ICPAK
Uphold Public Interest

DEVELOPING A PEOPLE-CENTRIC CYBERSECURITY STRATEGY

Presentation by:

Joan Mburu
Information Security Officer, Old Mutual
Friday, 13th September 2019

Agenda

1) Cybersecurity headlines
2) Why a people-centric strategy
3) Developing the strategy
4) Key takeaways

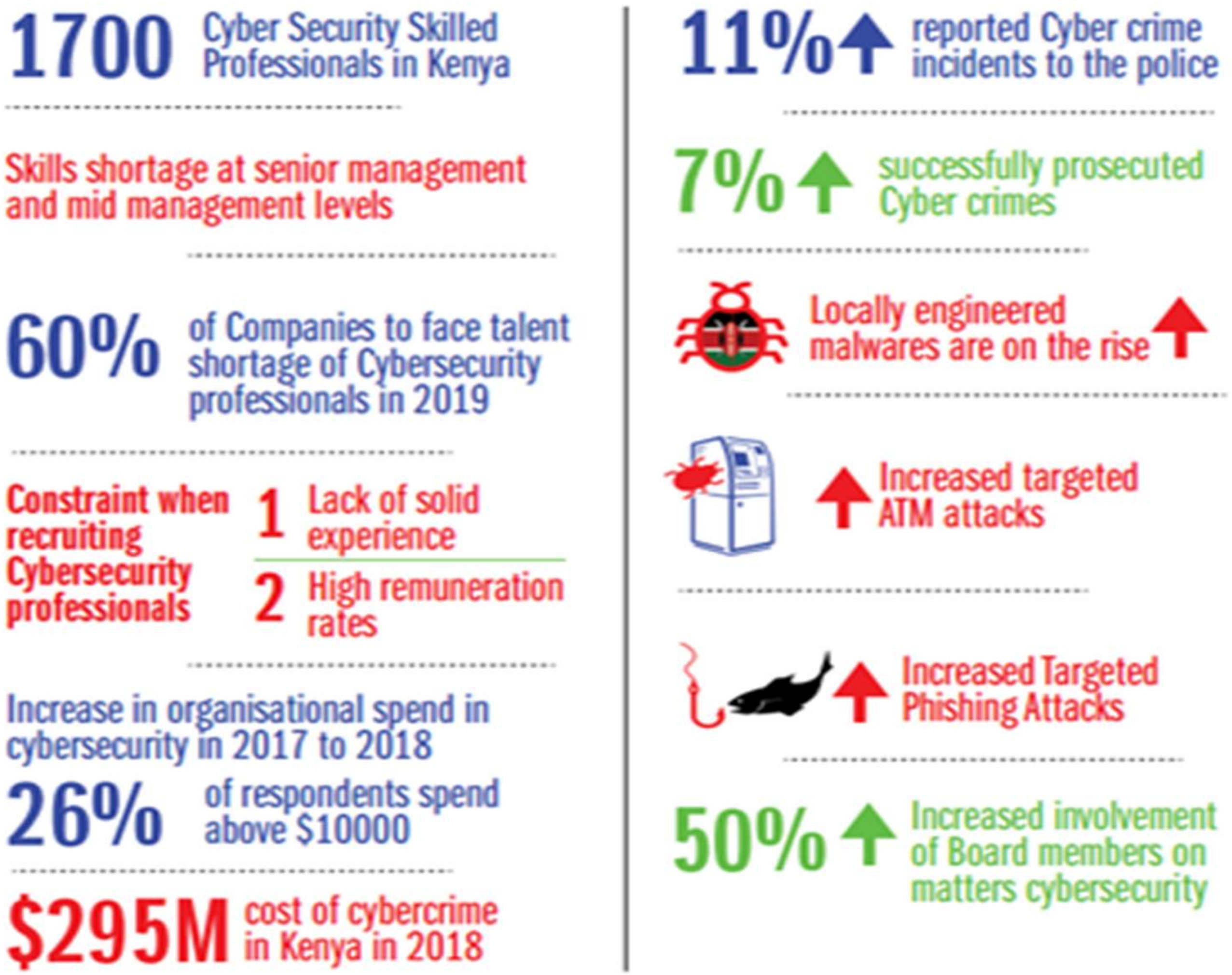
1. Cybersecurity headlines

- ❑ Alarm in Texas as 23 towns hit by ‘coordinated’ ransomware attack.
- ❑ Historic Capital One hack reaches 100 million customers affected by breach
- ❑ Safaricom ventures into cybersecurity business
- ❑ Review cybersecurity strategies to reflect global best practices

Regulator warns of rise in cybersecurity threats

- ❑ "The cyber threats detected varied from denial-of-service (DoS) including **botnet** and **brute-force attacks** that led to denial of computer services and illegal access to computer systems; **online impersonation** via social media accounts and domain names; **website attacks** including defacement; **malware** including phishing attacks; **online abuse** including online fraud, hate speech, incitement to violence and fake news; and **systems misconfiguration**," says the CA report. (Business daily, Jan 2019)

2018 Highlights



1700 Cyber Security Skilled Professionals in Kenya

Skills shortage at senior management and mid management levels

60% of Companies to face talent shortage of Cybersecurity professionals in 2019

Constraint when recruiting Cybersecurity professionals

1. Lack of solid experience
2. High remuneration rates

Increase in organisational spend in cybersecurity in 2017 to 2018

26% of respondents spend above $10000

$295M cost of cybercrime in Kenya in 2018

11% ↑ reported Cyber crime incidents to the police

7% ↑ successfully prosecuted Cyber crimes

Locally engineered malwares are on the rise ↑

↑ Increased targeted ATM attacks

↑ Increased Targeted Phishing Attacks

50% ↑ Increased involvement of Board members on matters cybersecurity

(Serianu cyber security report 2018)

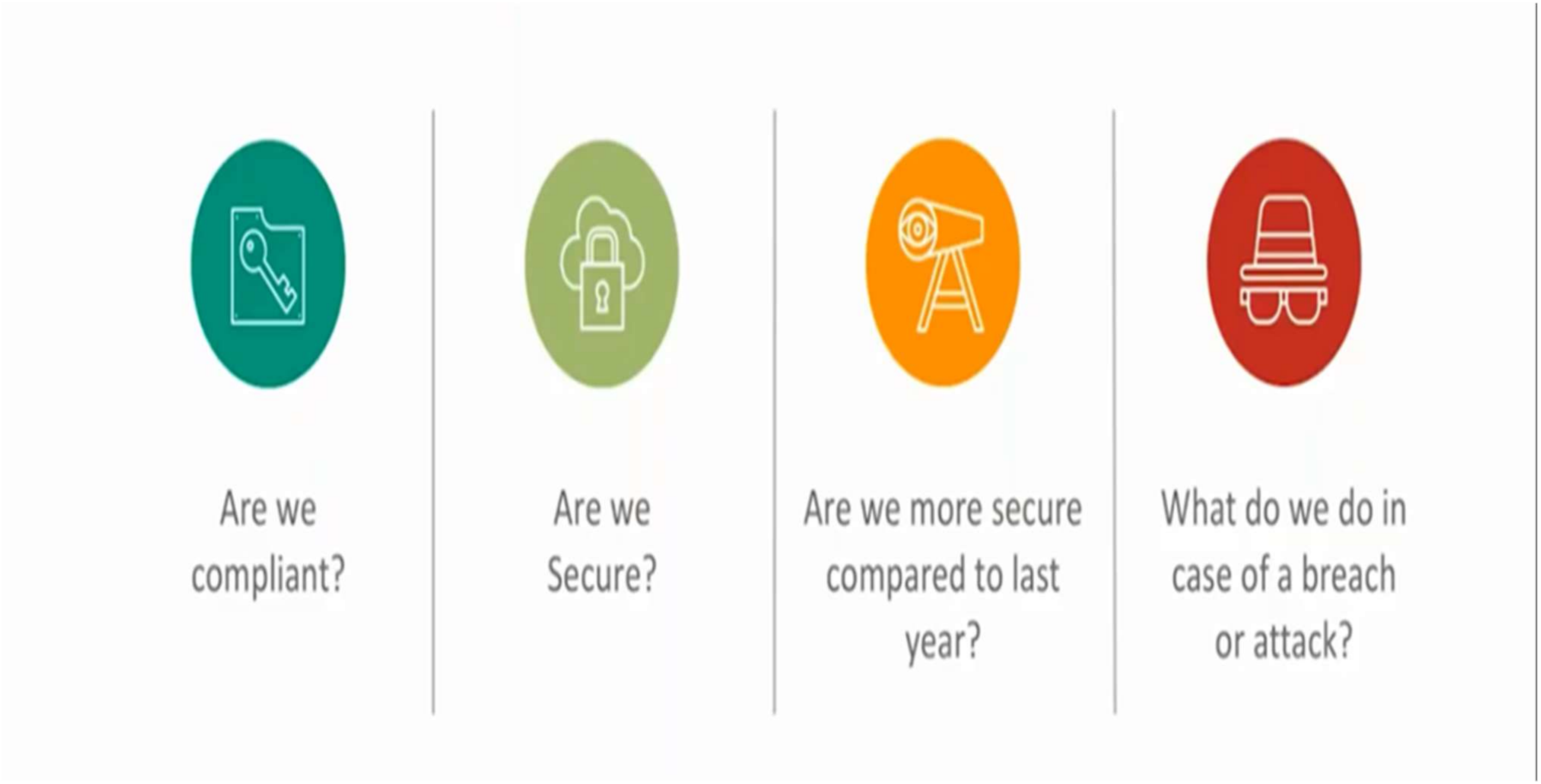
So what?

