Region of Peel
working with you

Security Assessment

Audit Committee Report

Arthur Michalec
IT Security Advisor - CISSP, TOGAF 9, GIAC GMOB
IT Services Delivery | IT Operations | Digital & Information Services

What is Cyber Security?

"*Cyber Security* refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access."

Did you know that for the month of July the Region of Peel…

Blocked 86% of all emails daily

Daily Incoming Emails	Unsolicited Emails				
	SPAM	Malware	Viruses	Bulk	Phishing
410,000	282,900 (69%)	36,900 (9%)	20,500 (5%)	12,300 (2%)	4,100 (1%)

Blocked 2% of all website sites daily

Daily Visited Web Pages	Blocked Sites			
	Malware	Phishing	Cryptomining	Regional Values Policy
9,600,000	105,500 (1%)	51,250 (0.5%)	32,565 (0.3%)	10,250 (0.1%)

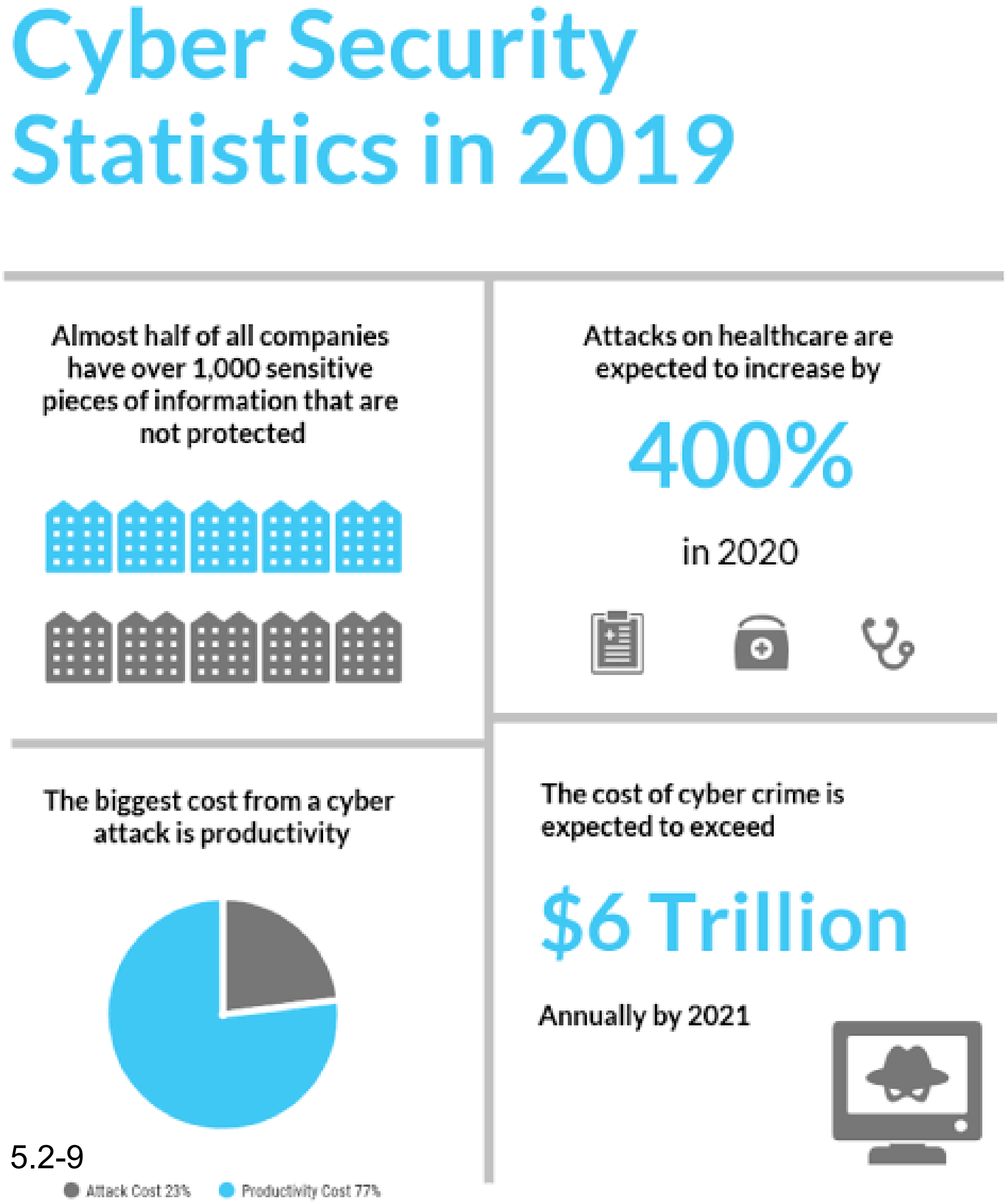
Achieved average scores as part of its first internal email phishing campaign

