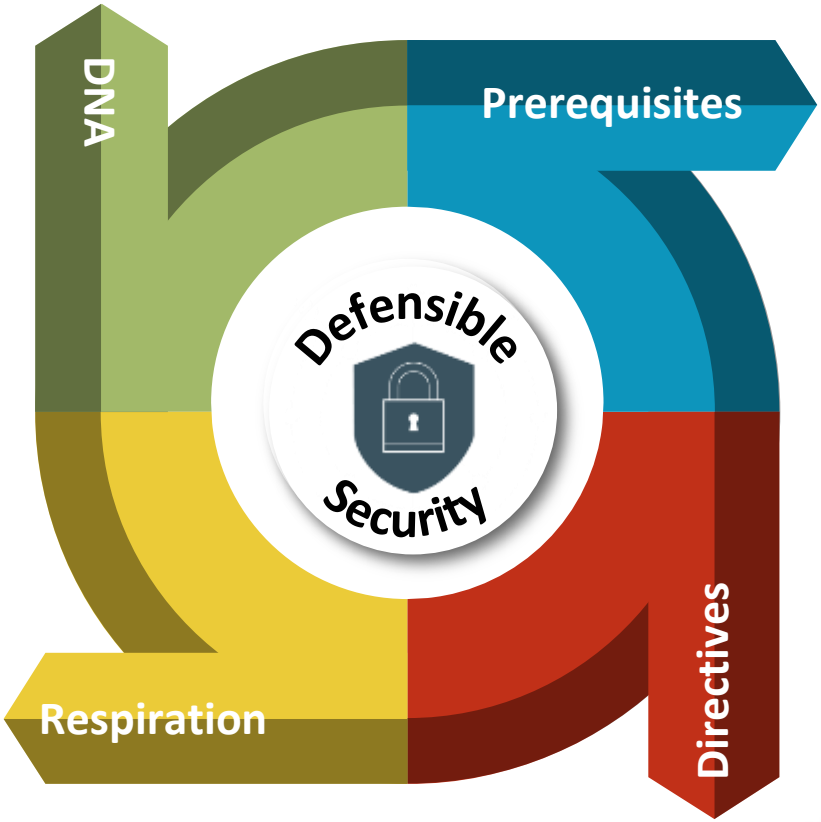
DefSec Triage

Security Embedding (DNA) Controls

Info Security Program
Info Security Classification
Security Awareness
Security Governance

Security Respiratory Controls

Backup & Retention
Logging & Monitoring
Physical Security & Visible ID
Criminal Record Checks
Vendor Security Requirements
Access Control
"DiD" for Endpoints & Networks
VM & Patching



Security Prerequisites

Executive Support
Roles & Responsibilities
Crown Jewels
Risk Appetite & Register
Risk Assessment
Security Assessment

Security Directives

Asset Management & Disposal
Change Management
Incident Management
Business Continuity Plan (BCP)
Disaster Recovery Plan (DRP)
Security Incident Response
Info Security Policy

"Covering the organization end-to-end"

DefSec -Security Prerequisites

Control Element	High-level Objective
Executive Support	• Presentation to Executive
Roles & Responsibilities	• Matrix documenting key security roles and who occupies them
Crown Jewels	• List of key systems, data it holds, and what security controls exist
Risk Appetite & Register	• Org risks are documented • Risk appetite is defined • Annual signoff on risk register
Risk Assessment	• Process is documented, followed by signoff on risk assessments
Security Assessment	• Appropriate security standard • Determine whether self-assessment or third-party

DefSec –Security Directives

Control Element	High-level Objective
Asset Management & Disposal	• Asset management policy and asset inventory
Change Management	• Change Management Policy, schedule reviewed annually, change approval
Incident Management	• Incident Management Policy • Schedule reviewed annually
Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP)	• Plans are in place, tested, and reviewed annually
Security Incident Response	• Play/run books should be in place, tested, and reviewed annually • SIRT is in place
Information Security Policy	• Information Security Policy & Appropriate Use • Schedule review annually

