BRITISH COLUMBIA

Information Management Branch
Serving the Natural Resource ministries

A strategy for success

How building a security strategy can help you achieve your security goals

Nick Corcoran, BEng, CISSP, TOGAF
Security Architect
NRS Information Security Officer

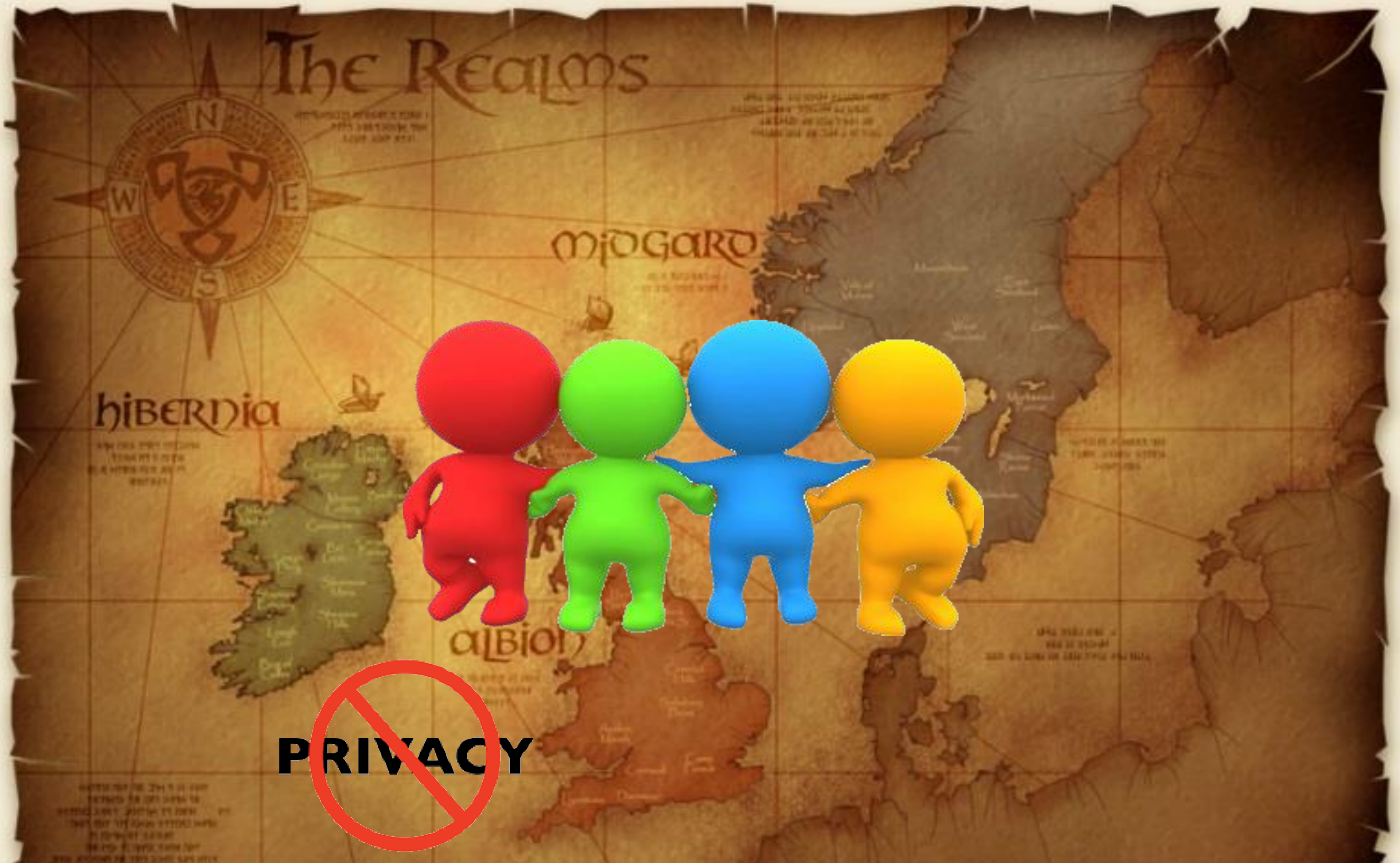
The baseline

The idea

Benefits

Alignment

Outcomes


The Realms
N
W
E
S
Midgard
Hibernia
Albion
PRIVACY

Tactical – the now	Strategic – the future
Incident Management (InfoSec, HR, Non)	Incident Management (InfoSec, HR, Non)
- Simple/moderate complexity	- Major System Incident
Data Replication	New tools and platforms
Data Classification	- Vulnerability management (Scanning tools)
Access Requests	- Logging
Access Reviews	- Credentials management
General Client Assistance	- Secure cloud connector(s)
- Policy compliance/advice	- Classification framework
- MOUs, ISAs	- DevOps
- Open Data	- Digital Services
- Setup vulnerability scan	Cross-Gov initiatives
- Policy Exemptions	- SIEM
- LAN Security	- Vendor engagement – IBM, Oracle
Helping with Audit responses	- ISAC, IS Strategic Committee
Awareness – Fast Facts	Awareness – Presentations
STRAs – Point in time, simple/moderate	STRAs – Future focussed – more complex