Phishing Campaign Targets	Users Who	
	Clicked Malware Link	Supplied Credentials
1000	193 (19%)	82 (8%)

Cyber Security

"When applied correctly in the enterprise, Cyber Security can reduce risk related to system or information compromise. However, the risk cannot be completely eliminated."

Source: stanfieldit.com



Cyber Security Statistics in 2019

Almost half of all companies have over 1,000 sensitive pieces of information that are not protected

Attacks on healthcare are expected to increase by

400%

in 2020

The biggest cost from a cyber attack is productivity

The cost of cyber crime is expected to exceed

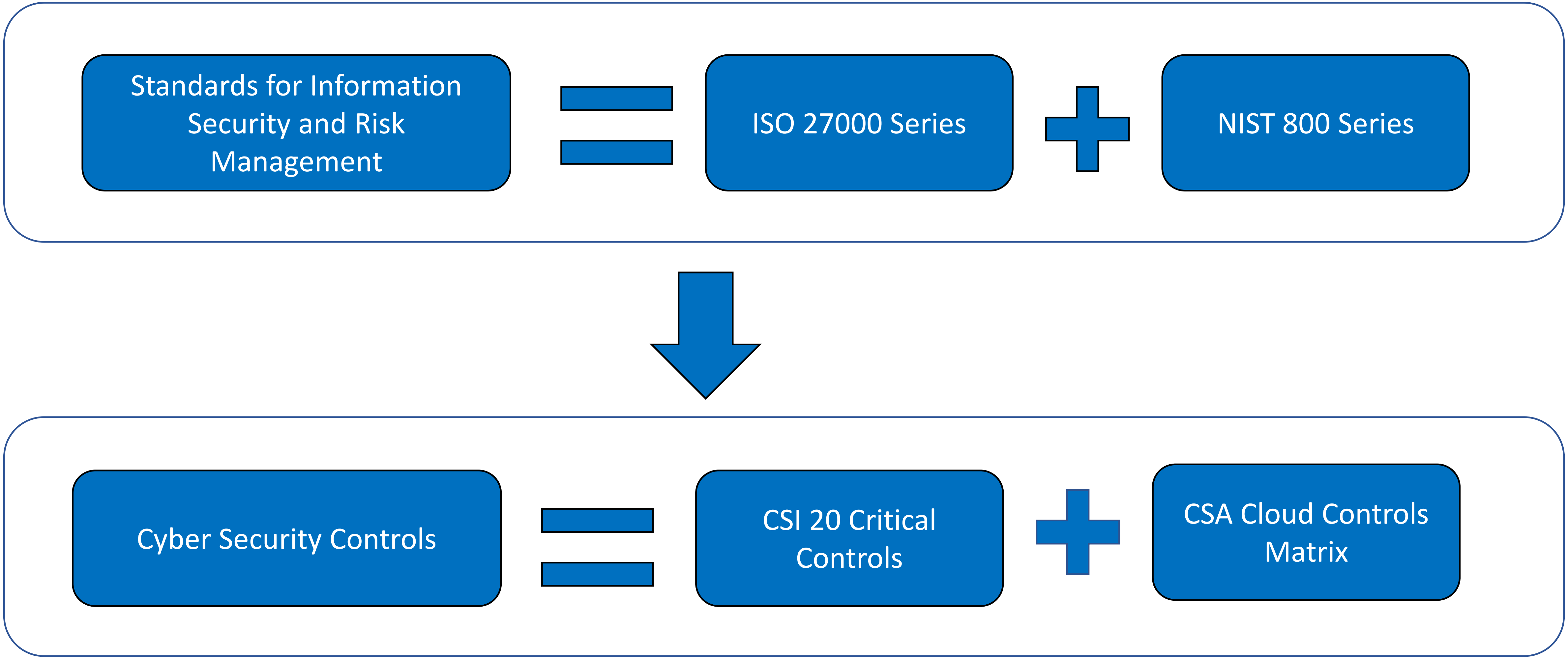
$6 Trillion

Annually by 2021

Remote Work - Risks

- Unsecure Networks
- Phishing attacks
- Sharing work computers with family
- Unpatched computers
- Physical security
- Lack of security awareness

The Region of Peel lives by industry standards

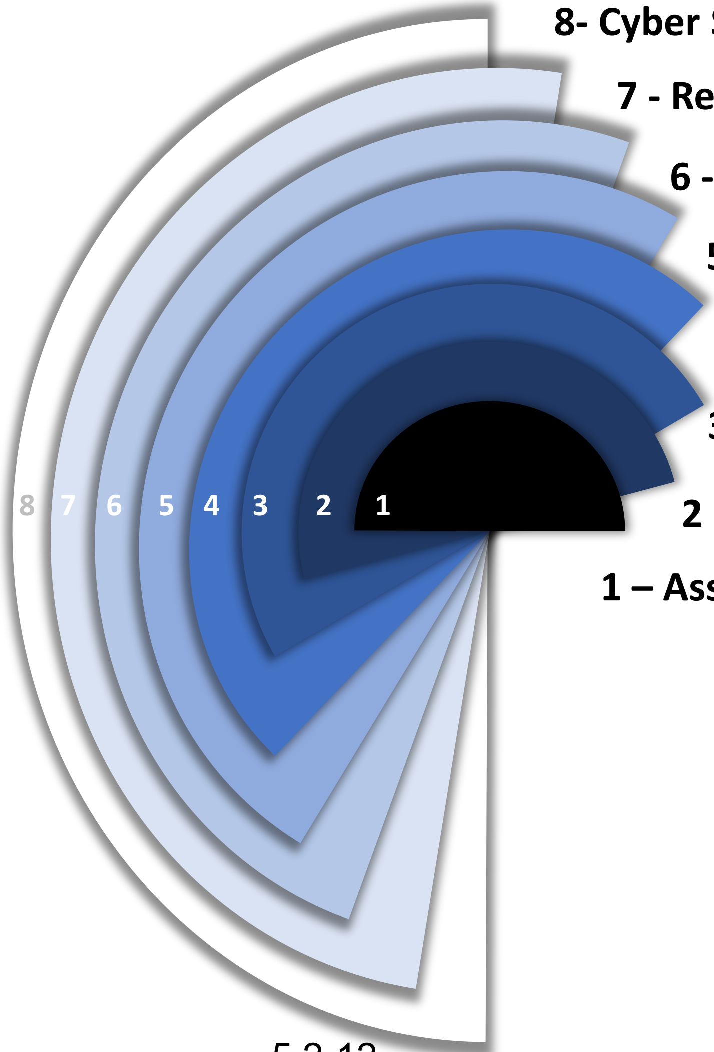

Standards for Information Security and Risk Management
ISO 27000 Series
NIST 800 Series
Cyber Security Controls
CSI 20 Critical Controls
CSA Cloud Controls Matrix