❑ What questions are execs asking when they see such headlines?

❑ How do you answer them?

❑ What measures are being taken in your organization?

Security vs compliance



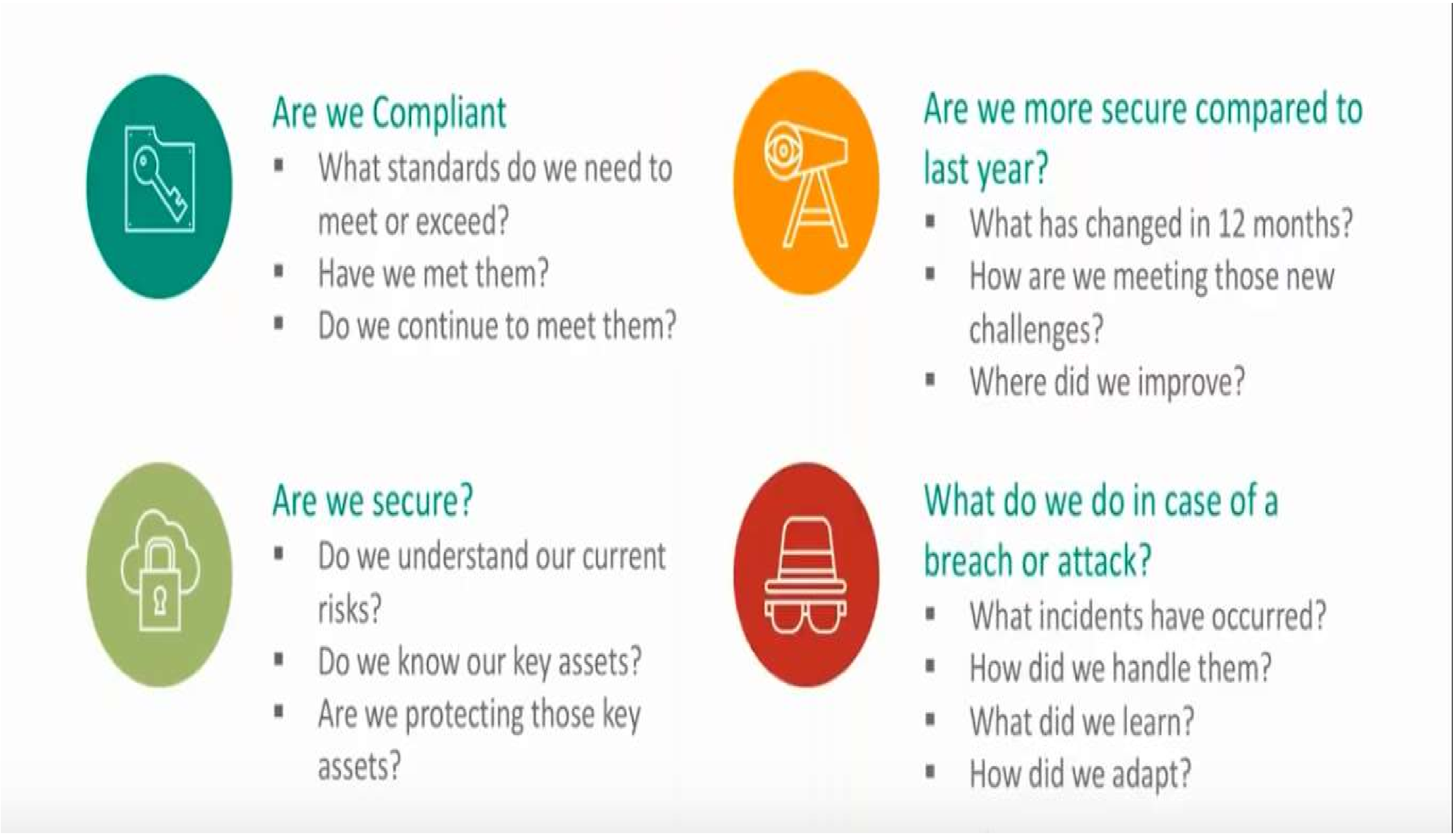
Are we compliant?

Are we Secure?

Are we more secure compared to last year?

What do we do in case of a breach or attack?

What do they mean?



Are we Compliant

- What standards do we need to meet or exceed?
- Have we met them?
- Do we continue to meet them?

Are we more secure compared to last year?

- What has changed in 12 months?
- How are we meeting those new challenges?
- Where did we improve?