NRS Security Strategy

KEEP
CALM
AND
DON'T
GET HACKED

147 ways we can improve security practices

OCIO STRATEGY
2016

CONNECTIVITY

SECURITY

DIGITAL

CLOUD

MOBILITY

OCIO | Office of the Chief Information Officer

BRITISH COLUMBIA

NRS Information Security Architecture STRATEGY 2017

NRS | Information Security Architecture

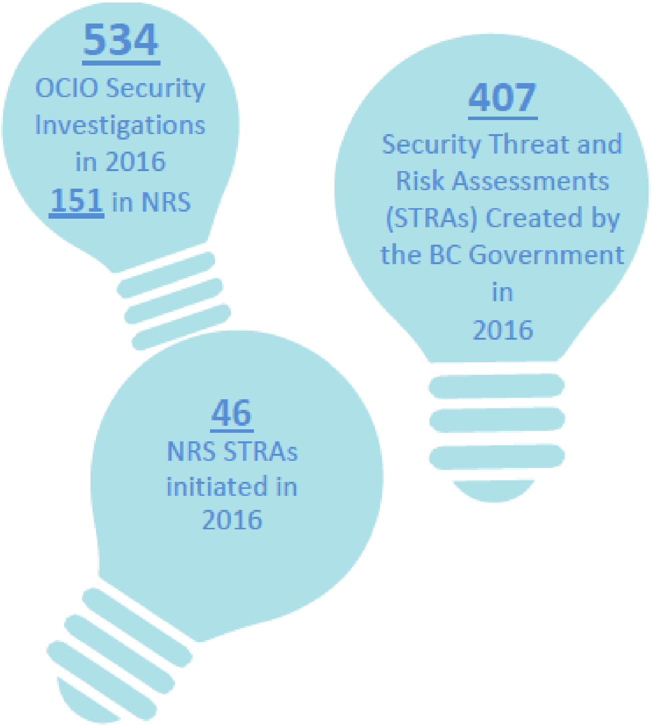
BRITISH COLUMBIA

ABOUT THE NRS Information Security Team:

We are a team of 4 employees

68 Information Security professionals in BC Government

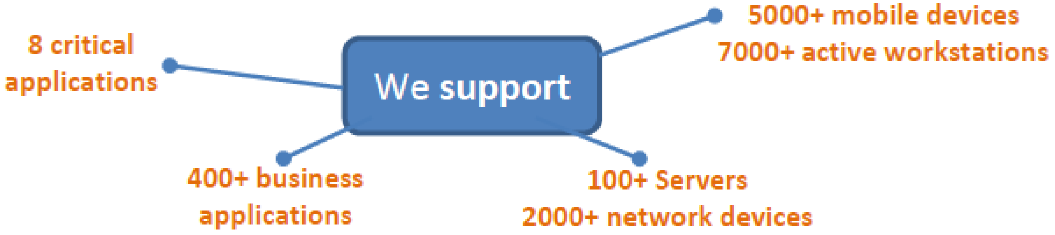
A few quick **facts!**



534
OCIO Security Investigations in 2016
151 in NRS

407
Security Threat and Risk Assessments (STRAs) Created by the BC Government in 2016

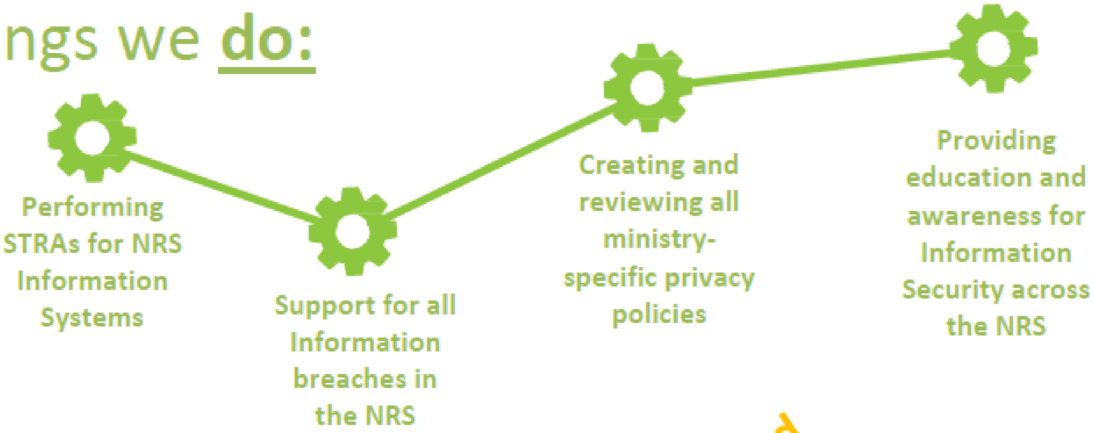
46
NRS STRAs initiated in 2016



We support

- 8 critical applications
- 5000+ mobile devices
- 7000+ active workstations
- 400+ business applications
- 100+ Servers
- 2000+ network devices

Things we **do:**



- Performing STRAs for NRS Information Systems
- Support for all Information breaches in the NRS
- Creating and reviewing all ministry-specific privacy policies
- Providing education and awareness for Information Security across the NRS

We Will Deliver:

IBM Guardium Showcase to other Ministries

And we **introduced**

- Data Classification Process
- Data Masking
- Credentials Management
- STRA Threat Modeling Process

BRITISH COLUMBIA

Natural Resource Sector

WHAT **WE DO**

Ministry Information Security Officer Role

The ministry privacy officer is responsible for implementing the Information Security Program in your ministry, serves as your primary contact for information security-related questions, and the primary contact between your ministry and the corporate information security office.

Conduct/Review all NRS STRAs.

As part of their duties your information security team manages and reviews all Security Threat and Risk Assessments (STRAs). We also review and advise on security controls when Information Sharing Agreements are developed.

Conduct a regular review of Sector Security Controls

The Information Security team performs an annual review of annual information security controls (AISR). These details are documented and recommendations are shared with the Sector CIO and Ministry Executive Teams. The Results are also reported to the OCIO Information Security Branch.

