NIS2
Steppingstones to Compliance

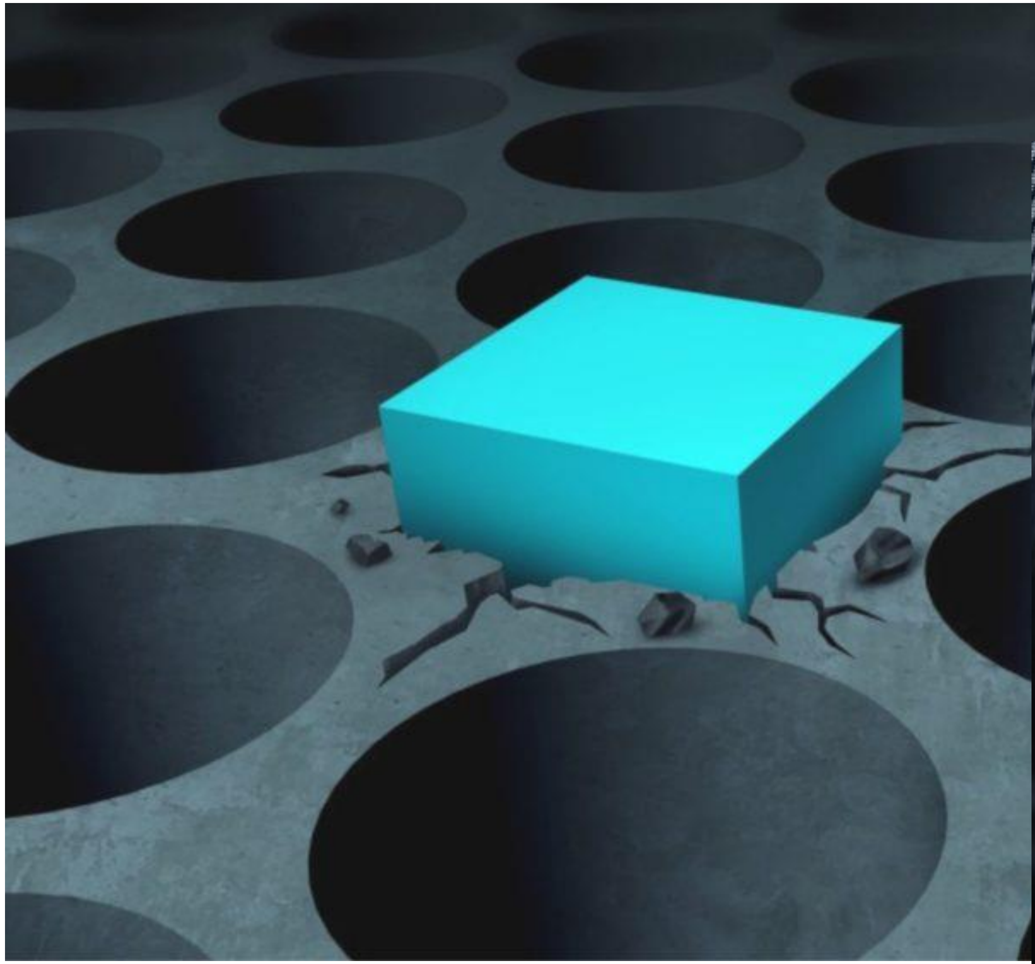
INTERCONNECTING NETWORKS AND PEOPLE FOR OVER 25 YEARS

