BCNET CONNECT

HIGHER ED & RESEARCH TECH SUMMIT

Using Information Security and Privacy Metrics Effectively

Deidre Brocklehurst, Privacy Advisor, BCIT
Nthusi Kaisara, Senior Cyber Security Analyst, BCIT

Agenda

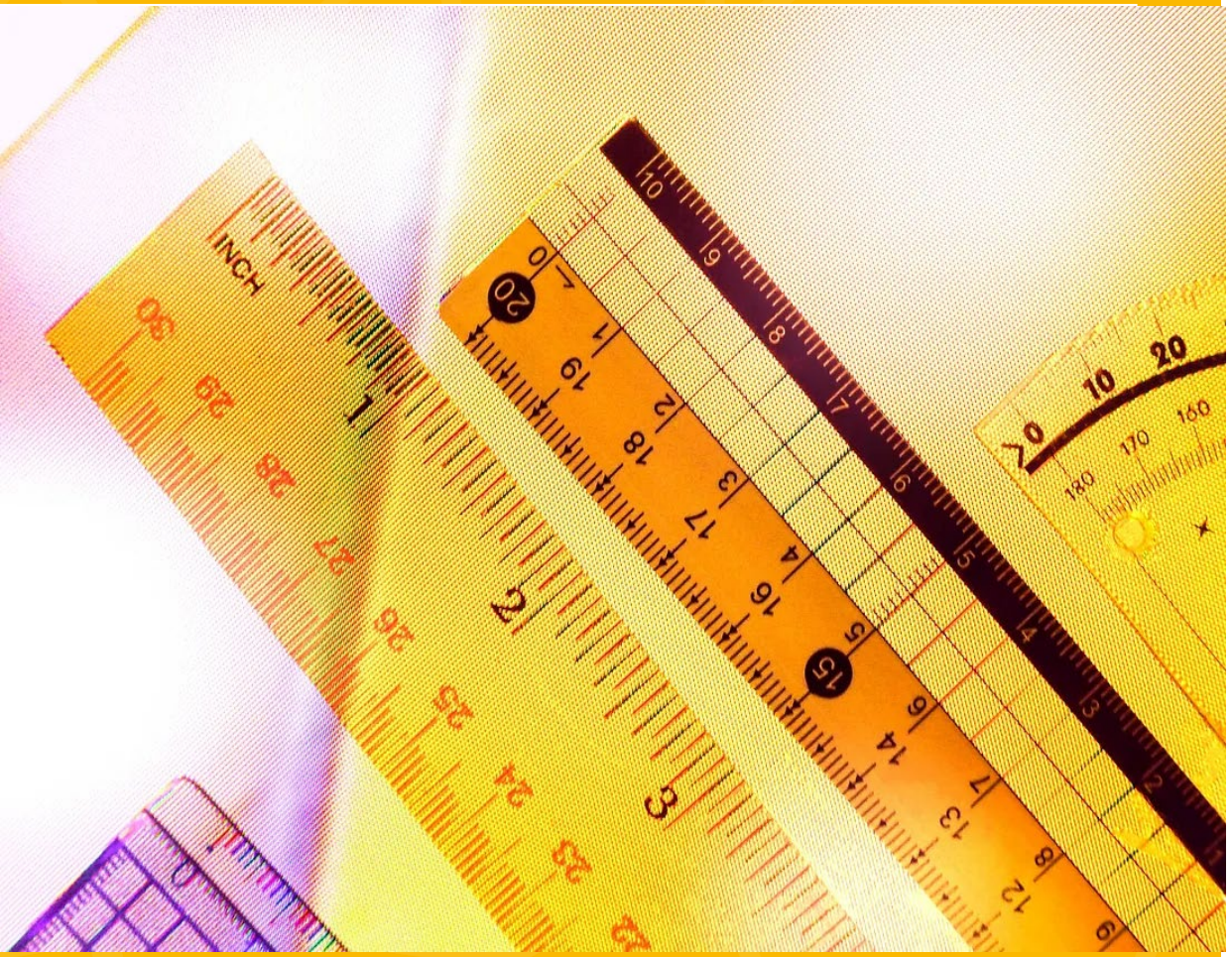
- Why we gather metrics
- Qualities that make good metrics
- Drivers behind metric gathering
- Cyber Security program
- Privacy program
- Conclusion

Why Program Metrics?

"Measurement is the first step that leads to control and eventually to improvement. If you can't measure something, you can't understand it. If you can't understand it, you can't control it."