Breach and Incident Management Response

Information breaches involve sensitive, confidential, or personal information and it is important that it be contained and mitigated with urgency. The Information Security Team will work closely with the OCIO Security Investigations Unit and the Ministry Privacy Officer.

Advise and Consulate on Information Security Policy and Training

Advise on the development, issuance, and maintenance of ministry specific security policies. Developing and delivering ministry specific security training. The Information Security team provides consultation services and expert security advice on the development of ministry systems and information management practices.

Communication and Liaise

The Information Security team is responsible for employees to understand their roles and responsibilities for helping protect information and computer systems. We provide information for ongoing audits and liaise between the ministry and the OAG and OCIO.

HOW WE COLLABORATE

OCIO Information Security Branch (ISB)

The ISB is the BC government's corporate information security office, under the Office of the Chief Information Officer (OCIO). We work closely with the Advisory Services, Vulnerability and Risk Management, and Awareness teams to provide consistent messaging to Sector clients. We partner with the ISP to initiate POC and Pilot engagements with corporate partners, work together on strategic initiatives, and regularly participate in awareness activities - like OCIO Security Day and the Annual Privacy and Security Conference.

Corporate Partners

Our main corporate partners include HPAS, IBM, Telus and Oracle. We work with these partners to leverage capabilities that can improve information security practices across government. Through sponsored POCs and Pilots, value in the tooling and services they provide can be demonstrated across government, and, as a result, joint ventures can be made possible where previously they would not have been. By driving towards corporate adoption of products and services, we can drive down the cost which in turn makes our decisions more fiscally responsible.

Information Security Advisory Committee (ISAC)

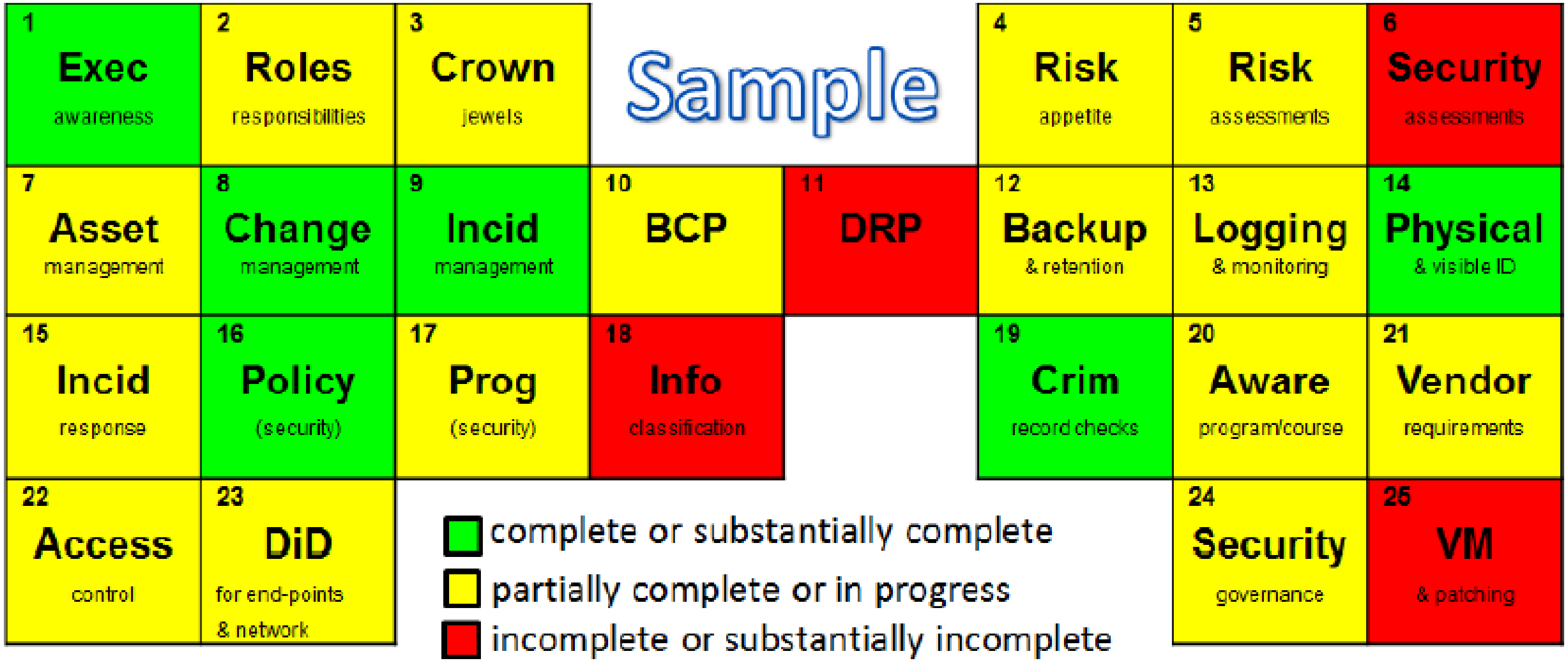
The Information Security Advisory Committee (ISAC) provides a forum for Ministry Information Security Officers (MISOs) to:

- Discuss issues and share information related to the security of the Province's information resources, and
- Provide advice and recommendations on information security related issues to the Chief Information Security Officer (CISO) and Ministry Chief Information Officers (MCIOs).

Director Level Security Committee

The Director Level Security Committee provides strategic leadership and direction on security initiatives across government. Membership includes strategic leaders from OCIO, NRS, GSO, TRAN, Social Sector and CSCD.

Defensible?



