Leading with Confidence: Board Oversight in Cyber Security Management

CFDCs Spring Conference Presentation

Introductions

Yehia (Ian) Ahmed (Ashore)

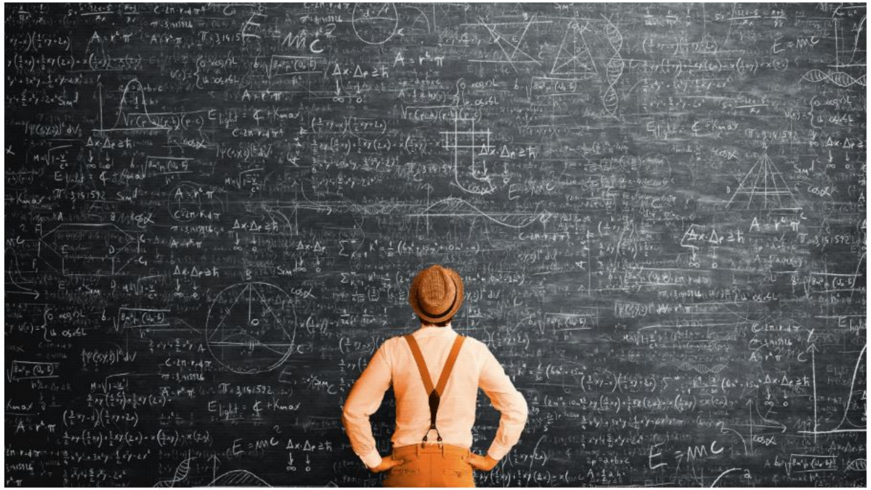
Bronwen Clewley

Presentation question:

What are the activities board of directors and top management can do to improve Cyber security management?

Ultimate Questions

1. Why do we have cyber security challenges?
2. How can we fix it?



Cyber Security Management

Let’s do ground work.
3 Concepts to get across.

"Slap me when he's done. I'm putting myself into a self-induced coma."

Cyber **security management?**

A well-informed sense of assurance that information risks and controls are in balance*

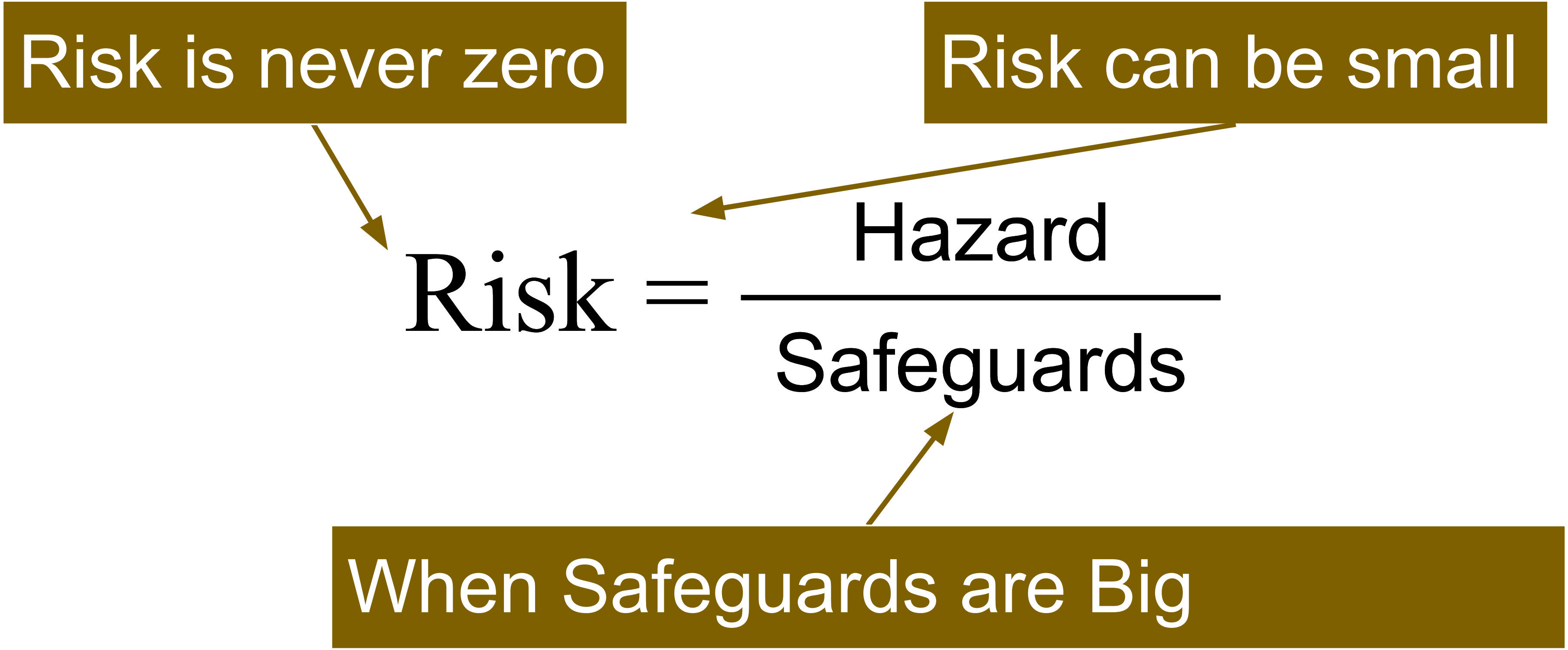
*James M. Anderson, 2003.