DefSec Security Embedding (DNA) Controls

Control Element	High-level Objective
Information Security Program	• Program is documented, approved, executed, reviewed, and updated regularly • Align with organization's mission, vision, and goals • Provides clear direction on security strategy
Information Security Classification	• Information Classification Standard • Employees are aware of what to do and how to do it; systems may be needed to support
Security Awareness Program & Course	• Security awareness plan (and promotional materials) • Security awareness course • Schedule review annually
Security Governance	• Guidance on security requirements for projects • Insert security review/signoff in IM/IT capital investment process • Secure development standard and encryption


Hey, I can assist you with DefSec?
No thanks!
We are too busy

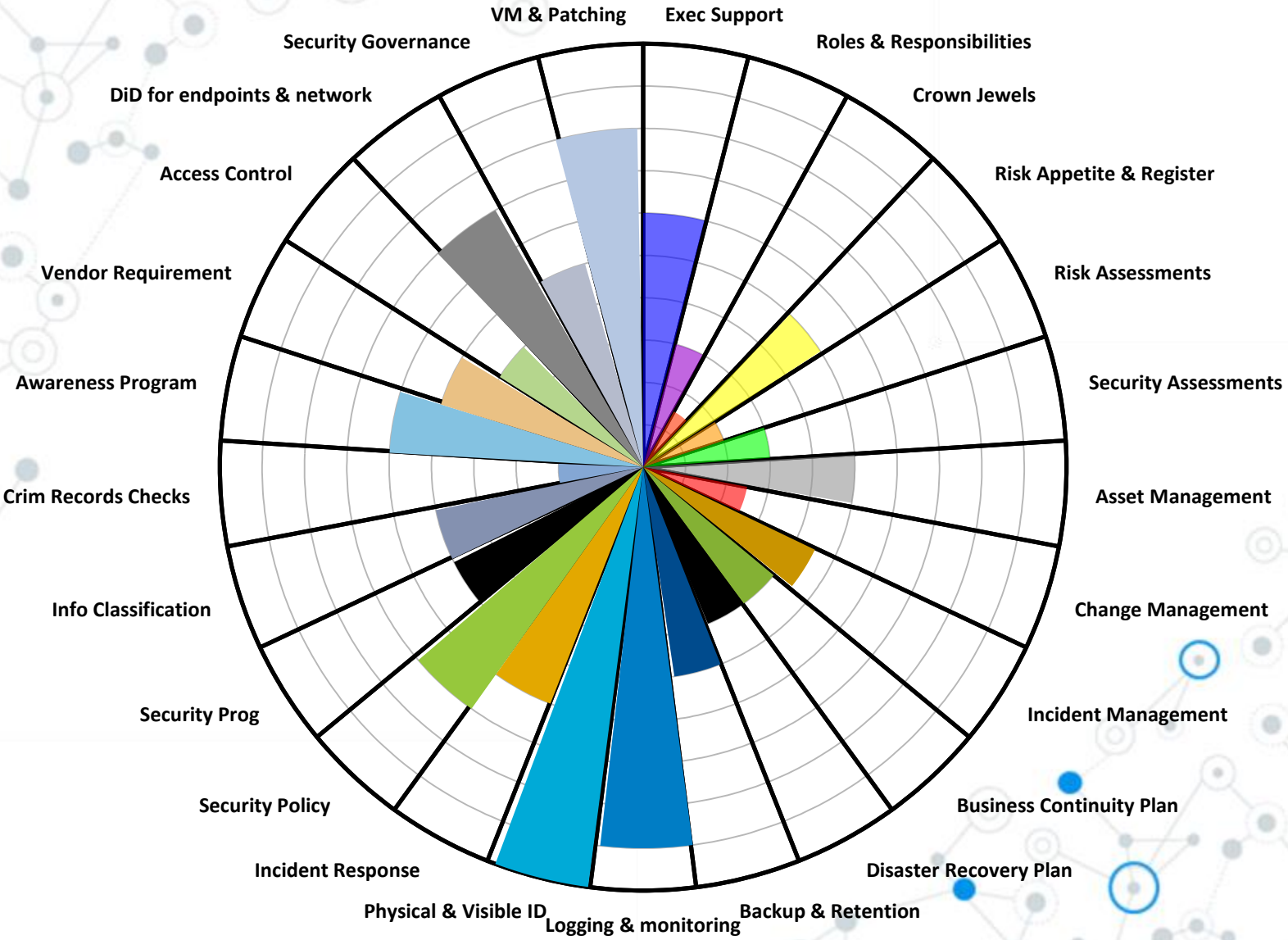
DefSec –Security Respiratory Controls

Control Element	High-level Objective
Backup & Retention	• Backup Policy & Retention Schedule • Schedule test and review annually