H. James Harrington

Qualities of Good Metrics:



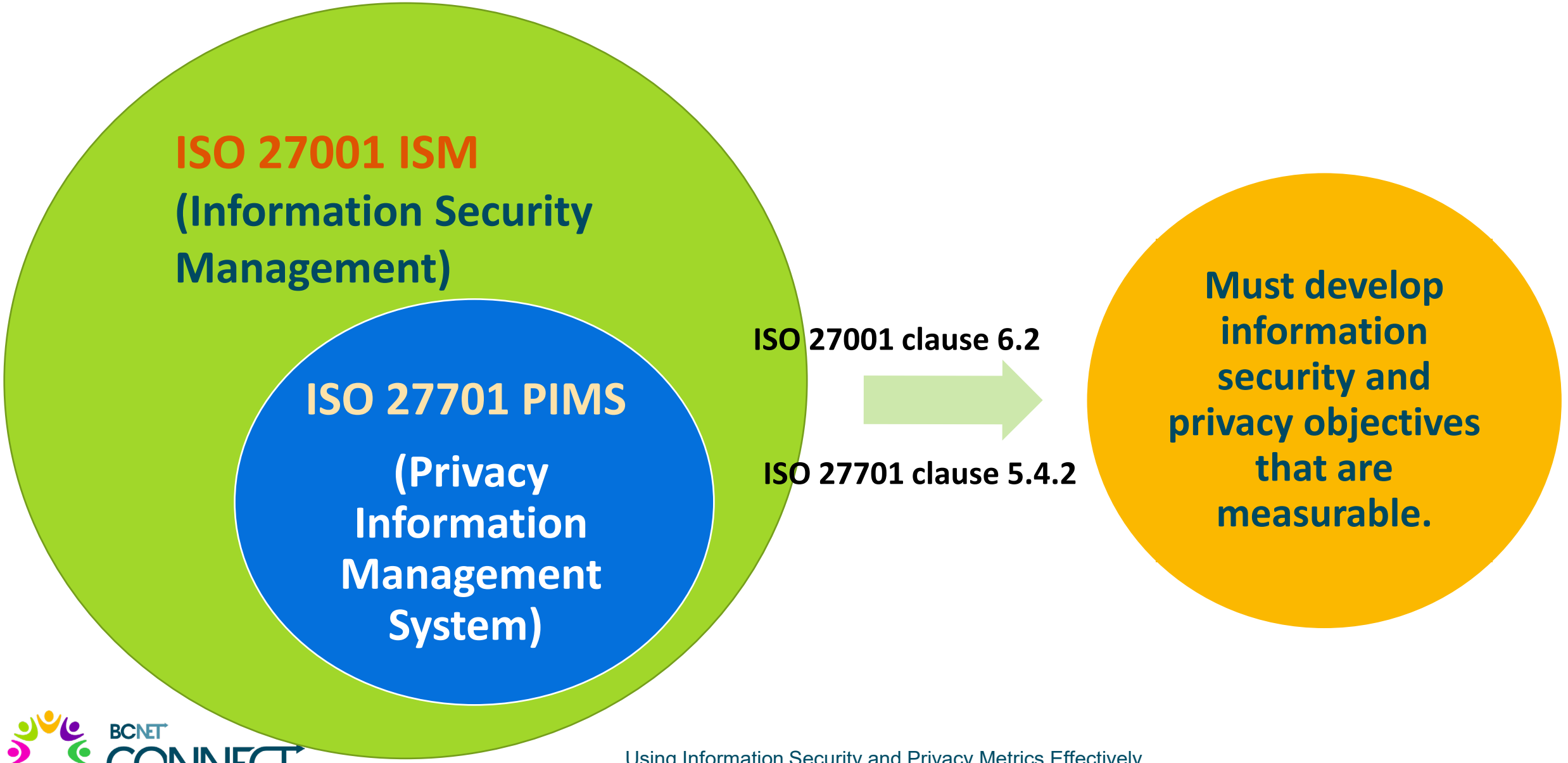
- Relevant
- Measurable
- Actionable
- Reliable
- Inexpensive
- Clearly defined

The Audience

Different metrics resonate differently depending on the audience:

Stakeholders	Nature of Metric	Purpose of Reporting Metrics
Executives (CEO/ Board of Directors)	• High level description of risk and program maturity • Material Incidents ILLUSTRATIVE	• Ensure buy in/support • Proper allocation of staff/resources to risks • Report on risk/impact on bottom line • Report on program maturity/status/progress
Senior Leadership (GC, CIO, CISO, CITO, CDO, CMO, CRO)	• In-depth review of risk • Impact of risk-based approaches • Incident numbers and trends • Program Implementation progress/ spend • High-level benchmarking results	• Ensure buy in/support and executive oversight • Risk acceptance/decisions • Triage priorities • Control effectiveness and maturity • Ensure support in gathering data

ISO Compliance



BCNET CONNECT

Cyber Security Program Metrics

Key Drivers - WHY

- Statutory & Regulatory Obligations
- Alignment With Business Strategy
- Understanding Threat Landscape
- Cyber Risk & Cyber Insurance

Challenges

- Incomplete data
- Outdated data
- Biased data

Cyber Security Metrics - WHAT

Training & Awareness

Vulnerability & Patch Management

Endpoint Security

Business Continuity Management

- Security Incident Management
- Disaster Recovery

IT Risk, Audit & Compliance

Peer Review

Cyber Security Metrics - HOW

Metrics are a means to an action to drive Cyber Security Program Maturity

- Target Audience
- S.M.A.R.T.
- Ensure quality & validity
- Standardize data collection

Map Cyber Security Goals & Key Performance Indicators (KPIs)

Category	Security Goal	KPI	Metrics
Training & Awareness	Implement a training & awareness program	% of staff trained biannually trained	% of trained staff per department
Vulnerability & Patch Management	Improve deployment time for patches on critical servers	% of critical patches fully deployed within target window as per Standard	% critical patch deployment on critical servers
End Point Security Compliance	Implement endpoint security solution on all desktops	% of desktops & servers with endpoint protection	% of endpoints missing
Business Continuity	Test Business Continuity Plans once a year	% of critical business units having defined RTOs/ RPOs	# of units completed tabletop exercise per year
	Improve incident remediation time	Mean time to remediate per incident type (#)	% deviation from target time
	Improve DR capabilities & preparedness of DR response team	% completeness of plan	DRP Test frequency (#)
IT Risk Audit & Compliance	Improve IT Risk Management	% of projects with a completed STRA	# of signed off SOARs Total # non-conformity audit findings

Sample Cyber Metrics 1/3

Training & Awareness

- Training & Awareness Program coverage (%)
- Periodic Phishing Campaigns statistics (% click rate)

Vulnerability & Patch Management

- Average vulnerability age (#)
- Identified, patched vulnerabilities by severity & system criticality (#)
- Identified unpatched vulnerabilities by severity & system criticality (#)

Sample Cyber Metrics 2/3

Endpoint Security

- # Threats detected over period of time
- % # Threats resolved
- % # Endpoints missing endpoint protection

IT Risk, Audit & Compliance

- # signed SOARs (Statement of Acceptable Risk)
- # Security Policy/Standard Exceptions
- Total # non-conformity audit findings
- # critical & high audit findings currently outstanding

Sample Cyber Metrics 3/3

Security Incident Management

- MTTD (Mean Time to Detect)
- MTTR (Meantime to Remediate /Recover)
- Average # /type/severity of incidents over time
- % of incidents closed within SLA (Service Level Agreements)