What is Risk?

$$\text{Risk} = \frac{\text{Hazard}}{\text{Safeguards}}$$

Reference: Kaplan & Garrick (1980)

What is Risk?



Risk is never zero

Risk can be small

$$\text{Risk} = \frac{\text{Hazard}}{\text{Safeguards}}$$

When Safeguards are Big

Cyber Security Functions?

$$\text{Cyber Security Risk} = \frac{\text{Harm}}{\text{Control}}$$

Cyber Security Functions?

Risk
Scenarios
-
Software,
hardware..etc

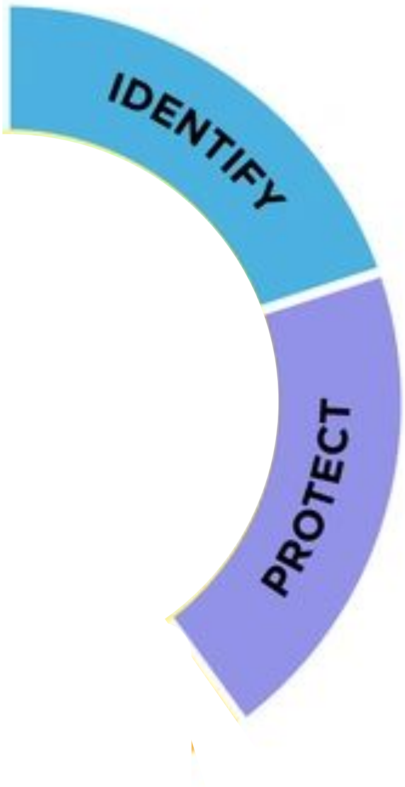
$$\text{Cyber Security Risk} = \frac{\text{Harm}}{\text{Control}}$$

Vulnerabilities

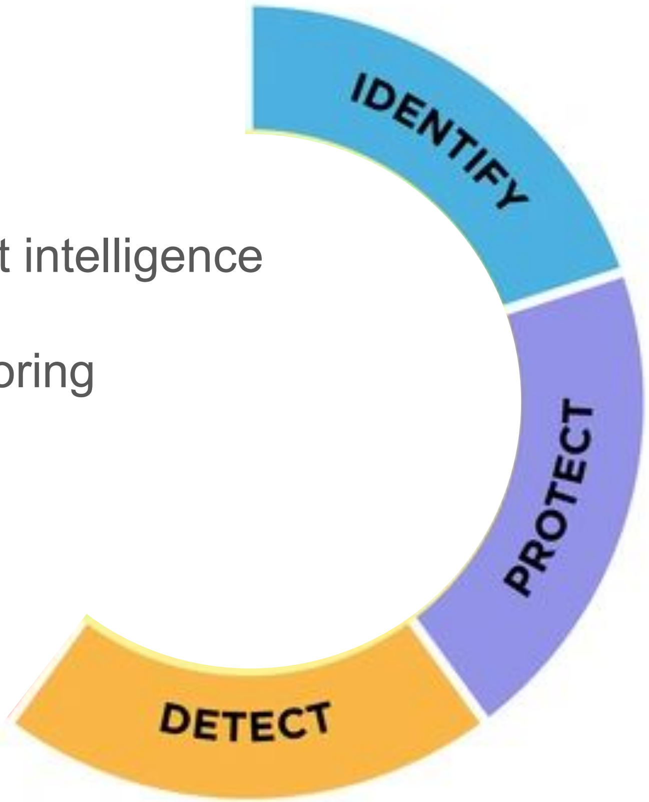
Cyber Security Functions?

$$\text{Cyber Security Risk} = \frac{\text{Harm}}{\text{Control}}$$

Training
Anti virus
Firewall



Cyber Security Functions?



Threat intelligence

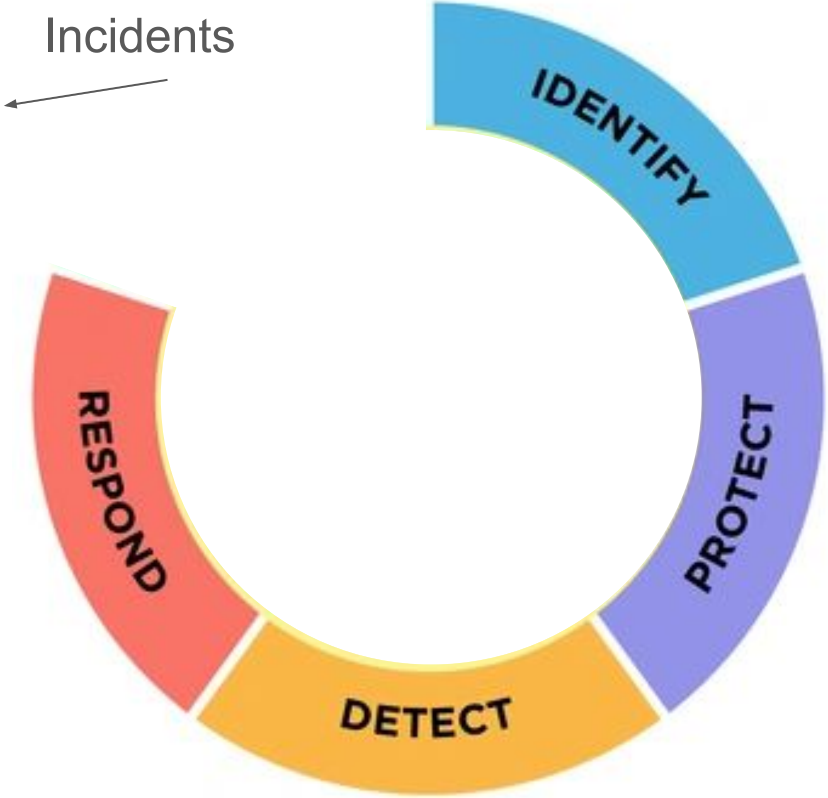
Monitoring

$$\text{Cyber Security Risk} = \frac{\text{Harm}}{\text{Control}}$$

Cyber Security Functions?

