15.

STAFF REPORT
INFORMATION ONLY

IT Security – Annual Report

Date: March 27, 2023

To: Toronto Public Library Board

From: City Librarian

SUMMARY

The purpose of this report is for the Toronto Public Library Board to receive the annual information report and to provide an update to the City of Toronto's Cybersecurity Confirmation Program.

Toronto Public Library (TPL) is committed to achieving a safe and secure IT environment, including a targeted level of protection from internal and external cyber security threats.

FINANCIAL IMPACT

This report has no financial impact beyond what has been approved in the current year's budget.

The Director, Finance & Treasurer has reviewed this financial impact statement and agrees with it.

ALIGNMENT WITH STRATEGIC PLAN

To enable TPL's Strategic Plan 2020 – 2024, a safe and secure IT environment is essential for both staff and customers. Consequently, the Digital Strategy 2020 – 2024 includes a priority to "adopt a modern security approach to improve cybersecurity and TPL's overall security position".

EQUITY IMPACT STATEMENT

The IT Security, Risk & Governance Program will enable equitable access to technology in a secure manner that protects the privacy and confidentiality of customers and staff. The maturity of TPL's security posture will promote confidence that TPL protects people's identities and activities to participate in the digital world.

DECISION HISTORY

At its January 25, 2021 meeting, the TPL Board approved the Digital Strategy 2020-2024. As identified in the digital strategy action plan 2021, there is a focus on IT Security Advancement.

At its December 6, 2021 meeting, the Board approved the Information Security Policy and TPL's participation in the City of Toronto Confirmation program.

At its September 19, 2022 meeting, the TPL Board received an update to the Risk Register. Cyber Security risks were reported in the update.

ISSUE BACKGROUND

Annual IT Security Report

As per the *Information Security Policy,* there will be a report to the Board on a regular basis regarding information security risk and major cyber security incidents. This is the second annual report on IT Security.

City of Toronto Cybersecurity Confirmation Program

At its October 29-30, 2019 meeting, City Council received report from the Auditor General on Cyber Safety: A Robust Cybersecurity Program Needed to Mitigate Current and Emerging Threats: Auditor General's Report in Item 2019.AU4.1.

A motion at City Council on November 9, 2021*: AU10.4 Auditor General's Cybersecurity Review: Toronto Fire Services Critical System Review* requested the Library Board to direct TPL staff to participate in the City of Toronto's Cybersecurity Confirmation Program. As part of this program, TPL's senior ITS managers would work in consultation with the City of Toronto's Chief Information Security Officer to develop a confirmation program which would identify and report out on rates of compliance, remediation plans and strategies to reduce risk and ensure corporate compliance.

At its meeting on December 6, 2021, the TPL Board approved participation in the City of Toronto's Confirmation Program.

TPL submitted the confidential Confirmation Form, which reported on the status of thirteen cyber security controls on January 31, 2022.

On October 6, 2022, the City of Toronto Office of the Chief Information Security Officer held the first meeting of the Executive Risk Cyber Management group to formalize a "Confirmation program" and establish accountability towards the management of cyber risk and control assurances.

COMMENTS

Update to City of Toronto Confirmation Program

The City of Toronto Confirmation program was a self-assessment of thirteen security controls. These controls are a subset of TPL's security framework. TPL has reported that it has eight of the thirteen controls in place. The remaining five (patching, safe passwords, administrator account management, network access management, and disaster recovery plans) have remediation plans.