Logging & Monitoring	• Configure systems to log system activity • Set up correlation and alerts response
Physical Security & Visible Identification	• Facilities must benefit from adequate physical controls • Staff and visitors must wear visible identification
Criminal Record Checks	• Process to conduct criminal record checks on employees
Vendor Security Requirements	• Vendor security schedule to be included in contracts, schedule should be reviewed annually

DefSec –Security Respiratory Controls (cont'd)

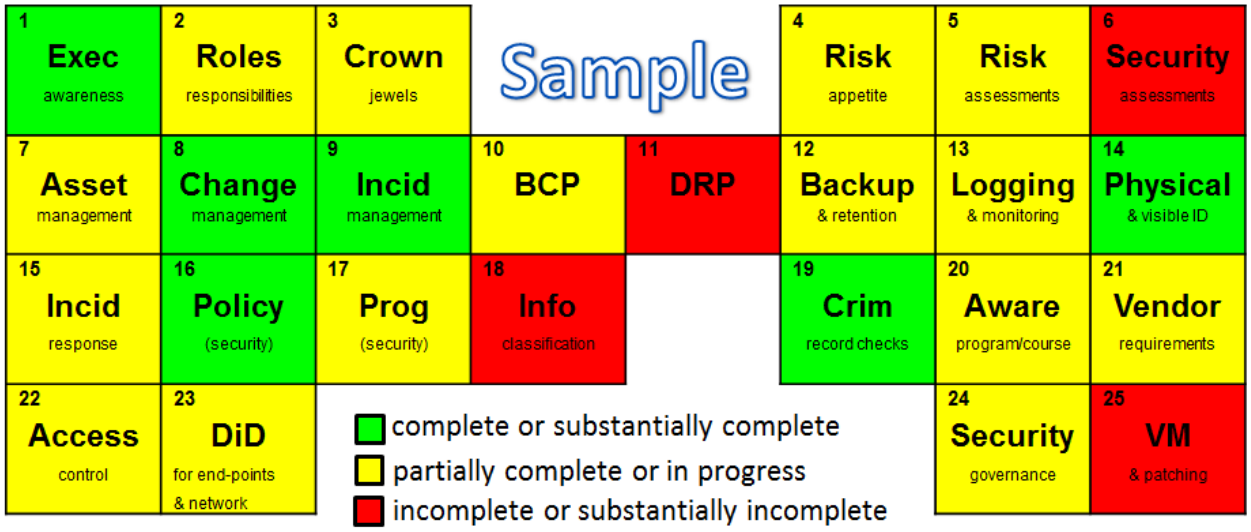
Control Element	High-level Objective
Access Control	• Role based Access Control list • Quarterly access reviews
Defence in Depth for Endpoints and Networks	• Firewall, intrusion prevention, web content filtering, email content filtering, and next generation anti-malware on network and endpoints • Configure devices according to best practices • Multifactor Authentication (MFA) • VPN
Vulnerability Management & Patching	• VM program to identify, notify, follow up, and report on high/critical vulnerabilities; schedule review annually • Patching policy • Recurring vulnerability scans