INEX

INTERCONNECTING NETWORKS
AND PEOPLE FOR OVER 25 YEARS

Agenda

Cultural Shift

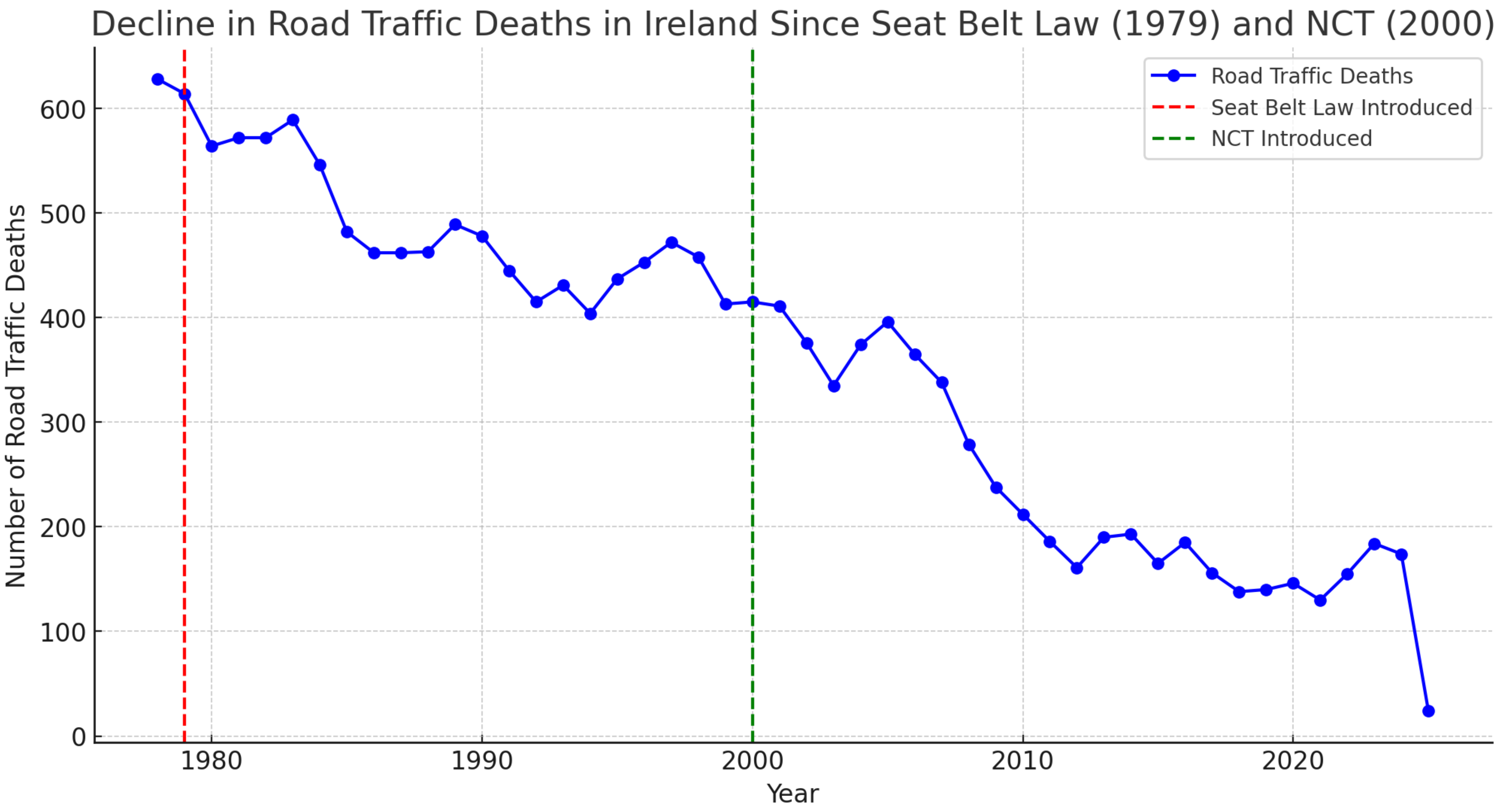


National Car Testing Service

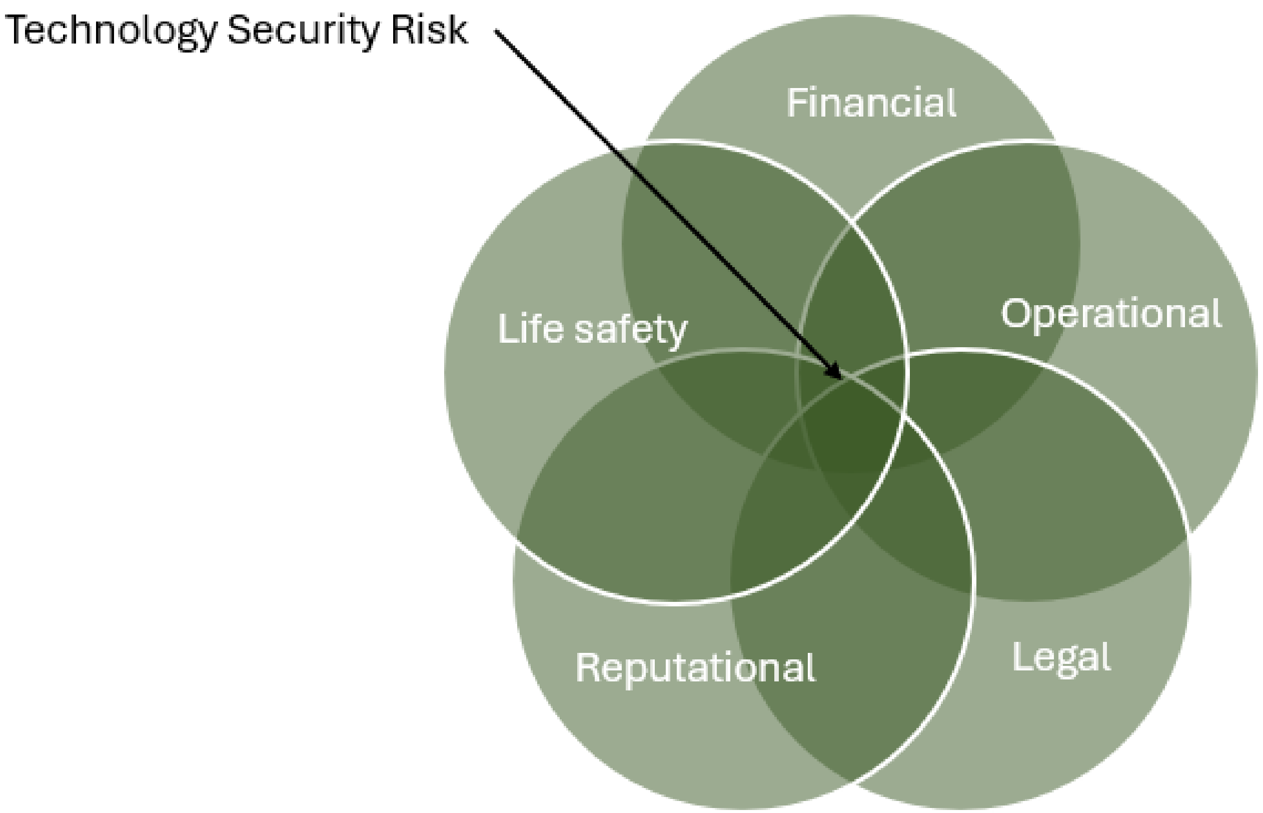
NCT

An tSeirbhís Náisiúnta Tástála Carranna

Benefits of Regulation



Technology Risk - Is Business Risk - Is Societal Risk

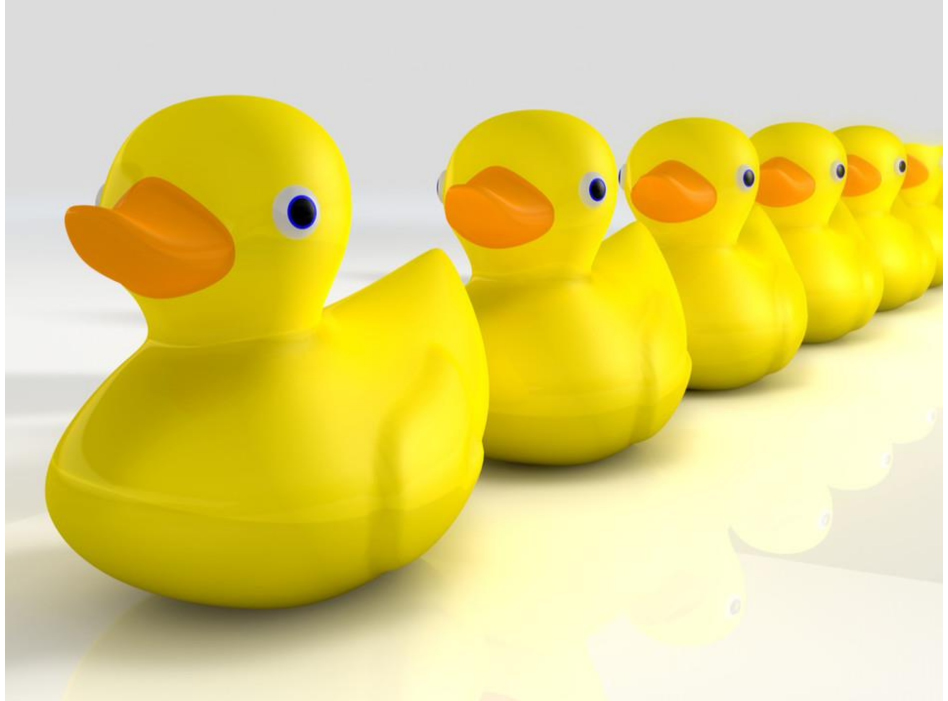


NIS2
COMPLIANCE
STEPPING STONES TO NIS2 COMPLIANCE
CE
RISK
ASSESSMENT
GOVERDENCE
& LEADERSHIP
SECURE
CONTURCHP
ASSESSMENT
INCIPONCE
LEADERSHIP
ACCESCE
CONTROL
RISK
ASSESMEST
SECURE
SUPPLY
CHAAIL
JNCUCE
MONTORING

Steppingstone #1

Cybersecurity Risk Management Governance

Two Types of Organisations



- Formal Program in place
- Have been implementing some degree of security best practice
- Checking the “doers”

- Ad hoc approach
- Busy building/scaling the business with little focus on security.
- Limited Resources
- Doing good but not able to evidence