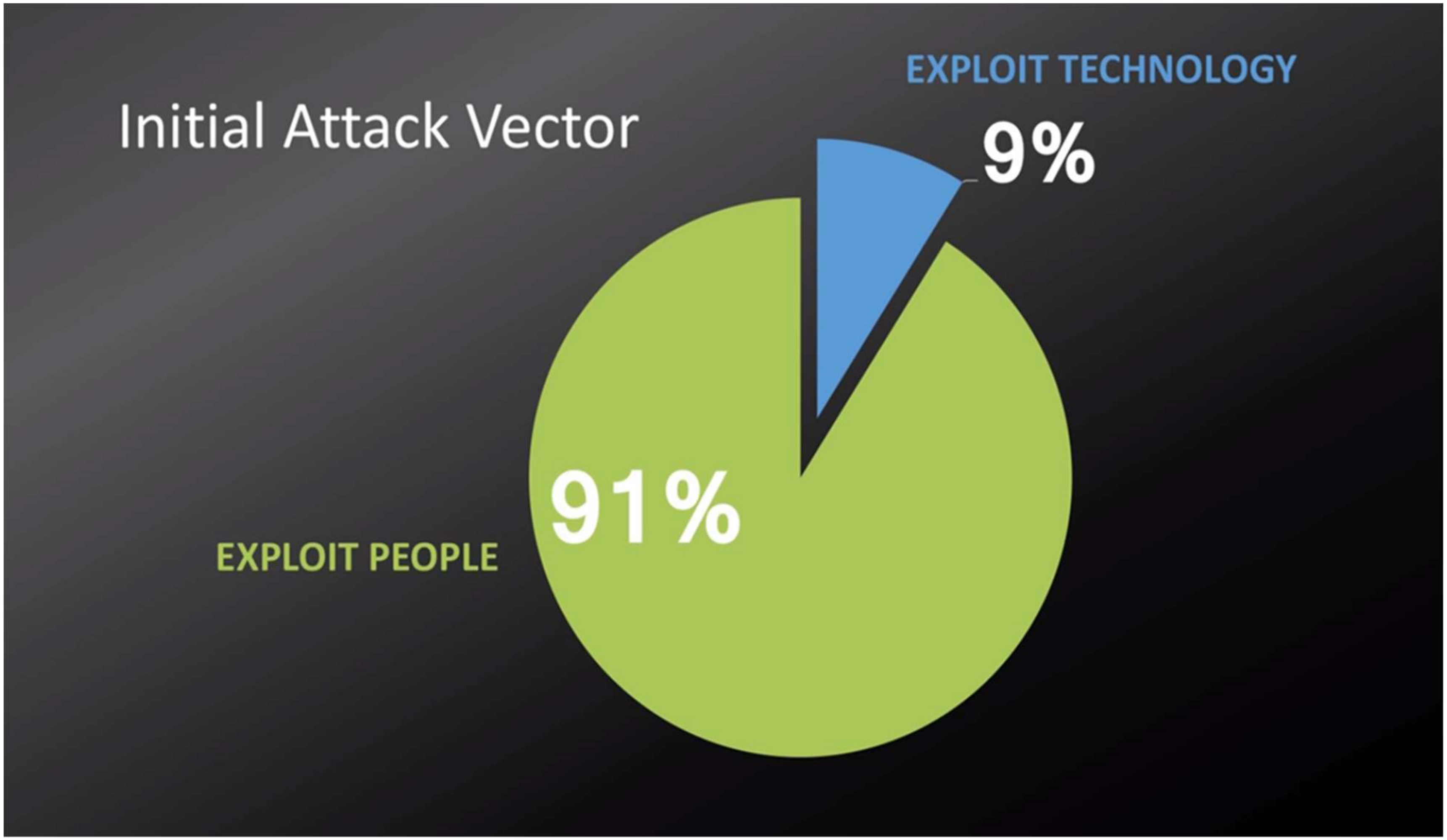
Are we secure?

- Do we understand our current risks?
- Do we know our key assets?
- Are we protecting those key assets?

What do we do in case of a breach or attack?

- What incidents have occurred?
- How did we handle them?
- What did we learn?
- How did we adapt?

2. Why a people-centric strategy



Why you are a target

- ❑ **HR managers** –access to payroll system and information (social engineering)
- ❑ **Finance/procurement** –authority to process payments (phishing emails)
- ❑ **System administrators** –privileged access to critical infrastructure (network sniffing and key loggers)
- ❑ **Board** –access to sensitive company information (phishing emails)
- ❑ **Personal/executive assistants** –access to CEO or senior management calendars, sensitive information, etc.

‘Expectations for 2019’

- ❑ **Board members** will become more proactive and there will be a need to streamline cyber risk reporting and quantification
- ❑ **Vendors** will be expected to communicate and show value for their services
- ❑ **Attackers** will continue to develop unique malware
- ❑ **Regulators** will develop stronger cybersecurity policies
- ❑ **Third parties** have become a weak link
- ❑ Skills gap means outsourcing for security services will continue

(Serianu cyber security report 2018 –www.serianu.com)

3. Developing the strategy

Information security principles

1. Support the business

- ❑ Focus on the business
- ❑ Deliver quality and value to stakeholders
- ❑ Comply with legal and regulatory requirements
- ❑ Provide timely and accurate metrics
- ❑ Evaluate current and future information threats
- ❑ Promote continuous improvement in information security

Information security principles

2. Defend the business

- ❑ Adopt a risk based approach
- ❑ Protect classified information
- ❑ Concentrate on critical business applications
- ❑ Develop systems securely

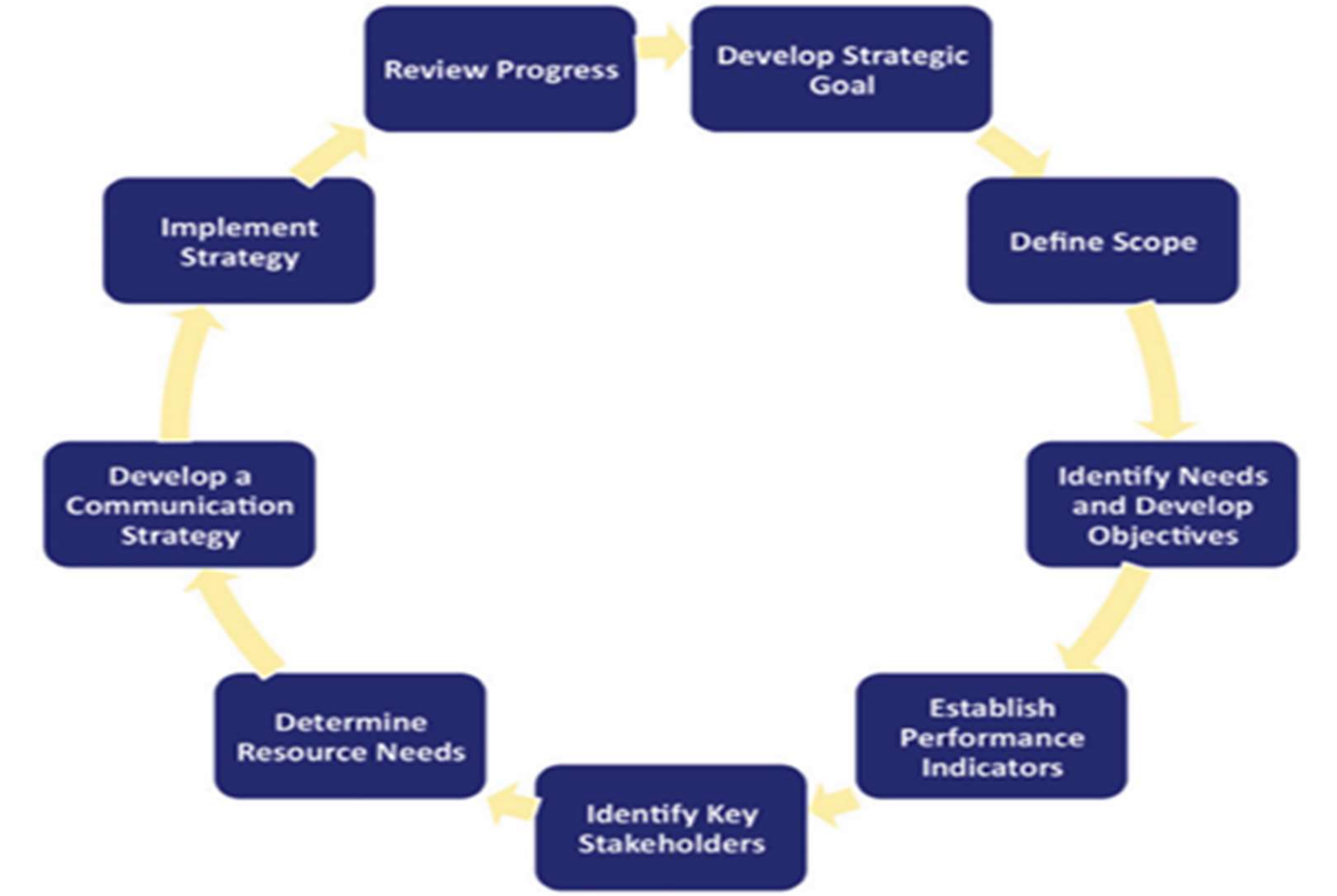
Information security principles

3. Promote responsible information security behavior

❑ Act in a professional and ethical manner

❑ Foster a positive security culture

Strategy development steps



Develop Strategic Goal

Define Scope

Identify Needs and Develop Objectives

Establish Performance Indicators

Identify Key Stakeholders

Determine Resource Needs

Develop a Communication Strategy

Implement Strategy

Review Progress

I.) Develop a strategic goal

Identify why cybersecurity is important and what you want to achieve through the strategy.