DefSec Effort Chart

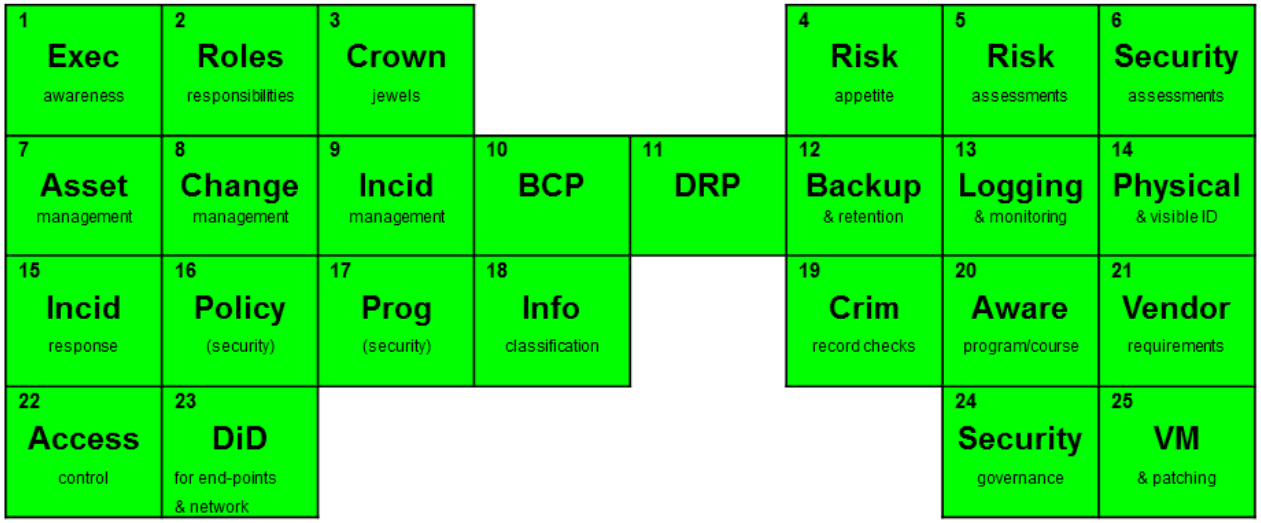


DefSec Dashboard

Present State:



Future State:



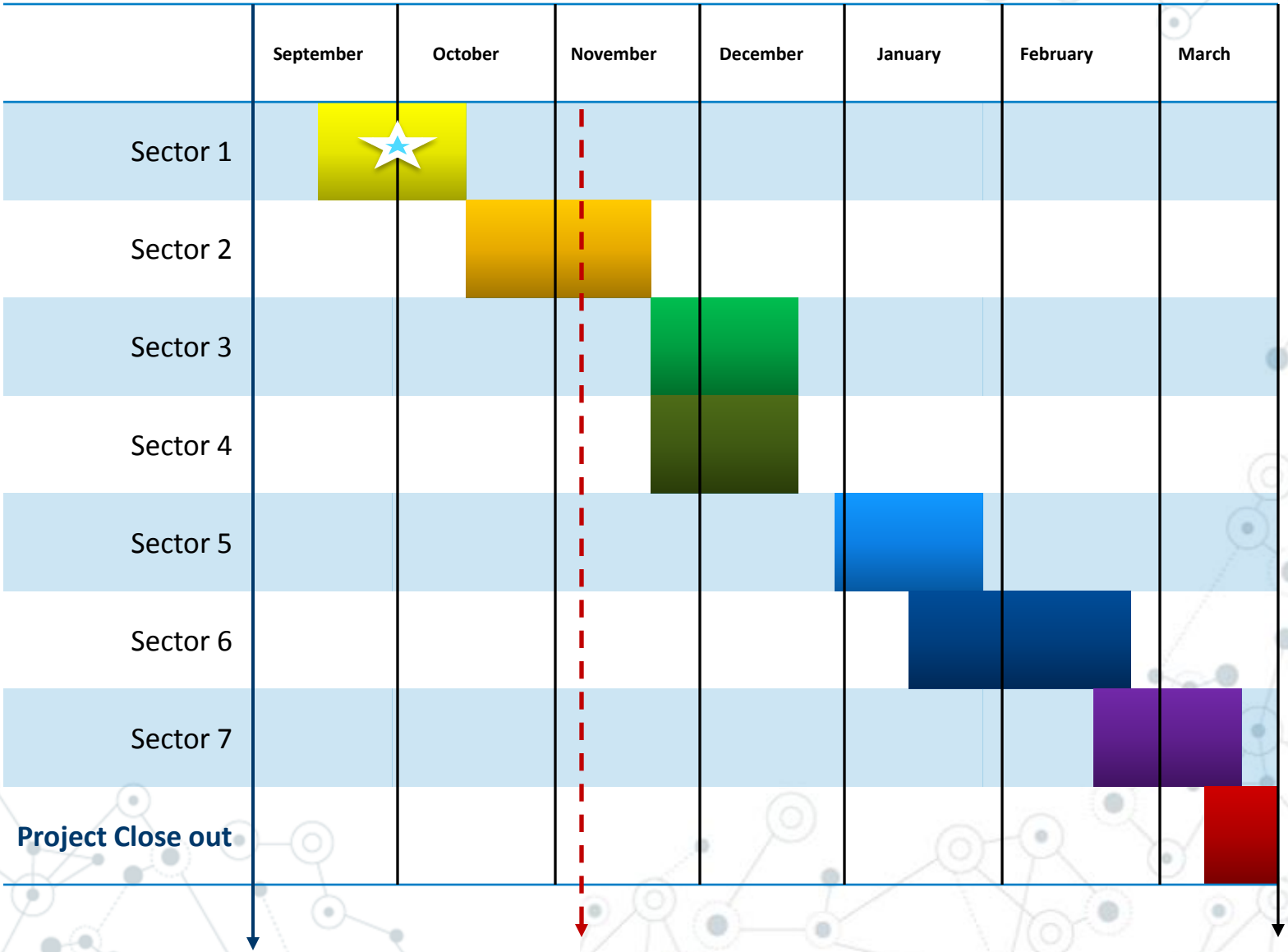
Cybersecurity is a complex issue that requires industry and government to partner in finding innovative ways to stay ahead of threats.