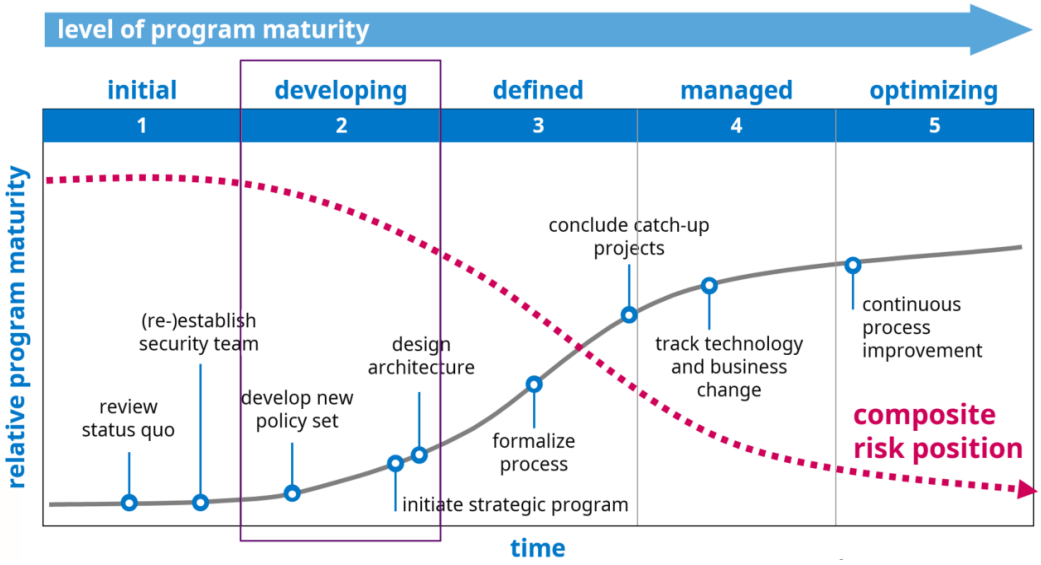
Compliance Objective	Description	2022
1	All employees must complete cybersecurity, phishing training	✓
2	Phishing campaigns must be carried out at least once annually	✓
3	All critical, high and medium security patches must be remediated	
4	All systems are adequately hardened and configured	✓

5	All outdated systems/equipment are removed	✓
6	Complex passwords are in place for all systems	
7	All administrative accounts are tightly controlled	
8	All open ports are closed	✓
9	All critical systems are segregated	✓
10	All network access is properly controlled	
11	All Wi-Fi access is secure and updated encryption is in place for critical communications	✓
12	Physical security around critical systems is in place	✓
13	Disaster recovery plans are in place	

As part of the next stage, the Confirmation Program will be reviewing the effectiveness of the security controls in place through documented evidence.

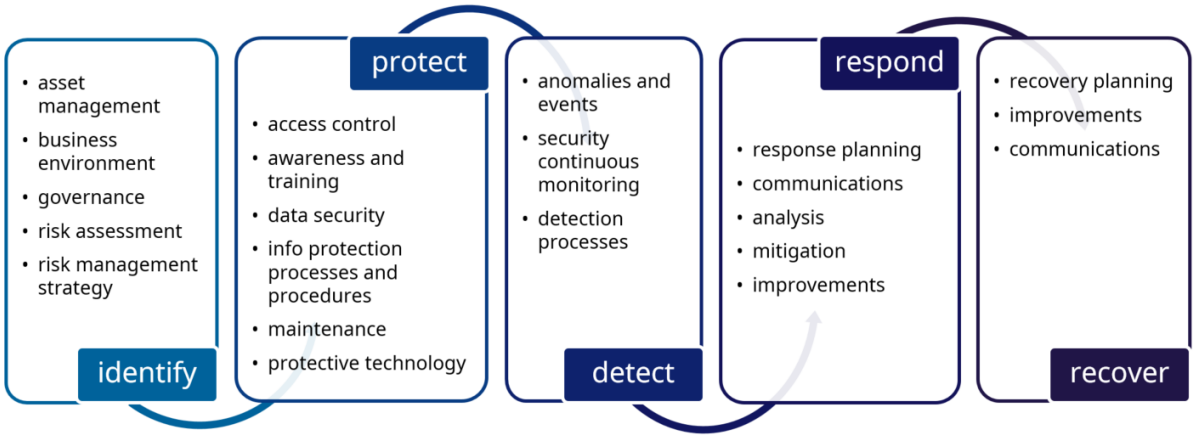
Annual IT Security Report

TPL is at a developing level of maturity for the IT security program. The focus for the last year has been to assess the current state, close quick-win gaps, and continue reporting on security operations.



TPL will mature the information security program by implementing selected controls from the NIST cyber security framework (summarized below). The risk-based

framework maps into other mature security frameworks to provide a consistent approach. This report provides updates based on the framework.



