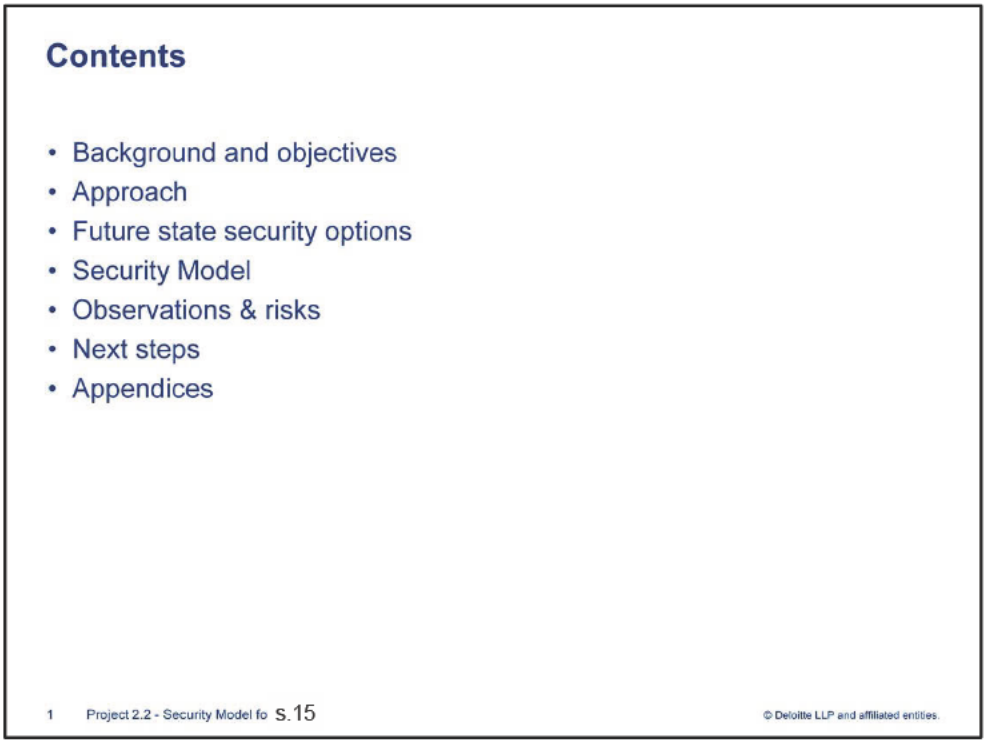
Deloitte.

BRITISH COLUMBIA
Ministry of Health

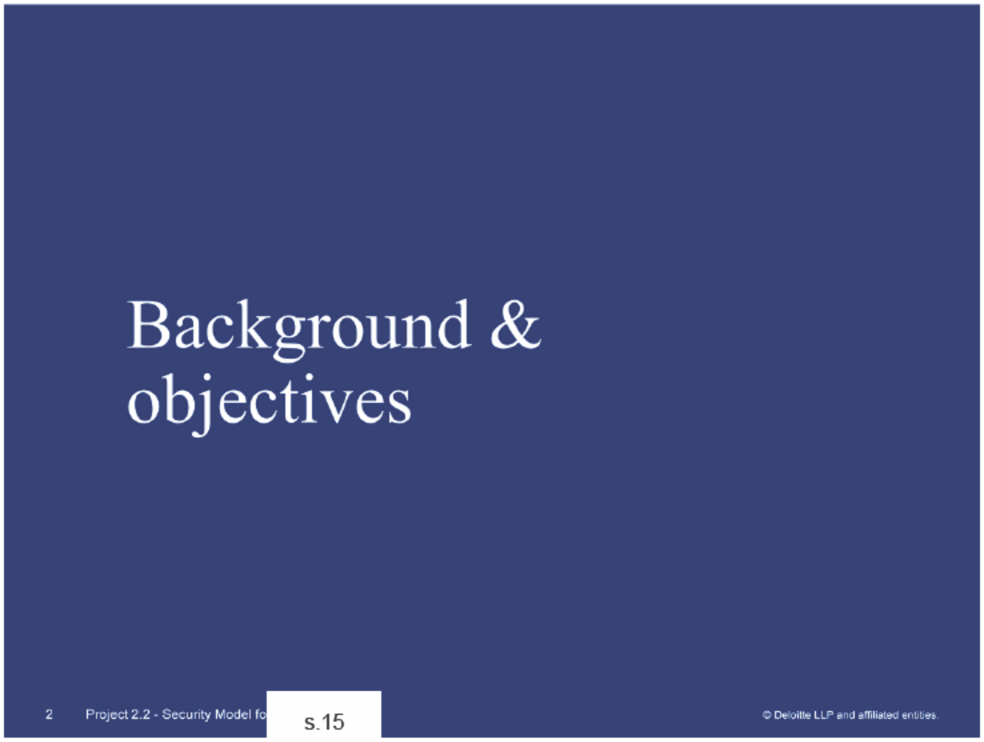
BC Ministry of Health
Security Model

s.15



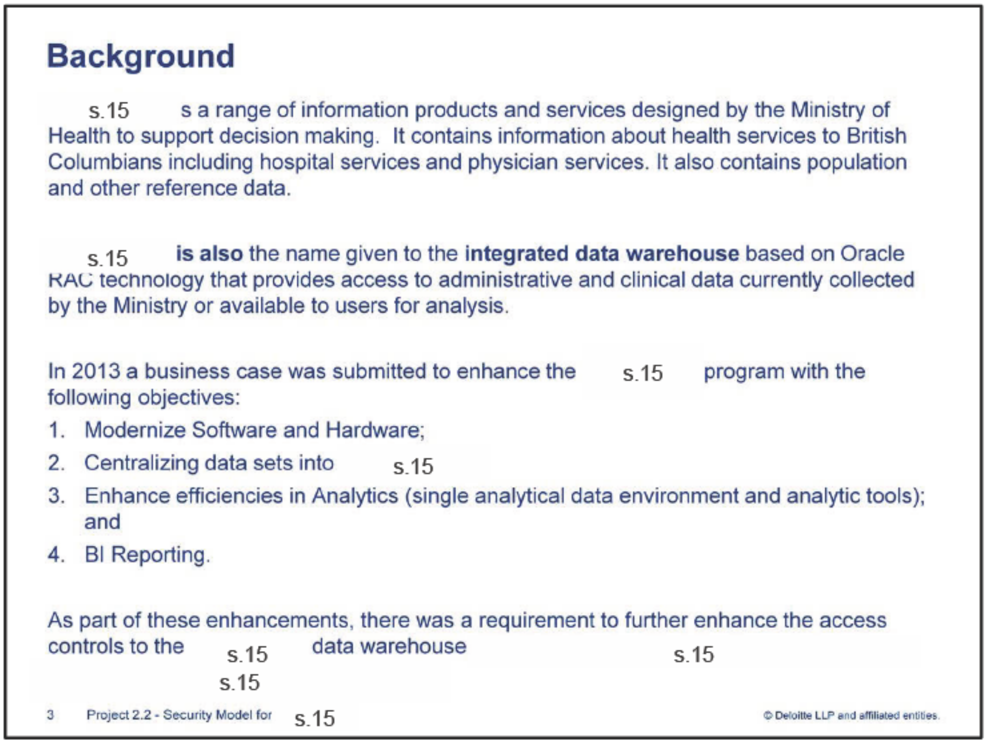
Contents

- Background and objectives
- Approach
- Future state security options
- Security Model
- Observations & risks
- Next steps
- Appendices



Background & objectives

2 Project 2.2 - Security Model fo s.15



Background

s.15 s a range of information products and services designed by the Ministry of Health to support decision making. It contains information about health services to British Columbians including hospital services and physician services. It also contains population and other reference data.

s.15 **is also** the name given to the **integrated data warehouse** based on Oracle RAC technology that provides access to administrative and clinical data currently collected by the Ministry or available to users for analysis.

In 2013 a business case was submitted to enhance the s.15 program with the following objectives:

1. Modernize Software and Hardware;
2. Centralizing data sets into s.15
3. Enhance efficiencies in Analytics (single analytical data environment and analytic tools); and
4. BI Reporting.

As part of these enhancements, there was a requirement to further enhance the access controls to the s.15 data warehouse s.15
s.15

3 Project 2.2 - Security Model for s.15

© Deloitte LLP and affiliated entities.

Background (*cont.)*

The s.15 initiative as defined by the Ministry, covers the following objectives:

- Providing a centralized portal through which users will gain access to only authorized applications and data;
- Centralization of the security approval and procurement functions for the s.15 s.15 each of which have different gatekeepers who authorize and facilitate access to data across Ministry);
- Enable security approval of access privileges at the enterprise role level, irrespective of platform;

s. 15

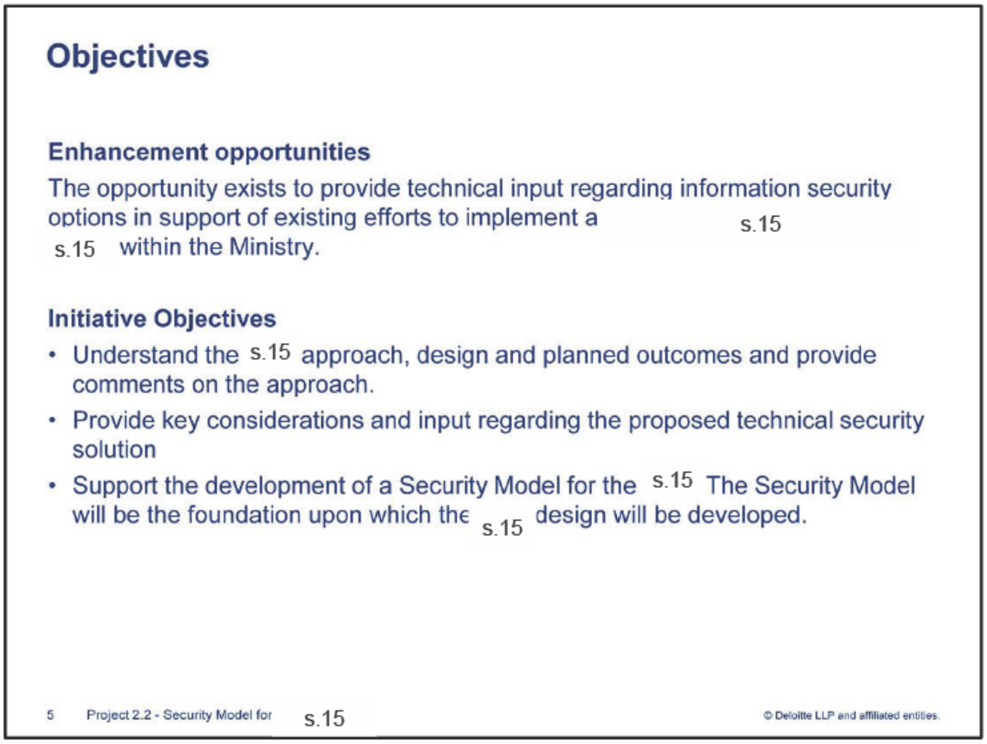
The s.15 initiative as defined by the Ministry **does not** include the following:

Areas to be addressed by current enhancement projects:

1. Database centralization;
2. Data security centralization with anonymization;
3. s.15 code quality improvements;
4. Develop common business objects;
5. Ministry wide Enterprise Roles definition and Access Management solution; and
6. Ministry wide Logging and Monitoring solution.

Areas identified to be addressed, however not yet funded:

1. Support Open Data access to citizens and Government-wide;
2. Self-service reporting and decision support for the Ministry, Health Authorities and other public sector partners;
3. Advanced analytics capabilities: Optimization, forecasting and adaptive learning for future planning; and
4. Amendments to existing service provider contract to support the above mentioned initiatives.



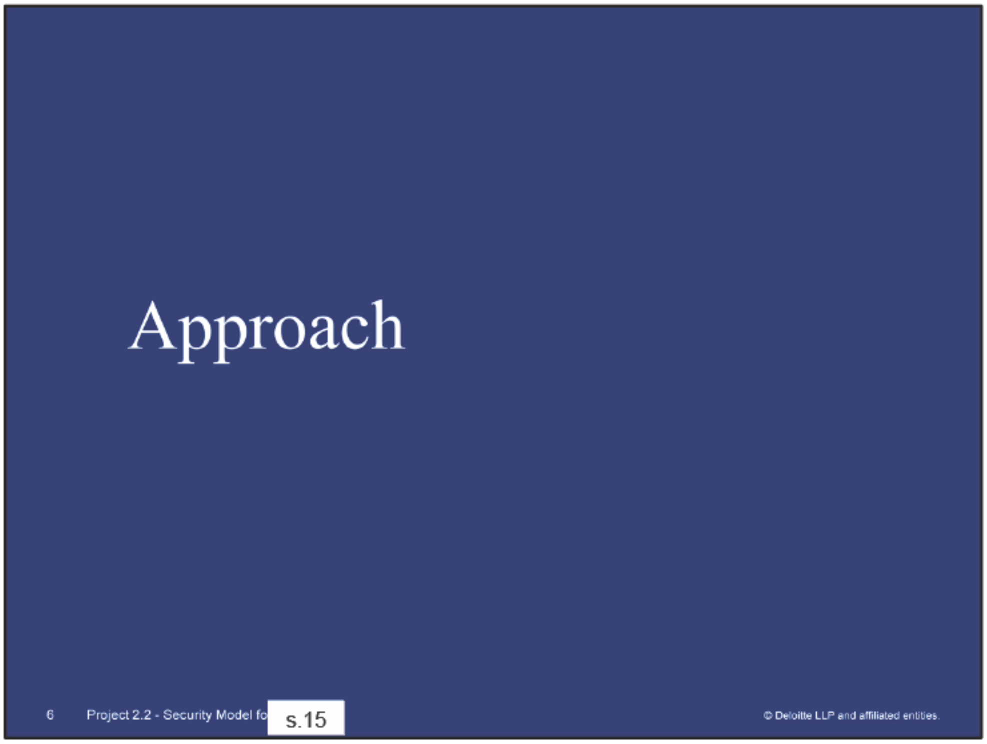
Objectives

Enhancement opportunities

The opportunity exists to provide technical input regarding information security options in support of existing efforts to implement a s.15 s.15 within the Ministry.

Initiative Objectives

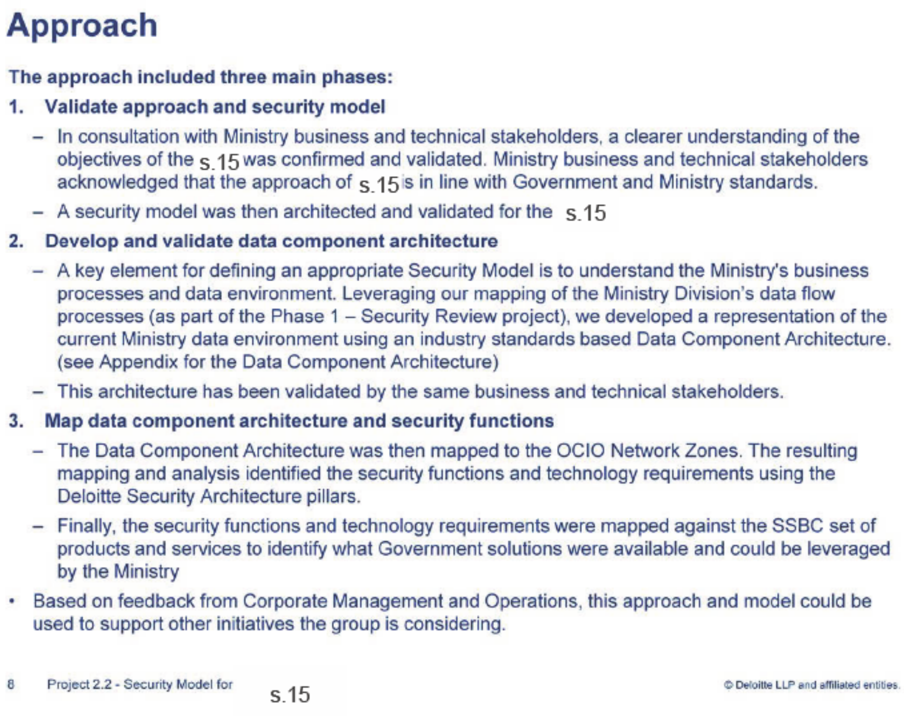
- Understand the s.15 approach, design and planned outcomes and provide comments on the approach.
- Provide key considerations and input regarding the proposed technical security solution
- Support the development of a Security Model for the s.15 The Security Model will be the foundation upon which the s.15 design will be developed.



Approach

Approach

- In consultation with Ministry business and technical stakeholders, a clearer understanding of the objectives of the s.15 was confirmed and validated. Ministry business and technical stakeholders acknowledged that the approach of s.15 is in line with Government and Ministry standards.
  - A security model was then architected and validated for the s.15
- A key element for defining an appropriate Security Model is to understand the Ministry's business processes and data environment. Leveraging our mapping of the Ministry Division's data flow processes (as part of the Phase 1 – Security Review project), we developed a representation of the current Ministry data environment using an industry standards based Data Component Architecture. (see Appendix for the Data Component Architecture)
  - This architecture has been validated by the same business and technical stakeholders.
- The Data Component Architecture was then mapped to the OCIO Network Zones. The resulting mapping and analysis identified the security functions and technology requirements using the s.21
- Finally, the security functions and technology requirements were mapped against the SSBC set of products and services to identify what Government solutions were available and could be leveraged by the Ministry
- Based on feedback from Corporate Management and Operations, this approach and model could be used to support other initiatives the group is considering.



Approach

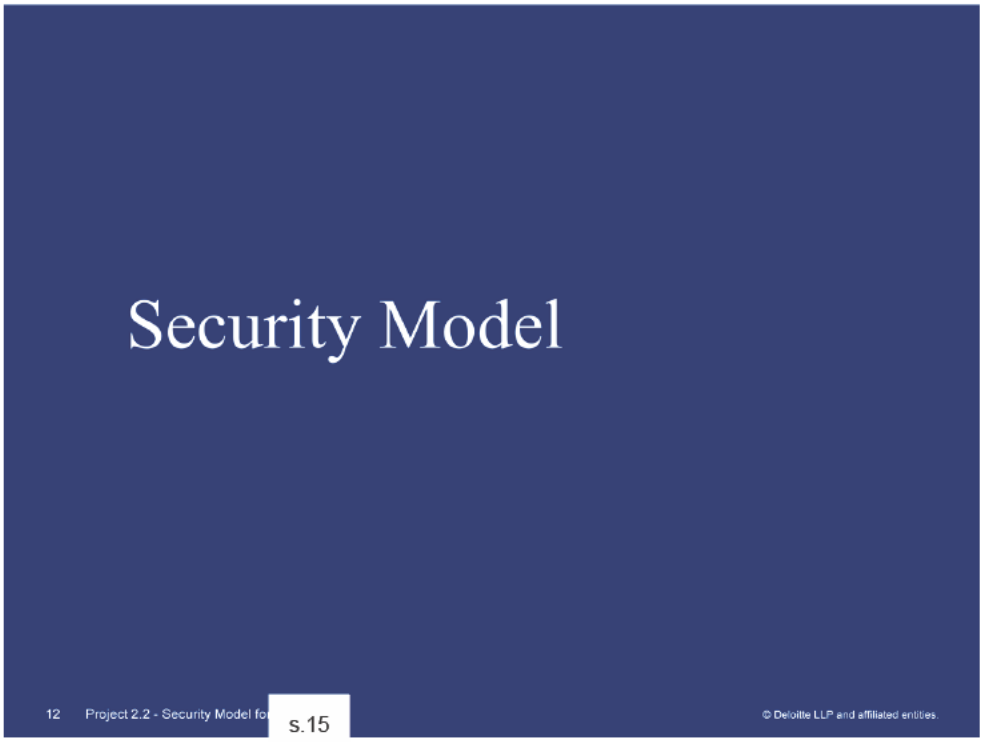
The approach included three main phases:

1. **Validate approach and security model**
   - In consultation with Ministry business and technical stakeholders, a clearer understanding of the objectives of the s.15 was confirmed and validated. Ministry business and technical stakeholders acknowledged that the approach of s.15 is in line with Government and Ministry standards.
   - A security model was then architected and validated for the s.15
2. **Develop and validate data component architecture**
   - A key element for defining an appropriate Security Model is to understand the Ministry's business processes and data environment. Leveraging our mapping of the Ministry Division's data flow processes (as part of the Phase 1 – Security Review project), we developed a representation of the current Ministry data environment using an industry standards based Data Component Architecture. (see Appendix for the Data Component Architecture)
   - This architecture has been validated by the same business and technical stakeholders.
3. **Map data component architecture and security functions**
   - The Data Component Architecture was then mapped to the OCIO Network Zones. The resulting mapping and analysis identified the security functions and technology requirements using the Deloitte Security Architecture pillars.
   - Finally, the security functions and technology requirements were mapped against the SSBC set of products and services to identify what Government solutions were available and could be leveraged by the Ministry

- Based on feedback from Corporate Management and Operations, this approach and model could be used to support other initiatives the group is considering.

Future state

Pages 11 through 12 redacted for the following reasons:
- -
s. 15



Security Model

12 Project 2.2 - Security Model fo s.15

Basic terminology

- **Security Zone**
  - a logical grouping of systems and processes with similar risk profiles
- **Security Management Function**
  - a process for managing a particular security control
  - part of a comprehensive set of functions defined in the Security Management Zone
- s.15 **Function**
  - a security enhancement activity defined in scope for the s.15
  - identified as 🟦 on the *Security Model diagram*
- **Security Model Component**
  - a specific technical attribute making up the security model.
  - Identified as □ on the *Security Model diagram*

Page 15 redacted for the following reason:
- -
s.15

Security Management Functions

s.21, s.15

Pages 17 through 28 redacted for the following reasons:
- -
s. 15
s. 15, s.21
s.15, s.21

Observations & risks

Pages 30 through 33 redacted for the following reasons:
- -
s. 15
s.15

Next steps

Next Steps

- The objective to date has been to develop the conceptual design of the security model, and has included an initial assessment of technology and cost options.
- Given that a majority of the anticipated services and technology options are available through existing Government services (SSBC, HPAS,etc), the next step should be to engage the SSBC technical architecture groups to validate the current security model and services options.
- The Ministry should open an iStore for a SSBC consultation around the s.15 design, constraints and cost options.
- In preparation for the discussion, the Ministry should document the s.15 business, function and technical requirements, to ensure that the appropriate SSBC technology SME is present during the consultation sessions.
- Once a viable technical solution is developed, the project plan should be updated to reflect the associated timelines, resources and costs.

Appendix

Pages 37 through 38 redacted for the following reasons:
- -
s. 15

Deloitte.

Deloitte.