Incidents

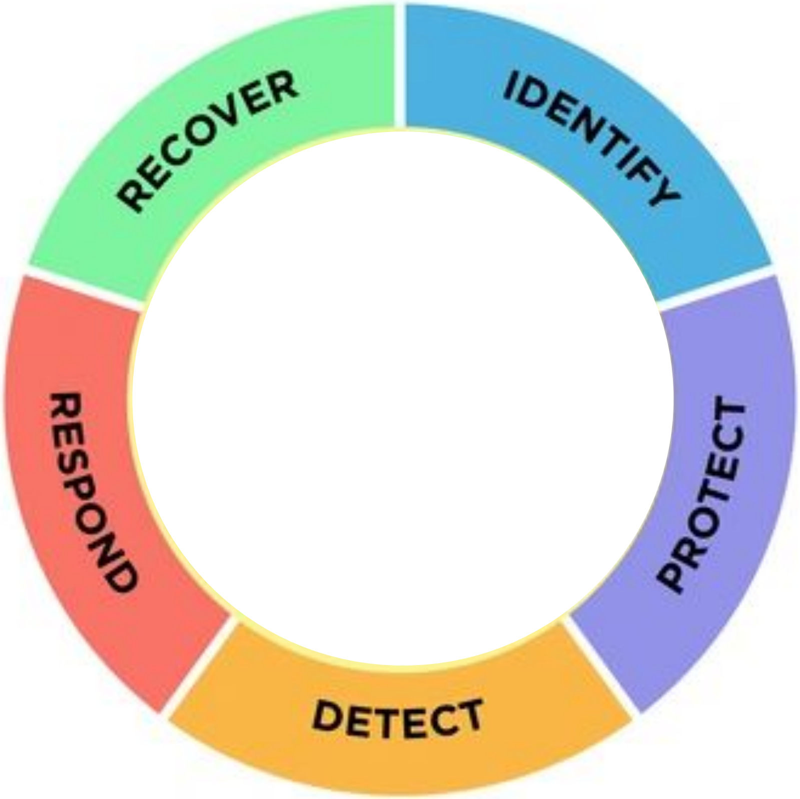
$$\text{Cyber Security Risk} = \frac{\text{Harm}}{\text{Control}}$$



Cyber Security Functions?

Recover
after attack

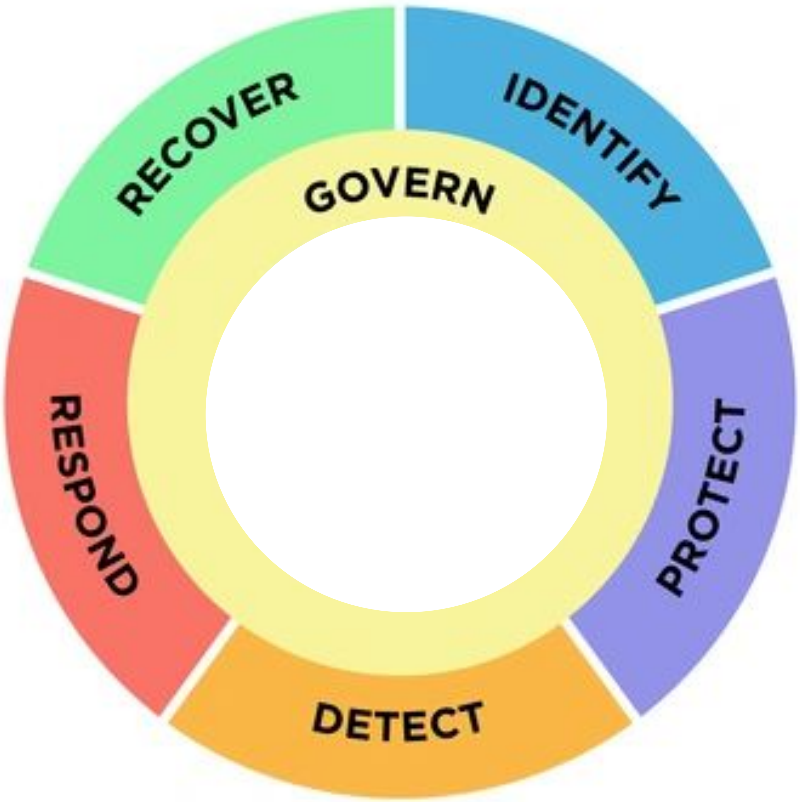
Cyber Security Risk = $\frac{\text{Harm}}{\text{Control}}$