-Bill O'Hern
Senior Vice President and Chief Security Officer, AT&T

DefSec Project Plan (Phase 1)

- Project duration
  - 7 months (Sept – Mar)
- Engagement structure
  - 4-5 weeks per engagement
  - Sector-by-sector approach
  - Kick-off & Closeout meeting
  - Continuous assistance and follow-up
- Identifying control element champions
- Knowledge sharing process

Agile Engagement Schedule



Engagement Structure

Kick-off meeting

This is an in-person, face-to-face meeting with the MISO(s) and Director(s). We begin with a brief introduction on DefSec, outline the project plan, and validate current state. At the end of the meeting, we should have a completed Stakeholder list and a Critical Systems list. Also we suggest creating a SharePoint site for the engagement.

Engage stakeholders

Once stakeholders for each control element are identified, we suggest MISOs inform them of the engagement. We then schedule meetings with each stakeholder, providing templates and assistance to improve control element ratings.

Assess findings

All supporting documents stay within the sector/ministry on their SharePoint site. We access the documents from the SharePoint site and don't take ownership of any document.

Closeout meeting

We present a straight-forward report comprising of pre- and post-DefSec dashboards, statistics on control changes, recommendations, and next steps. This is an in-person, face-to-face meeting with the MISO(s) and Director(s).