BRITISH COLUMBIA
Ministry of Health

BC Ministry of Health
Access Management Strategy

Table of Contents

Current State Landscape

Access Management Issues Analysis

Solution Options

Recommendations

Next Steps

Appendix

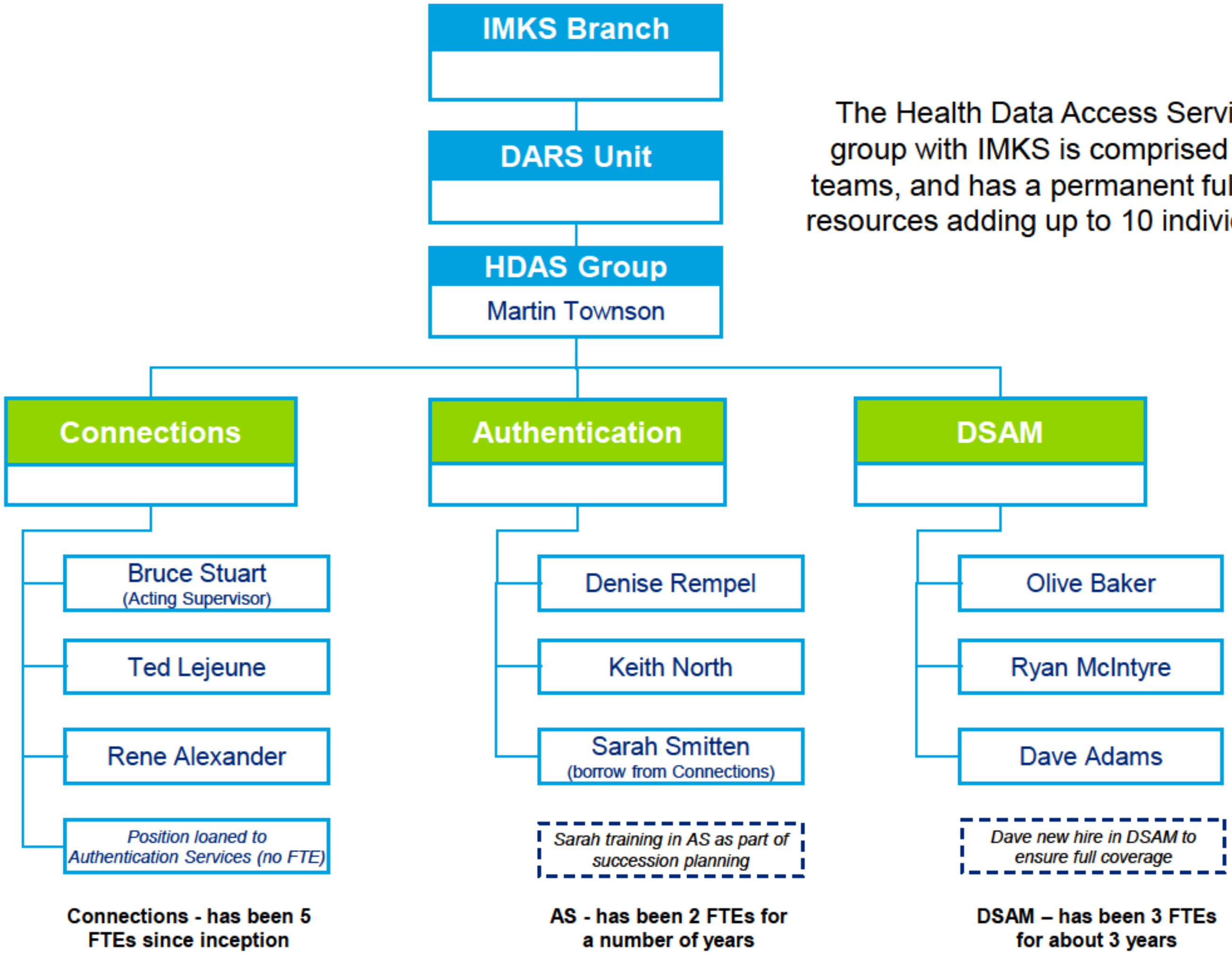
Current State Landscape

Access Management Structure

Health Data Access Services (HDAS) groups:

1) Connections
2) Authentication Services
3) Data Set Access Management (DSAM)

Access Management Org Chart



IMKS Branch

DARS Unit

HDAS Group
Martin Townson

The Health Data Access Services group with IMKS is comprised of 3 teams, and has a permanent full time resources adding up to 10 individuals.

Connections

- Bruce Stuart (Acting Supervisor)
- Ted Lejeune
- Rene Alexander
- *Position loaned to Authentication Services (no FTE)*

Connections - has been 5 FTEs since inception

Authentication

- Denise Rempel
- Keith North
- Sarah Smitten (borrow from Connections)

Sarah training in AS as part of succession planning

AS - has been 2 FTEs for a number of years

DSAM

- Olive Baker
- Ryan McIntyre
- Dave Adams

Dave new hire in DSAM to ensure full coverage

DSAM – has been 3 FTEs for about 3 years

Roles and Responsibilities

1) Connections

The Connections team is currently comprised of 3 fulltime employees (however 2.5 currently doing AM tasks), and a vacant supervisor position being performed by one of the team members, Bruce Stuart. Connections primary deals with access management requests for external parties like Health Authorities to such systems as MSP Direct, PharmaNet, LDAP ID's, Health Registries, secure file transfer etc. (*Please refer to appendix A for details*)

In terms of access granting procedures, Connections sees the greatest variability in requests of the 3 HDAS groups with diverse request types for a variety of systems and overlap with Authentication Services for s.15 LDAP and PharmaNet requests. Some of this overlap is intentional to facilitate Segregation of Duties between approval and granting of access. However, under the new information governance model, the ownership of information and approval of access is being shifted to business owners which will facilitate operational efficiency within HDAS. s.15 are being discontinued to enhance operational efficiency, and s.15 Forms are hoping to be transferred to another department.

As formal access termination procedures, i.e. Departing Employee Forms, are not rigorously completed by Ministry staff, it is making it difficult for this team to proactively manage access terminations.

Roles and Responsibilities

1) Authentication Services

The AS team is currently comprised of 3 fulltime employees, with a recently transferred employee (Sarah Smitten from Connections), training in AS for succession planning purposes. This team moved under HDAS in April 2013, and hence is the least understood of the 3 HDAS groups. The unit provides operational support, access, id management for the MOH staff, contracted resources and external stakeholders such as CGI, Maximus, SSBC by establishing IDIR ids, Exchange Mailboxes, LDAP Intraweb ids, PharmaNet ids, MVS ids, Remote VPN\DTS ids etc. In addition to completing direct MOH Access Management services, AS also focuses on coordinating between staff and service providers to facilitate processing of iStore requests. (*Please refer to appendix A for details*)

AS's responsibilities currently overlap with Connections for LDAP and PharmaNet requests, and with DSAM for LAN and Mainframe requests. It currently receives access requests through 6 separate web based forms for various application requests causing inconsistency and operational efficiency issues. As formal access termination procedures i.e. Departing Employee Forms are not rigorously being completed by Ministry staff, AS also struggles with proactively managing access terminations.

Roles and Responsibilities

3) DSAM

The DSAM team is also comprised of 3 fulltime employees, with one new employee training to replace a departing employee. DSAM is the most cohesive of the 3 HDAS teams with a single request form, and a standardized process. This team primarily deals with access management requests for [redacted] s.15 *Please refer to appendix A for details*)

DSAM is also responsible for enforcing security policy by liaising with the security architecture team while granting access, and providing recommendations to the security team for the creation of new database roles or data migrations from the old systems to [redacted] s.15 This unit is also responsible for removing individual's access in a timely manner when access is no longer required, but struggles with this due to limited following of access termination procedures i.e. Departing Employee Form throughout the ministry.

DSAM's current challenges include management of large number of roles (approximately 110), and supporting data management projects without being identified as a stakeholder.

Page 48 redacted for the following reason:
- -
s.15

IMKS System Landscape – Current State

The figure below shows the overall architecture of IMKS managed applications. It indicates that there are multiple user types for each application, causing the access requests to originate from multiple sources with varying user needs.

s. 15

Primary responsibility	DSAM	Connections	Auth. Services

Current Process Flow Summary

1) Connections

s.15

Current Process Flow Summary

2) Authentication Services

s.15

Current Process Flow Summary

3) DSAM

s.15

s. 15

Current Process Flow Detailed

To view detailed versions of the process flow summaries, please refer to the attached document below.

s.15

s. 15

To open the attached document, right click on the icon, select 'Visio Object' and click 'Open'

Current Volume and Service Levels

		Effort Estimate			Monthly Hours			
Team	Task Type	Volume per month	Time Consumption per request (mins)	Monthly Time Consumption (hours)	Processing time	Coordinating time	Other tasks	Available time
Manager Connections	s.15			150	150	0		150
		60	15	15				
		100	5	8				
		400	3	20				
		100	20	33				
		360	1	6				
		15	5	1				
		1	5	0				
		0.5	10	0				
		2	60	2				
		10%		16				
	Total			**102**	**102.1**	**302.9**	**45.0**	**450**
Authetication Services**	s.15	19%		63				
		23%		76				
		15%		51				
		11%		38				
		8%		25				
		25%		84				
	Total	**100%**		**337**	**337**		**113**	**450**
DSAM	s.15	3	30	1				
		24	120	48				
		1	720	17				
		35%		56				
	Total			**122**	**122**	**171**	**157**	**450**

** The volume estimates for Authentication Services are unavailable as the CAM calls have been logged incorrectly. So, estimates have been based on % of total time spent

Current Volume and Service Levels

The HDAS Time Consumption and Service Levels table indicate the following results:

- HDAS team members spend a large amount of time, indicated by coordinating time, corresponding with other parties to collect information and process request, as opposed to directly managing the Access Management function.
- This coordinating time can be reduced by introducing operational efficiencies through improvement in processes.

Access Management Issues Analysis

Overall observations

- High workload for the access management team.
- The access management team understands the processes very well implicitly.
- The access management team is very client focused as they try to resolve client issues in a proactive manner.
- The team is working with complex, cumbersome, manual processes that require staff to spend significant time coordinating.

Pages 58 through 60 redacted for the following reasons:
- -
s.15

Operational and Organizational Issues

"While there is no definitive evidence as to the particular reasons for the disclosures of research data discussed in this report, there is anecdotal evidence that some individuals became frustrated with the delays in processing their data requests and further delays in obtaining access to data that the Ministry had approved for disclosure. The circumstances surrounding the breaches present similarities to a pattern of attempts to work around the lengthy approval process that was apparent in the documentation the investigation reviewed. I note that, if this was the case, it does not excuse anyone for obtaining access to personal health data through unauthorized channels. However, in my view, a more streamlined process for access, combined with clear privacy obligations, would remove any impetus for researchers to seek alternative avenues of access to data outside of the formal approval process."

Source: Investigation Report F13 -02 – Information & Privacy Commissioner for BC, p29

Solution Options

Solution Options

Option 1 – Status Quo

- Continue with current processes
- The current issues will continue to persist
- This would not address MOH’s needs, so this should not be considered.

Option 2 – Manual Process Streamlining

- Redesign the access management processes without the use of new technology
- Focus on process improvement and organizational improvement
- Would need to monitor the processes to ensure that they are properly followed
- Improve the security from an access management perspective
- Will not replace the manual data entry work required
- Fully documented processes will be created

Option 3 – Automated User Management

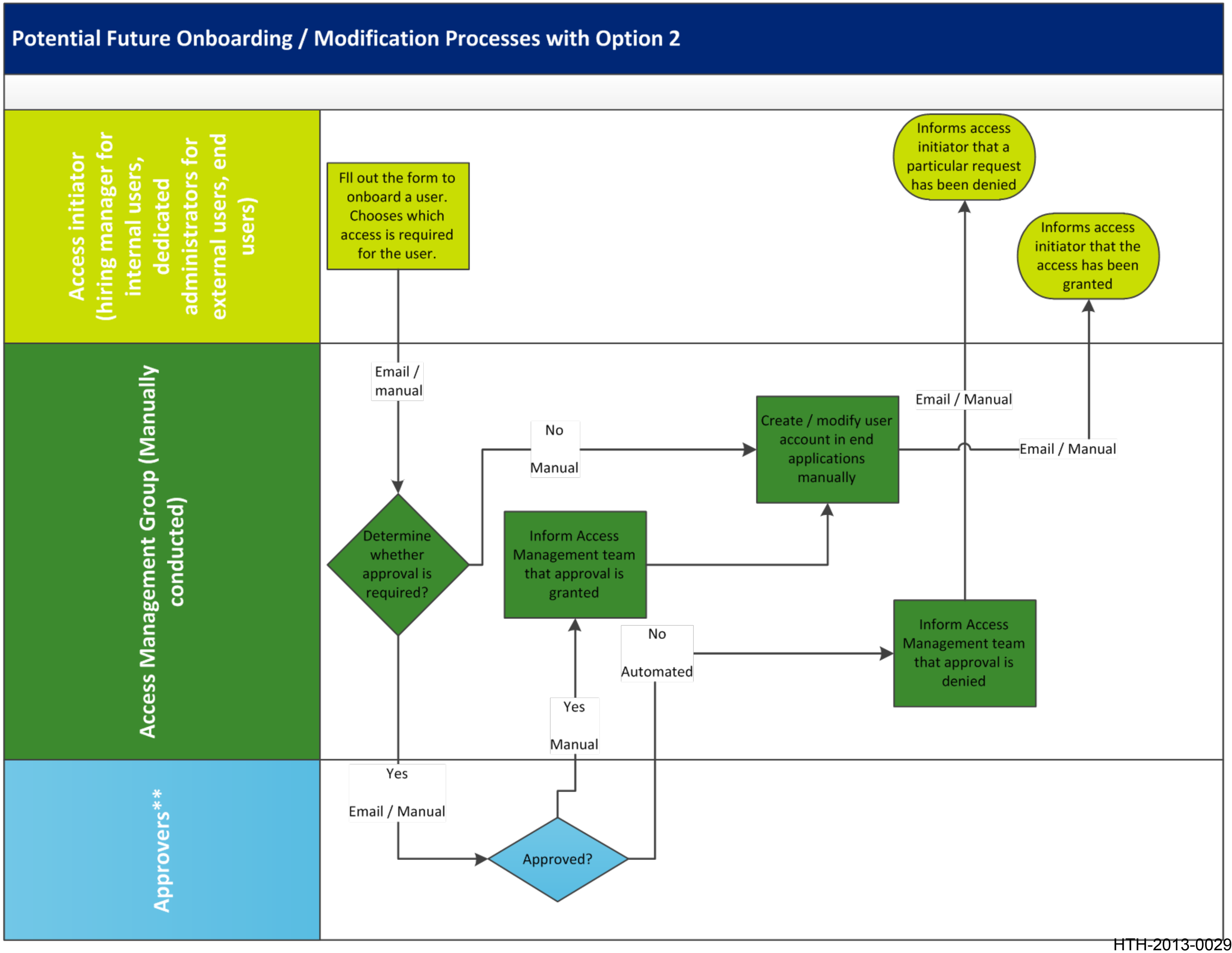
- Implement technology to streamline the access management processes
- This option incorporates process re-design and organizational re-design
- Leverage technology to automate the user administrative functionalities such as onboarding, modification, and offboarding
- Improve the security from an access management perspective
- Will eliminate many of the data entry tasks required
- Fully documented processes will be created

Option 2 – Manual Process Streamlining

Option 2 – Process enhancements

- Consider redesigning access processes using risk-based priority to improve efficiency and effectiveness.
- Priority enhancements include:
  - Streamlined manual user account creation
  - Streamlined manual account modification
  - Streamlined manual account deletion
  - Approval workflows definition (define who the approvers should be for each type of applications / datasets / network access)
  - Documentation of the new processes
  - Exception management processes
- Once the new processes are designed, tasks will still need to be manually performed as technology is not implemented to automate the user creation tasks under this option.
- However, increased efficiencies would enable staff to focus on value-added activities and reduce turnaround times over the long term.
- This would increase process effectiveness, enable less cumbersome access reviews and audits and also reduce frustration within the user community.

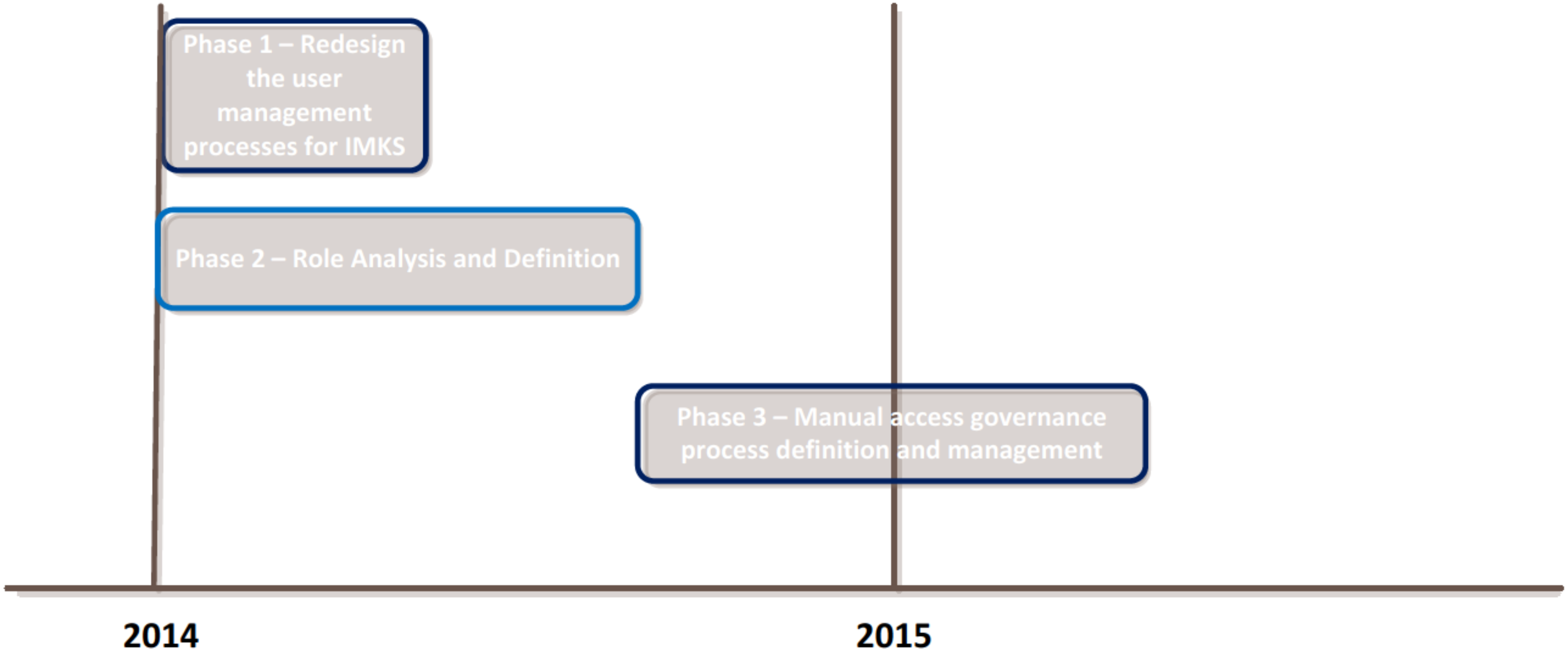
Option 2 – Potential Process for Access Management



Potential Future Onboarding / Modification Processes with Option 2
Access initiator (hiring manager for internal users, dedicated administrators for external users, end users)
Access Management Group (Manually conducted)
Approvers**
Fll out the form to onboard a user. Chooses which access is required for the user.
Email / manual
Determine whether approval is required?
No
Manual
Create / modify user account in end applications manually
Inform Access Management team that approval is granted
Yes
Email / Manual
Approved?
Yes
Manual
No
Automated
Inform Access Management team that approval is denied
Email / Manual
Informs access initiator that a particular request has been denied
Email / Manual
Informs access initiator that the access has been granted

Roadmap – Option 2

The following is the roadmap for Option 2. These phases involve perform business analysis tasks to streamline the access management processes.


Phase 1 – Redesign the user management processes for IMKS
Phase 2 – Role Analysis and Definition
Phase 3 – Manual access governance process definition and management
2014
2015

Description of Phases – Option 2

Phase 1 – Redesign the user management processes for IMKS

Objective: The objective of Phase 1 is to re-engineer the access request and ID creation / modification / deletion processes. In addition, a compliance monitoring process should be developed to ensure that these streamlined processes are properly followed. This would be a continuation of P5.5.

Estimated Duration: 5 months

Phase 2 – Role Analysis and Definition

Objective: The objective of Phase 2 is to define and simplify the roles for IMKS managed applications. The purpose is to define the roles so that users will not get more privileges than required.

Estimated Duration: 7 months

Phase 3 – Manual access governance process definition and management

Objective: The objective for this phase is to improve the access governance process by introducing regular access certification / attestation cycles using a manual approach.

Estimated Duration: 6 months

Detailed descriptions of the phases can be found in Appendix B

Option 3 – Automated User Management

Option 3 – Conceptual Diagram

The following conceptual diagram depicts option 3 which will allow MOH to effectively manage its users through a single point for user management.

s. 15

s. 15

Suggested Process for Access Management

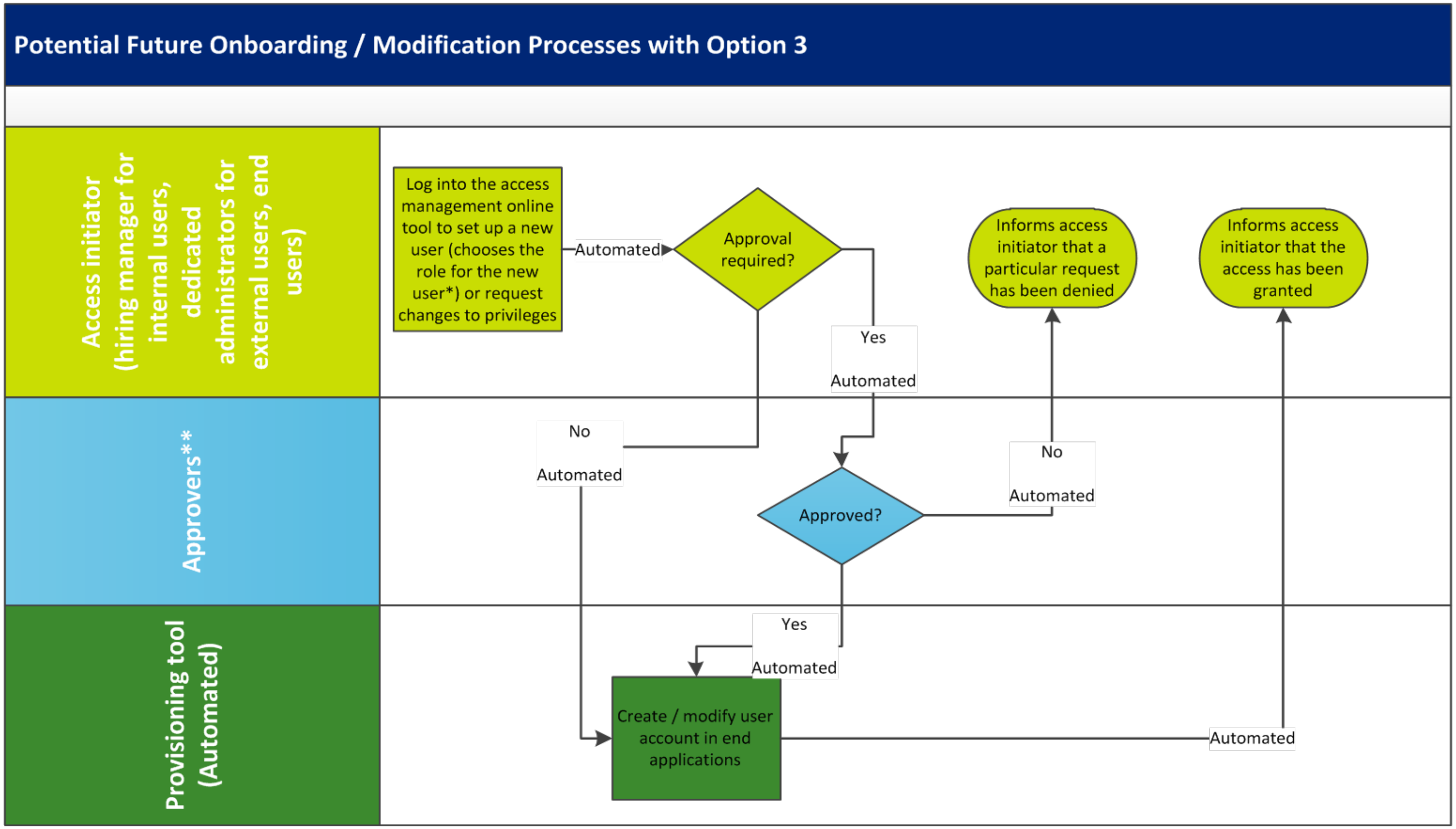
Once the automated user administration tool is set up, minimal interactions will be required from the access management group. During normal user administration activities, the access management groups would not need to be involved at all.