Example:

Our mission is to protect the people of the county of Wakanda by ensuring that their information and systems used in serving them are safe, reliable and available. The goals of our strategy are to:

- *Protect critical infrastructure against cyberattacks*
- *Reduce vulnerability to cyberattacks*
- *Minimize damage and recovery from successful cyberattacks*

II.) Define scope

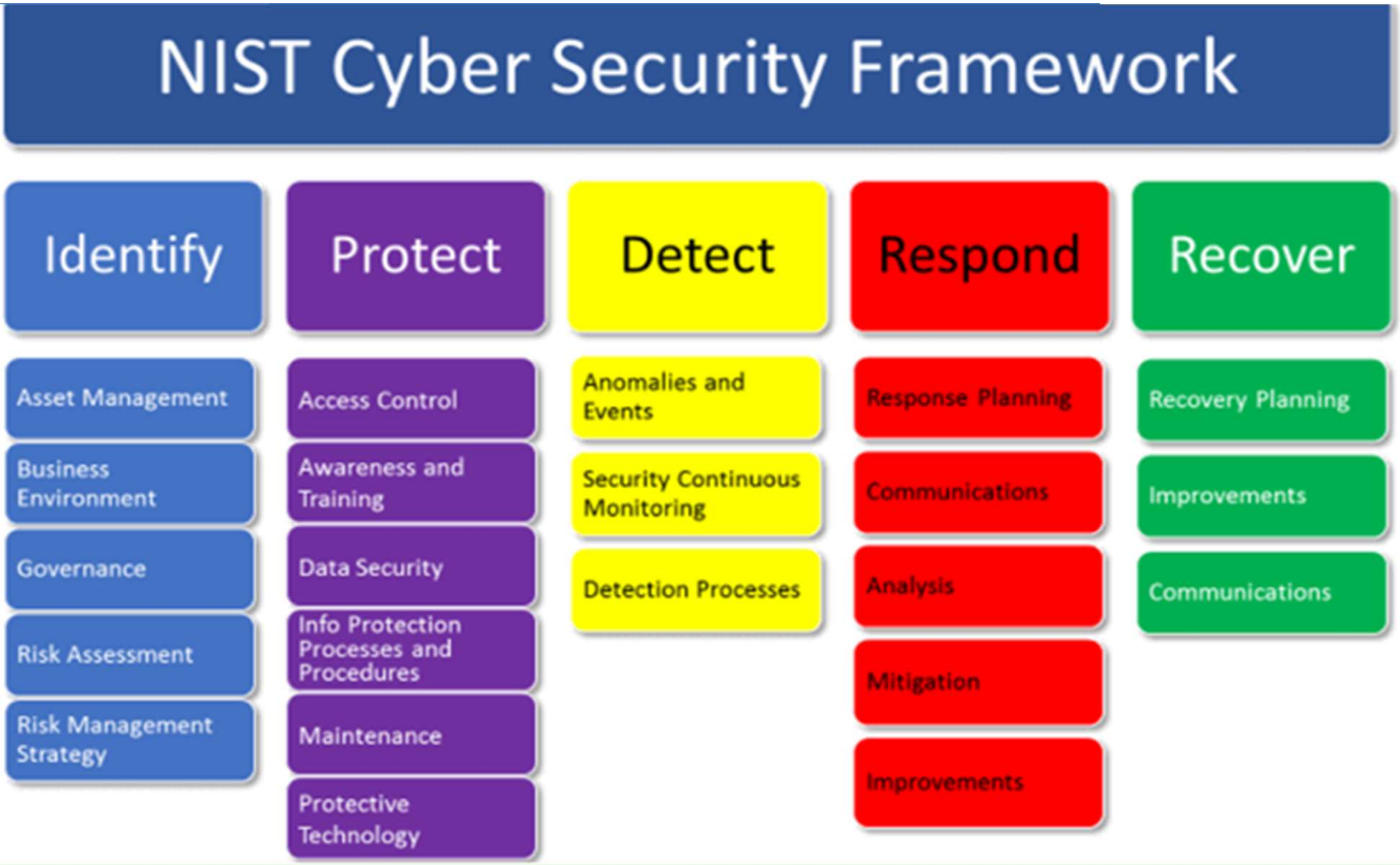
Outline the sectors that will be addressed by the strategy as well as the range of cyber security activities it will cover and extent to which the activities will be emphasized. Factor in advancement in technology, emerging issues (regulations/legislation), unforeseen cyber events, etc.

- *The scope of the information security strategy is to protect XYZ company, including all its subsidiaries and customers, from loss or compromise of confidential customer or proprietary information, and from disruption of systems and processes'.*