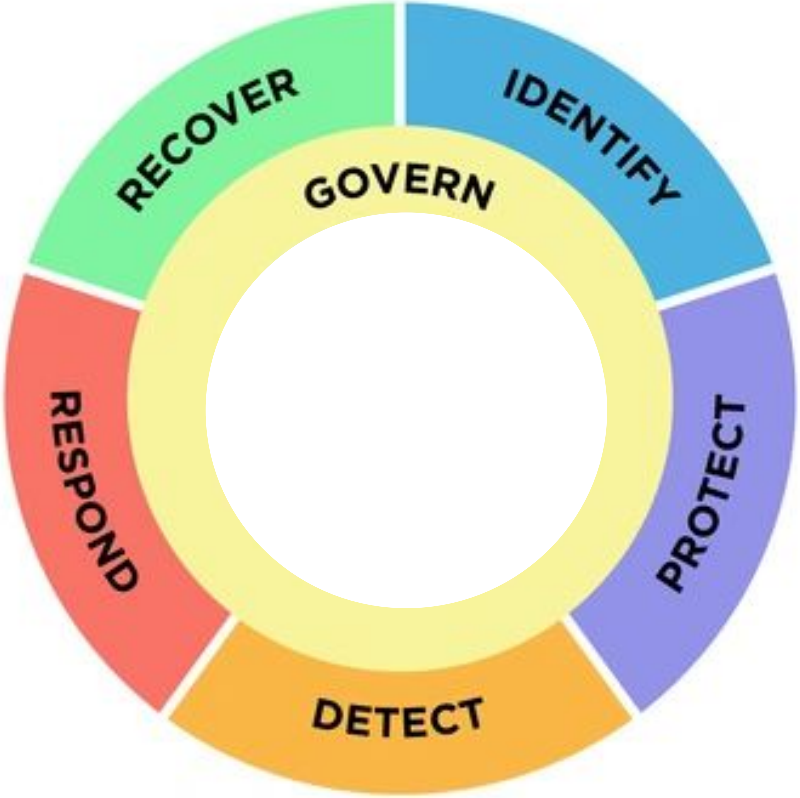
Cyber Security Functions?

Context,
strategy,
Roles,
Policy,
Oversight..

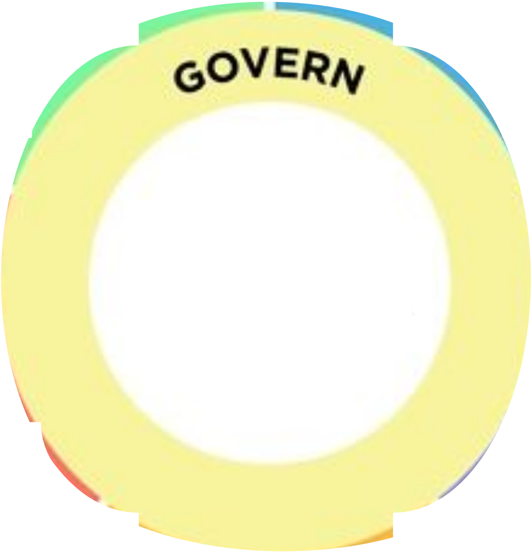
$$\text{Cyber Security Risk} = \frac{\text{Harm}}{\text{Control}}$$



Cyber Security Functions?



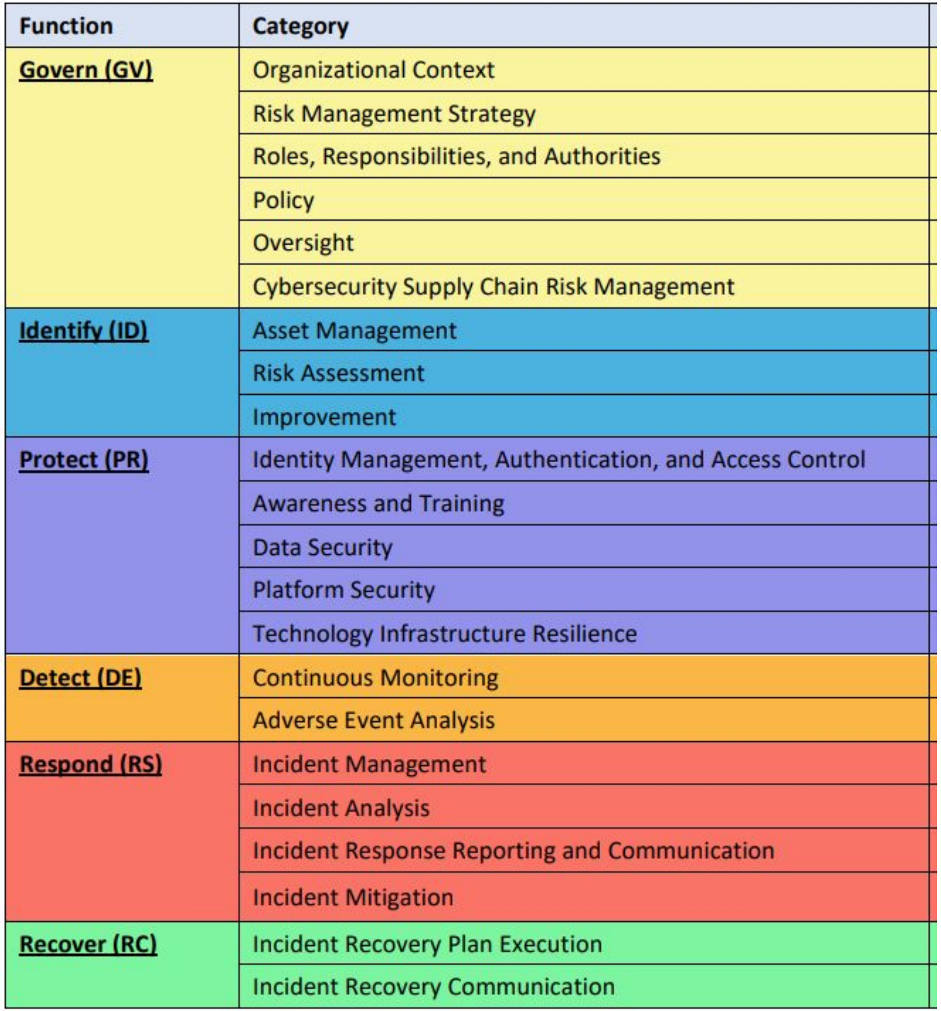
Let's Focus on Governance Today.