The access management staff can then deployed to perform higher value tasks such as supporting the automated user administration systems. In addition, some resources will need to be allocated to deal with exception processes.

We anticipate that half of the access management team (5 FTE) would be able to be deployed to perform other activities such as project work, etc. under this option.

Option 3 – Potential Process for Access Management

The following process flow depicts a potential streamlined access management process to onboard / modify a user at a conceptual level. This is used as a sample to demonstrate what could be accomplished with an automated tool.

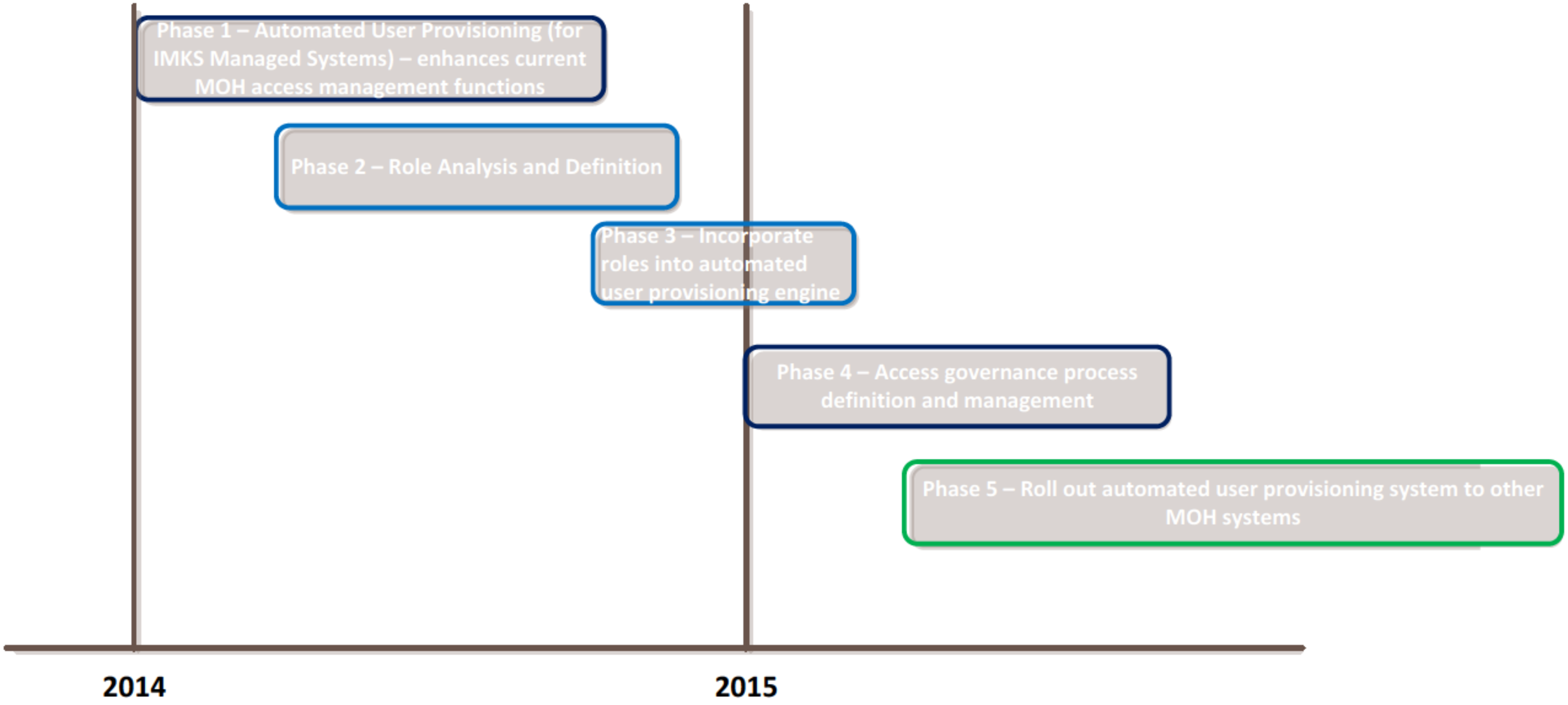

Potential Future Onboarding / Modification Processes with Option 3
Access initiator (hiring manager for internal users, dedicated administrators for external users, end users)
Approvers**
Provisioning tool (Automated)
Log into the access management online tool to set up a new user (chooses the role for the new user*) or request changes to privileges
Automated
Approval required?
Yes
Automated
No
Automated
Approved?
No
Automated
Yes
Automated
Informs access initiator that a particular request has been denied
Informs access initiator that the access has been granted
Create / modify user account in end applications
Automated

* If roles are not implemented at MOH, then the access initiator can choose the apps that are required for the new user

** Multiple approvals can be sent to different approvers. We can configure the system so that even if one approver denies the request for his / her specific apps, the rest of the apps will still get provisioned.

Roadmap – Option 3

Identity management program is usually a multi-year endeavor before an organization achieves its ultimate vision. The key for a successful automated user management program is to break down the work into smaller phases. Each phase should be self-contained and meet a portion of the overall objective. Key success factors should also be developed for each phase in order to measure the effectiveness of the solution. The following diagram illustrates a recommended identity management roadmap for MOH which outlines the different phases required before MOH can achieve its overall vision.



Phase 1 – Automated User Provisioning (for IMKS Managed Systems) – enhances current MOH access management functions

Phase 2 – Role Analysis and Definition

Phase 3 – Incorporate roles into automated user provisioning engine

Phase 4 – Access governance process definition and management

Phase 5 – Roll out automated user provisioning system to other MOH systems

Phase Description – Option 3

Phase 1 – Automated User Provisioning (for IMKS Managed Systems) – enhances current MOH access management functions

Objective: The objective of Phase 1 is to automate the access request and ID creation / modification / deletion processes.

Estimated Duration: 8 months

Phase 2 – Role Analysis and Definition

Objective: The objective of Phase 2 is to define and simplify the roles for IMKS managed applications. The purpose is to define the roles so that users will not get more privileges than required.

Estimated Duration: 7 months

Phase 3 – Incorporate roles into automated user provisioning engine

Objective: The objective of Phase 3 is to incorporate the roles that are created in Phase 2 into the automated provisioning solution. This would allow the access requester to choose the roles instead of the individual application access levels. This will further make the user onboarding / modification more efficient.

Estimated Duration: 3 months

Phase Description – Option 3

Phase 4 – Access governance process definition and management

Objective: The objective of Phase 4 is to improve the access governance process by introducing regular access certification / attestation cycles. This will help ensure that users are only getting access to what they have been approved for.

Estimated Duration: 6 months

Phase 5 – Roll out automated user provisioning system to other MOH systems

Objective: Once the IMKS applications have been integrated with the automated provisioning solution, MOH will be in a position to evaluate the effectiveness of the Identity Management Program and determine whether to roll the Identity Management solution out to the other MOH systems.

Estimated Duration: To be determined as this will be dependent on which systems MOH decide to integrate with the Identity Management solution.

Detailed descriptions of the phases can be found in Appendix C

Recommendations

Overall Vision / Principles for Identity and Access Management

- Streamlined / efficient user administration processes that are easily understood.
- Well controlled access request processes that are widely followed.
- Users are not getting more access than required.
- The access management teams are performing high value identity related tasks.
- The idle time for the end users are minimal when it comes to onboarding and modification of access.
- Compliance reporting and security investigations can be performed easily through an integrated reporting mechanism on identity related events.

Recommended Option

The following is a comparison between option 2 and option 3:

	Option 2 – Manual Process Streamlining	Option 3 – Automated User Management
Operational Efficiency Benefits	• No changes to technology required. • Potential reduction in costs by getting the existing access management staff to perform higher value tasks.	• Reduce cost on managing user administration. • Reduce ongoing compliance cost.
Security and Risk Management Benefits		s.15
Payback Period	Approximately 8 years	Approximately 7 years

Recommended Option

The following is a comparison between option 2 and option 3:

	Option 2 – Manual Process Streamlining	Option 3 – Automated User Management
Business Facilitation Benefits	• Reduce user frustration by streamlining user administration processes. • Potential reduction of user downtime during onboarding and job changes.	• Reduce user frustration by streamlining user administration processes with online tools and standardized accesses. • Reduce user downtime during onboarding and job changes.
Operational Effectiveness Benefits	• Streamlining of the user administration processes will result in less time being spent on the redundant tasks (e.g. multiple groups do not require to work on a single application) • Reduce likelihood of errors by standardizing forms, processes and roles within the organization • Improve consistency in access processes	• Improve user productivity by facilitating more streamlined provisioning services. • Reduce likelihood of errors by standardizing forms, processes and roles within the organization. • Streamlining of the user administration processes will result in less time being spent on the tasks, error checking and gathering data for reporting, thus freeing up the access management staff to process more complex requests and monitor inappropriate accesses. • ensure that the users will follow the streamlined processes.

Recommended Option

Option 2 is a potential option, however due to the lack of leveraging technology, it will be difficult to ensure that the users will follow the newly designed processes as it is all manually conducted unless a substantial compliance process is developed to monitor the implementation and adherence of the newly created processes. In addition, reporting of access rights will still be difficult to accomplish due to a lack of a centralized view of MOH identities.

Option 3 will adequately address all of MOH's needs in relations to access management. It will also ensure that the users will follow the streamlined processes as the technology will not allow the users to obtain access any other way.

The advantage option 2 has over option 3 is the initial costs of the access management product and the initial technology implementation costs. However option 3 will most likely result in a lower ongoing operational costs. In addition, option 3 will ensure higher user adoption rate.

Next Steps

Next Steps

1. **Define the mandate with respect to access management for IMKS**
   - Determine the scope of access management services for that should be offered by IMKS.
   - Document and communicate the scope of access management services for IMKS.
2. **Perform a re-org on the Access Management group (based on the defined IMKS mandate in step 1)**
   - Determine whether IMKS should be responsible for all three access management sub-groups and the access management of systems for other divisions.
   - Determine whether more efficiencies will be achieved with one larger team instead of three sub-groups.
3. **Address the quick fixes that will improve the efficiencies for access management**
   - Assign an independent lead to facilitate process improvement sessions.
   - The facilitator should be unbiased and be objective about the current processes and challenge them appropriately.
   - Leverage the current state process flow diagrams as the basis of the discussions.
4. **Select option 2 or option 3**
   - Depending on the outcome of step 1, the scope of option 2 and option 3 may change as some systems may not be considered within IMKS' responsibilities. Therefore, there will be less process changes required.

Appendix

Appendix A: DAS Primary Functions and Responsibilities

Primary Functions

1) Connections

- **Major Access Management Functions**

s.15

Primary Functions

1) Connections

- **Major Access Management Functions**

s.15

- **Minor non-Access Management Functions**

s.15

Primary Functions

2) Authentication Services

- **Major Access Management Functions**

s.15

Primary Functions

2) Authentication Services

- **Minor non-Access Management Functions** *(performed on periodic or annual basis)*

s.15

Primary Functions

3) DSAM

- **Major Access Management Functions**

s.15

Current Volume and Service Levels

1) Connections

- Target Service Level: **40 business days**
- % total time in direct AM tasks: **90%**
- % total time in other tasks: **10%**
  - Meetings
  - Documentation

Current Volume and Service Levels

1) Connections

- **Current Volume**

s.15

Current Volume and Service Levels

2) Authentication Services

- Target Service Level: 40 business days
- % total time in direct AM tasks: 75%
  - iStore related: 49%
  - Non-iSore related: 26%
- % total time in other tasks: 25%
  - Project support
  - GDSA Related Security events
  - Annual maintenance processes
  - Process Documentation

Current Volume and Service Levels

2) Authentication Services

- **Current Volume: July 2012 to June 2013 – 3,369 CAM Calls**
  - **New User Setup** (IDIR, Mail, LDAP, LAN access) – 25%
  - **User Transfers\Departures** (IDIR, Mail, LDAP, LAN access) – 30%
  - **LAN Access** (LOB, SFP, LAN access, Projects) – 20%
  - **MVS Support** (Corporate GDSA Resource & application support , New ids, Changes , Deletions) – 15%
  - **Other tasks** (Password Reset, Unix requests, GAL Updates, PNP, Remote Ids ,BA liaison with program areas & external stakeholders) – 10%

Current Volume and Service Levels

3) DSAM

- Target Service Level: **10 - 15 business days**
- % total time in direct AM tasks: **65%**
- % total time in other tasks: **35%**
  - Role Development: 5%
  - Password resets, Auditing, Condor project, Troubleshooting etc: 10%
  - Data Migration Projects: 20%

Current Volume and Service Levels

3) DSAM

- ### Current Volume

10% Best Case: 30 min per request

85% Regular: 1 – 2 hr per request

5% Worst Case: 12 hr per request

Breakdowns for the 7076 forms from DSAM:

– **30 minutes:** 152

– **30 minutes <120 minutes:** 56

– **120 minutes or longer:** 17

Average: 28 forms per month

Appendix B: Option 2 – Manual Process Streamlining Detailed Analysis

Phase Description – Option 2

Phase 1 – Redesign the user management processes for IMKS

Objective: The objective of Phase 1 is to re-engineer the access request and ID creation / modification / deletion processes. In addition, a compliance monitoring process should be developed to ensure that these streamlined processes are properly followed. This would be a continuation of P5.5.

Target Use Cases / Deliverables:

- Streamlined manual user account creation
- Streamlined manual account modification
- Streamlined manual account deletion
- Approval workflows definition (define who the approvers should be for each type of applications / datasets / network access)
- Documentation of the new processes
- Exception management processes

Estimated Duration: 5 months

Phase Description – Option 2

Phase 2 – Role Analysis and Definition

Objective: The objective of Phase 2 is to define and simplify the roles for IMKS managed applications. The purpose is to define the roles so that users will not get more privileges than required. This conforms to the principle of least privilege which is considered a security best practice. This will address the issue of users cloning other users to get similar access. This can be done in parallel with Phase1.

Target Use Cases / Deliverables:

– Defined functional roles for internal users

– Defined functional roles for external users

Estimated Duration: 7 months

Phase Description – Option 2

Phase 3 – Manual access governance process definition and management

Objective: The objective for this phase is to improve the access governance process by introducing regular access certification / attestation cycles using a manual approach.

Without the use of an automated tool, the effort for conducting ongoing access review would be higher as a team of staff would have to extract information relating user privileges from each end systems before the user certification / attestation process can be initiated.

This phase will help ensure that users are only getting access to what they have been approved for. This project would be the automation of P5.4.

Target Use Cases / Deliverables:

– Determine processes of extracting user privilege information from each end system

– Manual user attestation processes

Estimated Duration: 6 months

Appendix C: Option 3 – Automated User Management Detailed Analysis

Phase Description – Option 3

Phase 1 – Automated User Provisioning (for IMKS Managed Systems) – enhances current MOH access management functions

Objective: The objective of Phase 1 is to automate the access request and ID creation / modification / deletion processes. In addition to automating the current functions of the access management groups, it will provide streamlined and automated workflows to manage access approvals. This will also provide MOH with enhanced user access reporting. This will also assist MOH in meeting compliance requirements. This would be a continuation of P5.5.

Target Use Cases / Deliverables:

- Automated user account creation
- Automated user account modification
- Automated user account deletion
- Approval workflows automation
- User access reporting
- Documentation of the new processes
- Exception management processes

Estimated Duration: 8 months

Phase Description – Option 3

Phase 2 – Role Analysis and Definition

Objective: The objective of Phase 2 is to define and simplify the roles for IMKS managed applications. The purpose is to define the roles so that users will not get more privileges than required. This conforms to the principle of least privilege which is considered a security best practice. This will address the issue of users cloning other users to get similar access. As this is a business analytical task, this can be done in parallel with Phase1.

Target Use Cases / Deliverables:

– Defined functional roles for internal users

– Defined functional roles for external users

Estimated Duration: 7 months

Phase Description – Option 3

Phase 3 – Incorporate roles into automated user provisioning engine

Objective: The objective of Phase 3 is to incorporate the roles that are created in Phase 2 into the automated provisioning solution. This would allow the access requester to choose the roles instead of the individual application access levels. This will further make the user onboarding / modification more efficient.

Target Use Cases / Deliverables:

– Functional roles from phase 2 integrated into the Identity Management system

– Revised user administration screens in the Identity Management system

Estimated Duration: 3 months

Phase Description – Option 3

Phase 4 – Access governance process definition and management

Objective: The objective of this phase is to improve the access governance process by introducing regular access certification / attestation cycles. This will help ensure that users are only getting access to what they have been approved for. This project would be the automation of Project 5.4.

Target Use Cases / Deliverables:

- Automation of user attestation processes
- Enhanced user access review reports

Estimated Duration: 6 months

Phase Description – Option 3

Phase 5 – Roll out automated user provisioning system to other MOH systems

Objective: Once the IMKS applications have been integrated with the automated provisioning solution, MOH will be in a position to evaluate the effectiveness of the Identity Management Program and determine whether to roll the Identity Management solution out to the other MOH systems.

Target Use Cases / Deliverables:

– Integration of other MOH applications into the Identity Management system

Estimated Duration: To be determined as this will be dependent on which systems MOH decide to integrate with the Identity Management solution.

Appendix D: Option 2 cost estimates

Option 2 - High Level cost estimates

The following section provides a high level estimate and a + / - 25% variation should be taken into consideration when reviewing these figures.

Initial Costs (phase 1):

	s.21	
Internal Implementation Cost (cost of MOH staff on this project)	$80,000	5 months (800 hours) of effort with 2 FTE at a blended rate of $50 per hour (fully loaded cost).
s.21		

* Includes designing the compliance / monitoring process to ensure that the staff are following the re-engineered processes.

Option 2 - High Level cost estimates

Initial Costs (phase 2):

Description	Estimated Cost	Assumptions
	s.21	
Internal Cost (cost of MOH staff on this project)	$84,000	7 months (1,120 hours) of effort with 1.5 FTE at a blended rate of $50 per hour (fully loaded cost).
s.21		

Option 2 - High Level cost estimates

The following table shows the ongoing costs for phases 1 to 2.

Ongoing Costs (after completion of phase 2):

Description	Estimated Cost	Assumptions
Internal resourcing cost	$900,000	9 FTE's at $50 per hour. There will be some reduction in FTE for the resources. However, a compliance process will have to be put in place to ensure that the new processes are being followed. 2,000 hours per year.
Total	**$900,000**	

Appendix E: Option 3 cost estimates

Option 3 - High Level cost estimates

The following section provides a high level estimate and a + / - 25% variation should be taken into consideration when reviewing these figures.

Initial Costs (phase 1):

Description	Estimated Cost	Assumptions
Product licensing	$450,000*	15,000 total identities at $30 per user. 12,000 users from Health Authorities and 3,000 other users (internal, contractors, CSPBC, etc)
	s.21	
Internal Implementation Cost (cost of MOH staff on this project)	$192,000	8 months (1,280 hours) of effort with 3 FTE at a blended rate of $50 per hour (fully loaded cost).
s.21		

* SSBC has already purchase 30,000 licenses for user provisioning which is currently not being used. There may be an opportunity to reduce the initial costs pending discussions with SSBC regarding the licenses.

Option 3 - High Level cost estimates

Initial Costs (phase 2):

s.21		
Internal Cost (cost of MOH staff on this project)	$84,000	7 months (1,120 hours) of effort with 1.5 FTE at a blended rate of $50 per hour (fully loaded cost).
s.21		

Option 3 - High Level cost estimates

Initial Costs (phase 3):

Description	Estimated Cost	Assumptions
	s.21	
Internal Cost (cost of MOH staff on this project)	$24,000	3 months (480 hours) of effort with 1 FTE at a blended rate of $50 per hour (fully loaded cost).
s.21		

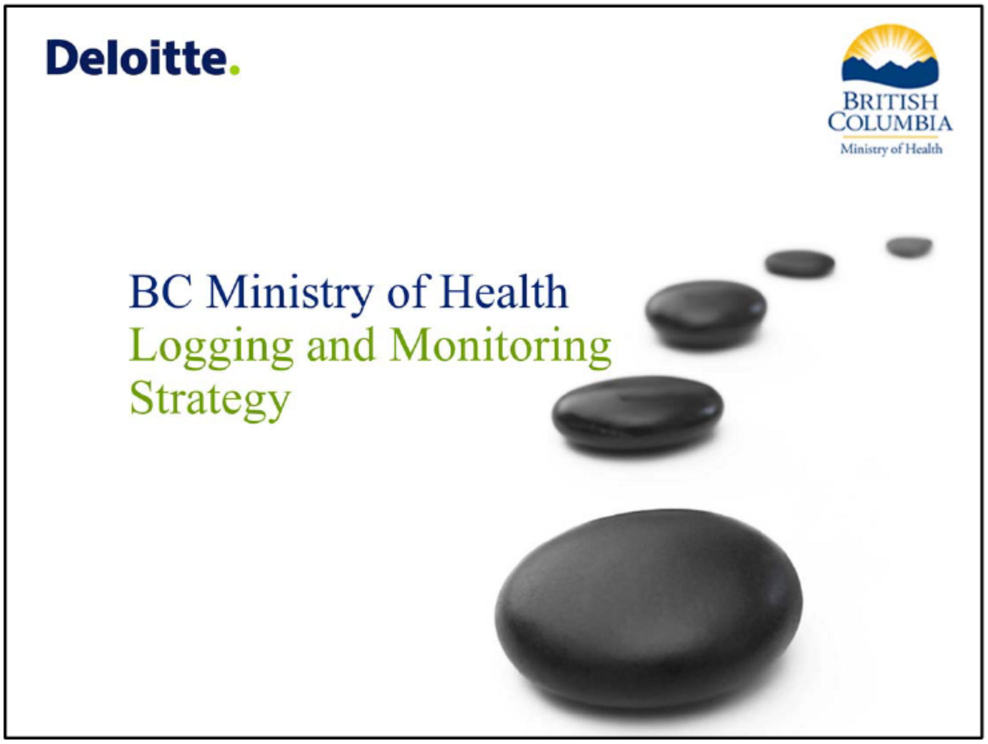
Option 3 - High Level cost estimates

The following table shows the ongoing costs for phases 1 to 3.

Ongoing Costs (after completion of phase 3):

Description	Estimated Cost	Assumptions
Product maintenance	$90,000	20% of the product licensing cost per year
Internal resourcing cost	$500,000	5 FTE's at $50 per hour. 1 manager and 2 resources for supporting the product and deal with exception processes and 2 FTE's for project related tasks outside of user administration. The coordination time (DSAM and Connections) equals approximately 3 FTE. In addition, If the iStore processes can be delegated to the business, 2 FTE from Authentication Services may be able to be redeployed for higher value activities. 2,000 hours per year.
Hardware cost	$96,000	$1,000 per month per server. We will require approximately 8 server for the Identity Management Infrastructure.
Total	**$686,000**	

Deloitte.



Deloitte.