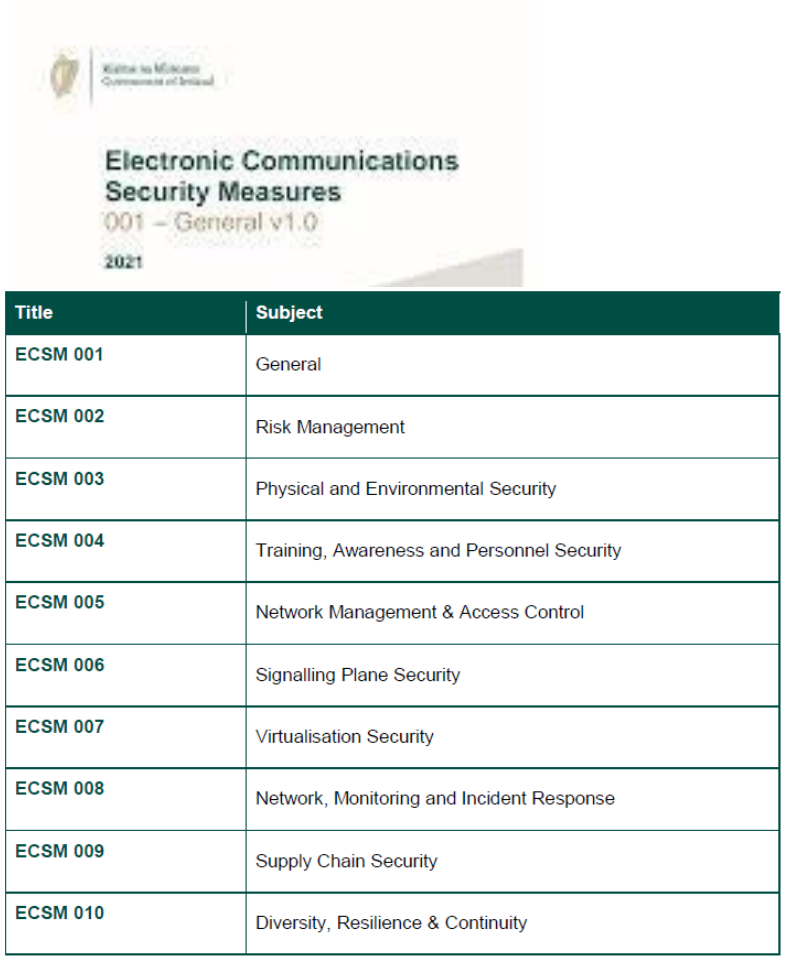
Cybersecurity Risk Management

Cybersecurity Risk Management
A state of Mind – Not a State of Being

Steppingstones to Compliance

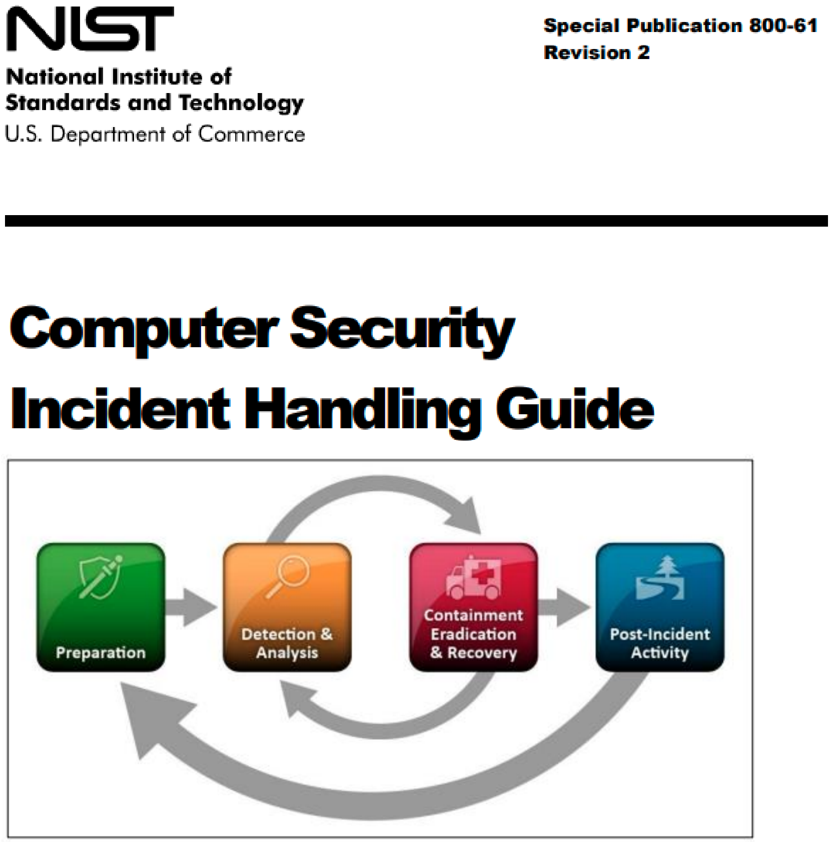
- Determine are you a critical or important entity.
- Develop cybersecurity risk management strategy aligned with business requirements
- Adopt a recognised security risk management framework, e.g. ISO 27001, IEC 62443, NIST 800 CSF 2.0
- Establish a multi-year security management program or risk mitigation roadmap
- Define security management roles and responsibilities
- Designate and communicate your organizations' “Single Point of Contract or SPOC
- Establish cybersecurity risk management as standing Board/SLT agenda item