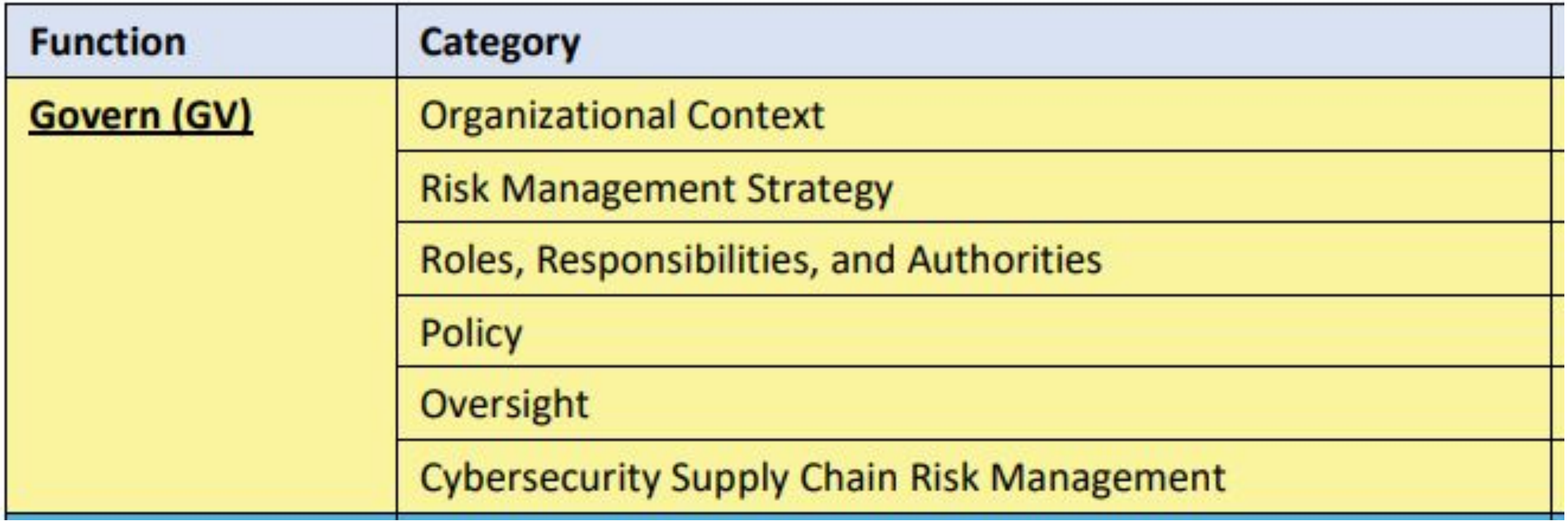
What is Cyber Security **Governance**?

To **Establish**, **Communicate** and **Monitor**:

Strategy, *Expectations*, *Policy*.



Function	Category
Govern (GV)	Organizational Context
	Risk Management Strategy
	Roles, Responsibilities, and Authorities
	Policy
	Oversight
	Cybersecurity Supply Chain Risk Management
Identify (ID)	Asset Management
	Risk Assessment
	Improvement
Protect (PR)	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience
Detect (DE)	Continuous Monitoring
	Adverse Event Analysis
Respond (RS)	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	Incident Mitigation
Recover (RC)	Incident Recovery Plan Execution
	Incident Recovery Communication