BRITISH COLUMBIA
Ministry of Health

BC Ministry of Health
Logging and Monitoring Strategy

- Click to edit Master text styles
  - Second level
    - Third level
      - Fourth level

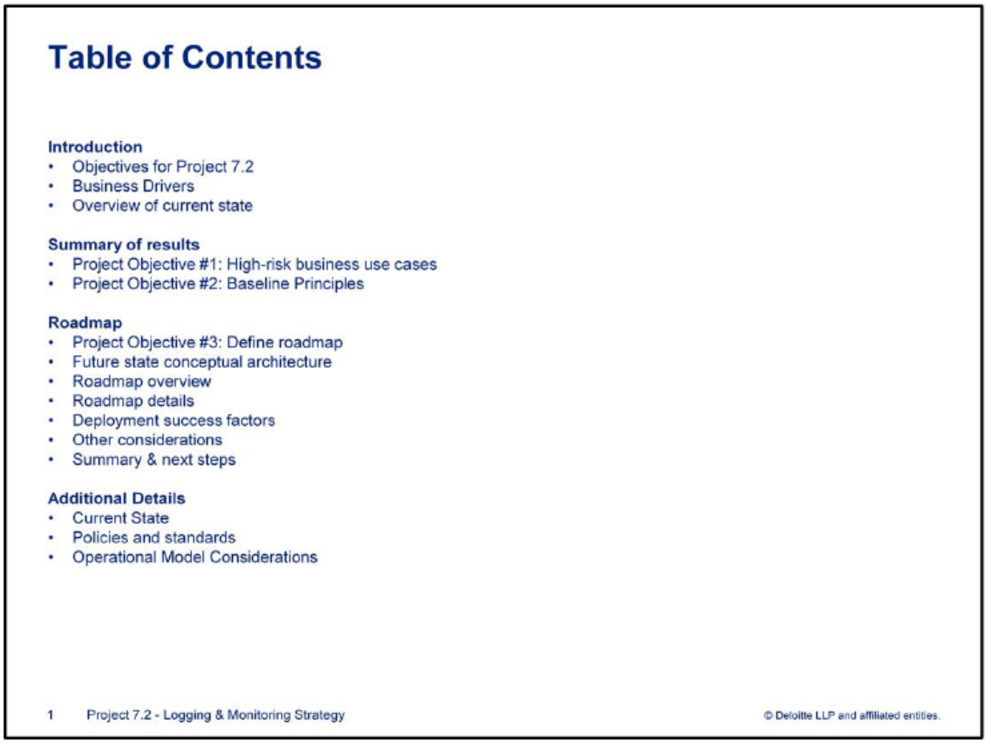


Table of Contents

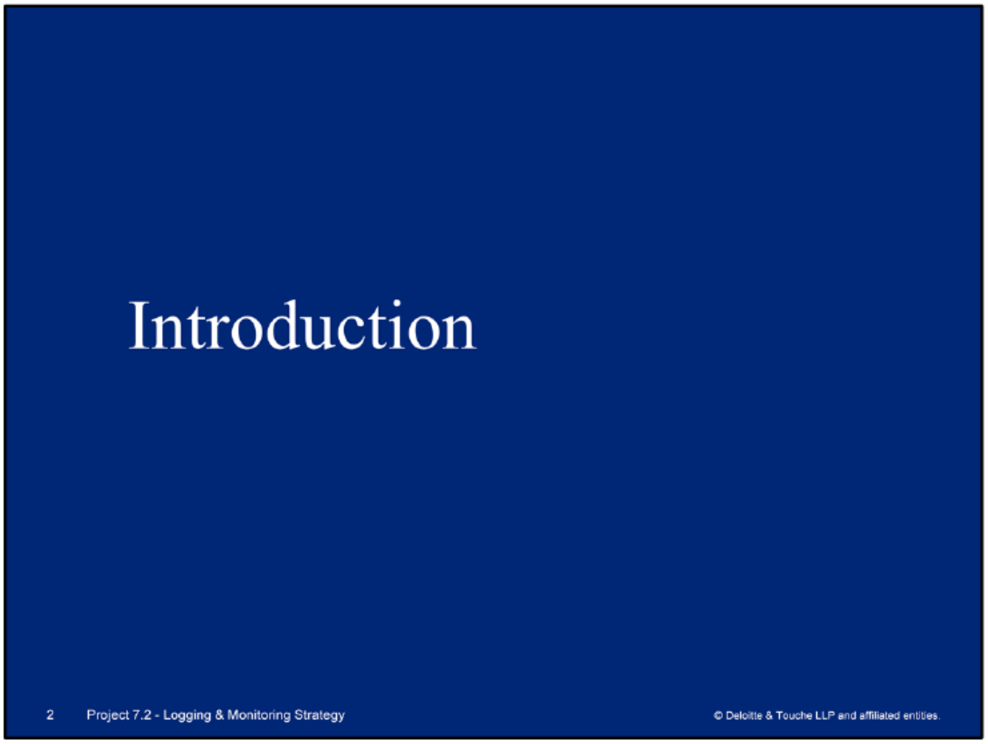
Introduction
- Objectives for Project 7.2
- Business Drivers
- Overview of current state

Summary of results
- Project Objective #1: High-risk business use cases
- Project Objective #2: Baseline Principles

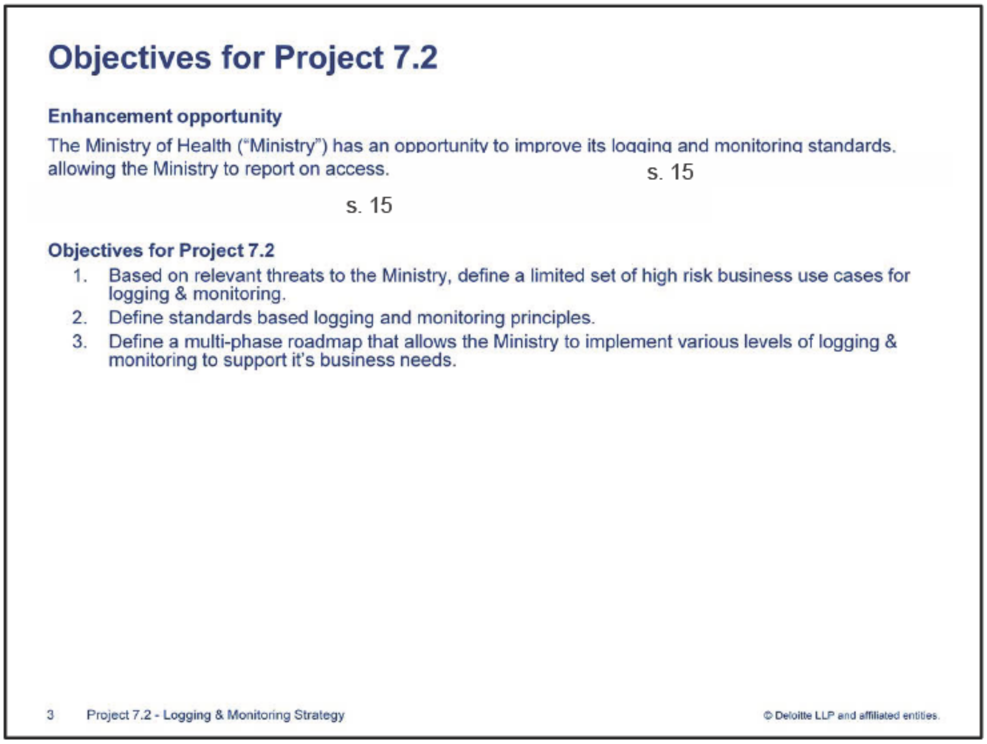
Roadmap
- Project Objective #3: Define roadmap
- Future state conceptual architecture
- Roadmap overview
- Roadmap details
- Deployment success factors
- Other considerations
- Summary & next steps

Additional Details
- Current State
- Policies and standards
- Operational Model Considerations

- Click to edit Master text styles
  - Second level
    - Third level
      - Fourth level



Introduction



Objectives for Project 7.2

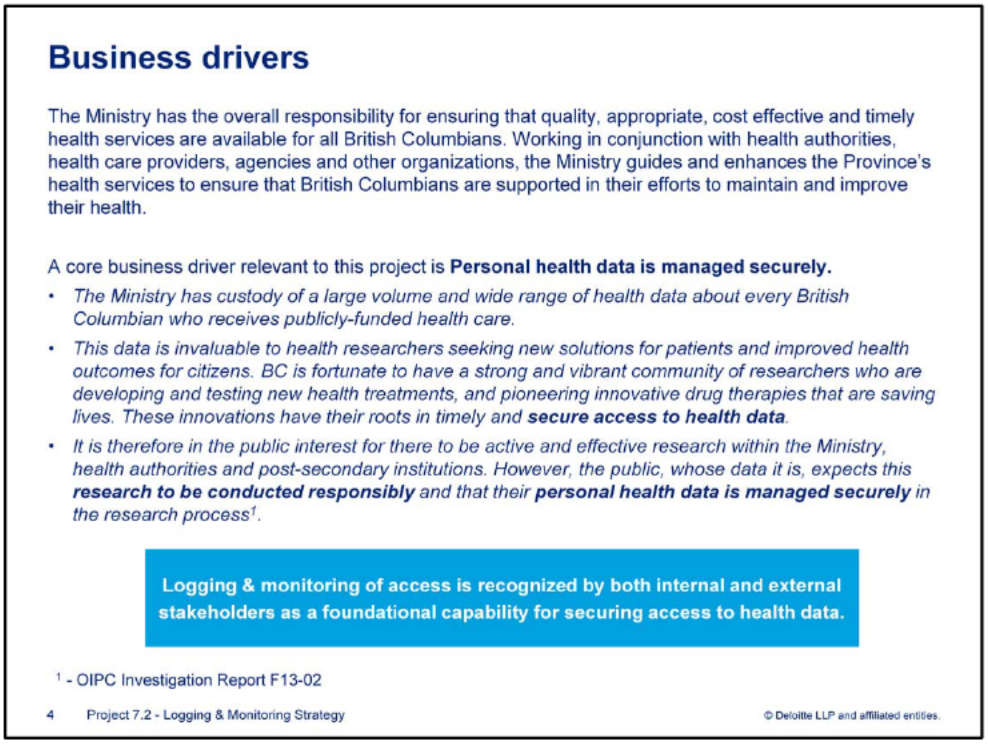
Enhancement opportunity

The Ministry of Health ("Ministry") has an opportunity to improve its logging and monitoring standards, allowing the Ministry to report on access. [redacted] s. 15

[redacted] s. 15

Objectives for Project 7.2

1. Based on relevant threats to the Ministry, define a limited set of high risk business use cases for logging & monitoring.
2. Define standards based logging and monitoring principles.
3. Define a multi-phase roadmap that allows the Ministry to implement various levels of logging & monitoring to support it's business needs.



Business drivers

The Ministry has the overall responsibility for ensuring that quality, appropriate, cost effective and timely health services are available for all British Columbians. Working in conjunction with health authorities, health care providers, agencies and other organizations, the Ministry guides and enhances the Province's health services to ensure that British Columbians are supported in their efforts to maintain and improve their health.

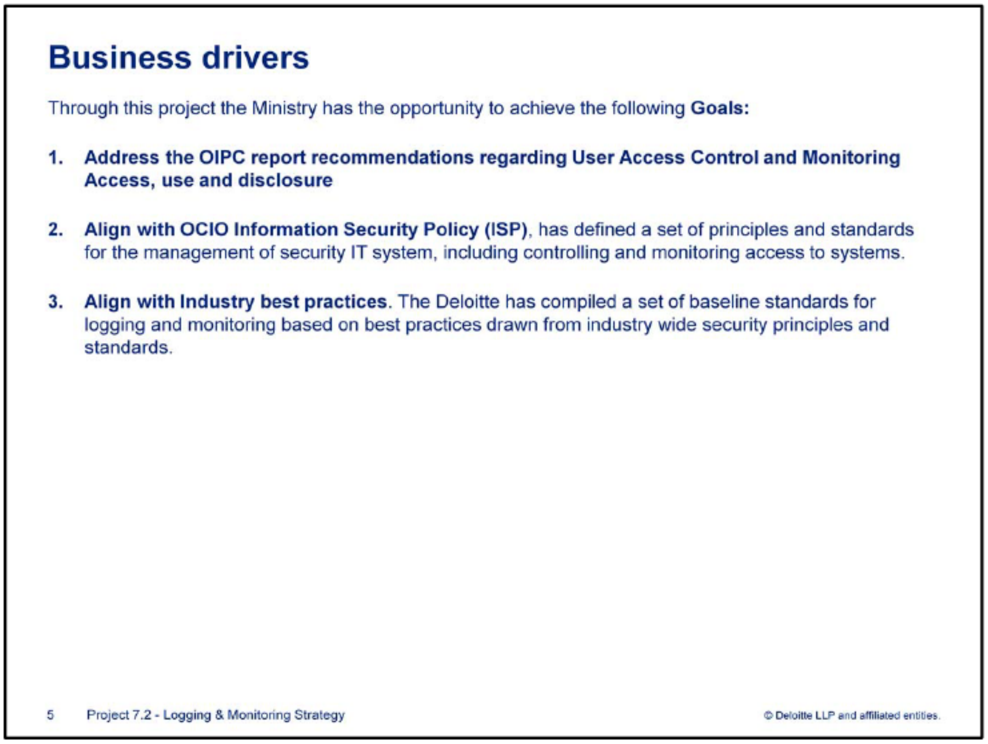
A core business driver relevant to this project is **Personal health data is managed securely.**

- *The Ministry has custody of a large volume and wide range of health data about every British Columbian who receives publicly-funded health care.*
- *This data is invaluable to health researchers seeking new solutions for patients and improved health outcomes for citizens. BC is fortunate to have a strong and vibrant community of researchers who are developing and testing new health treatments, and pioneering innovative drug therapies that are saving lives. These innovations have their roots in timely and **secure access to health data**.*
- *It is therefore in the public interest for there to be active and effective research within the Ministry, health authorities and post-secondary institutions. However, the public, whose data it is, expects this **research to be conducted responsibly** and that their **personal health data is managed securely** in the research process*[1].

Logging & monitoring of access is recognized by both internal and external stakeholders as a foundational capability for securing access to health data.

[1] - OIPC Investigation Report F13-02

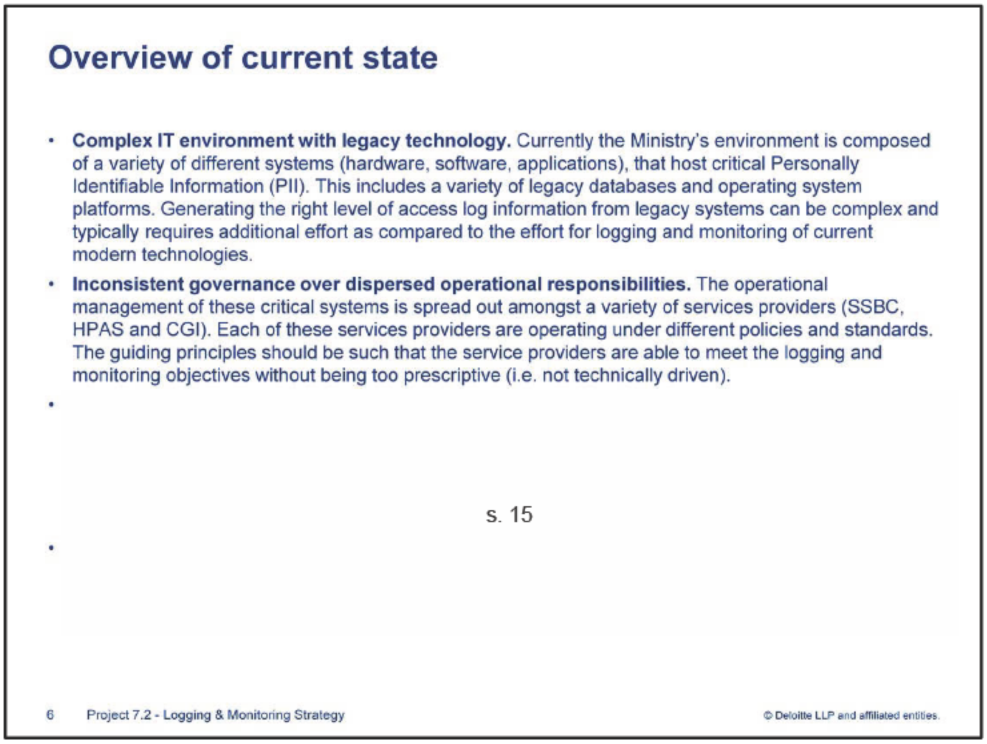
Everyone agrees LMR is necessary, the key question is “how much is enough?”



Business drivers

Through this project the Ministry has the opportunity to achieve the following **Goals:**

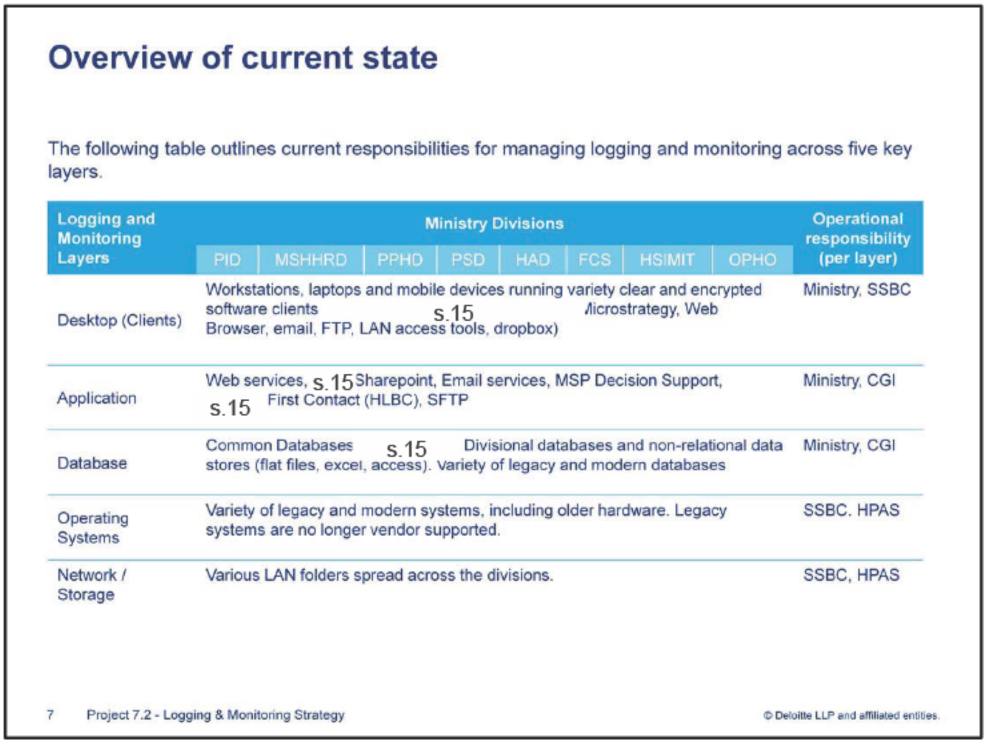
1. **Address the OIPC report recommendations regarding User Access Control and Monitoring Access, use and disclosure**
2. **Align with OCIO Information Security Policy (ISP)**, has defined a set of principles and standards for the management of security IT system, including controlling and monitoring access to systems.
3. **Align with Industry best practices**. The Deloitte has compiled a set of baseline standards for logging and monitoring based on best practices drawn from industry wide security principles and standards.



Overview of current state

- **Complex IT environment with legacy technology.** Currently the Ministry's environment is composed of a variety of different systems (hardware, software, applications), that host critical Personally Identifiable Information (PII). This includes a variety of legacy databases and operating system platforms. Generating the right level of access log information from legacy systems can be complex and typically requires additional effort as compared to the effort for logging and monitoring of current modern technologies.
- **Inconsistent governance over dispersed operational responsibilities.** The operational management of these critical systems is spread out amongst a variety of services providers (SSBC, HPAS and CGI). Each of these services providers are operating under different policies and standards. The guiding principles should be such that the service providers are able to meet the logging and monitoring objectives without being too prescriptive (i.e. not technically driven).

s. 15



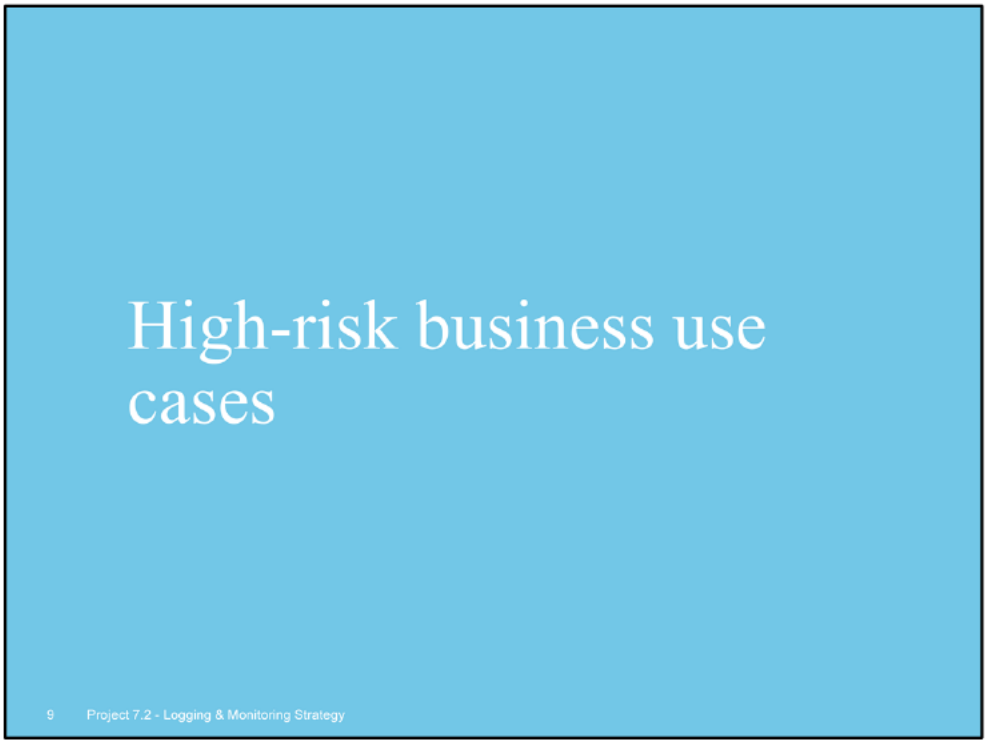
Overview of current state

The following table outlines current responsibilities for managing logging and monitoring across five key layers.