1. Identifying Organization Risk

The security program strategy is to develop an approach that aligns with the enterprise risk management program. Varying security controls will be designed based on organizational risk tolerances. The approach is to perform risk assessments and create standardized reporting to enable management decision-making.

i. Business environment

The focus has been to create a data classification system and assess requirements based on two mature compliance regimes: PCI-DSS and Privacy.

TPL conducted its first compliance self-assessment for the protection of payment processing: PCI-DSS (i.e. Payment Card Industry – Data Security Standard). The assessment revealed missing operational processes and documentation. Remediation plans are being prepared.

TPL has continued to build upon the existing privacy compliance practice by maturing the security program. With the recent hiring in TPL's Privacy, Risk and Governance office, a security controls catalog will be aligned with the compliance requirements of the privacy laws.

ii. Governance Reporting

Monthly management reports on information security started at the beginning of the year.

iii. Risk Assessment Program

The cyber security risk management program focused on defining cyber security risks and aligning them with the enterprise risk tolerances.

a. Data classification standard

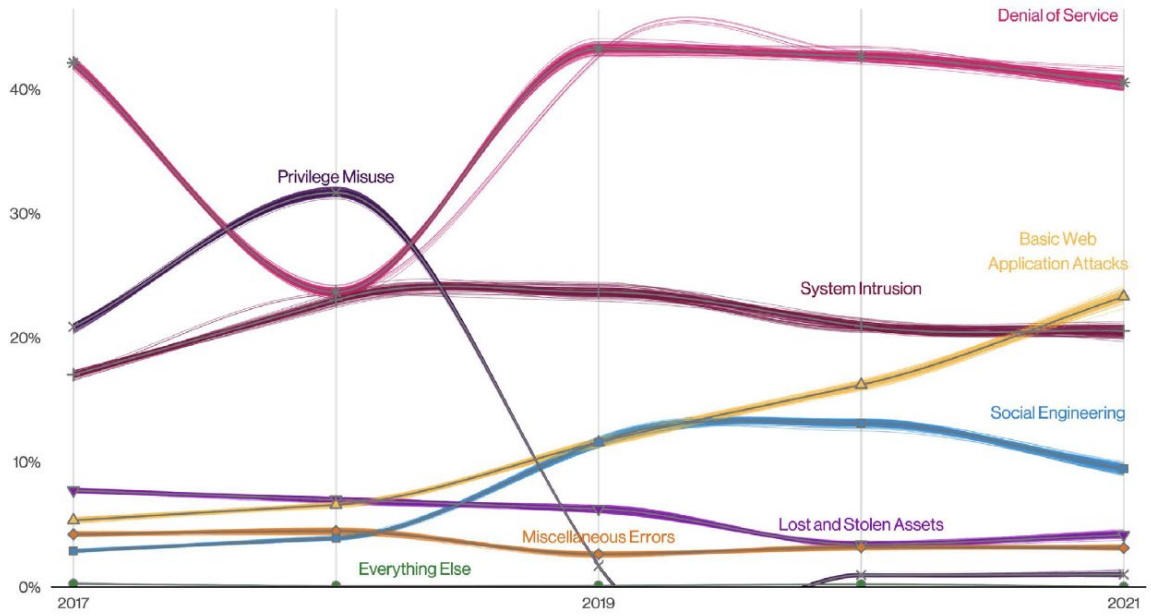
A data classification standard is in development. The data classification standard will contribute to the foundation of a risk-based approach to IT security controls. Restricted data will have the highest level of security controls; while public data will have a minimum set of security controls.

b. Enterprise Risk Register

The enterprise risk register was updated to separate cyber security risks from Privacy compliance risks. Although compliance and security are closely interconnected, they are distinct in the protection of information and assets.

The register for cyber security risk was further defined to focus on the likelihood and impact of the top-reported breaches in North America.

(Verizon, 2022)



Denial of Service, Basic Web Application Attacks, and System Intrusion were the top reported breaches. TPL is at risk from these top three cyber security threats and as such risk mitigations are warranted.

c. Phishing Risk Assessments

The risk assessment program also measured the risk of phishing attacks using a third-party phishing simulator. Phishing is a common attack where users are duped into providing confidential information through email. During the last year's assessment, an average of 3% of TPL's staff were successfully phished. The data will be used as a baseline for future assessments and targeted security training.