🟩 1 **Exec** awareness	🟨 2 **Roles** responsibilities	🟨 3 **Crown** jewels	Sample		🟨 4 **Risk** appetite	🟨 5 **Risk** assessments	🟥 6 **Security** assessments
🟨 7 **Asset** management	🟩 8 **Change** management	🟩 9 **Incid** management	🟨 10 **BCP**	🟥 11 **DRP**	🟨 12 **Backup** & retention	🟨 13 **Logging** & monitoring	🟩 14 **Physical** & visible ID
🟨 15 **Incid** response	🟩 16 **Policy** (security)	🟨 17 **Prog** (security)	🟥 18 **Info** classification		🟩 19 **Crim** record checks	🟨 20 **Aware** program/course	🟨 21 **Vendor** requirements
🟨 22 **Access** control	🟨 23 **DiD** for end-points & network					🟨 24 **Security** governance	🟥 25 **VM** & patching

🟩 complete or substantially complete

🟨 partially complete or in progress

🟥 incomplete or substantially incomplete

OUR **STRATEGIC GOALS**

Three overarching **strategic goals** set the direction for the NRS Information Security Architecture Strategy.

These goals will be achieved over the next three years through the actions outlined in this document. The following pages provide an outline of what we will do, how we will do it, and the outcomes we expect to achieve.

GOAL 1

Understand what data is sensitive

Understanding our data is a key driver to getting the most out of it. It also helps us to focus controls to protect sensitive information, while sharing data as much as possible.

18
InfoSec
classification

GOAL 2

Mitigate known weaknesses

One of the easiest ways we can reduce the risk of inappropriate data exposure is to ensure we don't have any obvious exploitable vulnerabilities exposed through the systems we create/manage. Also, by grouping application deployments we can focus our effort and controls around protecting those assets with common data and/or system criticality.

13
Logging
& monitoring

25
VM
& patching

GOAL 3

Ensure authentication between systems

Improper Credentials Management for machine-to-machine communications can result in unnecessary exposures and configuration errors that affect availability. Reducing those risks will help to provide a more robust platform for our clients systems and data.

.