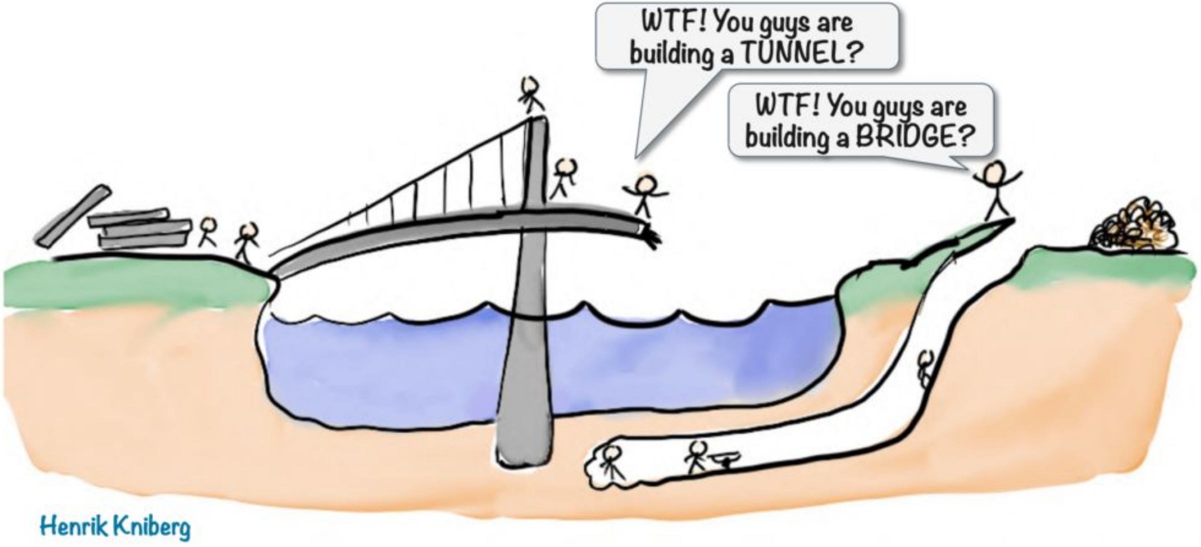


Function	Category
Govern (GV)	Organizational Context
	Risk Management Strategy
	Roles, Responsibilities, and Authorities
	Policy
	Oversight
	Cybersecurity Supply Chain Risk Management

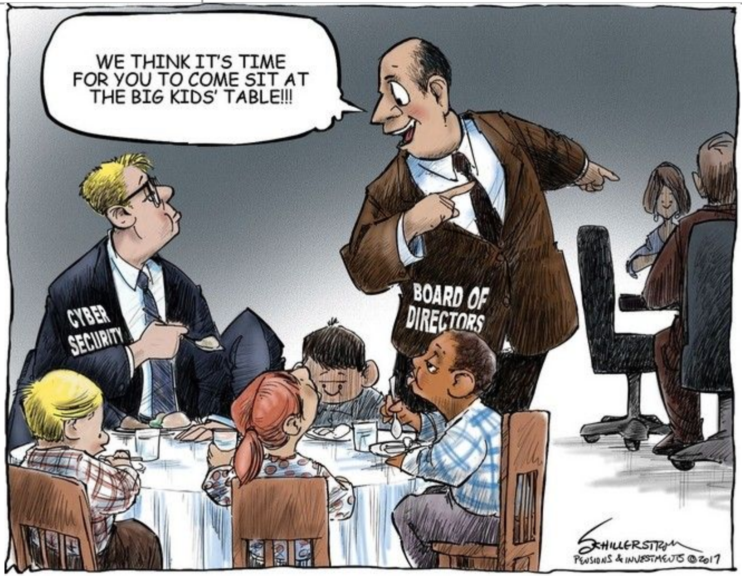
Now we know what **cyber security** is!

What are the challenges?

Governance Function	Challenge
Organizational Context	**Misalignment** between business and IT


WTF! You guys are building a TUNNEL?
WTF! You guys are building a BRIDGE?
Henrik Kniberg

Governance Function	Challenge
Roles, Responsibilities, and Authorities	Lack of cyber **skills** at the Top


WE THINK IT'S TIME FOR YOU TO COME SIT AT THE BIG KIDS' TABLE!!!
CYBER SECURITY
BOARD OF DIRECTORS
SCHILLERSTROM
PENSIONS & INVESTMENTS ©2017

Governance Function	Challenge
Policy	Lack of **adaptability**

Governance Function	Challenge
Cybersecurity Supply Chain Risk Management	Challenges with **transparency**

ca technologies
CA.COM/CLOUD-MONITORING
ALL I KNOW IS THE BOSS SAID WE HAD TO MONITOR THE CLOUD.
© D.Fletcher for CloudTweaks.com

CyberSecure Canada

How about **CyberSecure Canada**?

Where would CyberSecure Canada fit into this?

Where to get access to CyberSecure Canada Standard

To be eligible for Cybersecure certification your organization must implement ALL the controls in the National Standard CAN/CIOSC 104:2021 Baseline cyber security controls for small and medium organizations.