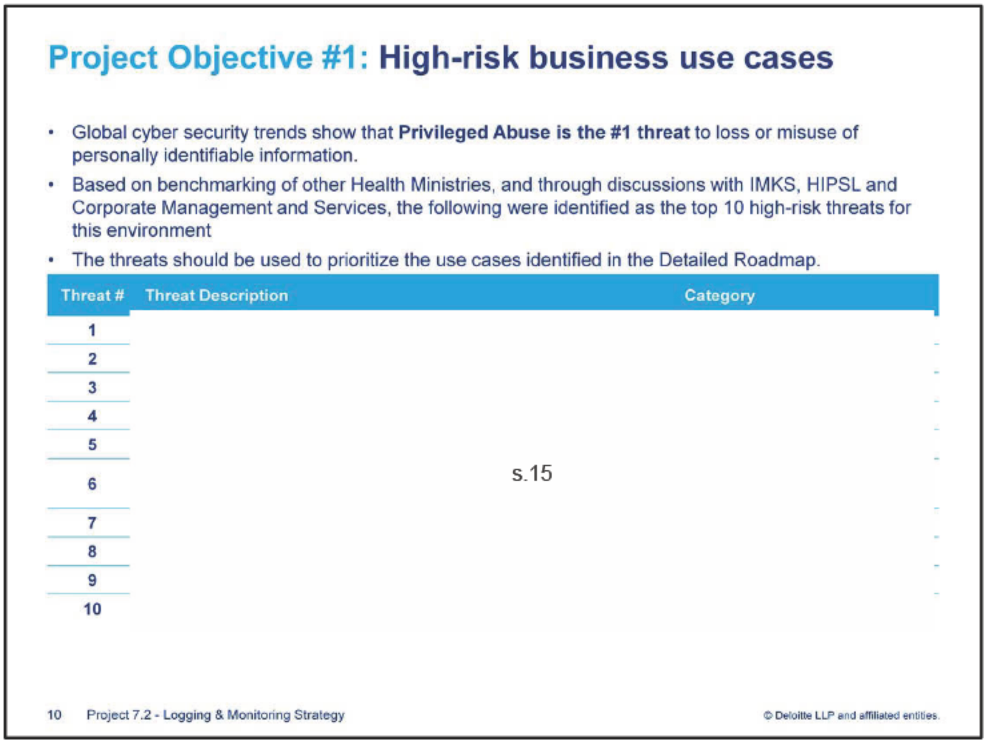
Logging and Monitoring Layers	Ministry Divisions								Operational responsibility (per layer)
	PID	MSHHRD	PPHD	PSD	HAD	FCS	HSIMIT	OPHO	
Desktop (Clients)	Workstations, laptops and mobile devices running variety clear and encrypted software clients s.15 /licrostrategy, Web Browser, email, FTP, LAN access tools, dropbox)								Ministry, SSBC
Application	Web services, s.15 Sharepoint, Email services, MSP Decision Support, s.15 First Contact (HLBC), SFTP								Ministry, CGI
Database	Common Databases s.15 Divisional databases and non-relational data stores (flat files, excel, access). Variety of legacy and modern databases								Ministry, CGI
Operating Systems	Variety of legacy and modern systems, including older hardware. Legacy systems are no longer vendor supported.								SSBC. HPAS
Network / Storage	Various LAN folders spread across the divisions.								SSBC, HPAS

Summary of results

8 Project 7.2 - Logging & Monitoring Strategy



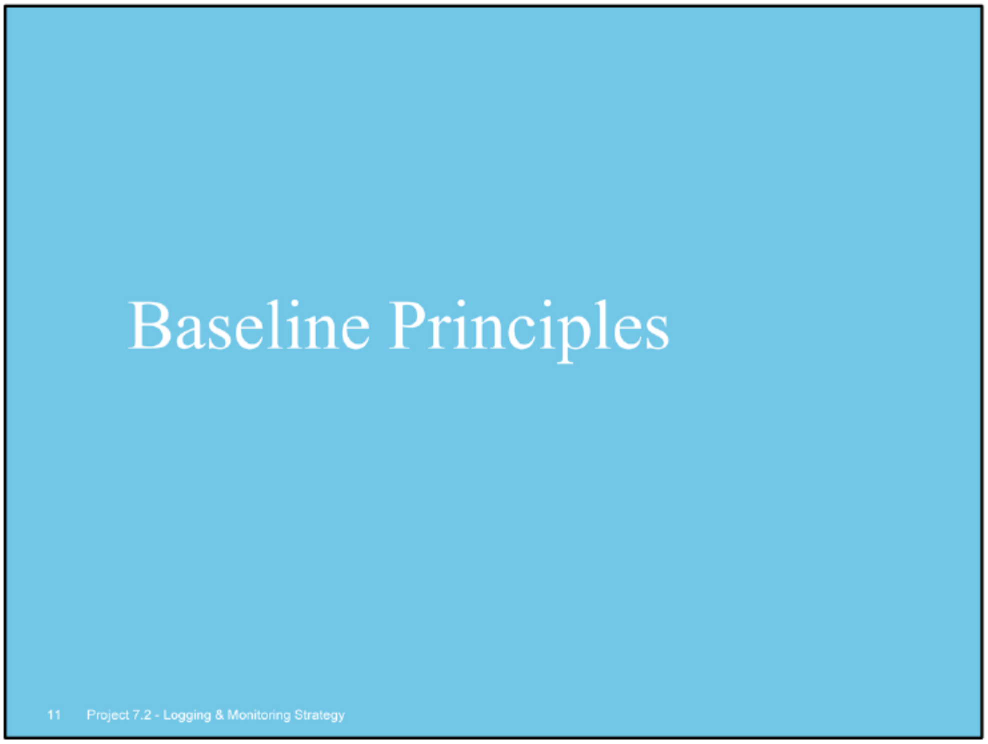
High-risk business use cases



Project Objective #1: High-risk business use cases

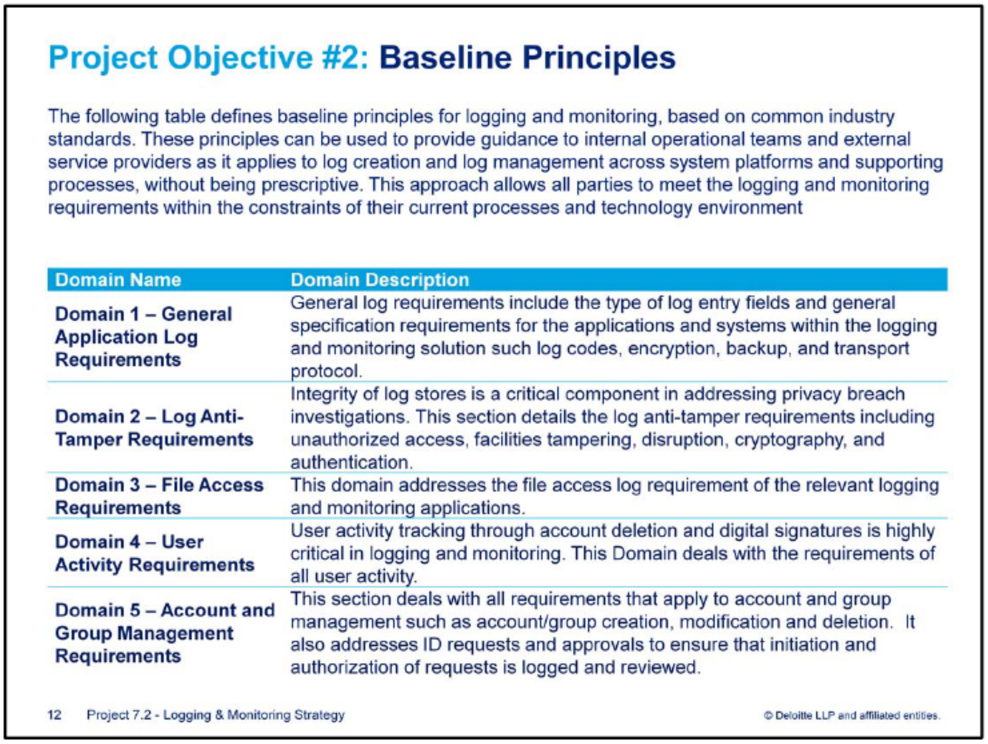
- Global cyber security trends show that **Privileged Abuse is the #1 threat** to loss or misuse of personally identifiable information.
- Based on benchmarking of other Health Ministries, and through discussions with IMKS, HIPSL and Corporate Management and Services, the following were identified as the top 10 high-risk threats for this environment
- The threats should be used to prioritize the use cases identified in the Detailed Roadmap.

Threat #	Threat Description	Category
1		
2		
3		
4		
5		
6	s.15	
7		
8		
9		
10		



Baseline Principles

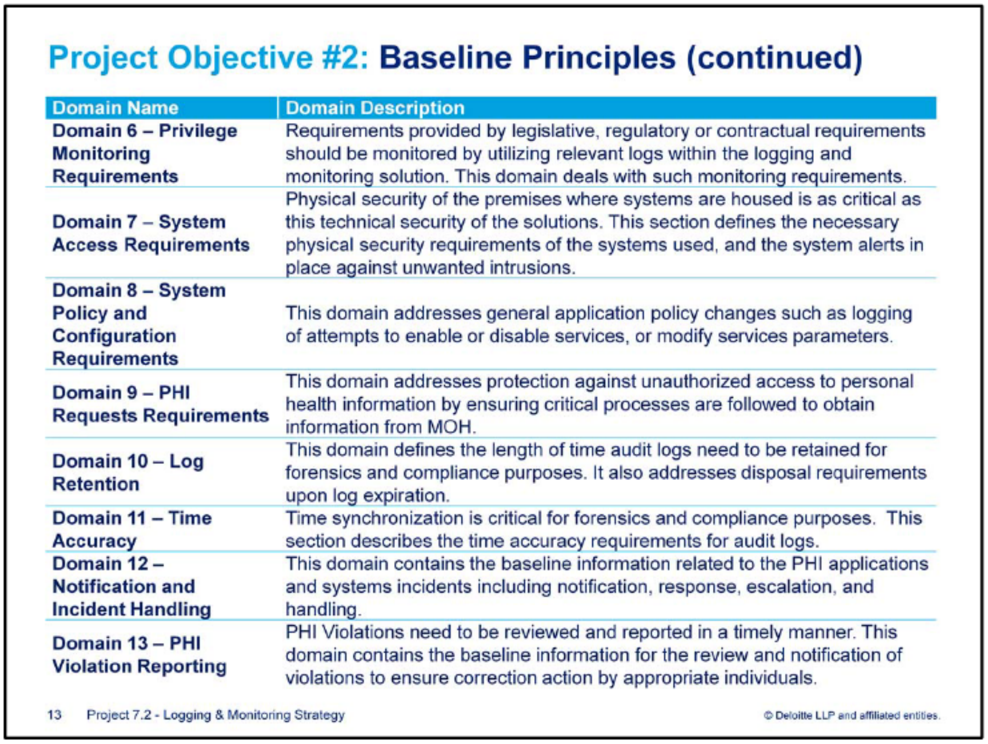
11 Project 7.2 - Logging & Monitoring Strategy



Project Objective #2: Baseline Principles

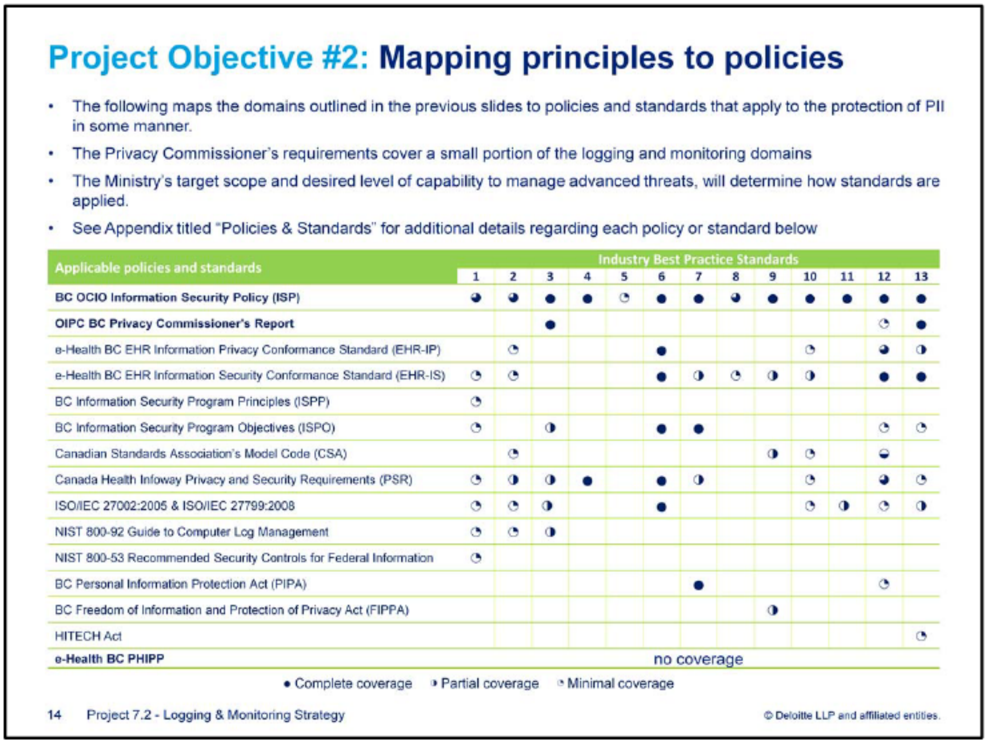
The following table defines baseline principles for logging and monitoring, based on common industry standards. These principles can be used to provide guidance to internal operational teams and external service providers as it applies to log creation and log management across system platforms and supporting processes, without being prescriptive. This approach allows all parties to meet the logging and monitoring requirements within the constraints of their current processes and technology environment

Domain Name	Domain Description
Domain 1 – General Application Log Requirements	General log requirements include the type of log entry fields and general specification requirements for the applications and systems within the logging and monitoring solution such log codes, encryption, backup, and transport protocol.
Domain 2 – Log Anti-Tamper Requirements	Integrity of log stores is a critical component in addressing privacy breach investigations. This section details the log anti-tamper requirements including unauthorized access, facilities tampering, disruption, cryptography, and authentication.
Domain 3 – File Access Requirements	This domain addresses the file access log requirement of the relevant logging and monitoring applications.
Domain 4 – User Activity Requirements	User activity tracking through account deletion and digital signatures is highly critical in logging and monitoring. This Domain deals with the requirements of all user activity.
Domain 5 – Account and Group Management Requirements	This section deals with all requirements that apply to account and group management such as account/group creation, modification and deletion. It also addresses ID requests and approvals to ensure that initiation and authorization of requests is logged and reviewed.



Project Objective #2: Baseline Principles (continued)

Domain Name	Domain Description
Domain 6 – Privilege Monitoring Requirements	Requirements provided by legislative, regulatory or contractual requirements should be monitored by utilizing relevant logs within the logging and monitoring solution. This domain deals with such monitoring requirements.
Domain 7 – System Access Requirements	Physical security of the premises where systems are housed is as critical as this technical security of the solutions. This section defines the necessary physical security requirements of the systems used, and the system alerts in place against unwanted intrusions.
Domain 8 – System Policy and Configuration Requirements	This domain addresses general application policy changes such as logging of attempts to enable or disable services, or modify services parameters.
Domain 9 – PHI Requests Requirements	This domain addresses protection against unauthorized access to personal health information by ensuring critical processes are followed to obtain information from MOH.
Domain 10 – Log Retention	This domain defines the length of time audit logs need to be retained for forensics and compliance purposes. It also addresses disposal requirements upon log expiration.
Domain 11 – Time Accuracy	Time synchronization is critical for forensics and compliance purposes. This section describes the time accuracy requirements for audit logs.
Domain 12 – Notification and Incident Handling	This domain contains the baseline information related to the PHI applications and systems incidents including notification, response, escalation, and handling.
Domain 13 – PHI Violation Reporting	PHI Violations need to be reviewed and reported in a timely manner. This domain contains the baseline information for the review and notification of violations to ensure correction action by appropriate individuals.



Project Objective #2: Mapping principles to policies

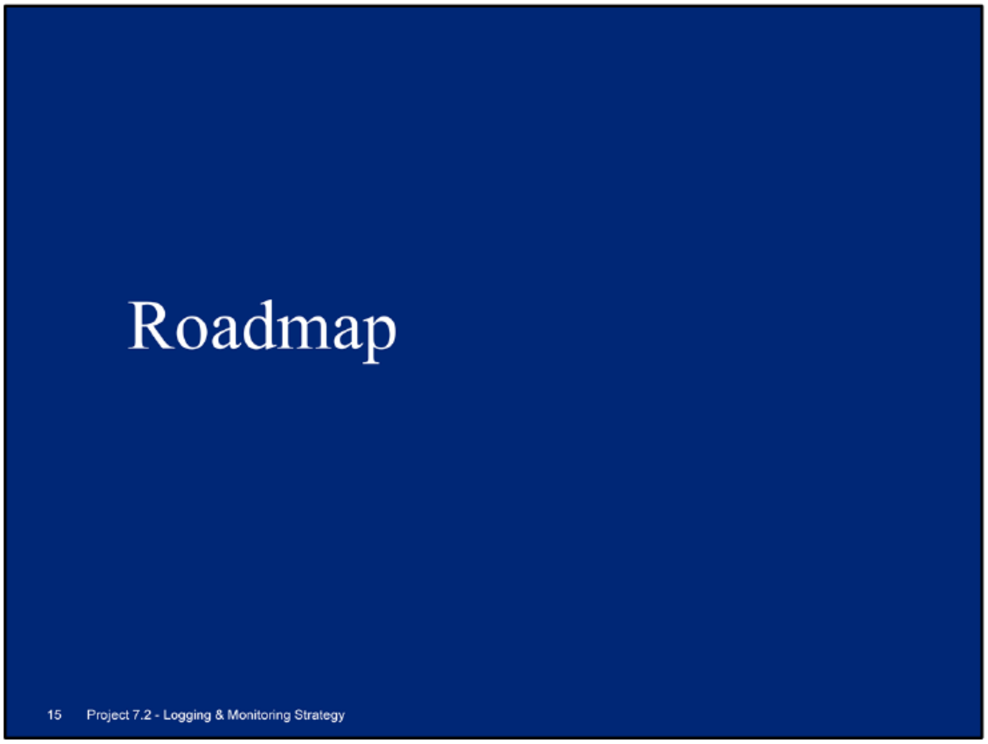
- The following maps the domains outlined in the previous slides to policies and standards that apply to the protection of PII in some manner.
- The Privacy Commissioner's requirements cover a small portion of the logging and monitoring domains
- The Ministry's target scope and desired level of capability to manage advanced threats, will determine how standards are applied.
- See Appendix titled "Policies & Standards" for additional details regarding each policy or standard below

Applicable policies and standards	Industry Best Practice Standards												
	1	2	3	4	5	6	7	8	9	10	11	12	13
BC OCIO Information Security Policy (ISP)	◕	◕	●	●	◔	●	●	◕	●	●	●	●	●
OIPC BC Privacy Commissioner's Report			●									◔	●
e-Health BC EHR Information Privacy Conformance Standard (EHR-IP)		◔				●				◔		◕	◑
e-Health BC EHR Information Security Conformance Standard (EHR-IS)	◔	◔				●	◑	◔	◑	◑		●	●
BC Information Security Program Principles (ISPP)	◔												
BC Information Security Program Objectives (ISPO)	◔		◑			●	●					◔	◔
Canadian Standards Association's Model Code (CSA)		◔							◑	◔		◒	
Canada Health Infoway Privacy and Security Requirements (PSR)	◔	◑	◑	●		●	◑			◔		◕	◔
ISO/IEC 27002:2005 & ISO/IEC 27799:2008	◔	◔	◑			●				◔	◑	◔	◑
NIST 800-92 Guide to Computer Log Management	◔	◔	◑										
NIST 800-53 Recommended Security Controls for Federal Information	◔												
BC Personal Information Protection Act (PIPA)							●					◔	
BC Freedom of Information and Protection of Privacy Act (FIPPA)									◑				
HITECH Act													◔
e-Health BC PHIPP	no coverage												

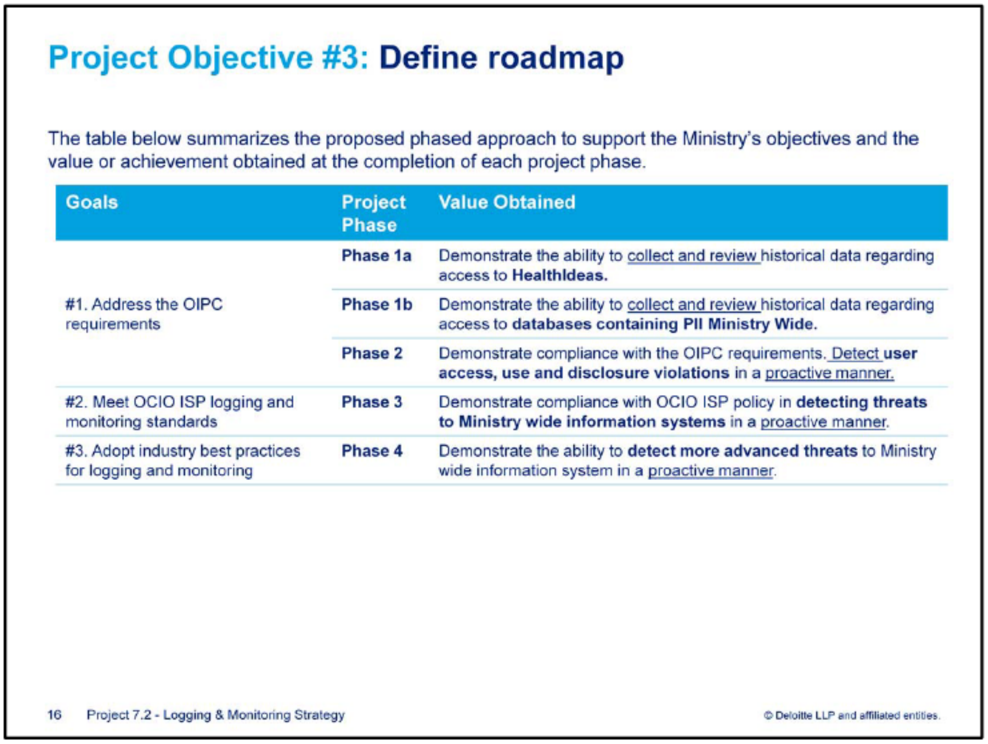
● Complete coverage ◑ Partial coverage ◔ Minimal coverage

14 Project 7.2 - Logging & Monitoring Strategy © Deloitte LLP and affiliated entities.

Policies form the basis of your requirements for logging and monitoring (the other is looking at the risks/threats). These help to identify "how much is enough". Conclusion is that there is a significant gap between the current state and ISP and OIPC requirements. Further, the OIPC only covers a subset of the ISP – opportunity to take a prioritized, small step to reach compliance.



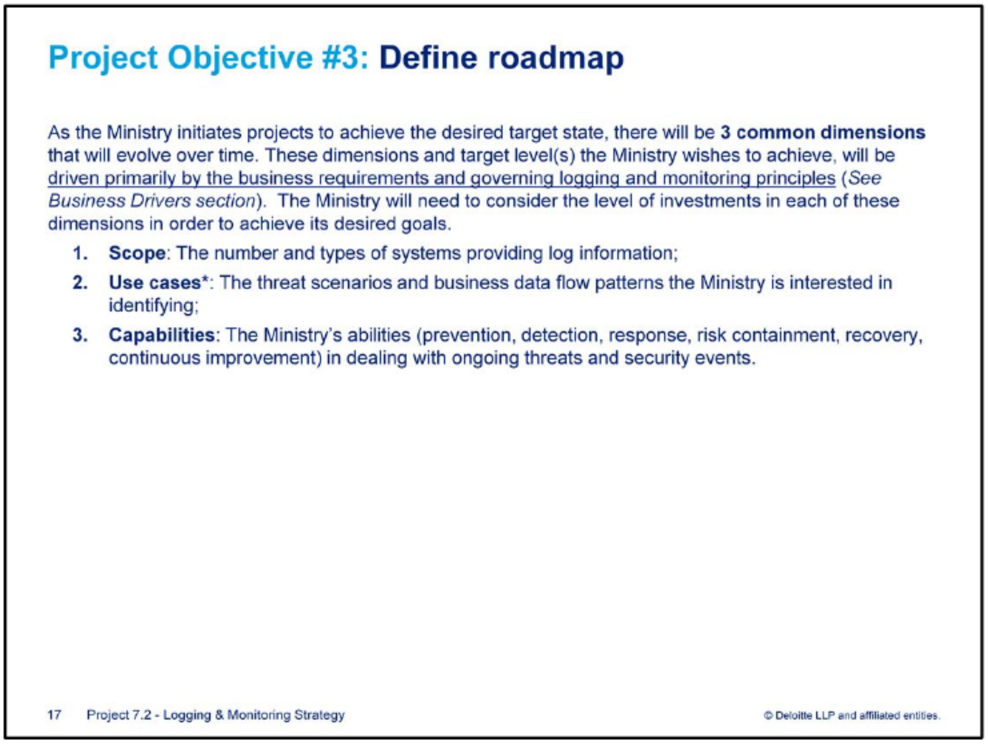
Roadmap



Project Objective #3: Define roadmap

The table below summarizes the proposed phased approach to support the Ministry's objectives and the value or achievement obtained at the completion of each project phase.