Disaster Recovery

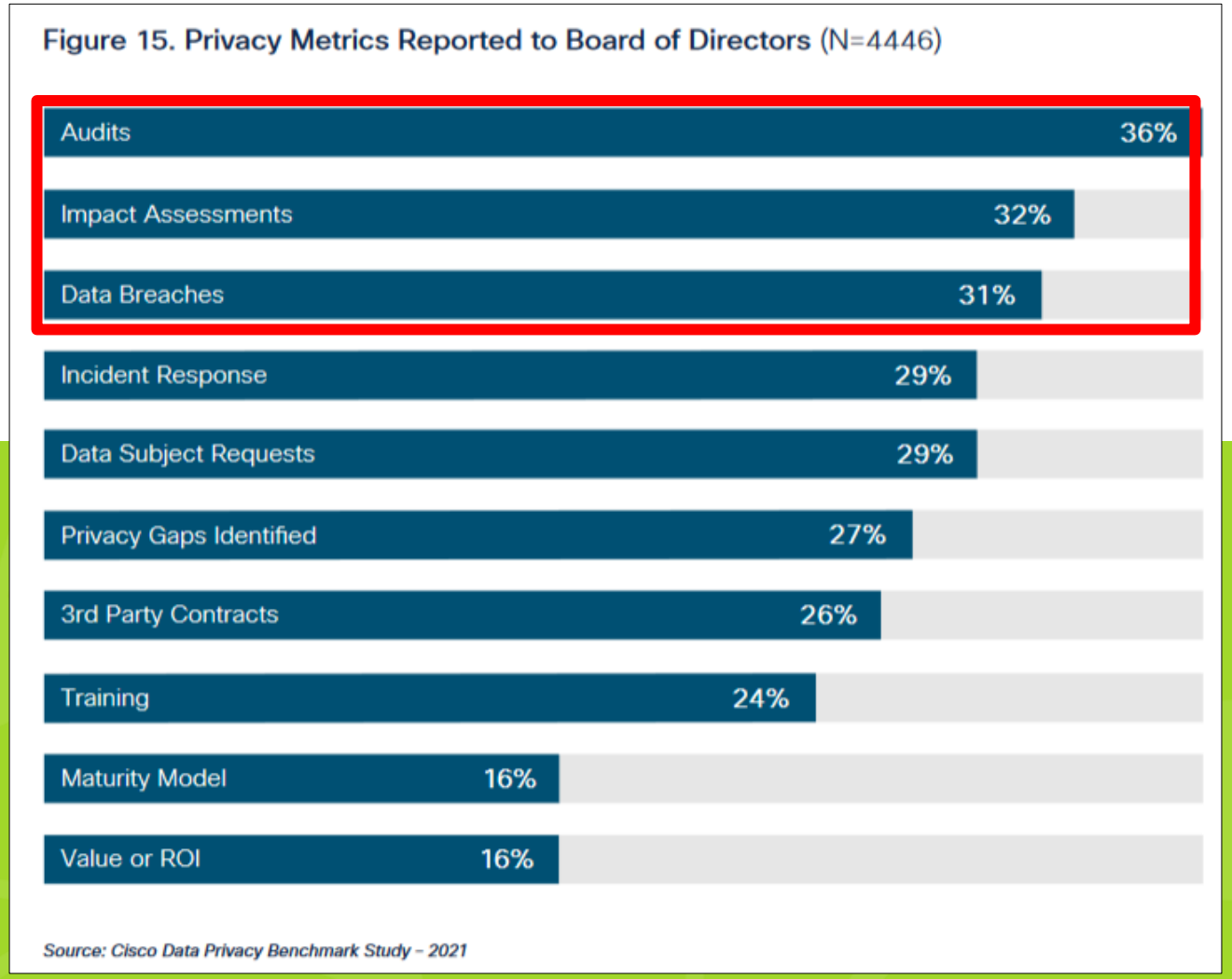
- Average time taken to recover critic al business process
- Difference between actual & target recovery time
- % completeness of the plan

BCNET CONNECT

Privacy Program Metrics

Cisco 2021 Data Privacy Benchmark Study

93 % of organizations are reporting privacy metrics to Snr management/ Boards



Compliance – One Driver for Metrics

2021

BC *Freedom of Information and Protection of Privacy Act* (FIPPA) Amended

Mandatory requirements

- Privacy Management Program
- Privacy Breach Reporting

2023

Privacy Management Program (PMP)

A PMP ensures that privacy is built into all initiatives, programs, or services by design.

Mandatory components include:

- Education and awareness
- Policies
- Privacy Impact Assessments (PIAs)
- Implementation of privacy breach reporting processes
- A process for monitoring & updating PMP to ensure it remains FIPPA compliant

ACCOUNTABLE PRIVACY MANAGEMENT IN BC'S PUBLIC SECTOR, OIPC 2023

PMP - Reporting Expectations

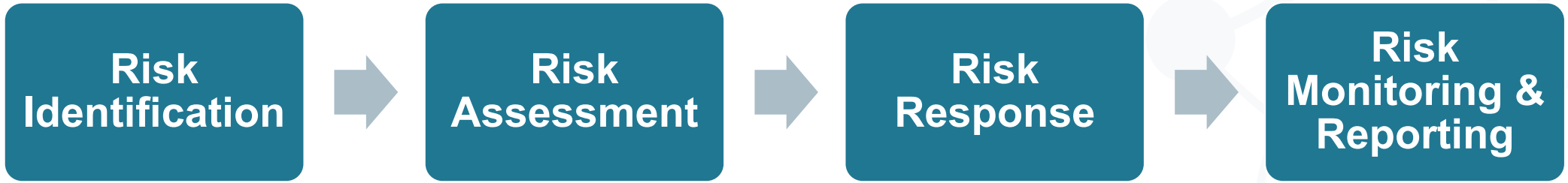
- Regular reports to executive on progress & identifiable risk and compliance issues.
- Final report of all findings to executive with full mapping against FIPPA requirements

ACCOUNTABLE PRIVACY MANAGEMENT IN BC'S PUBLIC SECTOR, OIPC 2023

Tools

- **Spreadsheets**
- **Privacy Risk Register**

  Tool to track & manage all privacy risks information in one place:
  (PIAs, Privacy Breaches, other privacy concerns identified...)