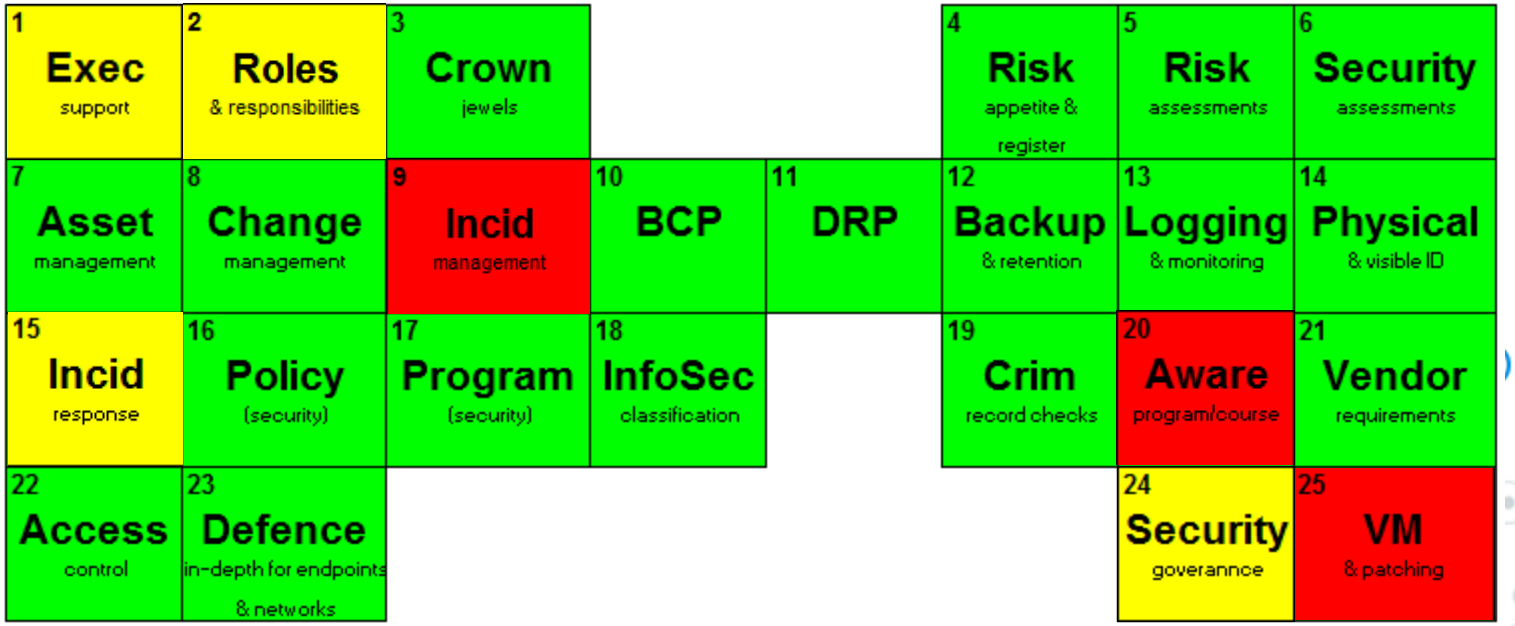
Next sector/ministry

We proceed to the next sector/ministry (and repeat steps) while providing ongoing support to previously assessed sectors/ministries.

Sample Exercise

An organization has recently been breached. The breach involved data exfiltration, root cause was determined to be inadequately patched systems. It is now in the media and the CEO blames the IT department for the incident.

Based on the scenario, which DefSec control(s) are not properly functioning within the organization?



What are the next steps?

Assess: Organization

A blank DefSec dashboard is available online. Use the DefSec document itself or use the dashboard to assess your organization to determine where you require support.

Utilize: DefSec Resources

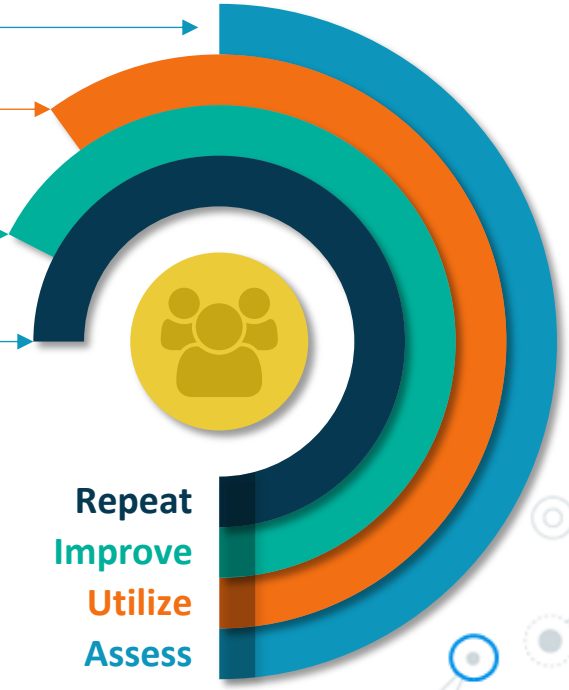
Templates are available online for the 25 control elements of DefSec. Utilize the templates to ensure prerequisites, directives, respiratory, and DNA controls are functioning within the organization.

Improve: Security Posture

Security posture is improved once the controls are in place. For security awareness –social engineering is a good test.

Repeat: Continuous Improvement

As the threat landscape is always changing, security controls should also evolve.



Security is everyone's responsibility:
Let's collaborate in improving the security posture across the public sector.

Thank You!

For more information visit: gov.bc.ca/defensible-security

BRITISH COLUMBIA

OCIO

Office of the Chief Information Officer