The Region of Peel’s layered security controls

CIS 20 Critical Controls

+

CSA Cloud Controls Matrix



8- Cyber Security Awareness Training

7 - Regulatory Compliance Controls

6 - Content Filtering

5 - Security Patch Management

4 - Vulnerability and Advanced Threat Protection

3 - Endpoint Protection

2 - Identity and Access Controls

1 – Asset Controls

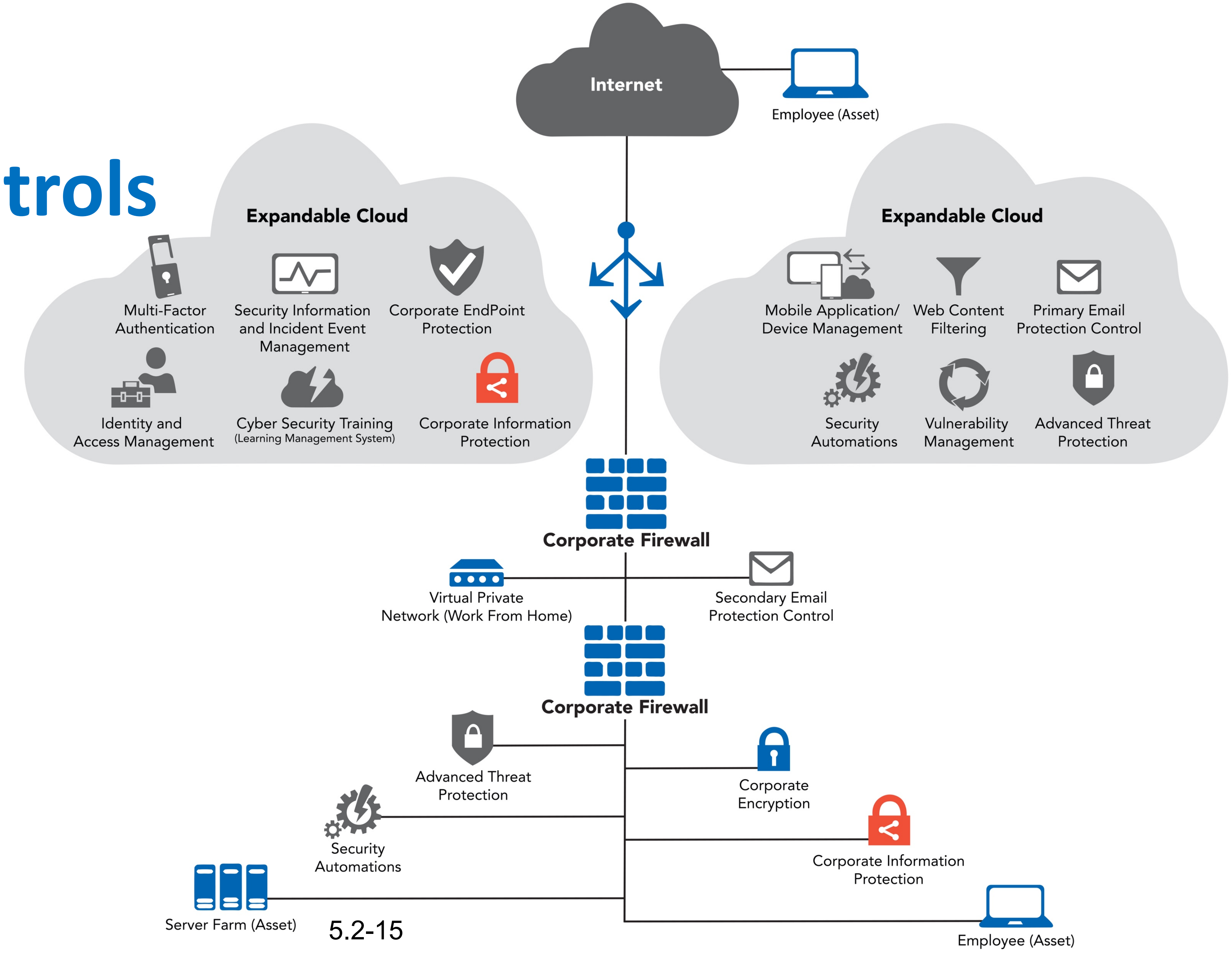
Examples of Security Controls

Asset Controls	System build procedure template Retain audit logs for compliance
Identity Access Controls	Identity Governance enforcement policies Least privilege access
Endpoint Protection	Antivirus software Machine Learning to identify threats
Vulnerability and Advanced Threat Protection	Technology Threat Risk Assessment process Automated Vulnerability Assessment risk