22
Access
control

OCIO | Office of the Chief Information Officer

Strategic Framework

Companion to the OCIO Strategy 2016

Alignment to Government Priorities

Government Priorities

Strong Economy

Where Ideas Work

Goal 1
Building our internal c

Ministry Strategic Plan

Modernize the Citizen Service Experience

Ministry Vision

Excellence and

The OCIO Business Priorities

OCIO Mission

Modernize the

Technology Pillars

CONNECTIVITY

Secure, reliable networks and internet access

F
av

Strategic Goals

1
ENABLE DIGITAL

Organizing for success

Core Functions

Telecommunications and Network Infrastructure

Hosting Infrastructure

NRS | Information Security Architecture

Strategic Framework

Companion to NRS IS Strategy 2017

Government Priorities

Natural Resources

Secure Tomorrow

IMB Goals

Goal 1
Clients are supported in achieving their business goals

Goal 2
A Trusted and Reliable Partner

Goal 3
A Great Place to Work

IMB Objectives

Successful Delivery PROCESSES

Effective and Reliable Tools and TECHNOLOGY

Empowered and Supported PEOPLE

InfoSec Goals

Goal 1
Understand what data is sensitive

Goal 2
Mitigate known weaknesses

Goal 3
Ensure authentication between systems

Key Enablers

DATA CLASSIFICATION
1 PLAN
2 DO
3 CHECK
4 ACT

Understand data classification program

Enhance internal ability to discover vulnerabilities

Influence infrastructure architecture

Better manage access to servers

Regular password rotation

Key Initiatives

Integrate into Data Modeling Standard

Implement metadata repository

Pilot
Data Discovery/Classification and Database Vulnerability Scanning

Introduce a COTS application scanning capability

Criticality based deployment groupings

Implement Privileged Access Management

Key Projects

CloudBC

Developers Exchange

My Service Centre

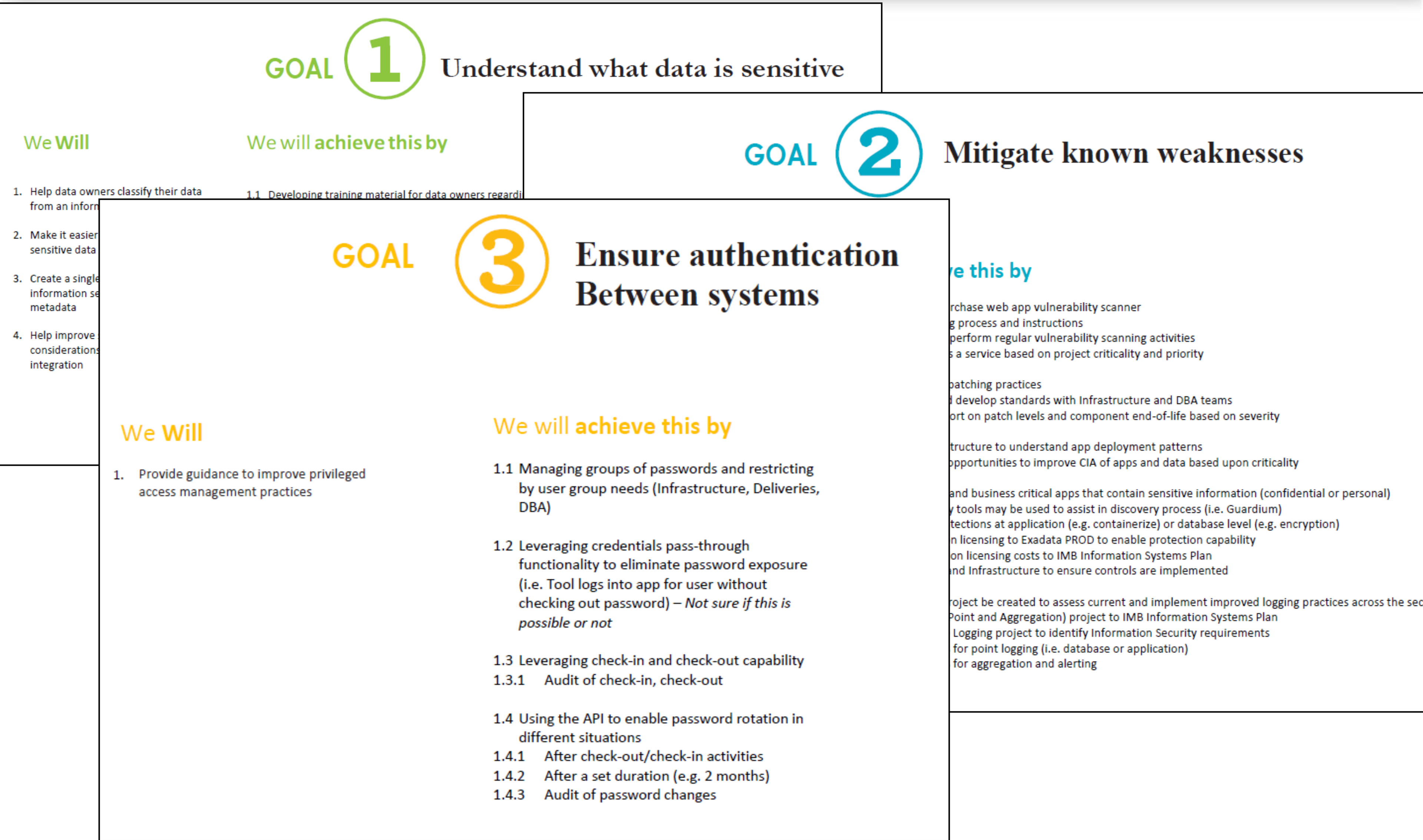
BC Services Card

Mobile Device Management

Network Modernization

IM/IT Talent Management

Natural Resource Sector



GOAL 1 Understand what data is sensitive

We Will

1. Help data owners classify their data from an inform

2. Make it easier sensitive data

3. Create a single information se metadata

4. Help improve considerations integration

We will achieve this by

1.1 Developing training material for data owners regardi

GOAL 2 Mitigate known weaknesses

e this by

rchase web app vulnerability scanner
g process and instructions
perform regular vulnerability scanning activities
s a service based on project criticality and priority

patching practices
d develop standards with Infrastructure and DBA teams
ort on patch levels and component end-of-life based on severity

tructure to understand app deployment patterns
pportunities to improve CIA of apps and data based upon criticality

and business critical apps that contain sensitive information (confidential or personal)
y tools may be used to assist in discovery process (i.e. Guardium)
tections at application (e.g. containerize) or database level (e.g. encryption)
n licensing to Exadata PROD to enable protection capability
on licensing costs to IMB Information Systems Plan
nd Infrastructure to ensure controls are implemented

roject be created to assess current and implement improved logging practices across the sec
Point and Aggregation) project to IMB Information Systems Plan
Logging project to identify Information Security requirements
for point logging (i.e. database or application)
for aggregation and alerting

GOAL 3 Ensure authentication Between systems

We Will

1. Provide guidance to improve privileged access management practices

We will achieve this by

1.1 Managing groups of passwords and restricting by user group needs (Infrastructure, Deliveries, DBA)

1.2 Leveraging credentials pass-through functionality to eliminate password exposure (i.e. Tool logs into app for user without checking out password) – *Not sure if this is possible or not*

1.3 Leveraging check-in and check-out capability
1.3.1 Audit of check-in, check-out

1.4 Using the API to enable password rotation in different situations
1.4.1 After check-out/check-in activities
1.4.2 After a set duration (e.g. 2 months)
1.4.3 Audit of password changes

OUTCOMES

By **achieving** our **goals**, we anticipate the following **outcomes.**

Over the next three years, we will ensure our commitments are realized by measuring, tracking and reporting on our progress. We will establish a strategic portfolio and governance model to deliver on the strategy.

OUTCOME 1

Improved understanding of sensitive data

We will better understand what data needs heightened protection and where it resides.
Better define access channels to data based upon sensitivity.
Demonstrate leadership of NRS in data security practices to other BC Government Ministries.

18
InfoSec
classification

OUTCOME 2

Known weaknesses mitigated

Reduces vulnerability scanning costs for sector web applications.
Reduces exposed vulnerabilities due to improved patching practices.
Improves CIA through deployment activities.
Provides reasonable security controls for sensitive and personal data at rest.
Enables improved detail collection and notification when anomalous and/or malicious behaviour is observed.
Enables improved issue resolution of application errors through aggregated logging capability.