Goals	Project Phase	Value Obtained
#1. Address the OIPC requirements	**Phase 1a**	Demonstrate the ability to collect and review historical data regarding access to **HealthIdeas.**
	Phase 1b	Demonstrate the ability to collect and review historical data regarding access to **databases containing PII Ministry Wide.**
	Phase 2	Demonstrate compliance with the OIPC requirements. Detect **user access, use and disclosure violations** in a proactive manner.
#2. Meet OCIO ISP logging and monitoring standards	**Phase 3**	Demonstrate compliance with OCIO ISP policy in **detecting threats to Ministry wide information systems** in a proactive manner.
#3. Adopt industry best practices for logging and monitoring	**Phase 4**	Demonstrate the ability to **detect more advanced threats** to Ministry wide information system in a proactive manner.



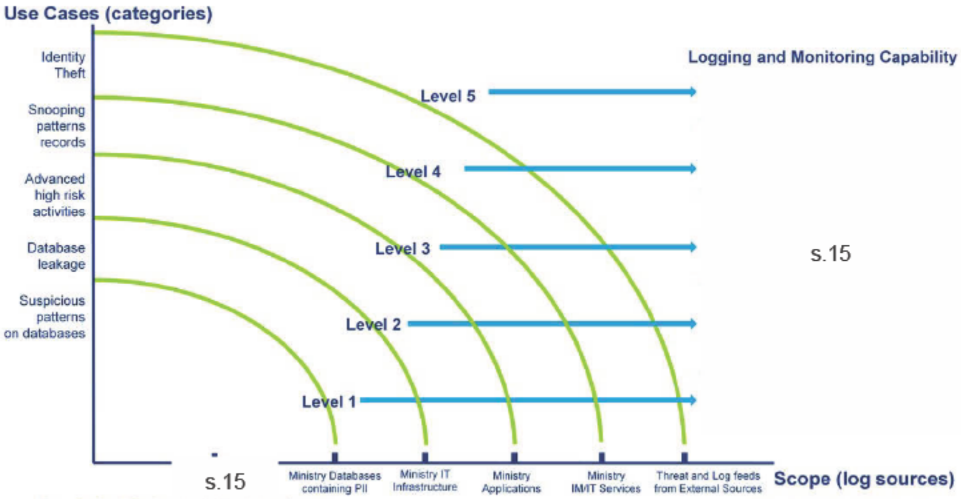
Project Objective #3: Define roadmap

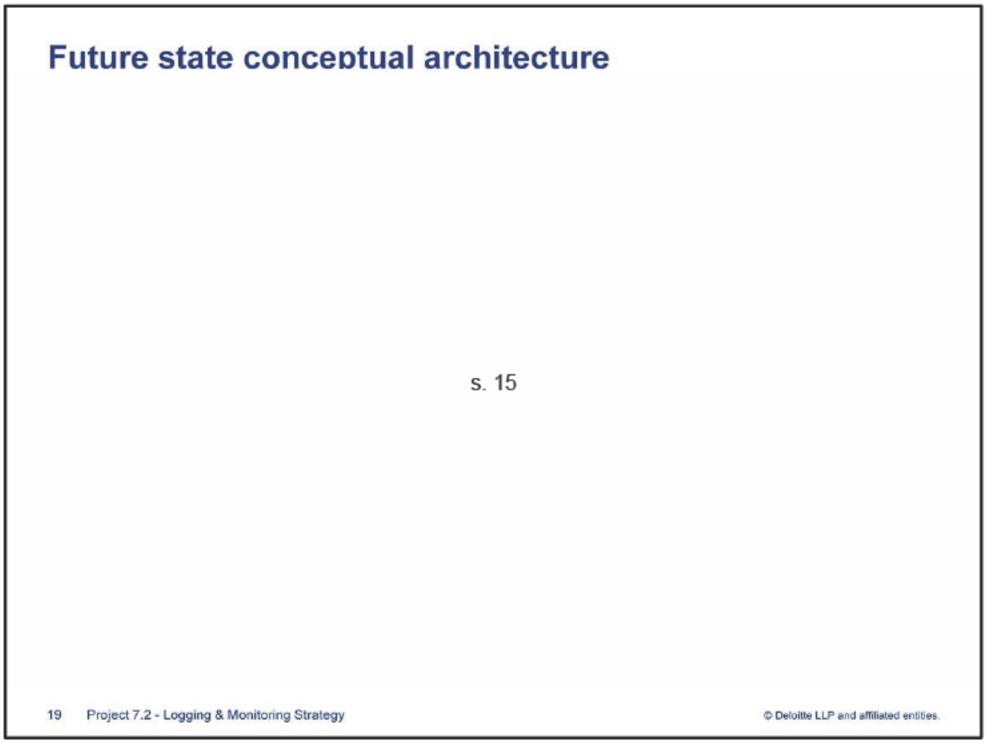
As the Ministry initiates projects to achieve the desired target state, there will be **3 common dimensions** that will evolve over time. These dimensions and target level(s) the Ministry wishes to achieve, will be driven primarily by the business requirements and governing logging and monitoring principles (*See Business Drivers section*). The Ministry will need to consider the level of investments in each of these dimensions in order to achieve its desired goals.

1. **Scope**: The number and types of systems providing log information;
2. **Use cases***: The threat scenarios and business data flow patterns the Ministry is interested in identifying;
3. **Capabilities**: The Ministry's abilities (prevention, detection, response, risk containment, recovery, continuous improvement) in dealing with ongoing threats and security events.

Project Objective #3: Define roadmap

The graph illustrates how increasing the **Scope** of systems and processes monitored (X-axis) and developing higher value sets of **Use Cases** (Y-axis), will direct the Ministry in achieving the desired target Logging and Monitoring level and build **Capability** over time. *Level 5 is included for illustrative purposes to demonstrate world-class capabilities targeted by organizations in highly regulated industries, and is not necessarily suggested as a target for the Ministry.*


Use Cases (categories)
Identity Theft
Snooping patterns records
Advanced high risk activities
Database leakage
Suspicious patterns on databases
Logging and Monitoring Capability
Level 5
Level 4
Level 3
Level 2
Level 1
s.15
s.15
Ministry Databases containing PII
Ministry IT Infrastructure
Ministry Applications
Ministry IM/IT Services
Threat and Log feeds from External Sources
Scope (log sources)

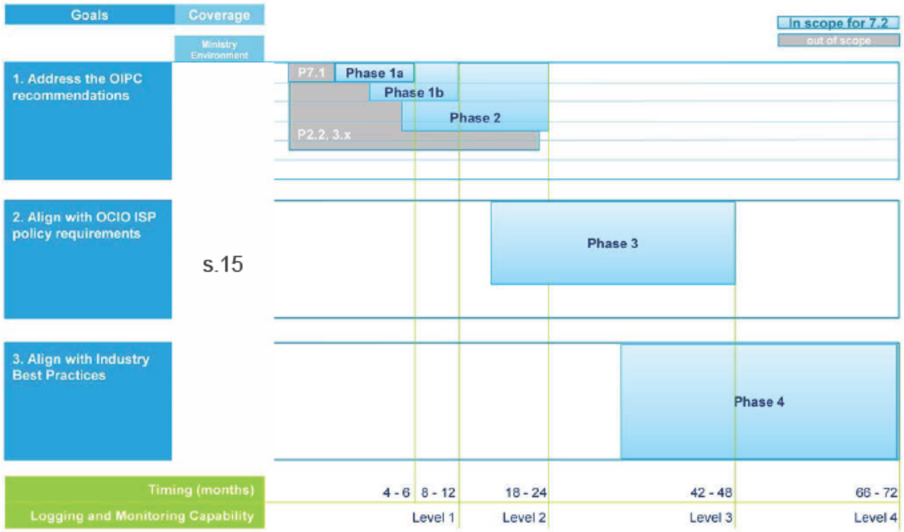


Future state conceptual architecture

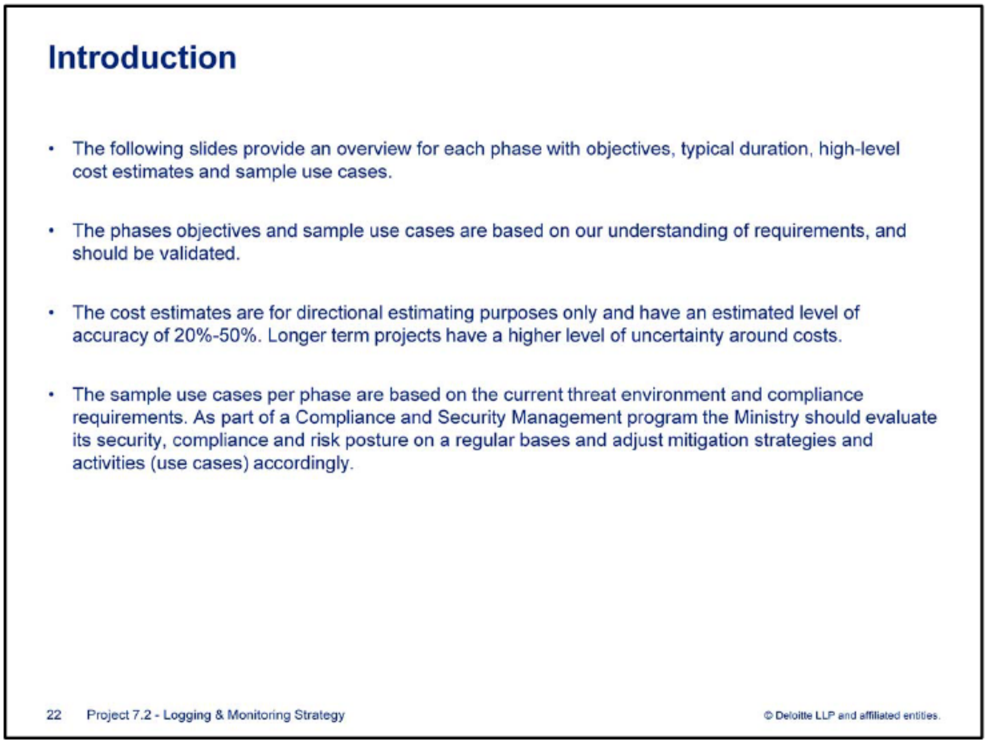
s. 15

Roadmap overview

The graph below illustrates the proposed method for achieving the project goals. Logging and monitoring capability levels indicate the sophistication of the Ministry's cyber threat management processes. These are defined on the next slide.



Roadmap details



Introduction

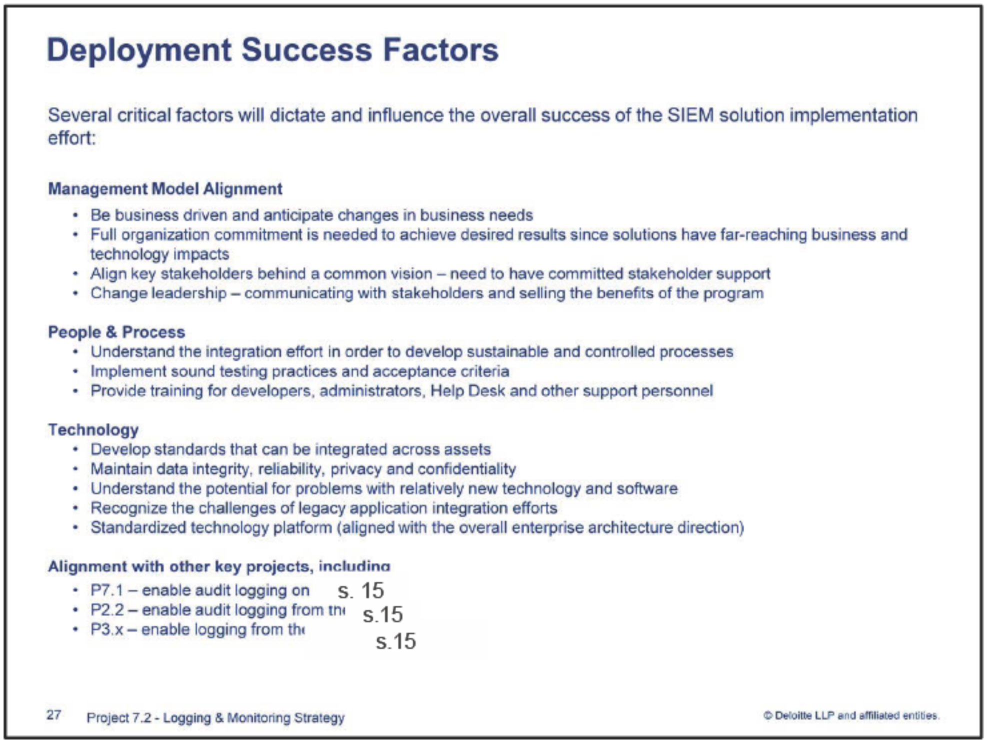
- The following slides provide an overview for each phase with objectives, typical duration, high-level cost estimates and sample use cases.

- The phases objectives and sample use cases are based on our understanding of requirements, and should be validated.

- The cost estimates are for directional estimating purposes only and have an estimated level of accuracy of 20%-50%. Longer term projects have a higher level of uncertainty around costs.

- The sample use cases per phase are based on the current threat environment and compliance requirements. As part of a Compliance and Security Management program the Ministry should evaluate its security, compliance and risk posture on a regular bases and adjust mitigation strategies and activities (use cases) accordingly.

Pages 139 through 142 redacted for the following reasons:
- -
s.15, s.21



Deployment Success Factors

Several critical factors will dictate and influence the overall success of the SIEM solution implementation effort:

Management Model Alignment

- Be business driven and anticipate changes in business needs
- Full organization commitment is needed to achieve desired results since solutions have far-reaching business and technology impacts
- Align key stakeholders behind a common vision – need to have committed stakeholder support
- Change leadership – communicating with stakeholders and selling the benefits of the program

People & Process

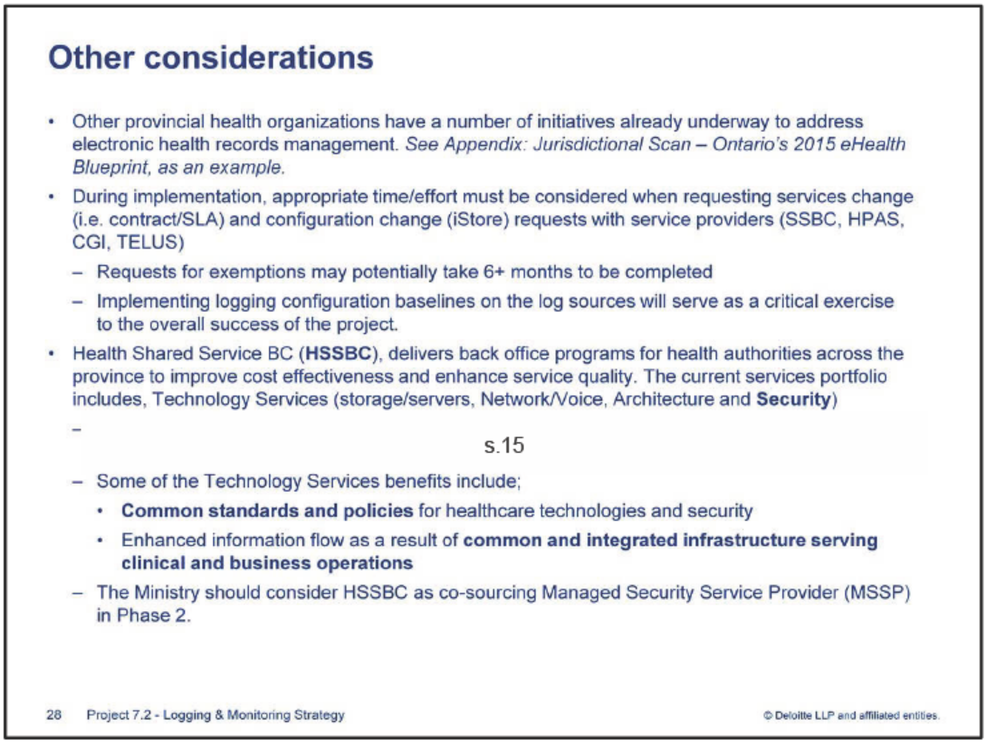
- Understand the integration effort in order to develop sustainable and controlled processes
- Implement sound testing practices and acceptance criteria
- Provide training for developers, administrators, Help Desk and other support personnel

Technology

- Develop standards that can be integrated across assets
- Maintain data integrity, reliability, privacy and confidentiality
- Understand the potential for problems with relatively new technology and software
- Recognize the challenges of legacy application integration efforts
- Standardized technology platform (aligned with the overall enterprise architecture direction)

Alignment with other key projects, including

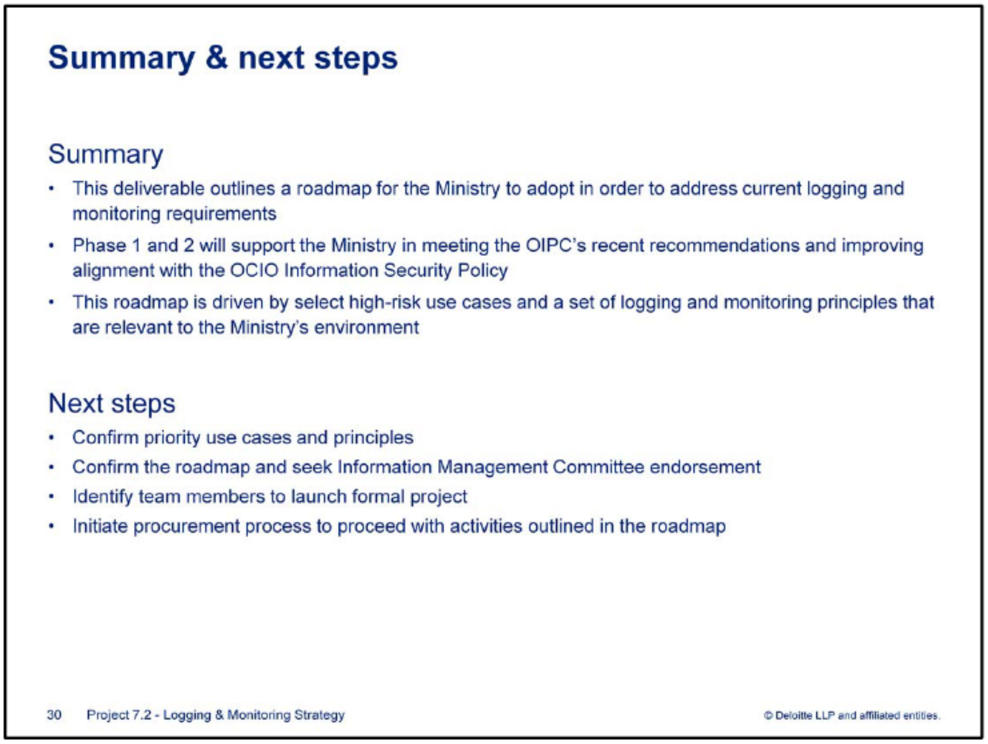
- P7.1 – enable audit logging on s. 15
- P2.2 – enable audit logging from th s.15
- P3.x – enable logging from th s.15



Other considerations

- Other provincial health organizations have a number of initiatives already underway to address electronic health records management. *See Appendix: Jurisdictional Scan – Ontario's 2015 eHealth Blueprint, as an example.*
- During implementation, appropriate time/effort must be considered when requesting services change (i.e. contract/SLA) and configuration change (iStore) requests with service providers (SSBC, HPAS, CGI, TELUS)
  - Requests for exemptions may potentially take 6+ months to be completed
  - Implementing logging configuration baselines on the log sources will serve as a critical exercise to the overall success of the project.
- Health Shared Service BC (**HSSBC**), delivers back office programs for health authorities across the province to improve cost effectiveness and enhance service quality. The current services portfolio includes, Technology Services (storage/servers, Network/Voice, Architecture and **Security**)
  - s.15
  - Some of the Technology Services benefits include;
    - **Common standards and policies** for healthcare technologies and security
    - Enhanced information flow as a result of **common and integrated infrastructure serving clinical and business operations**
  - The Ministry should consider HSSBC as co-sourcing Managed Security Service Provider (MSSP) in Phase 2.