- Define security program metrics to facilitate risk reporting/oversight
- Educate your management team and users

Be Authoritative in your Approach



Electronic Communications Security Measures
001 – General v1.0
2021

Title	Subject
ECSM 001	General
ECSM 002	Risk Management
ECSM 003	Physical and Environmental Security
ECSM 004	Training, Awareness and Personnel Security
ECSM 005	Network Management & Access Control
ECSM 006	Signalling Plane Security
ECSM 007	Virtualisation Security
ECSM 008	Network, Monitoring and Incident Response
ECSM 009	Supply Chain Security
ECSM 010	Diversity, Resilience & Continuity



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

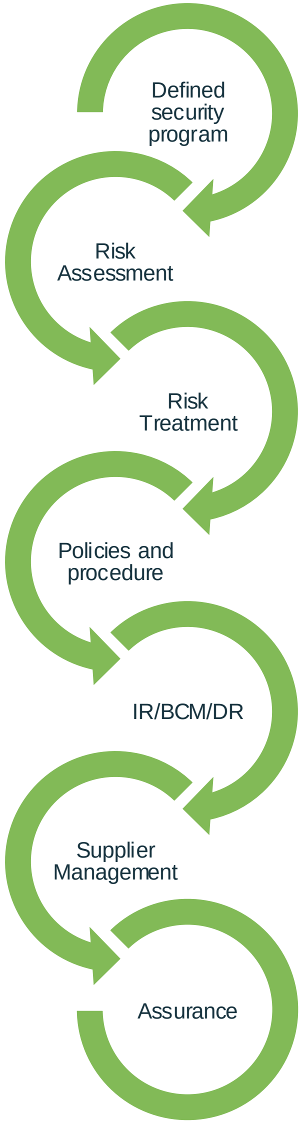
Computer Security Incident Handling Guide