2. Protection of Critical Services

TPL implemented several protective controls during the year.

i. Identity Management, Authentication and Access Control Program

The strategy was to focus on improving protection of staff identities by implementing protective controls included with Microsoft 365 licenses. These protections are industry best practices.

a. Updated Password Standard

An updated password standard was approved to reflect improving computer processing times. Updated passwords reduce the risks associated with guessing a weak password for a user's login. During this year, the updated password standard will be applied to all staff accounts.

TPL also conducted an assessment on customer identities. An architecture and roadmap will be developed this year through external consultation.

b. Multi-Factor Authentication

Multi-Factor Authentication (MFA) improves security by asking users to verify who they are using multiple sources. Multi-Factor Authentication will be implemented at the same time as the updated password standard for staff accounts this year.

MFA for customer identities will be considered as part of the external consultation.

ii. Network Protections and Access Controls

TPL also defined a reference architecture to simplify network access controls through consolidation. Removal of redundant network access controls will improve security by allowing the operations to focus on a reduced number of technologies. The re-architecture will address deficient services increasing protection against top two industry breaches: denial of service and web application attacks.

iii. Awareness and Training Program

The annual mandatory cyber security awareness training for all staff is in its second year. The approach is to leverage expert content and select topics based on risks to

TPL and common risks identified from the industry. This year, the annual cyber security training and awareness program focussed on the following topics:

- Business email compromise
- Creating safe passwords
- Cloud security
- Working remotely
- Phishing
- Mobile security

iv. Information Protection

a. Change Control

Change control is the management of technology changes. Historically, changes were frequently implemented with limited review, sometimes resulting in loss of availability, integrity, and confidentiality. During the past year, TPL has focussed on communicating production changes across stakeholder groups through the Architecture & Change Review Committee (ACRC). The ACRC reviewed an average of sixteen major production changes on a monthly basis.

3. Detection of Cyber Security Events

i. Continuous Monitoring for Security Events

Continuous monitoring provides threat intelligence to users and administrators across all of the systems.

a. Microsoft 365 Monitoring

As mentioned above, TPL has started to activate security functionality included with Microsoft 365 licenses; this includes detection of risky logins and unsafe links/attachments.

Microsoft detects risky logins when a user login occurs under potentially unlikely circumstances, such as logins from two locations where the travel time is improbable (e.g. Vancouver and Toronto within 5 minutes).

Microsoft detects unsafe links and attachments before reaching the end user's device. This augments anti-virus software using machine learning in the cloud.

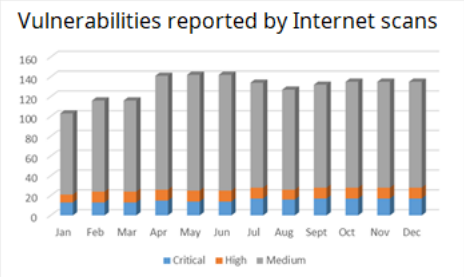
b. Security Information and Event Management System (SIEM)

A security information and event management system automatically detects security events by correlating information from multiple sources. The SIEM analyzes large amounts of complex data that humans cannot perform. Unfortunately, monitoring from the SIEM discontinued during this year due to a technology change by the third-

party service provider and competing priorities for internal resources. The focus for this year will be to re-establish a SIEM.

ii. Vulnerability Management Program

Vulnerability management is the process of assessing an organization's risks from cyber security threats. The approach last year was to focus on vulnerabilities that originate from the Internet and report them to operational teams.



The program receives industry reports from the Government of Canada and performs Internet scans. TPL received an average of 68 monthly vulnerability notifications from the industry. Internet scans have detected an average of 20 medium-to-critical vulnerabilities for TPL systems exposed directly to the Internet.

The focus for the upcoming year will be on expanding the program to assess internal risks through internal vulnerability scans.