III.) Identify needs & objectives

a) Conduct performance assessment and gap analysis
b) Develop objectives

a.) Conduct gap analysis



NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

NIST cybersecurity framework

1 **IDENTIFY**

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity

2 **PROTECT**

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees

3 **DETECT**

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

4 **RESPOND**

Develop a plan for disasters and information security incidents

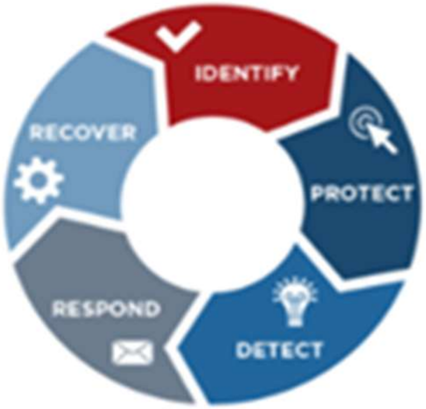
5 **RECOVER**

Make full backups of important business data and information

Continue to schedule incremental backups

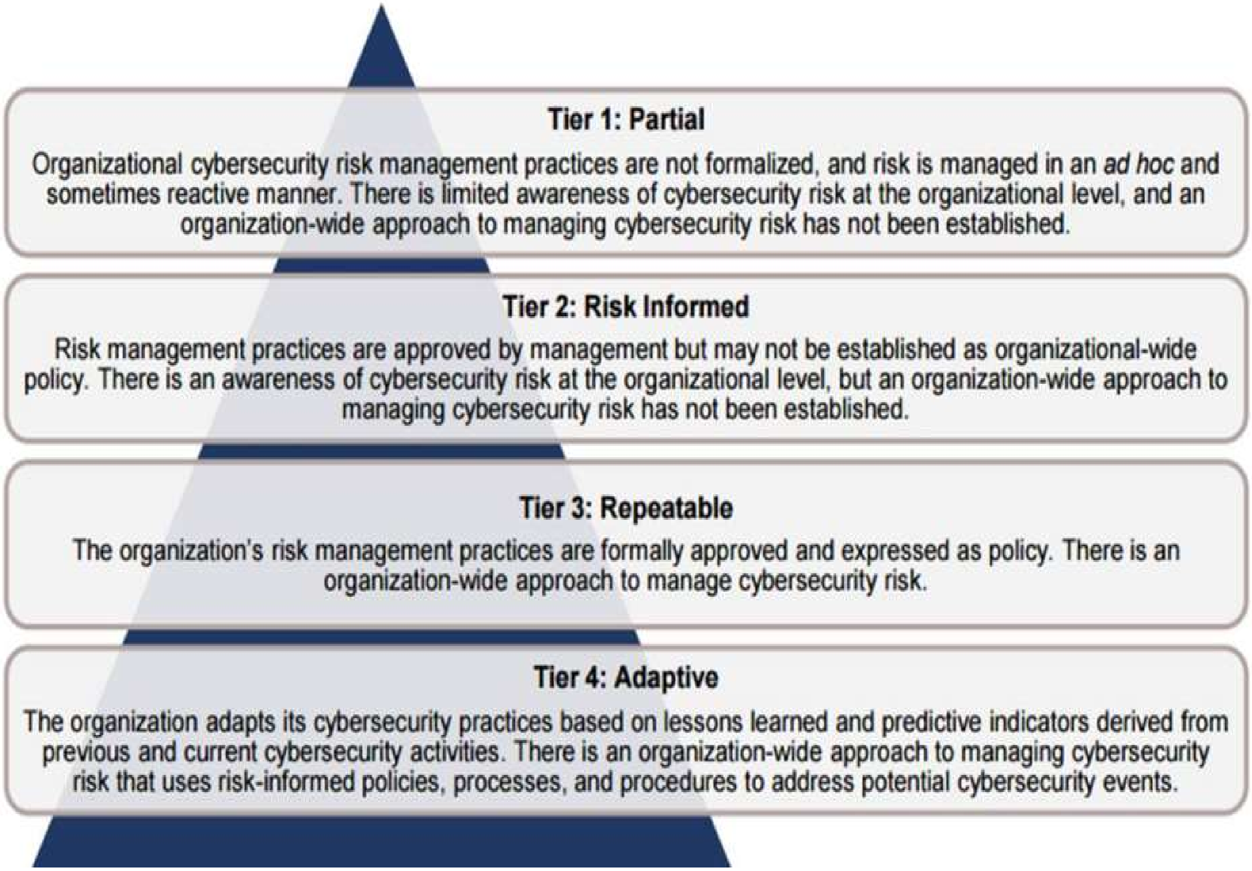
Consider cyber insurance

Make improvements to processes/ procedures/ technologies



Framework implementation tiers

Provide context for how an organization views cybersecurity risk and the processes in place to handle the risks



Tier 1: Partial

Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. There is limited awareness of cybersecurity risk at the organizational level, and an organization-wide approach to managing cybersecurity risk has not been established.

Tier 2: Risk Informed

Risk management practices are approved by management but may not be established as organizational-wide policy. There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established.

Tier 3: Repeatable

The organization's risk management practices are formally approved and expressed as policy. There is an organization-wide approach to manage cybersecurity risk.

Tier 4: Adaptive

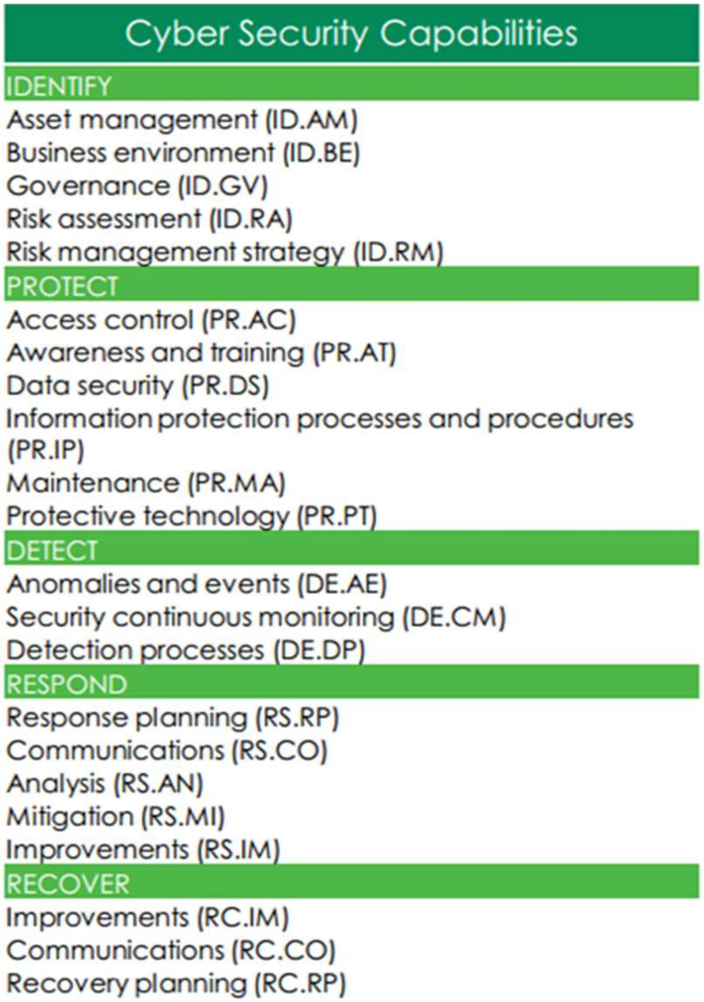
The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.

Framework implementation tiers

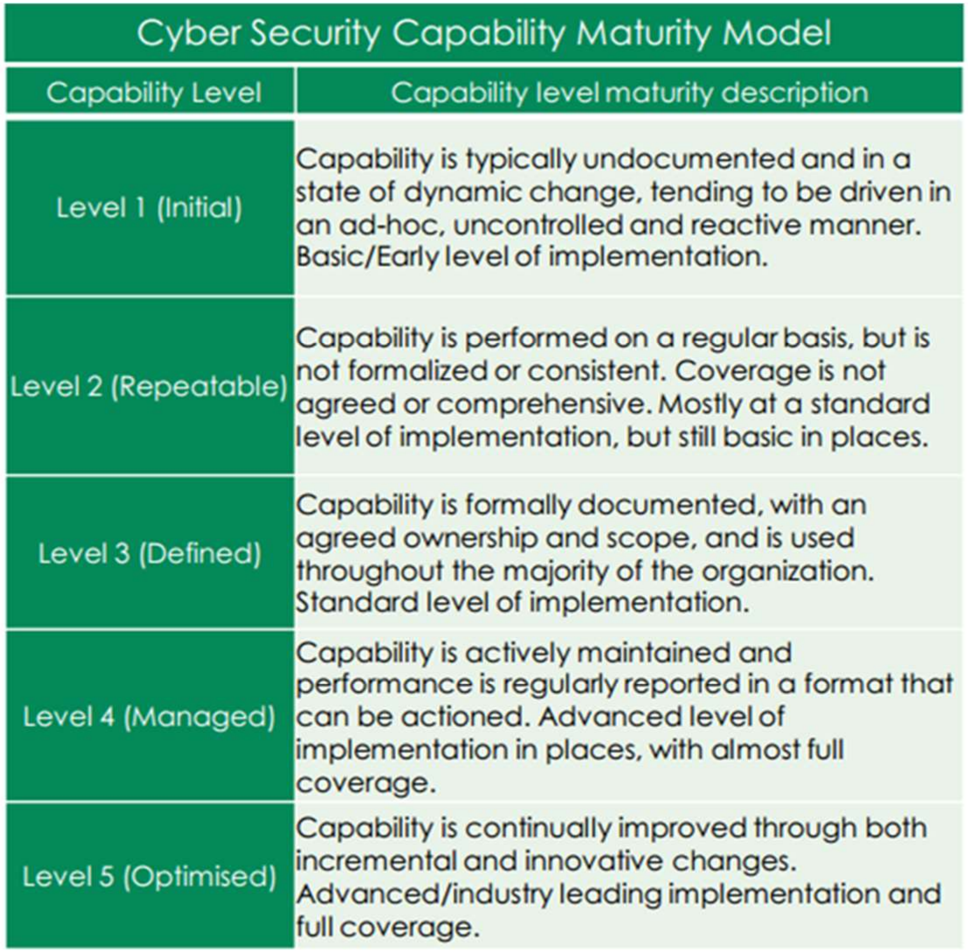
The Tiers describe an increasing **degree of rigor**, and how well **integrated cybersecurity risk decisions** are into broader risk decisions, and the degree to which the organization **shares and receives cybersecurity information** from external parties.