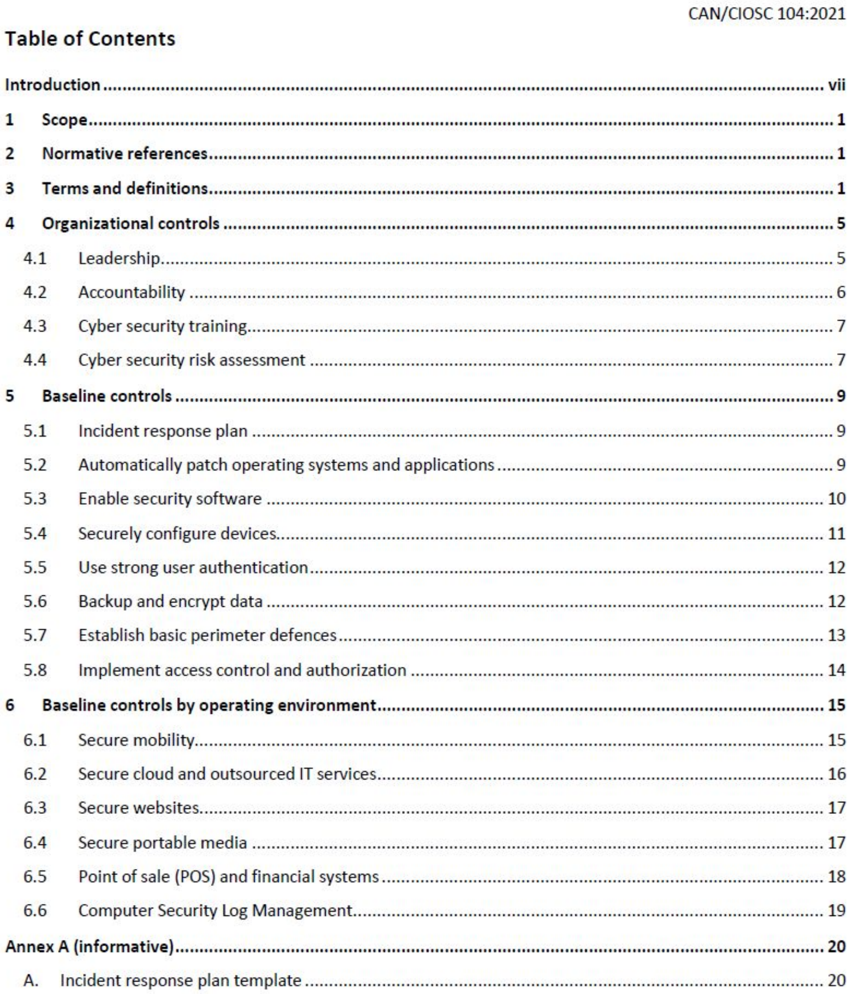
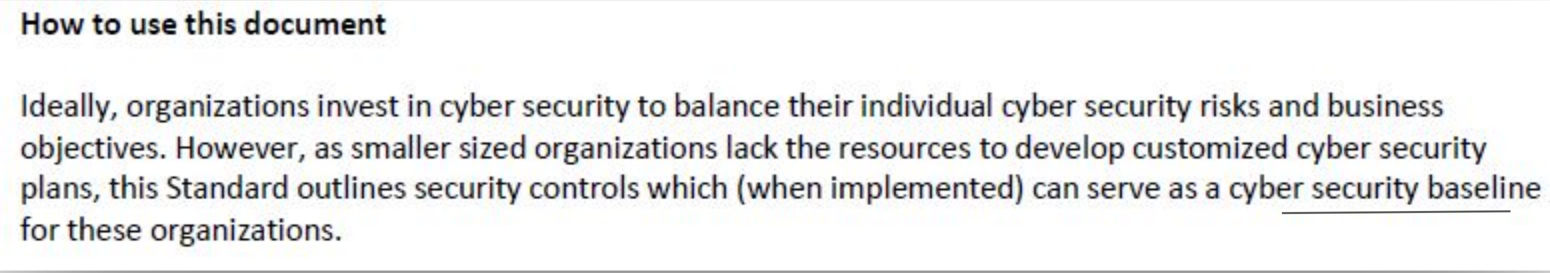


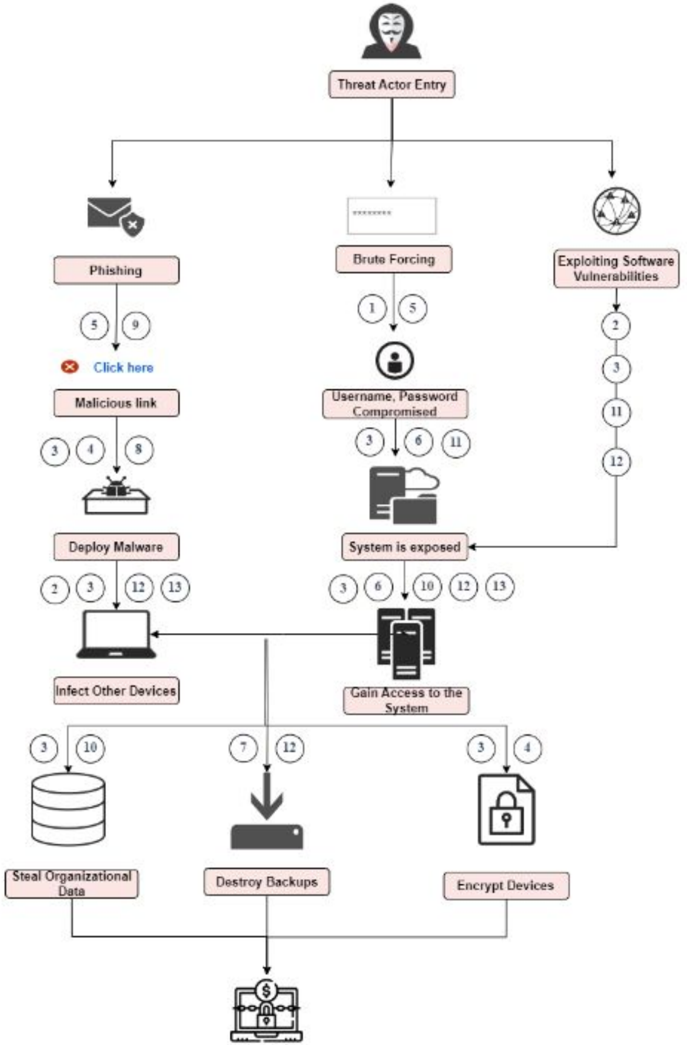
Table of Contents



How to use this document

Ideally, organizations invest in cyber security to balance their individual cyber security risks and business objectives. However, as smaller sized organizations lack the resources to develop customized cyber security plans, this Standard outlines security controls which (when implemented) can serve as a cyber security baseline for these organizations.