Examples of Security Controls

Security Patch Management	Inventory of vulnerable applications Audit compliance
Content Filtering	Email protection User of Safe Links and Safe Attachments
Regulatory Controls	Device or communication encryption Use of secondary forms of authentication
Cyber Security Training	Training delivered through Learning Management System Internal Phishing campaigns or simulations

Peel’s Cyber Security Controls

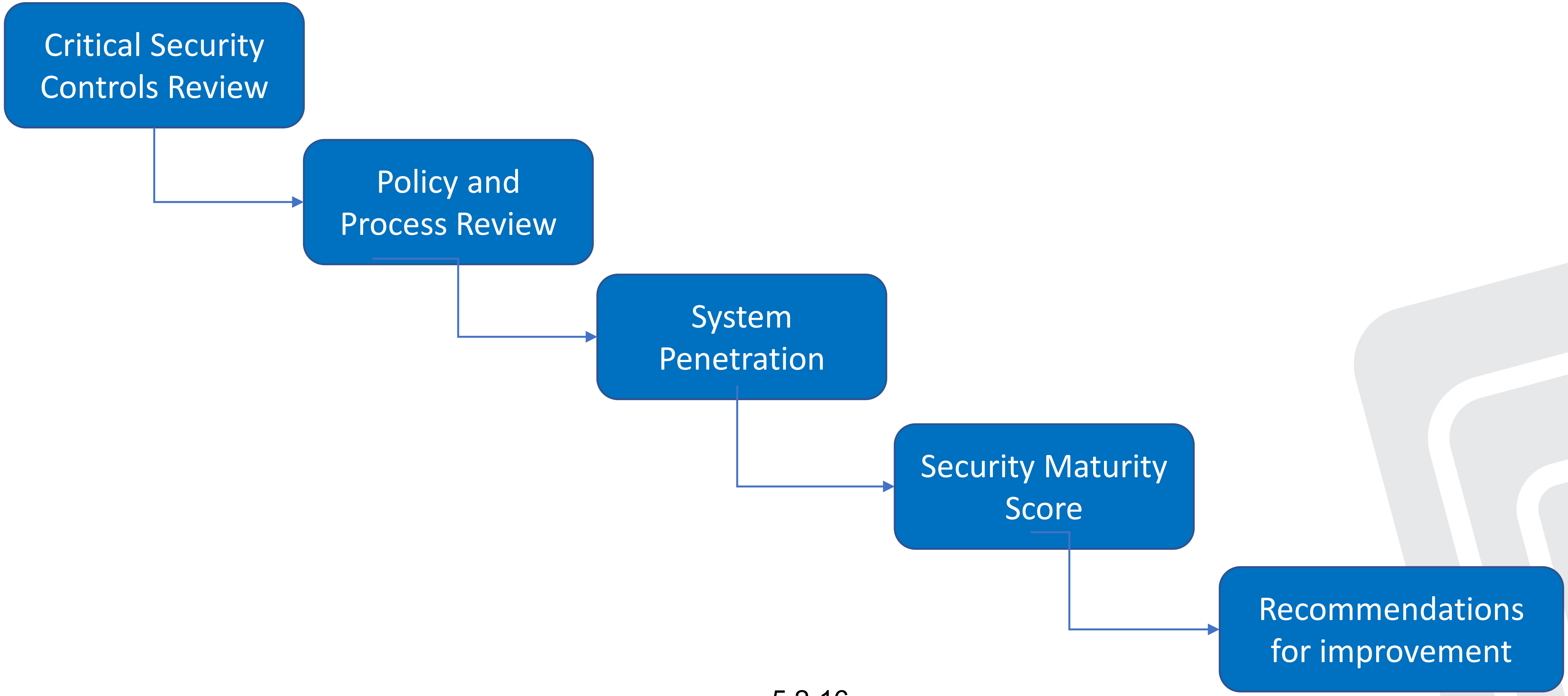

Internet
Employee (Asset)
Expandable Cloud
Multi-Factor Authentication
Security Information and Incident Event Management
Corporate EndPoint Protection
Identity and Access Management
Cyber Security Training (Learning Management System)
Corporate Information Protection
Expandable Cloud
Mobile Application/ Device Management
Web Content Filtering
Primary Email Protection Control
Security Automations
Vulnerability Management
Advanced Threat Protection
Corporate Firewall
Virtual Private Network (Work From Home)
Secondary Email Protection Control
Corporate Firewall
Advanced Threat Protection
Corporate Encryption
Security Automations
Corporate Information Protection
Server Farm (Asset)
Employee (Asset)

Peel’s Cyber Security Controls

⬛	Cloud/Hybrid Controls
🟦	On-premises Controls
🟥	Future Controls

Third Party Security Assessment

Completed in April of 2019



Critical Security Controls Review
Policy and Process Review
System Penetration
Security Maturity Score
Recommendations for improvement

Security Maturity Assessment (Findings)

The Region of Peel’s overall **Critical Security Controls maturity score is 42%.**

This is higher than the current municipalities sector average of **39%.**

Status Indicators:

✓ Completed

✓ Ongoing

✓ Not Started

Security Maturity Assessment (Findings)

The Region of Peel has higher maturity than the sector average in the following areas:

CSC 2 – Inventory and Control of Software Assets – 35%

✓ CSC 3 – Continuous Vulnerability Management – 43%

CSC 15 – Wireless Access Control – 50%

Security Maturity Assessment (Findings)

The Region of Peel has lower maturity than the sector average in the following areas:

- ✓ CSC 9 - Limitation and Control of Network Ports, Protocols, and Services - 5%
- ✓ CSC 14 – Controlled Access Based on the Need to Know - 3%