13
Logging
& monitoring

25
VM
& patching

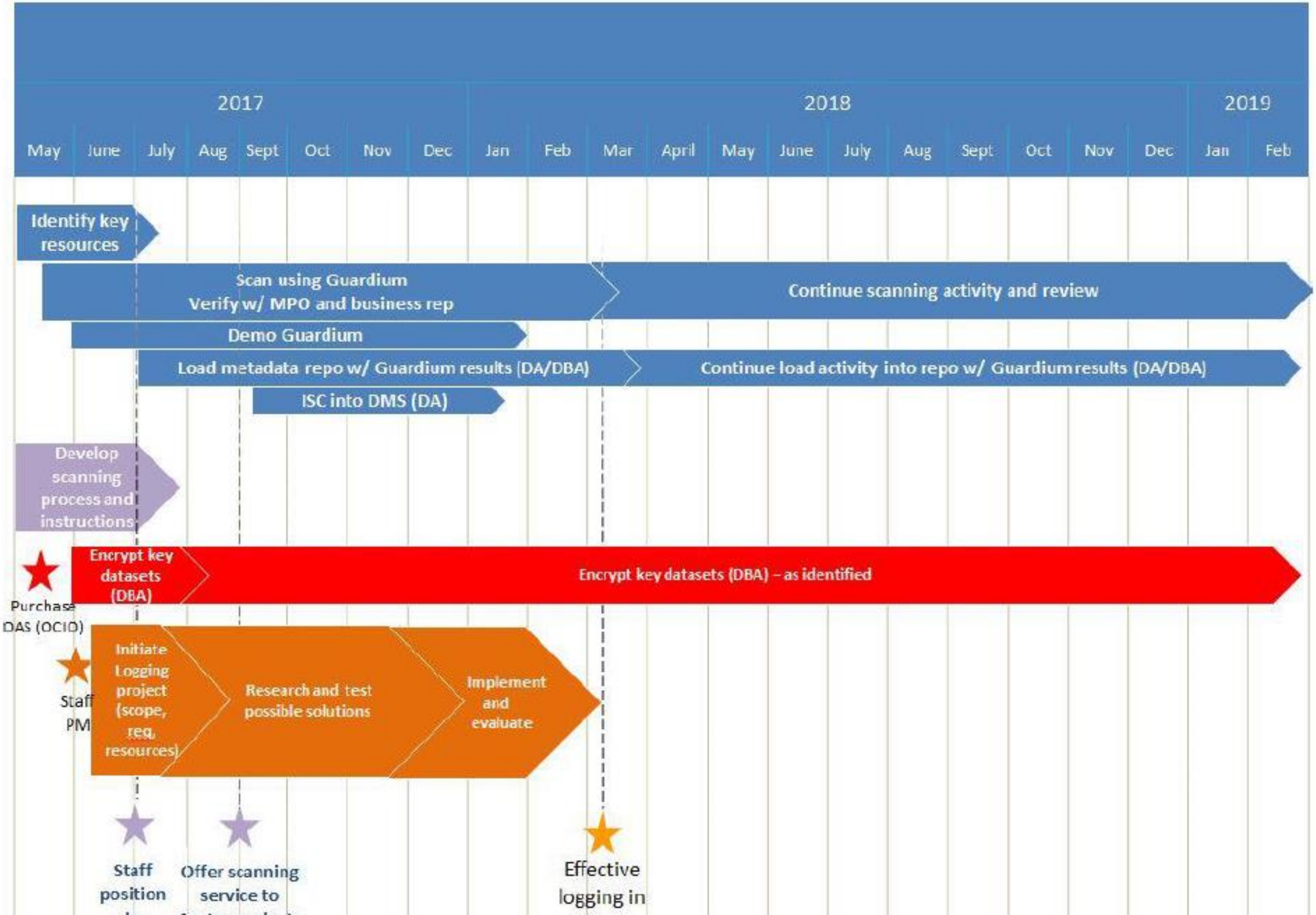
OUTCOME 3

Secure authentication between systems

More secure automated transmission of credentials between systems.
Automated rotation of credentials.
Auditability of credentials used by individuals through check-out capability.
Single, audited, managed repository of credentials with visibility based on team needs.

22
Access
control

Roadmap



2017 | 2018 | 2019

May | June | July | Aug | Sept | Oct | Nov | Dec | Jan | Feb | Mar | April | May | June | July | Aug | Sept | Oct | Nov | Dec | Jan | Feb

Identify key resources

Scan using Guardium
Verify w/ MPO and business rep

Continue scanning activity and review

Demo Guardium

Load metadata repo w/ Guardium results (DA/DBA)

Continue load activity into repo w/ Guardium results (DA/DBA)

ISC into DMS (DA)

Develop scanning process and instructions

Purchase DAS (OCIO)

Encrypt key datasets (DBA)

Encrypt key datasets (DBA) – as identified

Staff PM

Initiate Logging project (scope, req, resources)