Risk Management



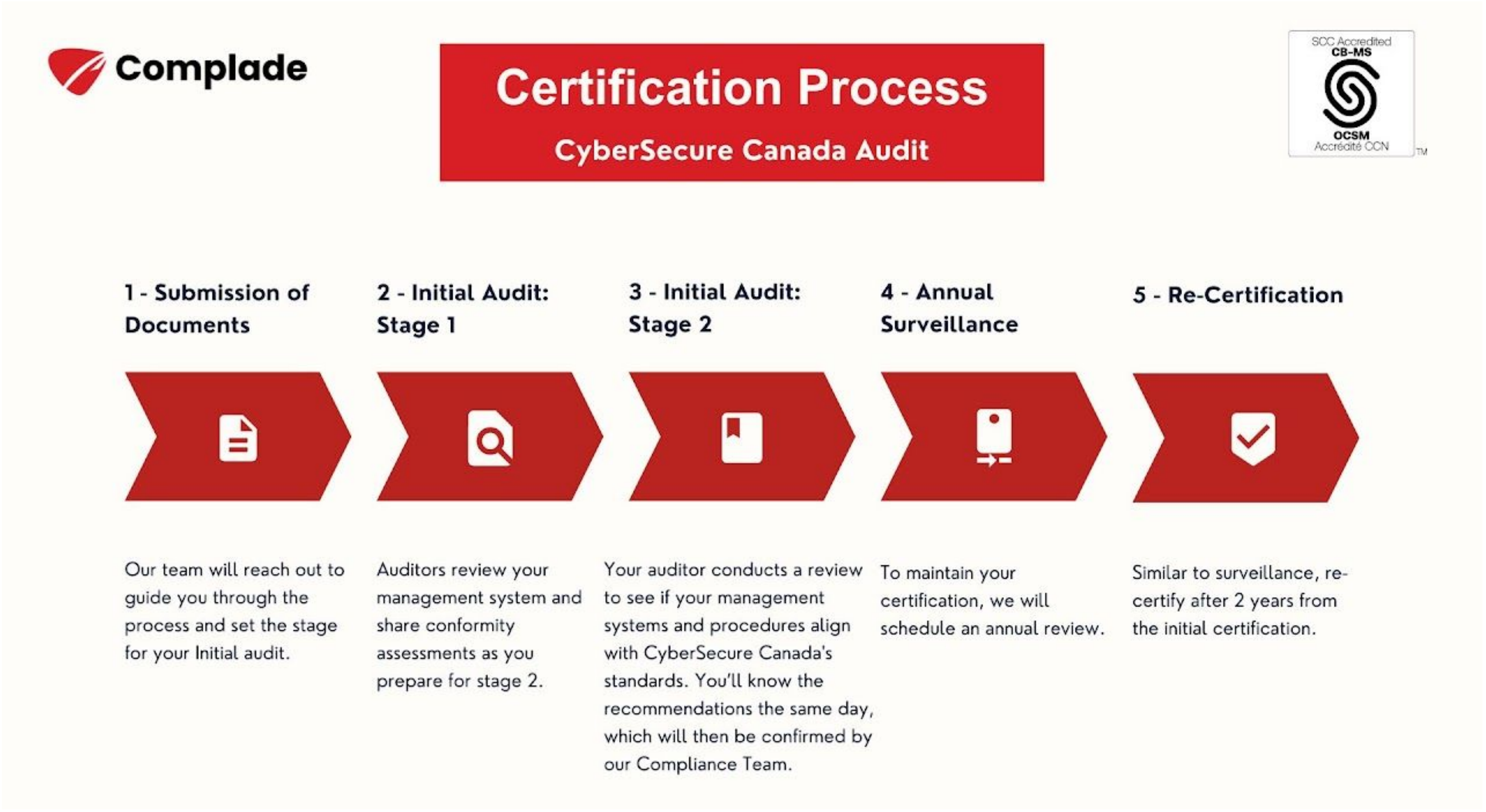
Governance, Risk, and Compliance (GRC) Tools

Cybersecurity Certifications

Controls

1	Password Manager
2	Updating and patching
3	Logging and alerting
4	Application Allowlisting
5	Cyber security training
6	Multi-factor Authentication
7	Backups
8	Disable Macros
9	Email Domain Protection
10	Least Privilege
11	Network Segmentation
12	Security Tools (Anti-Virus Software)
13	Protective (DNS)

Certification Audit Process



Complade

Certification Process

CyberSecure Canada Audit

SCC Accredited CB-MS
OCSM Accrédité CCN

1 - Submission of Documents

Our team will reach out to guide you through the process and set the stage for your Initial audit.

2 - Initial Audit: Stage 1

Auditors review your management system and share conformity assessments as you prepare for stage 2.

3 - Initial Audit: Stage 2

Your auditor conducts a review to see if your management systems and procedures align with CyberSecure Canada's standards. You'll know the recommendations the same day, which will then be confirmed by our Compliance Team.

4 - Annual Surveillance

To maintain your certification, we will schedule an annual review.

5 - Re-Certification

Similar to surveillance, re-certify after 2 years from the initial certification.

Next Steps

Next Steps:

1. Ask questions in your next board meeting.
   a. About context and alignment
   b. About risk strategy
   c. About policy
   d. About measurement and oversight

2. Use CyberSecure Canada as first step to implement cybersecurity.

3. Get CyberSecure Canada certified check Complade.com