Summary & next steps



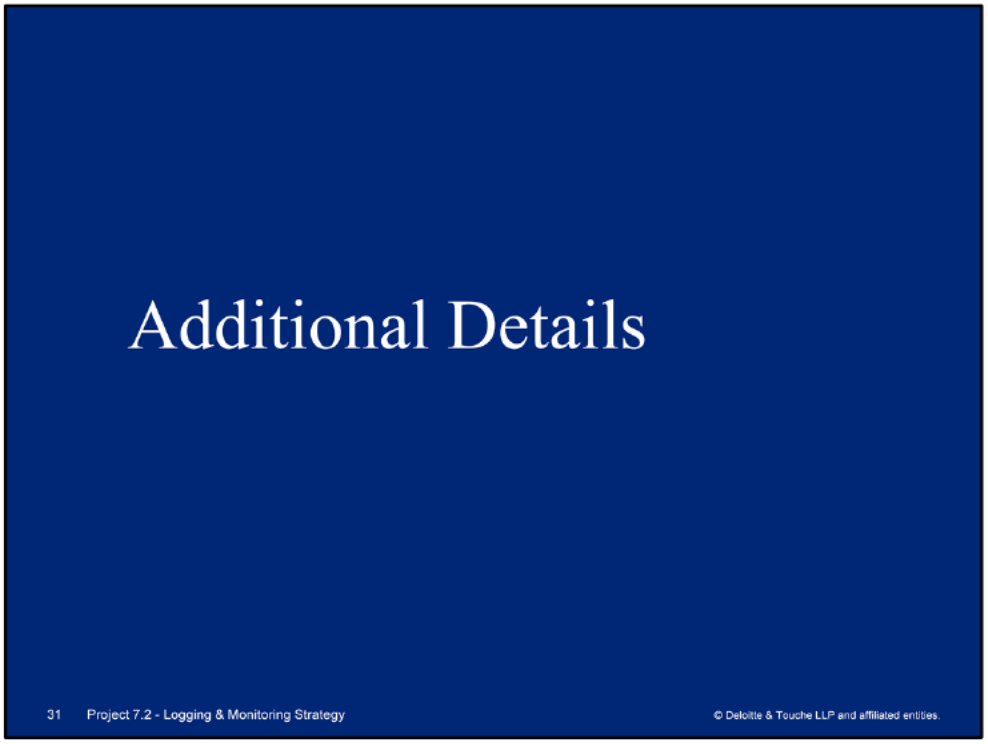
Summary & next steps

Summary

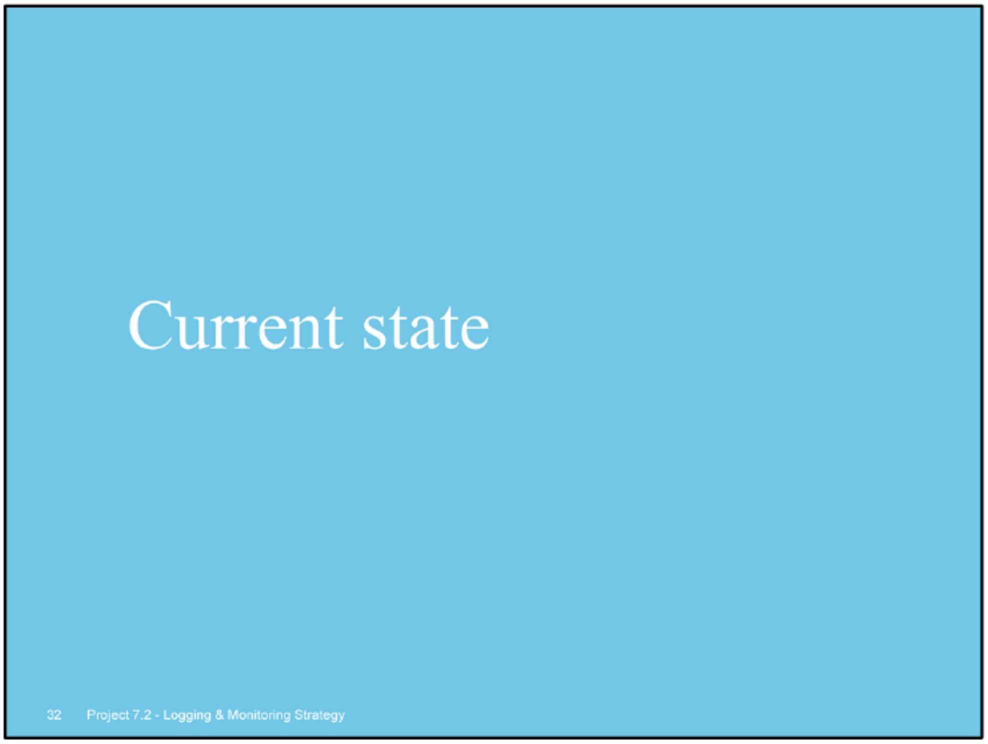
- This deliverable outlines a roadmap for the Ministry to adopt in order to address current logging and monitoring requirements
- Phase 1 and 2 will support the Ministry in meeting the OIPC's recent recommendations and improving alignment with the OCIO Information Security Policy
- This roadmap is driven by select high-risk use cases and a set of logging and monitoring principles that are relevant to the Ministry's environment

Next steps

- Confirm priority use cases and principles
- Confirm the roadmap and seek Information Management Committee endorsement
- Identify team members to launch formal project
- Initiate procurement process to proceed with activities outlined in the roadmap

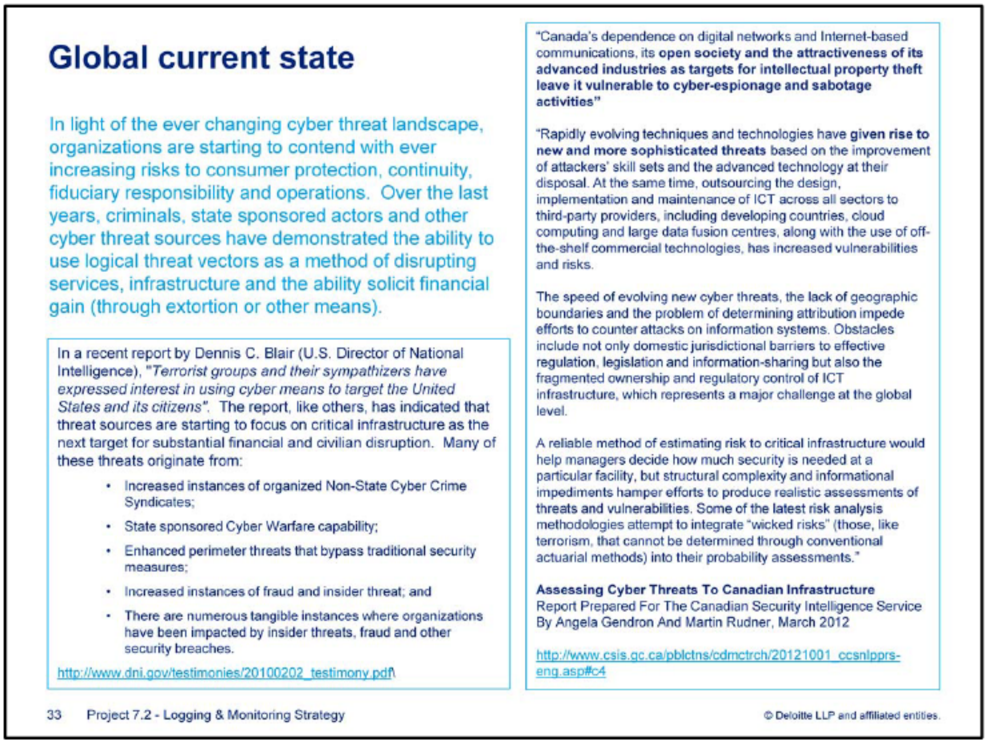


Additional Details



Current state

32 Project 7.2 - Logging & Monitoring Strategy



Global current state

In light of the ever changing cyber threat landscape, organizations are starting to contend with ever increasing risks to consumer protection, continuity, fiduciary responsibility and operations. Over the last years, criminals, state sponsored actors and other cyber threat sources have demonstrated the ability to use logical threat vectors as a method of disrupting services, infrastructure and the ability solicit financial gain (through extortion or other means).

In a recent report by Dennis C. Blair (U.S. Director of National Intelligence), "*Terrorist groups and their sympathizers have expressed interest in using cyber means to target the United States and its citizens*". The report, like others, has indicated that threat sources are starting to focus on critical infrastructure as the next target for substantial financial and civilian disruption. Many of these threats originate from:

- Increased instances of organized Non-State Cyber Crime Syndicates;
- State sponsored Cyber Warfare capability;
- Enhanced perimeter threats that bypass traditional security measures;
- Increased instances of fraud and insider threat; and
- There are numerous tangible instances where organizations have been impacted by insider threats, fraud and other security breaches.

http://www.dni.gov/testimonies/20100202_testimony.pdf\

"Canada's dependence on digital networks and Internet-based communications, its **open society and the attractiveness of its advanced industries as targets for intellectual property theft leave it vulnerable to cyber-espionage and sabotage activities"**

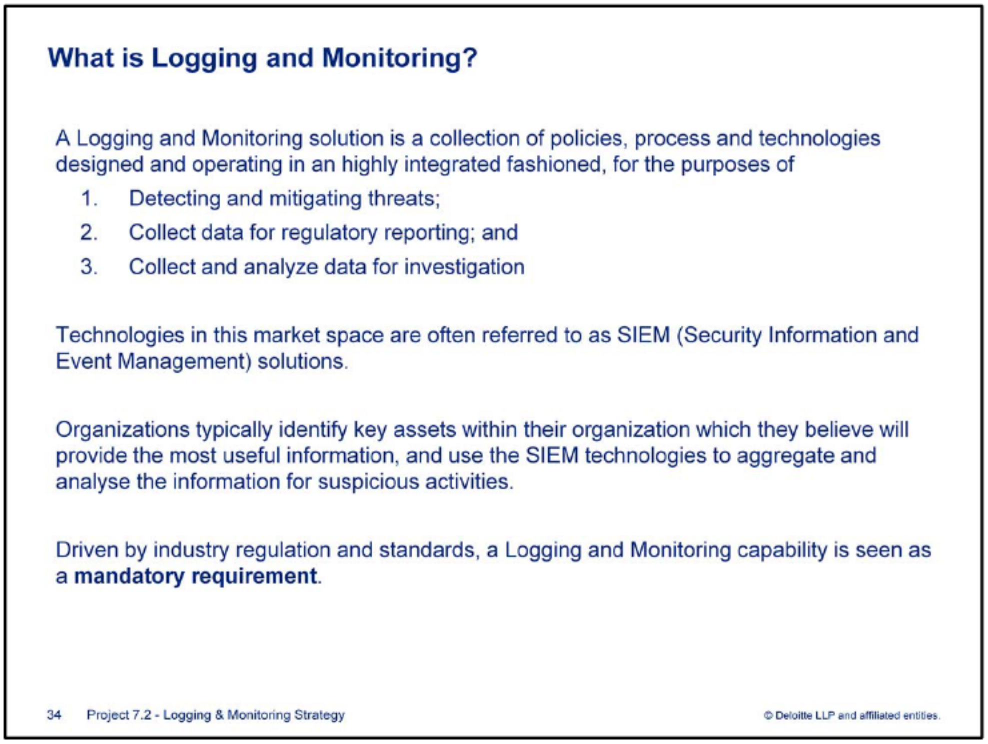
"Rapidly evolving techniques and technologies have **given rise to new and more sophisticated threats** based on the improvement of attackers' skill sets and the advanced technology at their disposal. At the same time, outsourcing the design, implementation and maintenance of ICT across all sectors to third-party providers, including developing countries, cloud computing and large data fusion centres, along with the use of off-the-shelf commercial technologies, has increased vulnerabilities and risks.

The speed of evolving new cyber threats, the lack of geographic boundaries and the problem of determining attribution impede efforts to counter attacks on information systems. Obstacles include not only domestic jurisdictional barriers to effective regulation, legislation and information-sharing but also the fragmented ownership and regulatory control of ICT infrastructure, which represents a major challenge at the global level.

A reliable method of estimating risk to critical infrastructure would help managers decide how much security is needed at a particular facility, but structural complexity and informational impediments hamper efforts to produce realistic assessments of threats and vulnerabilities. Some of the latest risk analysis methodologies attempt to integrate "wicked risks" (those, like terrorism, that cannot be determined through conventional actuarial methods) into their probability assessments."

Assessing Cyber Threats To Canadian Infrastructure
Report Prepared For The Canadian Security Intelligence Service
By Angela Gendron And Martin Rudner, March 2012

http://www.csis.gc.ca/pblctns/cdmctrch/20121001_ccsnlpprs-eng.asp#c4



What is Logging and Monitoring?

A Logging and Monitoring solution is a collection of policies, process and technologies designed and operating in an highly integrated fashioned, for the purposes of

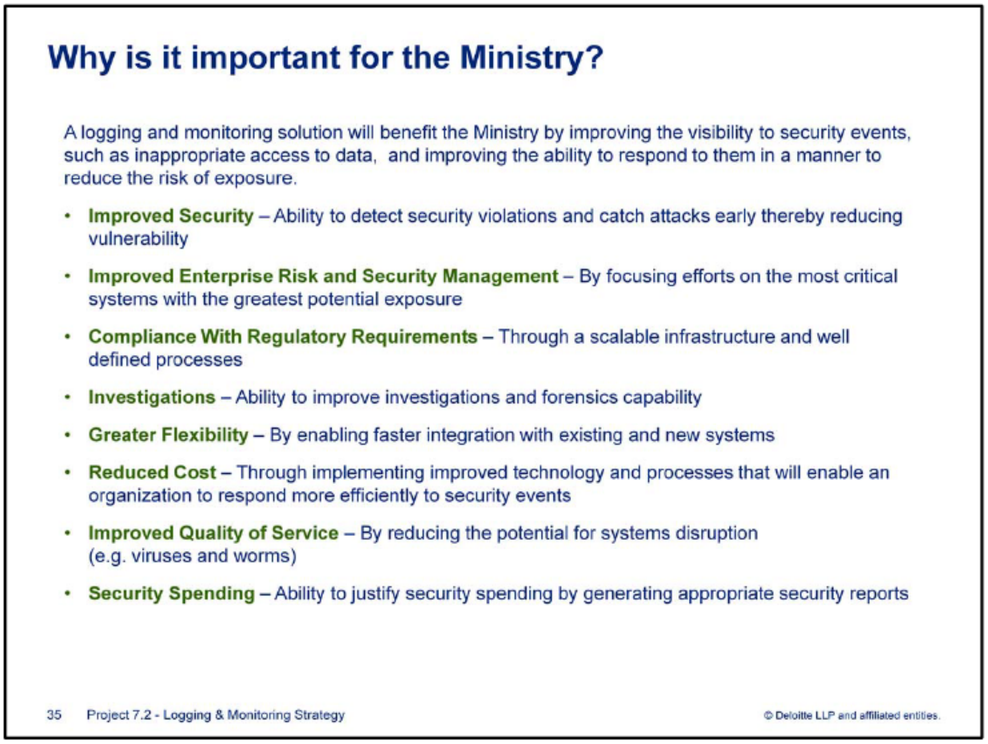
1. Detecting and mitigating threats;
2. Collect data for regulatory reporting; and
3. Collect and analyze data for investigation

Technologies in this market space are often referred to as SIEM (Security Information and Event Management) solutions.

Organizations typically identify key assets within their organization which they believe will provide the most useful information, and use the SIEM technologies to aggregate and analyse the information for suspicious activities.

Driven by industry regulation and standards, a Logging and Monitoring capability is seen as a **mandatory requirement**.

- Click to edit Master text styles
  - Second level
    - Third level
      - Fourth level

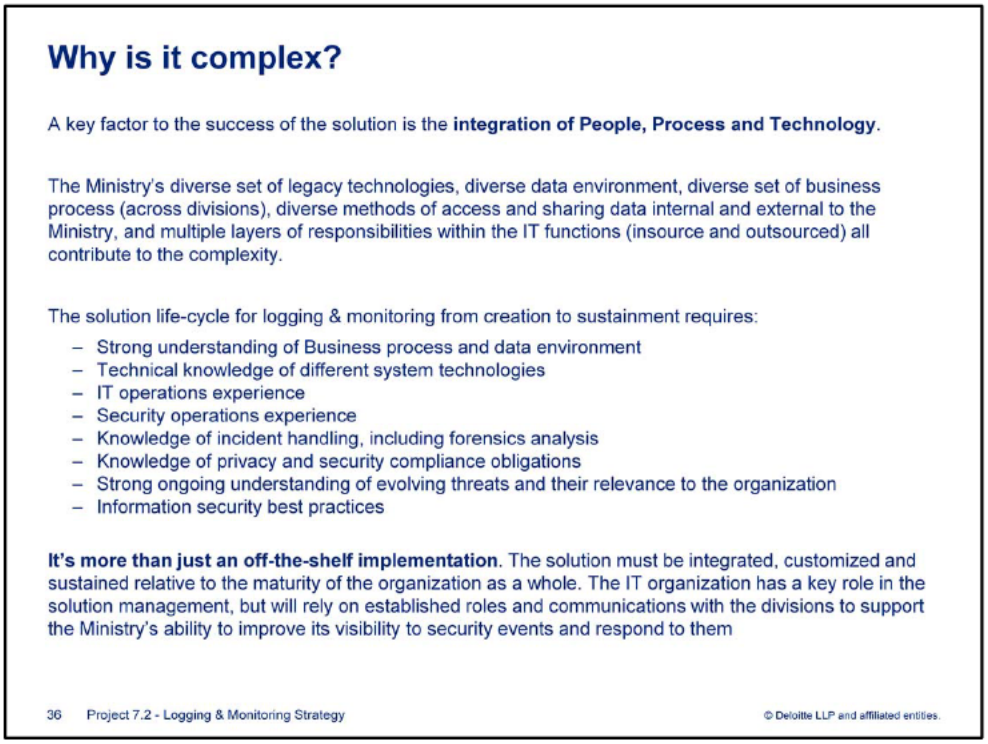


Why is it important for the Ministry?

A logging and monitoring solution will benefit the Ministry by improving the visibility to security events, such as inappropriate access to data, and improving the ability to respond to them in a manner to reduce the risk of exposure.

- **Improved Security** – Ability to detect security violations and catch attacks early thereby reducing vulnerability
- **Improved Enterprise Risk and Security Management** – By focusing efforts on the most critical systems with the greatest potential exposure
- **Compliance With Regulatory Requirements** – Through a scalable infrastructure and well defined processes
- **Investigations** – Ability to improve investigations and forensics capability
- **Greater Flexibility** – By enabling faster integration with existing and new systems
- **Reduced Cost** – Through implementing improved technology and processes that will enable an organization to respond more efficiently to security events
- **Improved Quality of Service** – By reducing the potential for systems disruption (e.g. viruses and worms)
- **Security Spending** – Ability to justify security spending by generating appropriate security reports

- Click to edit Master text styles
  - Second level
    - Third level
      - Fourth level



Why is it complex?

A key factor to the success of the solution is the **integration of People, Process and Technology**.

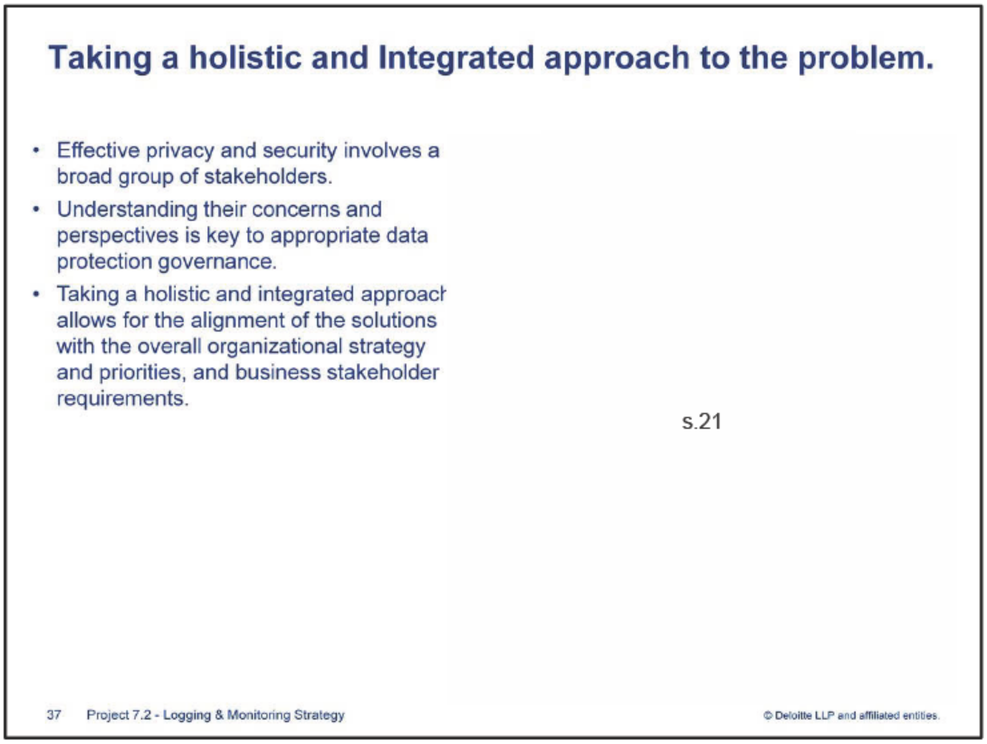
The Ministry's diverse set of legacy technologies, diverse data environment, diverse set of business process (across divisions), diverse methods of access and sharing data internal and external to the Ministry, and multiple layers of responsibilities within the IT functions (insource and outsourced) all contribute to the complexity.

The solution life-cycle for logging & monitoring from creation to sustainment requires:

- Strong understanding of Business process and data environment
- Technical knowledge of different system technologies
- IT operations experience
- Security operations experience
- Knowledge of incident handling, including forensics analysis
- Knowledge of privacy and security compliance obligations
- Strong ongoing understanding of evolving threats and their relevance to the organization
- Information security best practices

It's more than just an off-the-shelf implementation. The solution must be integrated, customized and sustained relative to the maturity of the organization as a whole. The IT organization has a key role in the solution management, but will rely on established roles and communications with the divisions to support the Ministry's ability to improve its visibility to security events and respond to them

- Click to edit Master text styles
  - Second level
    - Third level
      - Fourth level



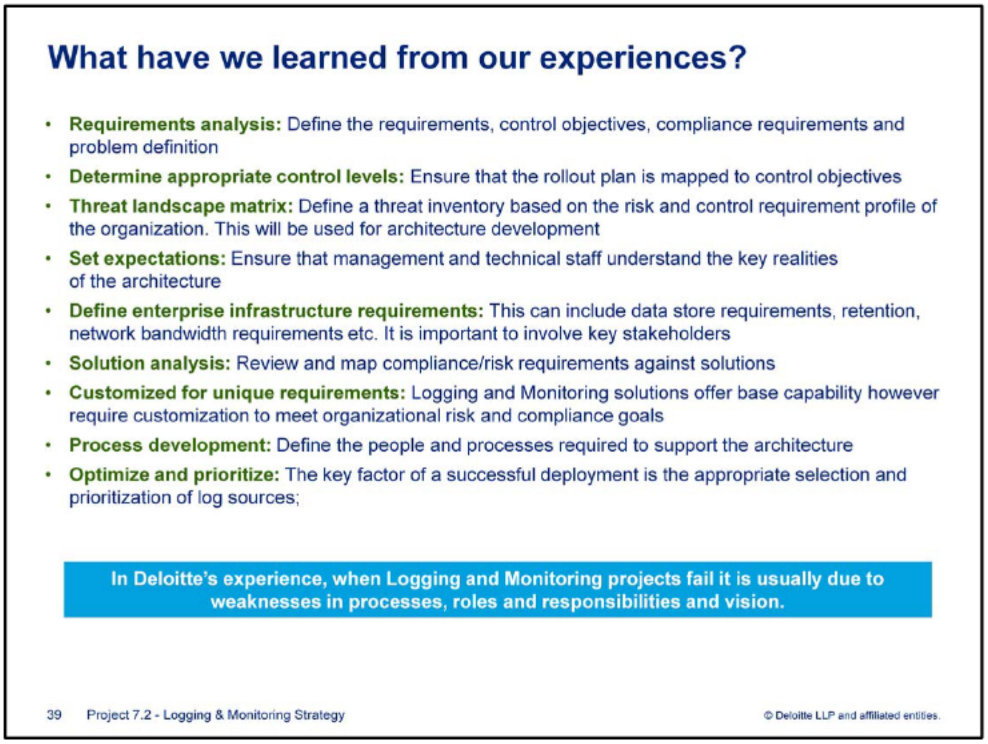
Taking a holistic and Integrated approach to the problem.

- Effective privacy and security involves a broad group of stakeholders.
- Understanding their concerns and perspectives is key to appropriate data protection governance.
- Taking a holistic and integrated approach allows for the alignment of the solutions with the overall organizational strategy and priorities, and business stakeholder requirements.

s.21

- Click to edit Master text styles
  - Second level
    - Third level
      - Fourth level

Page 154 redacted for the following reason:
- -
s. 15

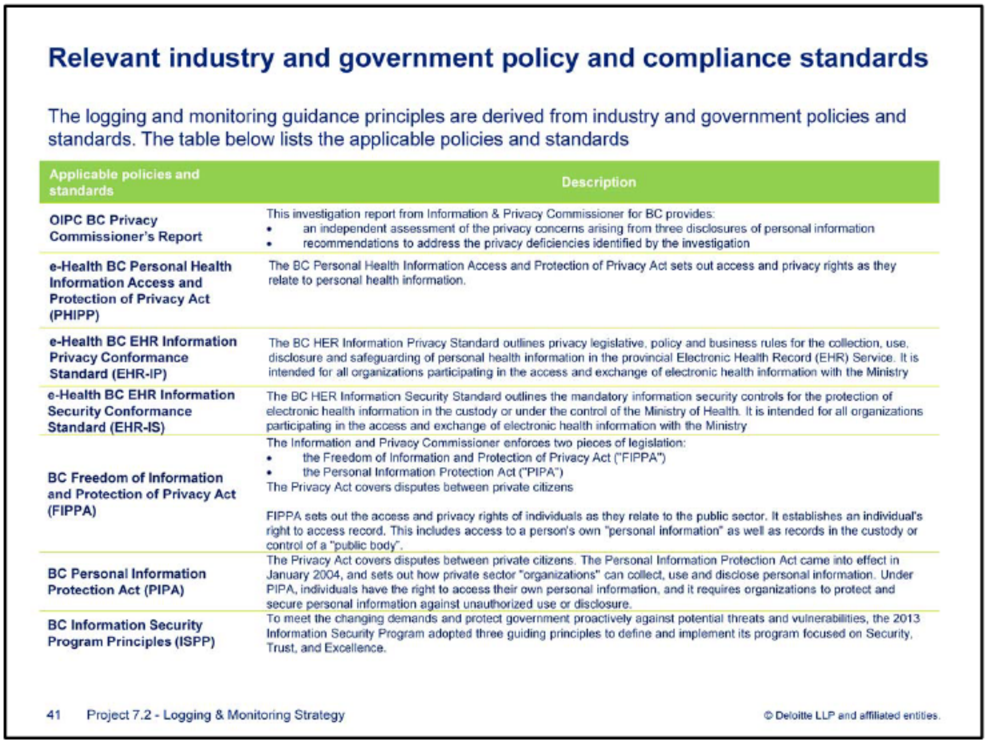


What have we learned from our experiences?