- ✓ CSC 19 - Incident Response and Management - 9%

Internal Penetration Testing (Findings)

✓ Vulnerability Assessment

- Aging applications prevent deployment of latest server operating systems.
  - 40% of all the servers are running on unsupported operating systems.
  - Some vulnerable operating system weaknesses are 10 years and older.
- Numerous outdated software applications were discovered

✓ Technical Deficiencies

- In some cases system build procedures were not followed
- Lack of centralized log management & event management system
- No formal Incident Response Plan

IT Policies and Documentation (Findings)

Missing or inaccurate policy statements

- ✓ Recording Policy, Bring Your Own Device Policy, Information Classification Policy, Information Protection Policy
- ✓ Review existing IT Technology policies and keep them updated regularly

Documentation

- ✓ Some systems lacked the design detail
- ✓ Some threat risk assessment recommendations were not applied correctly

Work Plan

Activities	2019	2020	2021
Deliver continuous Cyber Security awareness training for the organization	✓	✓	✓
Conducted internal email phishing campaign within the organization		✓	✓
Introduced three new technology and security policy statements	✓	✓	
Implemented Identity Access technology system policies to protect corporate information against unauthorized access		✓	
Developed security incident response plan		✓	

Work Plan

Activities	2019	2020	2021
Implemented next generation endpoint protection solution	✓	✓	
Implemented Security Incident and Event management solution	✓		
Automated corporate systems build processes	✓	✓	
Modernize cyber security tools	✓	✓	✓

Work Plan

Activities	2019	2020	2021
Enhance security of mobile devices (smartphones)		✓	✓
Review and update existing security and technology policy statements		✓	✓
State of Good Repair (SOGR) program is underway to address the legacy applications by retiring, replacing, or upgrading the applications	✓	✓	✓
Remediate technical deficiencies such as missing application updates	✓	✓	✓

Work Plan

Activities	2019	2020	2021
Operationalize Security Incident Response Plan		✓	
Enhance regulatory compliance controls		✓	✓
Improve lower scored areas to increase the security maturity assessment scores.	✓	✓	✓
Complete follow up IT security assessment			✓

Questions?