Organizations should determine the desired Tier, ensuring that the selected level **meets organizational goals, reduces cybersecurity risk** to acceptable levels, and is practical to implement.

NIST maturity model



Cyber Security Capabilities
IDENTIFY
Asset management (ID.AM)
Business environment (ID.BE)
Governance (ID.GV)
Risk assessment (ID.RA)
Risk management strategy (ID.RM)
PROTECT
Access control (PR.AC)
Awareness and training (PR.AT)
Data security (PR.DS)
Information protection processes and procedures (PR.IP)
Maintenance (PR.MA)
Protective technology (PR.PT)
DETECT
Anomalies and events (DE.AE)
Security continuous monitoring (DE.CM)
Detection processes (DE.DP)
RESPOND
Response planning (RS.RP)
Communications (RS.CO)
Analysis (RS.AN)
Mitigation (RS.MI)
Improvements (RS.IM)
RECOVER
Improvements (RC.IM)
Communications (RC.CO)
Recovery planning (RC.RP)



Cyber Security Capability Maturity Model

Capability Level	Capability level maturity description
Level 1 (Initial)	Capability is typically undocumented and in a state of dynamic change, tending to be driven in an ad-hoc, uncontrolled and reactive manner. Basic/Early level of implementation.
Level 2 (Repeatable)	Capability is performed on a regular basis, but is not formalized or consistent. Coverage is not agreed or comprehensive. Mostly at a standard level of implementation, but still basic in places.
Level 3 (Defined)	Capability is formally documented, with an agreed ownership and scope, and is used throughout the majority of the organization. Standard level of implementation.
Level 4 (Managed)	Capability is actively maintained and performance is regularly reported in a format that can be actioned. Advanced level of implementation in places, with almost full coverage.
Level 5 (Optimised)	Capability is continually improved through both incremental and innovative changes. Advanced/industry leading implementation and full coverage.

Maturity assessment questions:

For all questions ask '*is it documented, and do the right people know it exists?*'

❑ Do you have policies? Acceptable use, Information security, others?

❑ Is there a risk assessment process in place?
How long ago was the last risk assessment
What happened with the findings?
What % of the treatments were implemented

❑ Do you have an asset register?
How up to date is it?
Does it include information assets?

Maturity assessment questions …

□ What tools do you have?

□ Do you have an incidence response plan? When was it last used? Did you identify the root cause? Did you fix it? Do you perform simulations against the plan?

□ How many dormant accounts exist?

□ Who approves access to data?

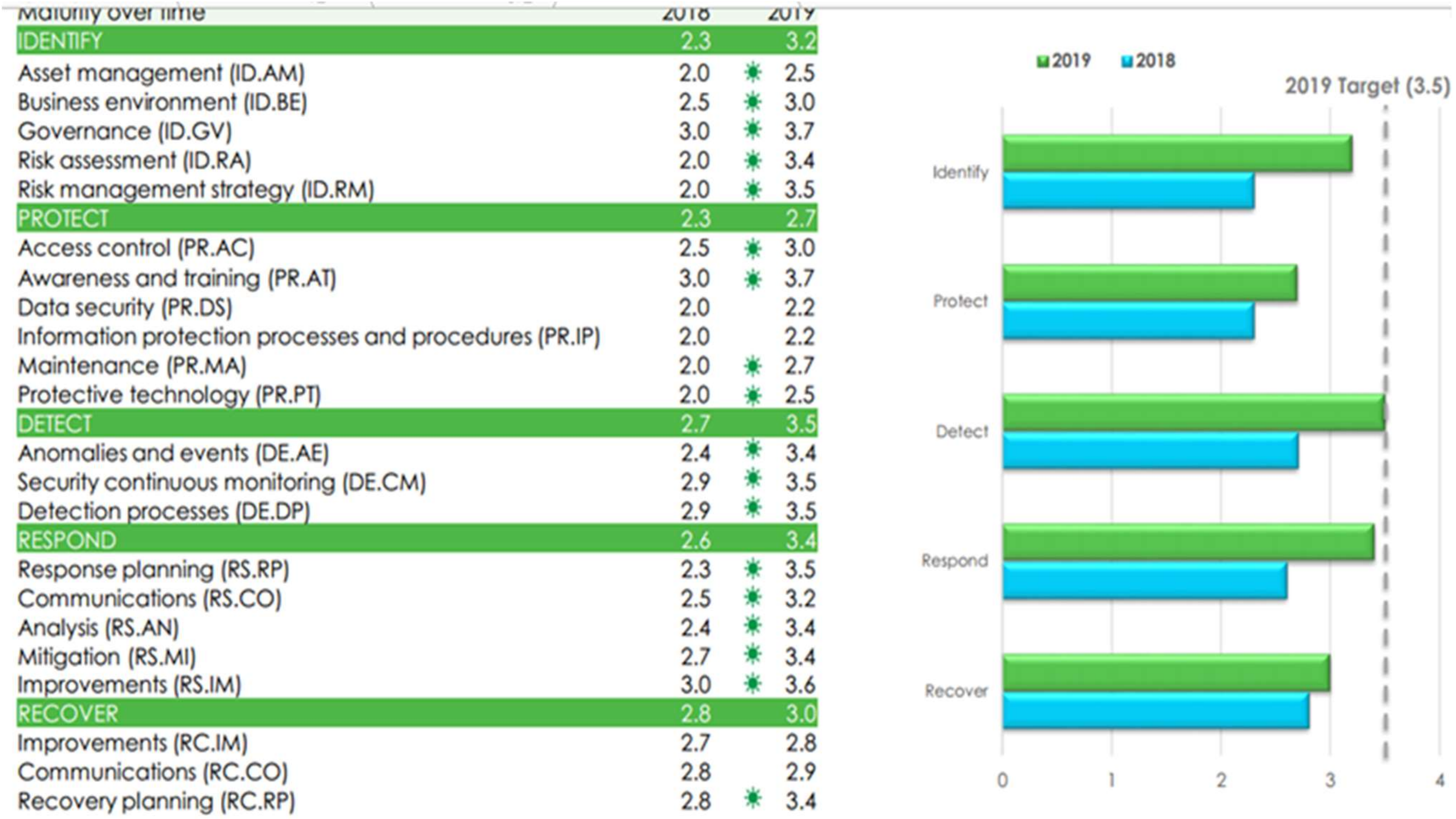
□ How are user accounts created?

□ Who has responsibility to create, amend or delete users

□ Who performs user access reviews and how often?

□ How often do you perform user awareness and training?