4. Response & Recovery from Cyber Security Incidents

Cyber security incident response and recovery is based on TPL's general IT incident management process.

i. Response Planning

Cyber security incident playbooks are being created for specific scenarios e.g. ransomware, system compromise. An annual exercise will be conducted this year to validate the ransomware playbook.

ii. Recovery Planning

Cyber security recovery planning relies on the IT disaster recovery plans (backup/ restore). Cyber security incident recovery planning will focus on unique aspects of cyber security incidents.

CONCLUSION

TPL's IT Security, Governance & Risk Program is based on the NIST cyber security framework. This is a risk-based framework with the objective of providing a safe and secure IT environment.

By maintaining and improving policy, practices and technology, the risk of internal and external cyber security threats are minimized. The Program is key to achieve the following objectives:

- ensure the protection of TPL's data and information assets;
- establish controls for protecting TPL's information and information systems against theft, abuse, and other forms of harm or loss;
- enable the requirements for confidentiality, privacy, integrity, and availability for TPL's employees, contractors, vendors, and other users;
- ensure business continuity, including the recovery of data and operational capabilities in the event of a security breach;
- motivate administrators and employees to maintain the responsibility for, ownership of, and knowledge about information security;
- ensure that external service providers are made aware of, and comply with, TPL's information security needs and requirements and continuously assess whether they maintain an acceptable security posture;
- balance the need for the above with the investment and policy constraints required to achieve an appropriate level of protection while maintaining business agility; and
- ensure compliance with all applicable laws, regulations, and TPL's policies, controls, standards, and guidelines.

CONTACT

Steve Till-Rogers; Director, Digital Strategy & CIO; 416-393-7104; stillrogers@tpl.ca

Frank Kim, Manager; IT Security & Enterprise Architecture; 416-395-5816; fkim@tpl.ca

SIGNATURE

_____

Vickery Bowles
City Librarian

ATTACHMENTS

Attachment 1: Presentation: Annual Report on IT Security

Attachment 1

Annual Update on IT Security

Frank Kim
Manager IT Security & Enterprise Architecture

Steve Till-Rogers
Director, Digital Strategy & CIO

TPL Board
March 2023

agenda

- Background
- Update of the City of Toronto confirmation program
- Annual IT security update

background

TPL Digital Strategy 2020 – 2024

- Approval of IT security advancement projects under the adaptive technology foundation program

TPL Board of Directors meeting Dec 2021

- Receipt of previous IT security update and annual report
- Approval of TPL's first security policy, creating accountability under Director, Digital Strategy and Chief Information Officer and commitment to mature security framework

City of Toronto confirmation program

- AU10.4 Auditor General's Cybersecurity Review: Toronto Fire Services Critical System Review requesting TPL to participate with City of Toronto Confirmation Program in Nov 2021
- Approval to participate in City of Toronto confirmation program at TPL's Dec 2021 Board meeting
- Executive Risk Cyber Management Group established Oct 2022 to formalize the confirmation program