- Compliments Cyber Security Risk Register
- Linked to Enterprise Risk Register
- Supports reporting requirements

PMP - Training & Awareness

- **Privacy Awareness Training - Intro & Advanced/customized**
- **Privacy Education**

Collection – Ongoing

Reporting – Annual

- # Training/education sessions offered
- # attendees (in person/online)
- % employees completed basic training/ Advanced training
- # educational materials created (BCIT News/intranet/web pages...)

PMP - Accountability

- **Policies & procedures**
- **Privacy Notices (students, employees, alumni)**
- **Advisory**
- **Collection** – Ongoing
- **Reporting** – Annual

Policies/procedures/ Date updated

notices provided/ % by type of notice (survey/intake form...)

School/business area requesting advice

technologies/business models advised on

PMP - Privacy Impact Assessments

What is a PIA?

PIAs - a risk management & compliance review process used to identify & address potential privacy & information security issues.

Legislated

FIPPA now requires public bodies to conduct a PIA for all new or substantially modified initiatives that involve personal information.

An initiative refers to a system, project, program, or activity that supports BCIT business.

Projects are reviewed & risk is assessed in partnership with Cyber Security

Privacy Impact Assessments

PIAs use a risk matrix scale for impact & likelihood ratings
- which then calculate privacy & Information security risk scores.

			Potential Consequences				
			L6	L5	L4	L3	L2
			Minor injuries or discomfort. No medical treatment or measurable physical effects	Injuries or illness requiring medical treatment. Temporary impairment.	Injuries or illness requiring hospital admission.	Injury or illness resulting in permanent impairment.	Fatality
			Not Significant	Minor	Moderate	Major	Severe
Likelihood	Expected to occur regularly under normal circumstances	Almost Certain	Medium	High	Very High	Very High	Very High
	Expected to occur at some time	Likely	Medium	High	High	Very High	Very High
	May occur at some time	Possible	Low	Medium	High	High	Very High
	Not likely to occur in normal circumstances	Unlikely	Low	Low	Medium	Medium	High
	Could happen, but probably never will	Rare	Low	Low	Low	Low	Medium

Privacy Impact Assessments KPIs

Collection – Ongoing I **Reporting** – Annual

KPI Name	KPI Goal	KPI Measure	KPI Formula
Risk Mitigation Completion Rate	To measure the success rate in deploying & executing the identified risk action treatment plan	% of risk mitigation plan completed on target date	(Total # of risk mitigations deployed) – (risk mitigations delayed + on hold) / Total # of risk mitigations deployed * 100
Risk Mitigation (Privacy Training) Completion Rate	To measure the success rate in completion of privacy trainings	% of privacy trainings completed	Total # of privacy trainings completed (trainings identified as risk mitigations in PIA) / total # of privacy trainings deployed as risk mitigations in a PIA * 100

Privacy Risk Register

– Tracks Moderate or High risks identified in PIA & the mitigation strategies

- Shifts in risk scoring are recorded.

PMP - Mandatory Privacy Breach Notification & Reporting

Public bodies **must** notify an affected individual and the OIPC if a privacy breach could reasonably be expected to result in **significant harm** to an individual.

Privacy Risk Register

- ALL privacy breaches recorded & tracked & risk scores calculated
  - Risk score supports & documents decision to notify/not notify OIPC & affected individual.

BCIT Privacy Incident/Breach Metrics

Collection – Ongoing
Reporting – Annual

- # incidents.
- # of confirmed privacy breaches.
  - % of privacy breaches by cause.
  - % privacy breaches by risk rating (Minor/Moderate/Severe).
- # affected individuals by group (students/employees/alumni)
- # breaches with notification to OIPC & affected individuals.
- % privacy complaints (resolved/ submitted to OIPC)

BCNET CONNECT

Conclusion

Benefits of Effective Metrics

- Meet compliance requirements
- Informed decisions
- Manage risk
- Improve program maturity & performance


Q
&
A