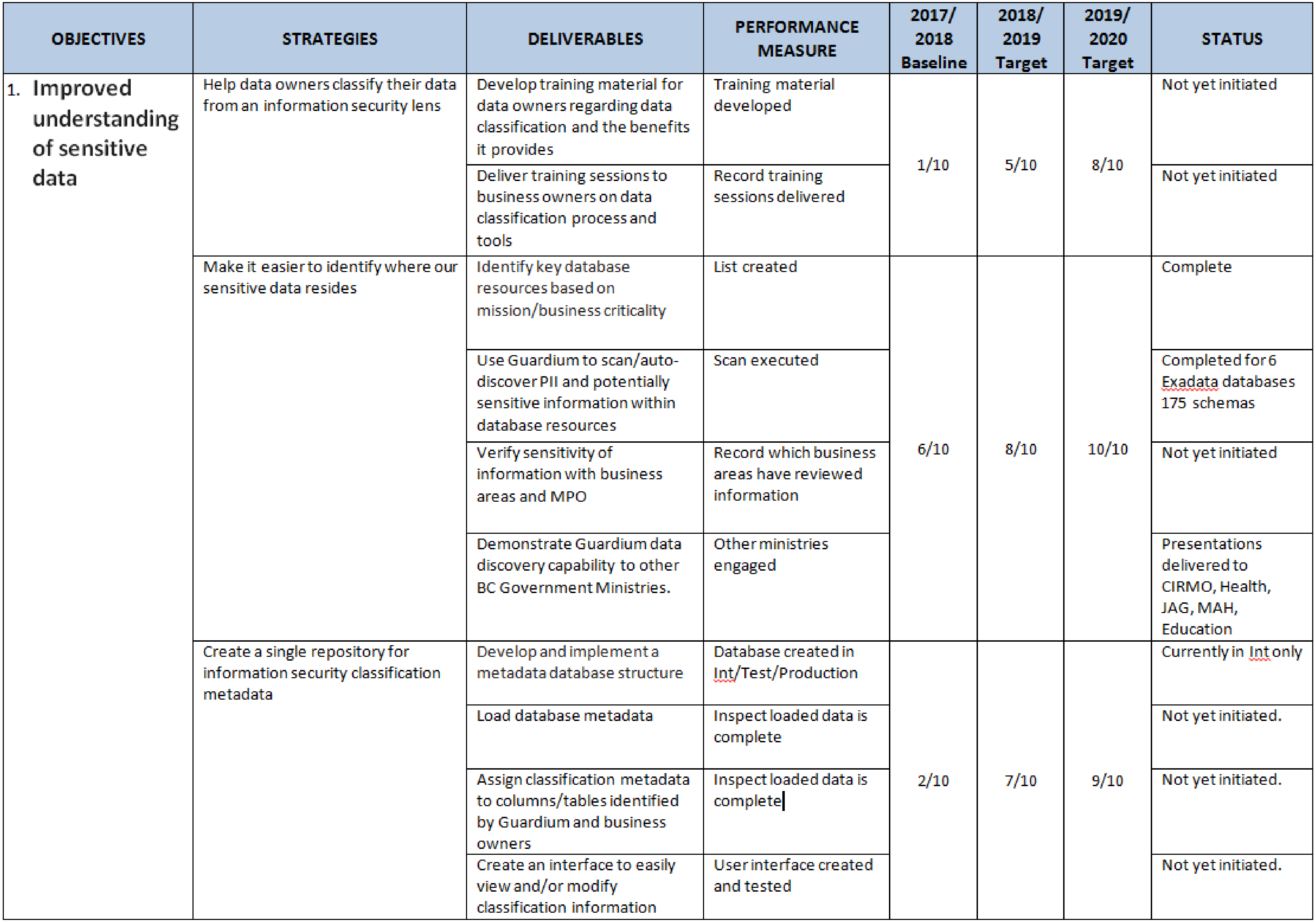
Research and test possible solutions

Implement and evaluate

Staff position

Offer scanning service to

Effective logging in



OBJECTIVES	STRATEGIES	DELIVERABLES	PERFORMANCE MEASURE	2017/ 2018 Baseline	2018/ 2019 Target	2019/ 2020 Target	STATUS
1. Improved understanding of sensitive data	Help data owners classify their data from an information security lens	Develop training material for data owners regarding data classification and the benefits it provides	Training material developed	1/10	5/10	8/10	Not yet initiated
		Deliver training sessions to business owners on data classification process and tools	Record training sessions delivered				Not yet initiated
	Make it easier to identify where our sensitive data resides	Identify key database resources based on mission/business criticality	List created	6/10	8/10	10/10	Complete
		Use Guardium to scan/auto-discover PII and potentially sensitive information within database resources	Scan executed				Completed for 6 Exadata databases 175 schemas
		Verify sensitivity of information with business areas and MPO	Record which business areas have reviewed information				Not yet initiated
		Demonstrate Guardium data discovery capability to other BC Government Ministries.	Other ministries engaged				Presentations delivered to CIRMO, Health, JAG, MAH, Education
	Create a single repository for information security classification metadata	Develop and implement a metadata database structure	Database created in Int/Test/Production	2/10	7/10	9/10	Currently in Int only
		Load database metadata	Inspect loaded data is complete				Not yet initiated.
		Assign classification metadata to columns/tables identified by Guardium and business owners	Inspect loaded data is complete				Not yet initiated.
		Create an interface to easily view and/or modify classification information	User interface created and tested				Not yet initiated.

MEASURES

WARNING

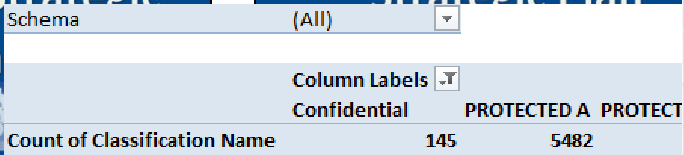
ERROR

Natural Resource Sector

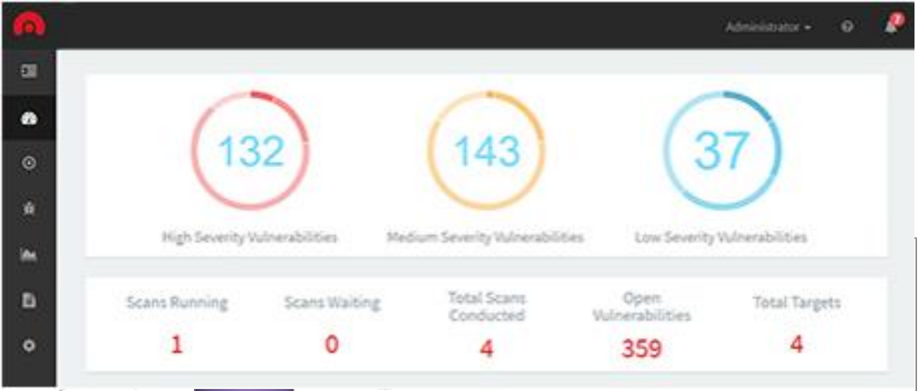
Social Sector Security Strategic Pla

SDSI | Security

NRS Privacy Strategic Plan



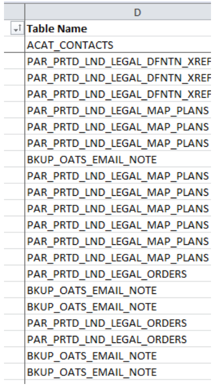
Schema	(All)	
	Column Labels	
	Confidential	**PROTECTED A** **PROTECT**
Count of Classification Name	145	5482