- **Requirements analysis:** Define the requirements, control objectives, compliance requirements and problem definition
- **Determine appropriate control levels:** Ensure that the rollout plan is mapped to control objectives
- **Threat landscape matrix:** Define a threat inventory based on the risk and control requirement profile of the organization. This will be used for architecture development
- **Set expectations:** Ensure that management and technical staff understand the key realities of the architecture
- **Define enterprise infrastructure requirements:** This can include data store requirements, retention, network bandwidth requirements etc. It is important to involve key stakeholders
- **Solution analysis:** Review and map compliance/risk requirements against solutions
- **Customized for unique requirements:** Logging and Monitoring solutions offer base capability however require customization to meet organizational risk and compliance goals
- **Process development:** Define the people and processes required to support the architecture
- **Optimize and prioritize:** The key factor of a successful deployment is the appropriate selection and prioritization of log sources;

In Deloitte's experience, when Logging and Monitoring projects fail it is usually due to weaknesses in processes, roles and responsibilities and vision.

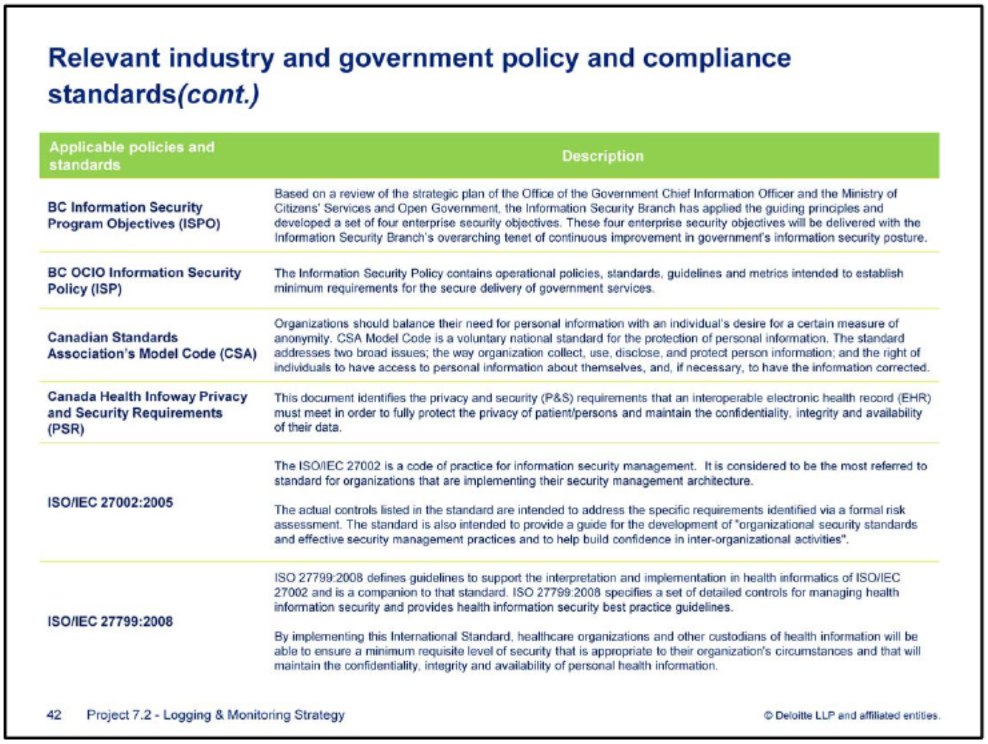
Policies and standards



Relevant industry and government policy and compliance standards

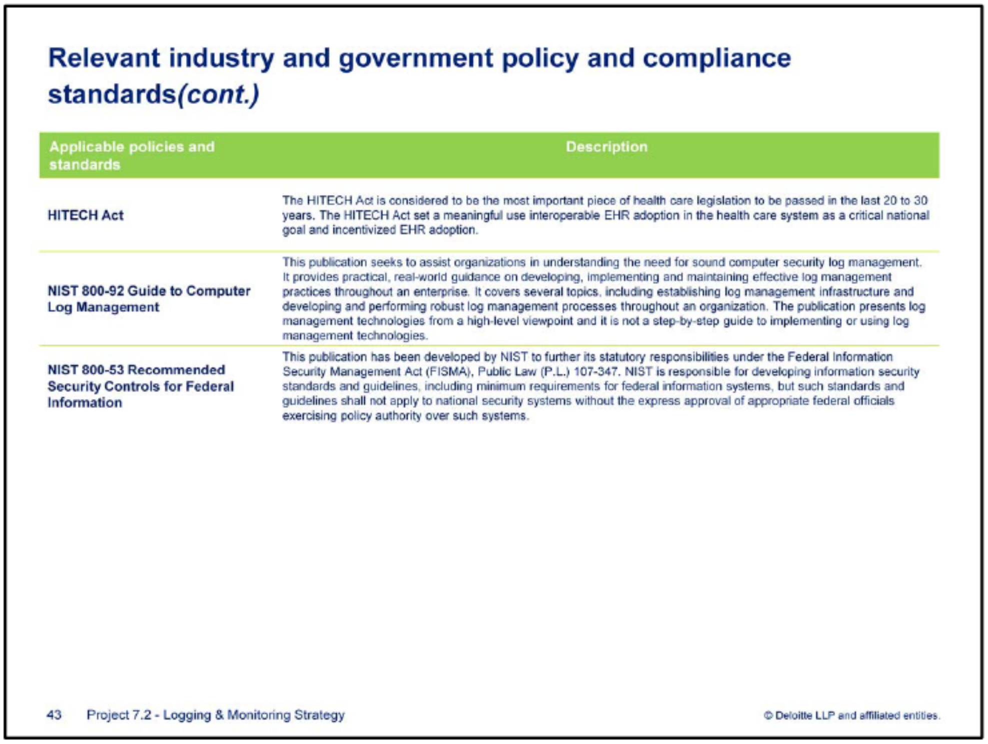
The logging and monitoring guidance principles are derived from industry and government policies and standards. The table below lists the applicable policies and standards

Applicable policies and standards	Description
OIPC BC Privacy Commissioner's Report	This investigation report from Information & Privacy Commissioner for BC provides: • an independent assessment of the privacy concerns arising from three disclosures of personal information • recommendations to address the privacy deficiencies identified by the investigation
e-Health BC Personal Health Information Access and Protection of Privacy Act (PHIPP)	The BC Personal Health Information Access and Protection of Privacy Act sets out access and privacy rights as they relate to personal health information.
e-Health BC EHR Information Privacy Conformance Standard (EHR-IP)	The BC HER Information Privacy Standard outlines privacy legislative, policy and business rules for the collection, use, disclosure and safeguarding of personal health information in the provincial Electronic Health Record (EHR) Service. It is intended for all organizations participating in the access and exchange of electronic health information with the Ministry
e-Health BC EHR Information Security Conformance Standard (EHR-IS)	The BC HER Information Security Standard outlines the mandatory information security controls for the protection of electronic health information in the custody or under the control of the Ministry of Health. It is intended for all organizations participating in the access and exchange of electronic health information with the Ministry
BC Freedom of Information and Protection of Privacy Act (FIPPA)	The Information and Privacy Commissioner enforces two pieces of legislation: • the Freedom of Information and Protection of Privacy Act ("FIPPA") • the Personal Information Protection Act ("PIPA") The Privacy Act covers disputes between private citizens FIPPA sets out the access and privacy rights of individuals as they relate to the public sector. It establishes an individual's right to access record. This includes access to a person's own "personal information" as well as records in the custody or control of a "public body".
BC Personal Information Protection Act (PIPA)	The Privacy Act covers disputes between private citizens. The Personal Information Protection Act came into effect in January 2004, and sets out how private sector "organizations" can collect, use and disclose personal information. Under PIPA, individuals have the right to access their own personal information, and it requires organizations to protect and secure personal information against unauthorized use or disclosure.
BC Information Security Program Principles (ISPP)	To meet the changing demands and protect government proactively against potential threats and vulnerabilities, the 2013 Information Security Program adopted three guiding principles to define and implement its program focused on Security, Trust, and Excellence.



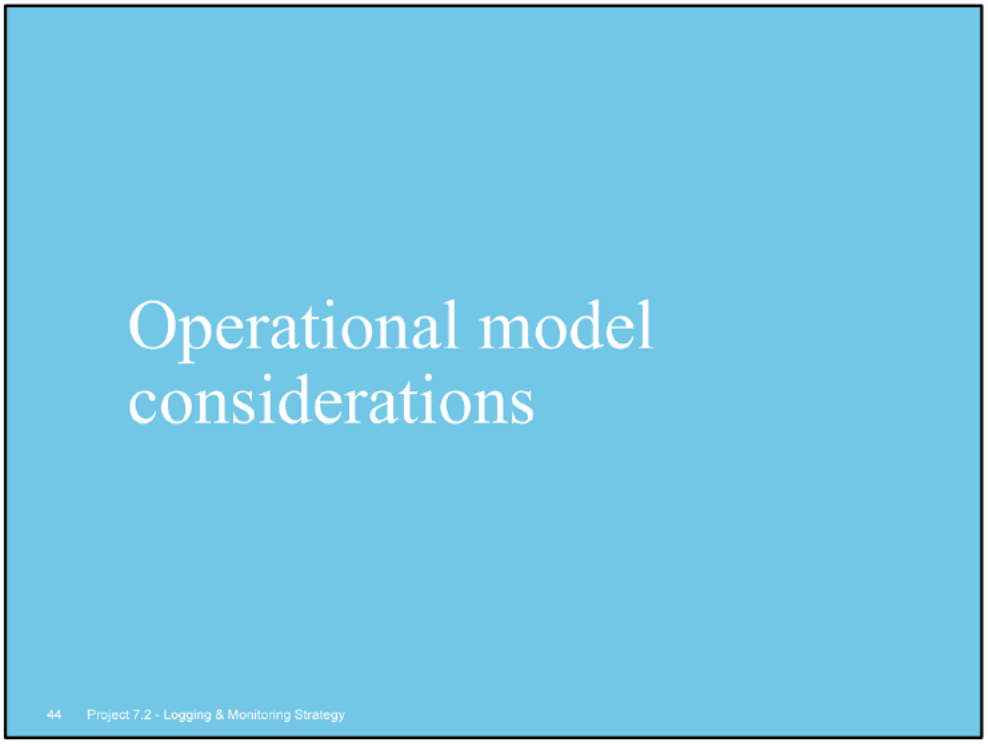
Relevant industry and government policy and compliance standards*(cont.)*

Applicable policies and standards	Description
BC Information Security Program Objectives (ISPO)	Based on a review of the strategic plan of the Office of the Government Chief Information Officer and the Ministry of Citizens' Services and Open Government, the Information Security Branch has applied the guiding principles and developed a set of four enterprise security objectives. These four enterprise security objectives will be delivered with the Information Security Branch's overarching tenet of continuous improvement in government's information security posture.
BC OCIO Information Security Policy (ISP)	The Information Security Policy contains operational policies, standards, guidelines and metrics intended to establish minimum requirements for the secure delivery of government services.
Canadian Standards Association's Model Code (CSA)	Organizations should balance their need for personal information with an individual's desire for a certain measure of anonymity. CSA Model Code is a voluntary national standard for the protection of personal information. The standard addresses two broad issues; the way organization collect, use, disclose, and protect person information; and the right of individuals to have access to personal information about themselves, and, if necessary, to have the information corrected.
Canada Health Infoway Privacy and Security Requirements (PSR)	This document identifies the privacy and security (P&S) requirements that an interoperable electronic health record (EHR) must meet in order to fully protect the privacy of patient/persons and maintain the confidentiality, integrity and availability of their data.
ISO/IEC 27002:2005	The ISO/IEC 27002 is a code of practice for information security management. It is considered to be the most referred to standard for organizations that are implementing their security management architecture. The actual controls listed in the standard are intended to address the specific requirements identified via a formal risk assessment. The standard is also intended to provide a guide for the development of "organizational security standards and effective security management practices and to help build confidence in inter-organizational activities".
ISO/IEC 27799:2008	ISO 27799:2008 defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that standard. ISO 27799:2008 specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. By implementing this International Standard, healthcare organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity and availability of personal health information.

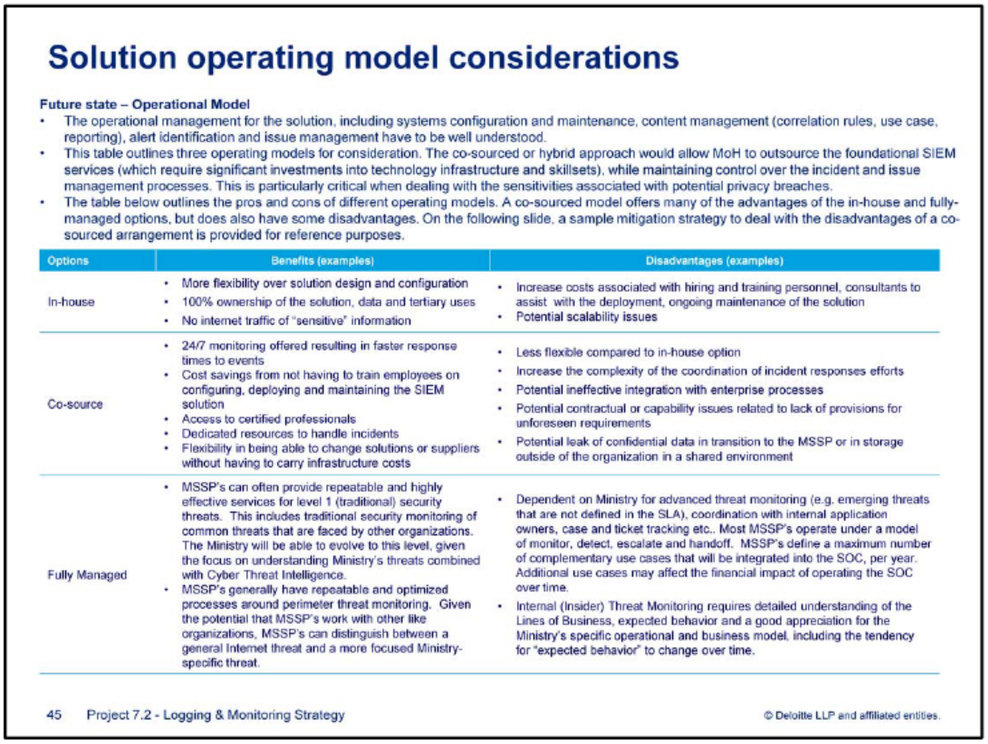


Relevant industry and government policy and compliance standards*(cont.)*

Applicable policies and standards	Description
HITECH Act	The HITECH Act is considered to be the most important piece of health care legislation to be passed in the last 20 to 30 years. The HITECH Act set a meaningful use interoperable EHR adoption in the health care system as a critical national goal and incentivized EHR adoption.
NIST 800-92 Guide to Computer Log Management	This publication seeks to assist organizations in understanding the need for sound computer security log management. It provides practical, real-world guidance on developing, implementing and maintaining effective log management practices throughout an enterprise. It covers several topics, including establishing log management infrastructure and developing and performing robust log management processes throughout an organization. The publication presents log management technologies from a high-level viewpoint and it is not a step-by-step guide to implementing or using log management technologies.
NIST 800-53 Recommended Security Controls for Federal Information	This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems.



Operational model considerations

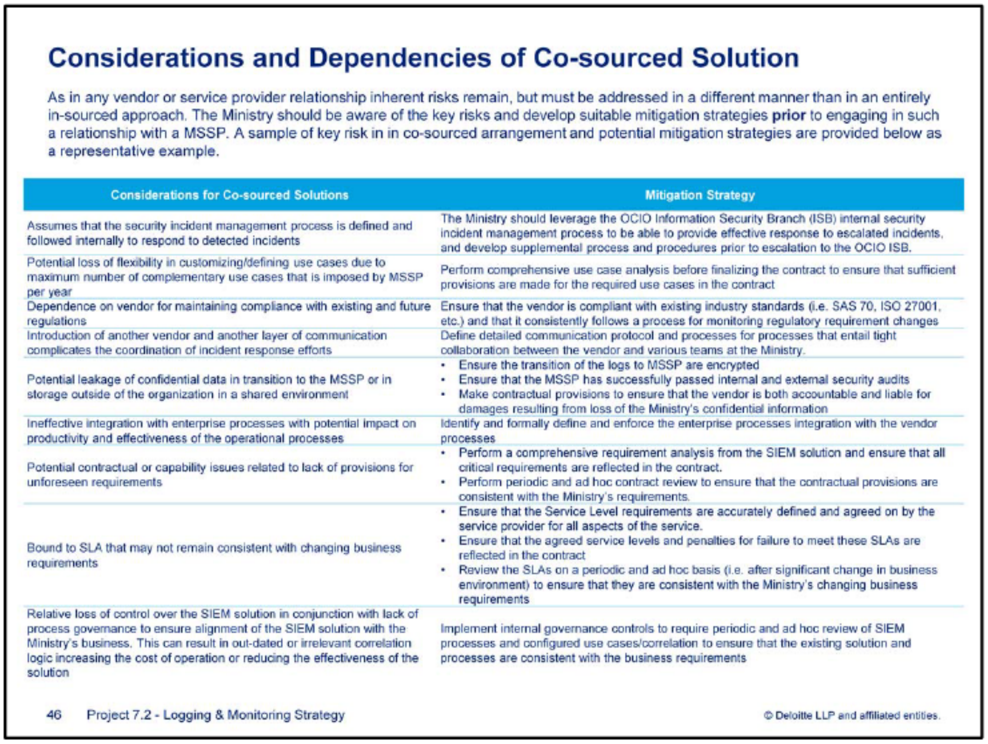


Solution operating model considerations

Future state – Operational Model

- The operational management for the solution, including systems configuration and maintenance, content management (correlation rules, use case, reporting), alert identification and issue management have to be well understood.
- This table outlines three operating models for consideration. The co-sourced or hybrid approach would allow MoH to outsource the foundational SIEM services (which require significant investments into technology infrastructure and skillsets), while maintaining control over the incident and issue management processes. This is particularly critical when dealing with the sensitivities associated with potential privacy breaches.
- The table below outlines the pros and cons of different operating models. A co-sourced model offers many of the advantages of the in-house and fully-managed options, but does also have some disadvantages. On the following slide, a sample mitigation strategy to deal with the disadvantages of a co-sourced arrangement is provided for reference purposes.

Options	Benefits (examples)	Disadvantages (examples)
In-house	• More flexibility over solution design and configuration • 100% ownership of the solution, data and tertiary uses • No internet traffic of "sensitive" information	• Increase costs associated with hiring and training personnel, consultants to assist with the deployment, ongoing maintenance of the solution • Potential scalability issues
Co-source	• 24/7 monitoring offered resulting in faster response times to events • Cost savings from not having to train employees on configuring, deploying and maintaining the SIEM solution • Access to certified professionals • Dedicated resources to handle incidents • Flexibility in being able to change solutions or suppliers without having to carry infrastructure costs	• Less flexible compared to in-house option • Increase the complexity of the coordination of incident responses efforts • Potential ineffective integration with enterprise processes • Potential contractual or capability issues related to lack of provisions for unforeseen requirements • Potential leak of confidential data in transition to the MSSP or in storage outside of the organization in a shared environment
Fully Managed	• MSSP's can often provide repeatable and highly effective services for level 1 (traditional) security threats. This includes traditional security monitoring of common threats that are faced by other organizations. The Ministry will be able to evolve to this level, given the focus on understanding Ministry's threats combined with Cyber Threat Intelligence. • MSSP's generally have repeatable and optimized processes around perimeter threat monitoring. Given the potential that MSSP's work with other like organizations, MSSP's can distinguish between a general Internet threat and a more focused Ministry-specific threat.	• Dependent on Ministry for advanced threat monitoring (e.g. emerging threats that are not defined in the SLA), coordination with internal application owners, case and ticket tracking etc.. Most MSSP's operate under a model of monitor, detect, escalate and handoff. MSSP's define a maximum number of complementary use cases that will be integrated into the SOC, per year. Additional use cases may affect the financial impact of operating the SOC over time. • Internal (Insider) Threat Monitoring requires detailed understanding of the Lines of Business, expected behavior and a good appreciation for the Ministry's specific operational and business model, including the tendency for "expected behavior" to change over time.



Considerations and Dependencies of Co-sourced Solution

As in any vendor or service provider relationship inherent risks remain, but must be addressed in a different manner than in an entirely in-sourced approach. The Ministry should be aware of the key risks and develop suitable mitigation strategies **prior** to engaging in such a relationship with a MSSP. A sample of key risk in in co-sourced arrangement and potential mitigation strategies are provided below as a representative example.

Considerations for Co-sourced Solutions	Mitigation Strategy
Assumes that the security incident management process is defined and followed internally to respond to detected incidents	The Ministry should leverage the OCIO Information Security Branch (ISB) internal security incident management process to be able to provide effective response to escalated incidents, and develop supplemental process and procedures prior to escalation to the OCIO ISB.
Potential loss of flexibility in customizing/defining use cases due to maximum number of complementary use cases that is imposed by MSSP per year	Perform comprehensive use case analysis before finalizing the contract to ensure that sufficient provisions are made for the required use cases in the contract
Dependence on vendor for maintaining compliance with existing and future regulations	Ensure that the vendor is compliant with existing industry standards (i.e. SAS 70, ISO 27001, etc.) and that it consistently follows a process for monitoring regulatory requirement changes
Introduction of another vendor and another layer of communication complicates the coordination of incident response efforts	Define detailed communication protocol and processes for processes that entail tight collaboration between the vendor and various teams at the Ministry.
Potential leakage of confidential data in transition to the MSSP or in storage outside of the organization in a shared environment	• Ensure the transition of the logs to MSSP are encrypted • Ensure that the MSSP has successfully passed internal and external security audits • Make contractual provisions to ensure that the vendor is both accountable and liable for damages resulting from loss of the Ministry's confidential information
Ineffective integration with enterprise processes with potential impact on productivity and effectiveness of the operational processes	Identify and formally define and enforce the enterprise processes integration with the vendor processes
Potential contractual or capability issues related to lack of provisions for unforeseen requirements	• Perform a comprehensive requirement analysis from the SIEM solution and ensure that all critical requirements are reflected in the contract. • Perform periodic and ad hoc contract review to ensure that the contractual provisions are consistent with the Ministry's requirements.
Bound to SLA that may not remain consistent with changing business requirements	• Ensure that the Service Level requirements are accurately defined and agreed on by the service provider for all aspects of the service. • Ensure that the agreed service levels and penalties for failure to meet these SLAs are reflected in the contract • Review the SLAs on a periodic and ad hoc basis (i.e. after significant change in business environment) to ensure that they are consistent with the Ministry's changing business requirements
Relative loss of control over the SIEM solution in conjunction with lack of process governance to ensure alignment of the SIEM solution with the Ministry's business. This can result in out-dated or irrelevant correlation logic increasing the cost of operation or reducing the effectiveness of the solution	Implement internal governance controls to require periodic and ad hoc review of SIEM processes and configured use cases/correlation to ensure that the existing solution and processes are consistent with the business requirements

Page 163 redacted for the following reason:
- -
s.15, s.21

Deloitte.