Example



Maturity over time	2018		2019
IDENTIFY	2.3		3.2
Asset management (ID.AM)	2.0	✳	2.5
Business environment (ID.BE)	2.5	✳	3.0
Governance (ID.GV)	3.0	✳	3.7
Risk assessment (ID.RA)	2.0	✳	3.4
Risk management strategy (ID.RM)	2.0	✳	3.5
PROTECT	2.3		2.7
Access control (PR.AC)	2.5	✳	3.0
Awareness and training (PR.AT)	3.0	✳	3.7
Data security (PR.DS)	2.0		2.2
Information protection processes and procedures (PR.IP)	2.0		2.2
Maintenance (PR.MA)	2.0	✳	2.7
Protective technology (PR.PT)	2.0	✳	2.5
DETECT	2.7		3.5
Anomalies and events (DE.AE)	2.4	✳	3.4
Security continuous monitoring (DE.CM)	2.9	✳	3.5
Detection processes (DE.DP)	2.9	✳	3.5
RESPOND	2.6		3.4
Response planning (RS.RP)	2.3	✳	3.5
Communications (RS.CO)	2.5	✳	3.2
Analysis (RS.AN)	2.4	✳	3.4
Mitigation (RS.MI)	2.7	✳	3.4
Improvements (RS.IM)	3.0	✳	3.6
RECOVER	2.8		3.0
Improvements (RC.IM)	2.7		2.8
Communications (RC.CO)	2.8		2.9
Recovery planning (RC.RP)	2.8	✳	3.4

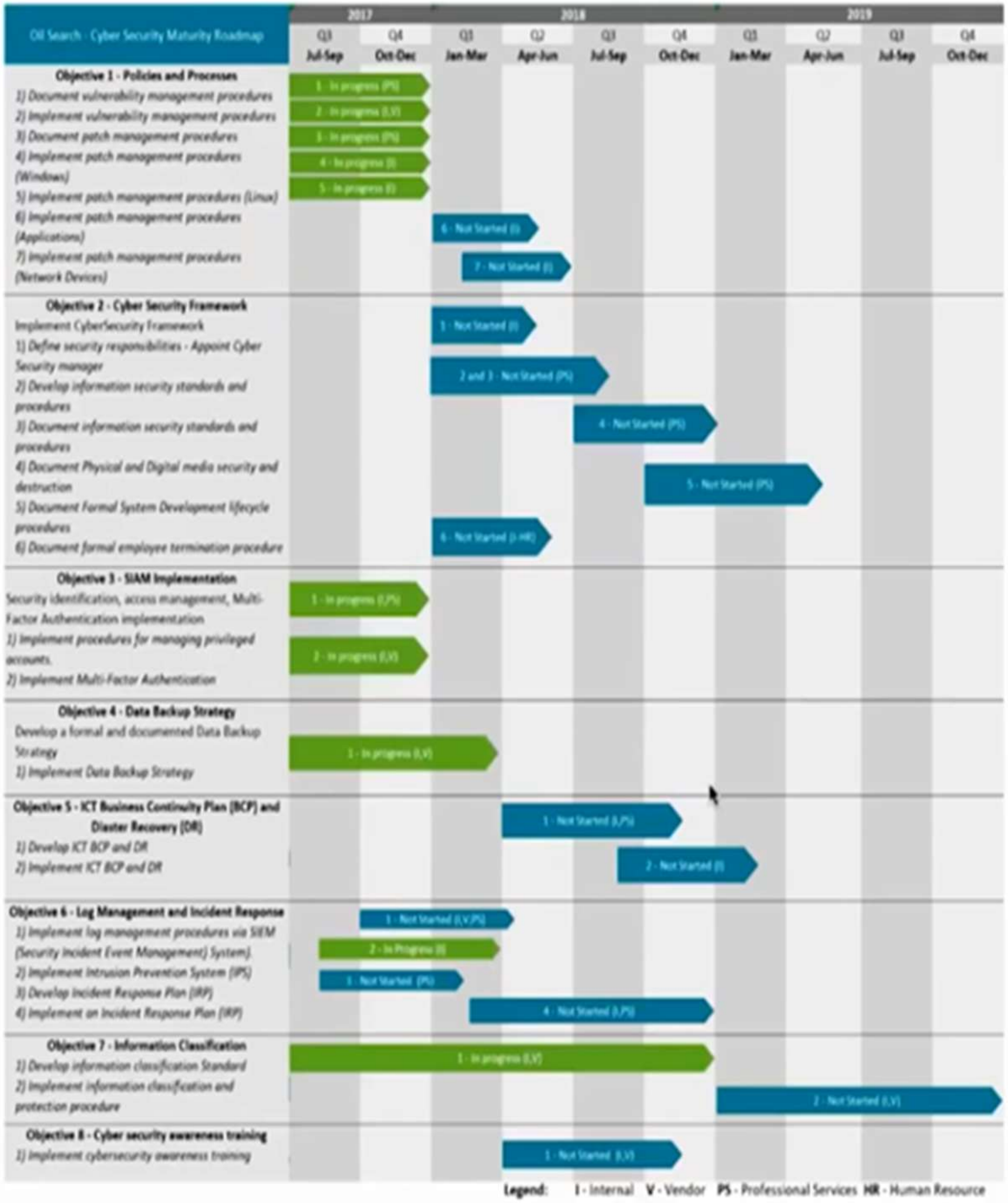
b.) Develop objectives

- ❑ Identify what you are protecting
- ❑ What you are protecting it from
- ❑ What are your main concerns? (CEOs or customers')
- ❑ What would hurt the organization the most?

Where we are now:

- No Security Framework
- No formal data classification or identification of critical assets
- Information Security processes and network visualisation inadequate
- No vulnerability Management program
- Informal patch management procedure
- Security roles and responsibilities not defined
- Lack of Multi Factor Authentication
- Security identification and access management not defined
- Partial Security awareness training and documentation provided to staff
- Physical and Digital Media Security and Destruction Not clearly identified
- Formal or documented SDLC (System Development Life Cycle) process
- Formalized employee termination process exists, but is undocumented
- No internal IDS/IPS, security monitoring and unauthorised network connections detection implemented
- Informal log management and analysis of security events
- Informal backup procedures
- No ICT Business Continuity Plan (BCP) documented or implemented
- No ICT Disaster Recovery (DR) Plan documented or implemented.

What we need to do



Oil Search - Cyber Security Maturity Roadmap

Objective 1 - Policies and Processes

1) Document vulnerability management procedures
2) Implement vulnerability management procedures
3) Document patch management procedures
4) Implement patch management procedures (Windows)
5) Implement patch management procedures (Linux)
6) Implement patch management procedures (Applications)
7) Implement patch management procedures (Network Devices)

Objective 2 - Cyber Security Framework

Implement CyberSecurity Framework
1) Define security responsibilities - Appoint Cyber Security manager
2) Develop information security standards and procedures
3) Document information security standards and procedures
4) Document Physical and Digital media security and destruction
5) Document Formal System Development lifecycle procedures
6) Document formal employee termination procedure

Objective 3 - SIAM Implementation

Security identification, access management, Multi-Factor Authentication implementation
1) Implement procedures for managing privileged accounts.
2) Implement Multi-Factor Authentication

Objective 4 - Data Backup Strategy

Develop a formal and documented Data Backup Strategy
1) Implement Data Backup Strategy

Objective 5 - ICT Business Continuity Plan (BCP) and Diaster Recovery (DR)

1) Develop ICT BCP and DR
2) Implement ICT BCP and DR

Objective 6 - Log Management and Incident Response

1) Implement log management procedures via SIEM (Security Incident Event Management) System).
2) Implement Intrusion Prevention System (IPS)
3) Develop Incident Response Plan (IRP)
4) Implement an Incident Response Plan (IRP)

Objective 7 - Information Classification

1) Develop information classification Standard
2) Implement information classification and protection procedure

Objective 8 - Cyber security awareness training

1) Implement cybersecurity awareness training

Legend: I - Internal V - Vendor PS - Professional Services HR - Human Resource

Where we want to be:

- Integrated NIST Cybersecurity Framework into the business
- Data audited and classified
- Critical assets identified and protected
- Information security Standard documented and implemented
- Vulnerability Management procedures implemented
- Officially assigned information security office.
- Multi-Factor Authentication Implemented
- Security identification and access management procedures implemented.
- Security awareness training program maintained
- Physical and Digital Media security procedures maintained
- System development life cycle procedures implemented
- Employee termination procedures implemented
- IDS/IPS and security monitoring implemented and maintained
- SIEM implemented and procedures maintained
- ICT Incident response plan integrated with existing Incident Response Standard
- Full BCP and DR standards and procedures documented and implemented

IV.) Establish performance indicators

a) Specific: Provides an explicit and clear explanation of what needs to be achieved to prepare for, mitigate, respond to, and recover from cyber attack scenarios.

b) Measurable: defined operational metric with a target that indicates success

c) Attainable: challenging and realistic target for cyber security readiness

d) Relevant: Maintains consistency between strategic objectives and higher level ambitions

e) Timely: Determines a specified date by which to meet a goal

V.) Identify key stakeholders

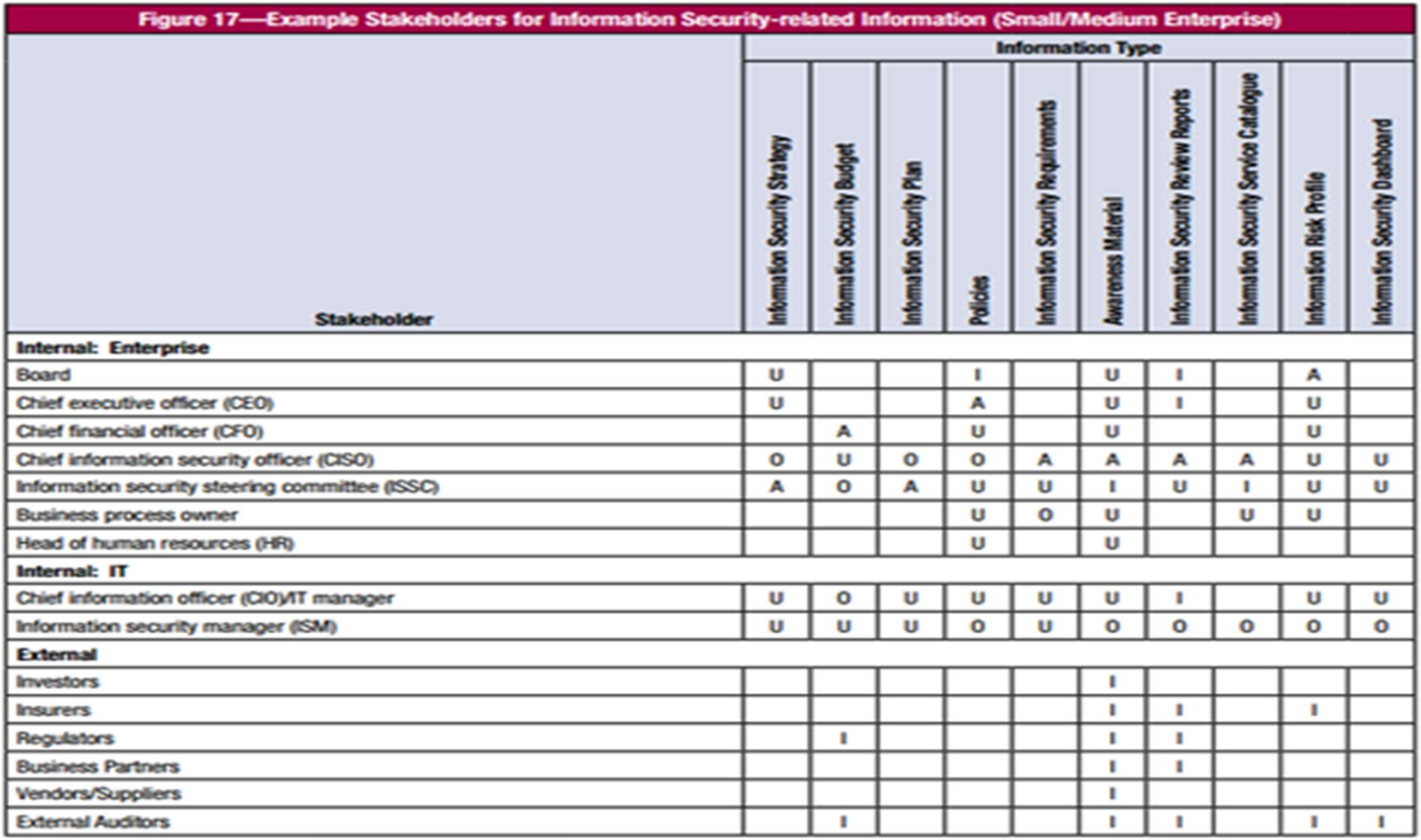


Figure 17—Example Stakeholders for Information Security-related Information (Small/Medium Enterprise)

	Information Type									
Stakeholder	Information Security Strategy	Information Security Budget	Information Security Plan	Policies	Information Security Requirements	Awareness Material	Information Security Review Reports	Information Security Service Catalogue	Information Risk Profile	Information Security Dashboard
Internal: Enterprise										
Board	U			I		U	I		A	
Chief executive officer (CEO)	U			A		U	I		U	
Chief financial officer (CFO)		A		U		U			U	
Chief information security officer (CISO)	O	U	O	O	A	A	A	A	U	U
Information security steering committee (ISSC)	A	O	A	U	U	I	U	I	U	U
Business process owner				U	O	U		U	U	
Head of human resources (HR)				U		U				
Internal: IT										
Chief information officer (CIO)/IT manager	U	O	U	U	U	U	I		U	U
Information security manager (ISM)	U	U	U	O	U	O	O	O	O	O
External										
Investors						I				
Insurers						I	I		I	
Regulators		I				I	I			
Business Partners						I	I			
Vendors/Suppliers						I				
External Auditors		I				I	I		I	I

Define roles

Key stakeholders, both internal and external to the organization, have an important role in executing the strategy.

By clearly outlining their roles and responsibilities, the organization can improve internal processes, establish accountability, and increase preparedness.

VI.) Determine resource needs

- ❑ Identify the amount of time and level of resources that the organization is willing to invest in cyber security.
- ❑ Identify the personnel who will engage in cyber security activities on behalf of the organization
- ❑ Establish dedicated funding for the cyber team to function effectively
- ❑ Develop a working group or steering committee where different user groups are represented, and can help in managing operational processes and competing interests
- ❑ Institutionalize cyber defenses through senior management buy in, and creating a culture of security.

VI.) Determine resource needs …

- Identify a champion within leadership who can drive the strategy development process, as well as champions within the different functional areas
- Incorporate both technical and policy expertise

VII.) Develop a communications plan

- ❑ Identify everyday communication guidelines, crisis communications, mandatory reporting requirements, how sensitive information is to be handled
- ❑ Effective communication with internal and external stakeholders is essential as it sometimes needs to be different from the standard organization communication.
- ❑ Develop templates for key stakeholders, especially in addressing incidence or crisis communication.

VIII.) Implement the strategy

- ❑ This is the process of accomplishing the strategic goals and objectives laid out in the cyber security strategy.
- ❑ Once the strategy has been developed, the organization needs to ensure that it is proactively implemented and overseen by a formal project manager.
- ❑ A typical implementation and monitoring process includes:
- Initializing change processes
- Evaluating milestones for success or concern
- Implementing any necessary ad hoc revision
- Finalizing processes and reporting data for evaluation

4. Finally…

"In reality, strategy is actually very straightforward. You pick a general direction and implement like hell."

Jack Welch

"A strategy is necessary because the future is unpredictable."

Robert Waterman

Frameworks that can be used

1. NIST cyber security framework
2. COBIT 5 for information security
3. ISO 27001/2
4. PCI DSS
5. Existing regulations

The end

Any questions?