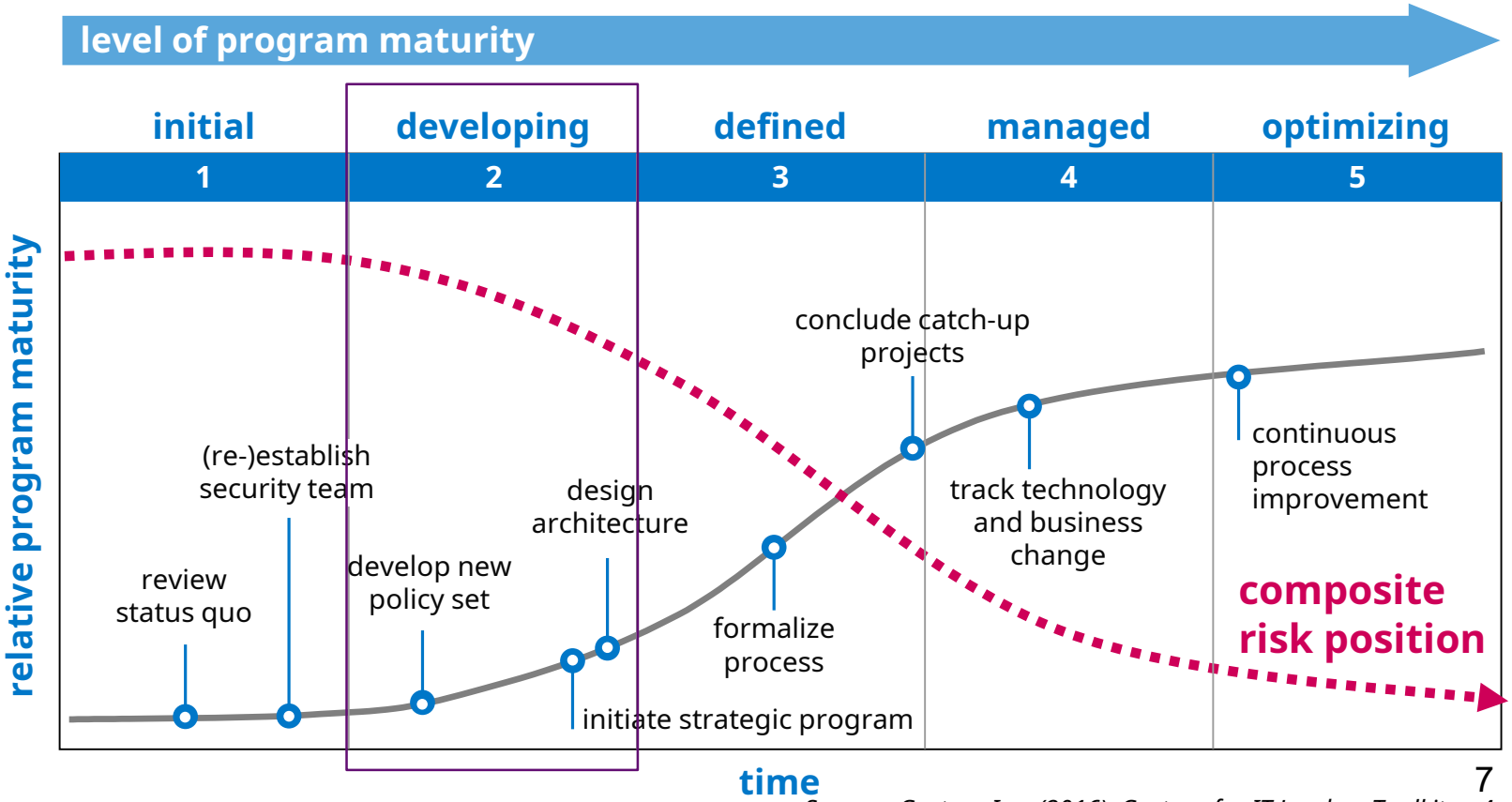
Update to City of Toronto confirmation program

Update to City of Toronto confirmation program

Compliance Objective	Description	2022
1	All employees must complete cybersecurity, phishing training	✓
2	Phishing campaigns must be carried out at least once annually	✓
3	All critical, high and medium security patches must be remediated	
4	All systems are adequately hardened and configured	✓
5	All outdated systems/equipment are removed	✓
6	Complex passwords are in place for all systems	
7	All administrative accounts are tightly controlled	
8	All open ports are closed	✓
9	All critical systems are segregated	✓
10	All network access is properly controlled	
11	All Wi-Fi access is secure and updated encryption is in place for critical communications	✓
12	Physical security around critical systems is in place	✓
13	Disaster recovery plans are in place	