Administrator

132	143	37
High Severity Vulnerabilities	Medium Severity Vulnerabilities	Low Severity Vulnerabilities

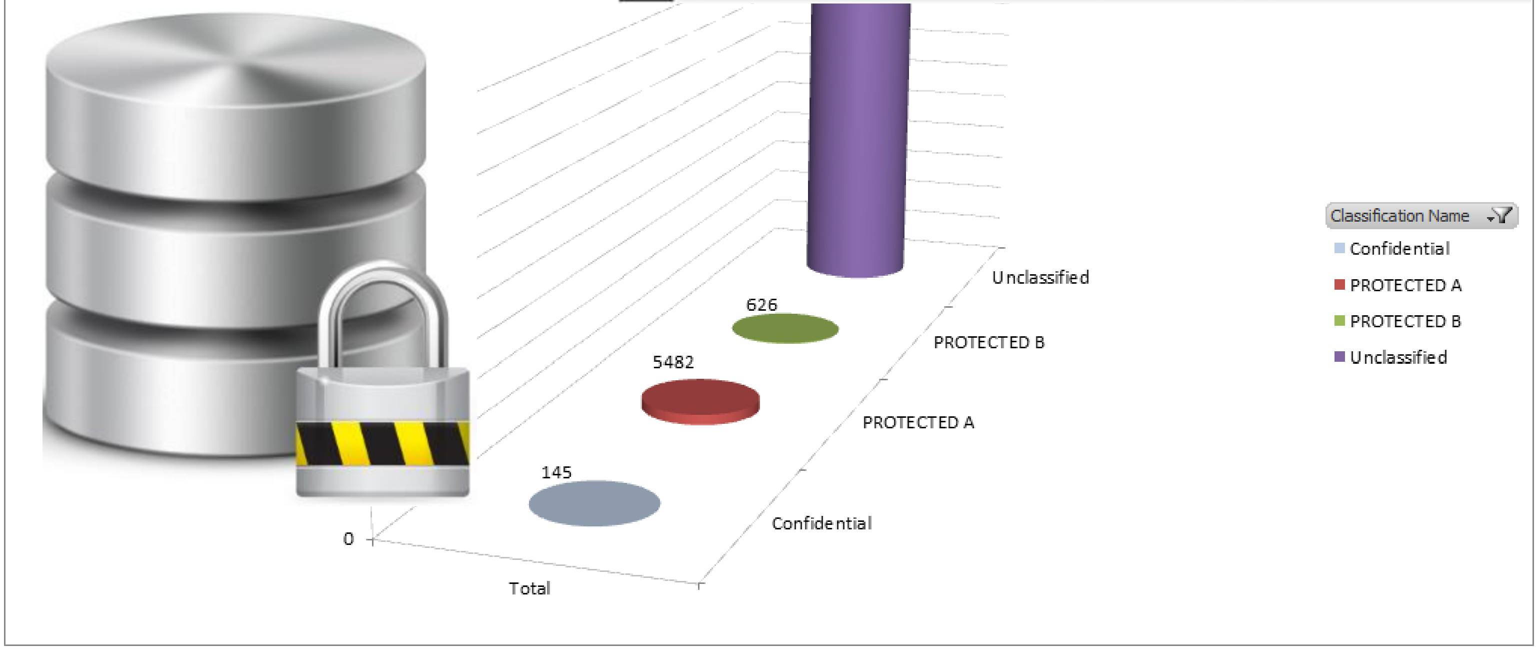
Scans Running	Scans Waiting	Total Scans Conducted	Open Vulnerabilities	Total Targets
1	0	4	359	4



D
Table Name
ACAT_CONTACTS
PAR_PRTD_LND_LEGAL_DFNTN_XREF
PAR_PRTD_LND_LEGAL_DFNTN_XREF
PAR_PRTD_LND_LEGAL_DFNTN_XREF
PAR_PRTD_LND_LEGAL_MAP_PLANS
PAR_PRTD_LND_LEGAL_MAP_PLANS
PAR_PRTD_LND_LEGAL_MAP_PLANS
BKUP_OATS_EMAIL_NOTE
PAR_PRTD_LND_LEGAL_MAP_PLANS
PAR_PRTD_LND_LEGAL_MAP_PLANS
PAR_PRTD_LND_LEGAL_MAP_PLANS
PAR_PRTD_LND_LEGAL_MAP_PLANS
PAR_PRTD_LND_LEGAL_MAP_PLANS
PAR_PRTD_LND_LEGAL_MAP_PLANS
PAR_PRTD_LND_LEGAL_ORDERS
BKUP_OATS_EMAIL_NOTE
BKUP_OATS_EMAIL_NOTE
PAR_PRTD_LND_LEGAL_ORDERS
PAR_PRTD_LND_LEGAL_ORDERS
BKUP_OATS_EMAIL_NOTE
BKUP_OATS_EMAIL_NOTE

Schema

Count of Classification Name



Questions?

Nick Corcoran, BEng, CISSP, TOGAF
Security Architect
NRS Information Security Officer
Nick.corcoran@gov.bc.ca