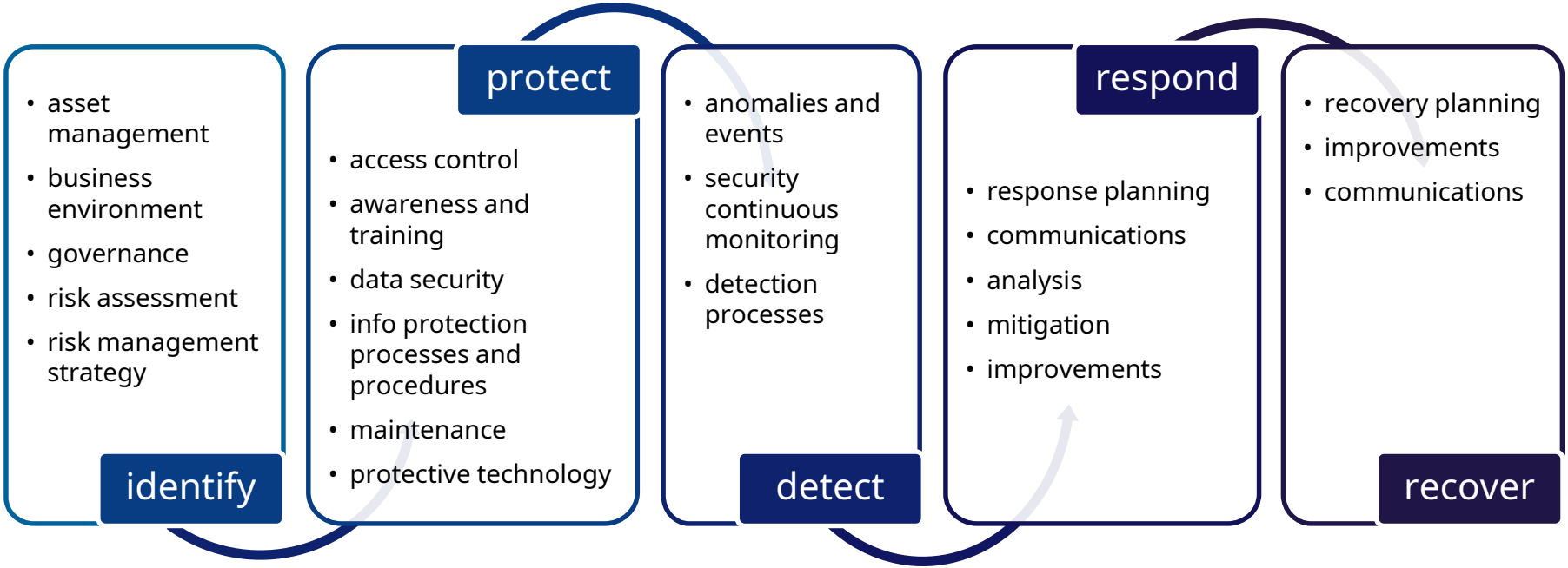
Annual report on IT security

current program status



Source: Gartner Inc. (2016). Gartner for IT Leaders Toolkit. p.4.

IT security risk & governance program framework
(based on NIST Cyber Security Framework)



identifying organizational risk

identify

2022 update

Business environment
- First PCI self-assessment

Governance
- Started monthly executive reporting

Risk assessment
- Enterprise risk register – cyber security methodology updated for risks based on industry breaches
- phishing risks based on simulated attacks

2023 approach

Business environment
- Remediation of PCI compliance: documentation, processes

Governance
- Continue reporting with alignment to framework

Risk assessment
- Data classification standard to define risks

protecting critical services

protect

2022 update

Identity management, authentication & access control
- Creation of standards: modern passwords

Awareness & Training Program
- Annual sustainment

Information Protection
- Focus on change communications

2023 approach

Identity management, authentication & access control
- Focus on staff: Microsoft Office 365 protections (modern passwords, multi-factor authentication)
- Develop roadmaps for customer IAM: solution architecture through external consultation
- Simplify wide area network access controls through consolidation

Information protection
- Improve change compliance
- Develop of data security controls based on risk from data classification

detecting cyber security events

detect

2022 update

Anomalies & events
- Implement Microsoft 365 security features: risky login detection, safe links/ safe attachments

Continuous monitoring for security events
- Service disruptions for security information and event management system (SIEM) and security operations centre (SOC)
- Initiate external vulnerability management program: industry notifications, Internet scans

2023 approach

Anomalies & Events
- Stabilize health of security logging for servers

Continuous monitoring for security events
- Restore disrupted services: SIEM, SOC
- Initiate internal vulnerability management program

responding to cyber security incidents

respond

2023 approach

- Create cyber security playbooks, including ransomware
- First cyber security incident tabletop exercise

recovering from cyber security incidents

recover

2023 approach

- Communications plan

thank you
questions