Standards Based Approach

ENISA THREAT LANDSCAPE 2024

July 2023 to June 2024

Evidence Based



Defined security program

Risk Assessment

Risk Treatment

Policies and procedure

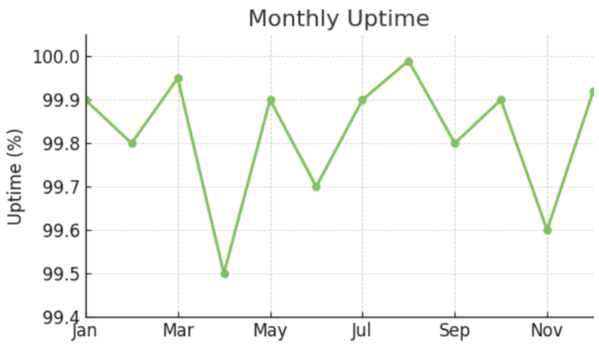
IR/BCM/DR

Supplier Management

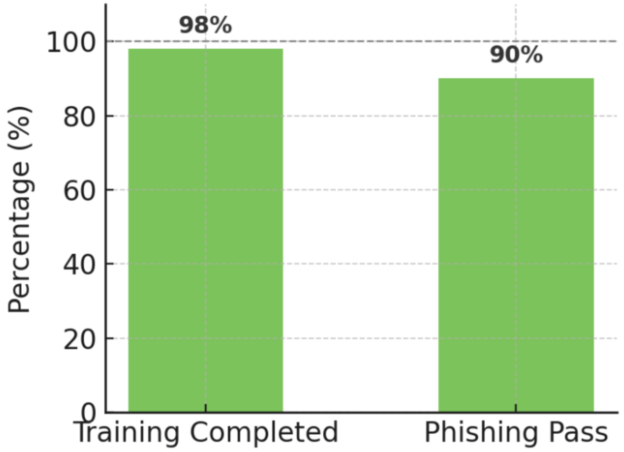
Assurance

Management Risk Oversight

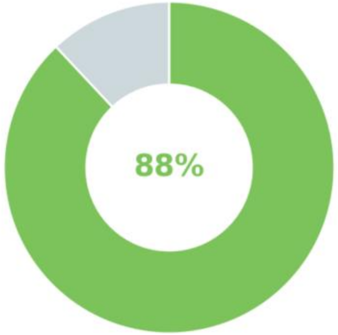
Service Availability



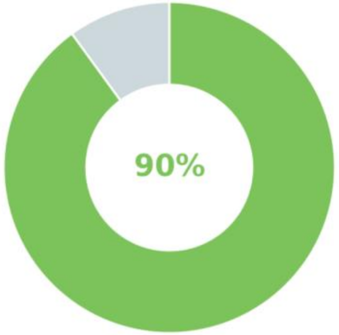
Security Awareness Training



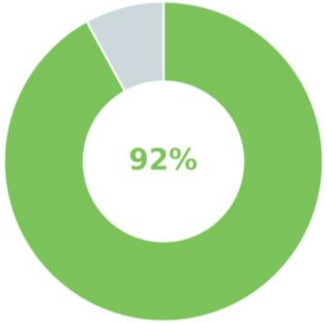
Security Assurance Testing % Approval



System Patching within SLA %



Security Policy % Approval



Steppingstone # 2

Cybersecurity
Risk Assessment

Risk Assessment

Principle of Proportionality

Balancing Point

is unique to each organisation
based on their size, complexity and risk profile

Article 21- Cybersecurity Risk Management Measures

When assessing the proportionality of those measures, due account shall be taken of the degree of the **entity's exposure to risks**, the **entity's size** and the **likelihood of occurrence** of incidents and their severity, including their **societal and economic impact**.

Risk Category	Remarks	Risk Appetite
Operational	H&S, IT, Continuity, staff retention	?
Financial	Loss of revenue, disruption loss of customers, financial sanction, incident recovery	?
Reputational	Brand damage, loss of customers	?
Regulatory	Legal risk	?
Societal	Impact on IRL Inc	?

Risk Averse

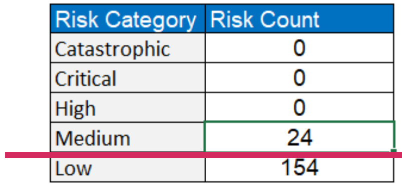
Risk Tolerance

Define Risk Profile

What Do You Care Most About?

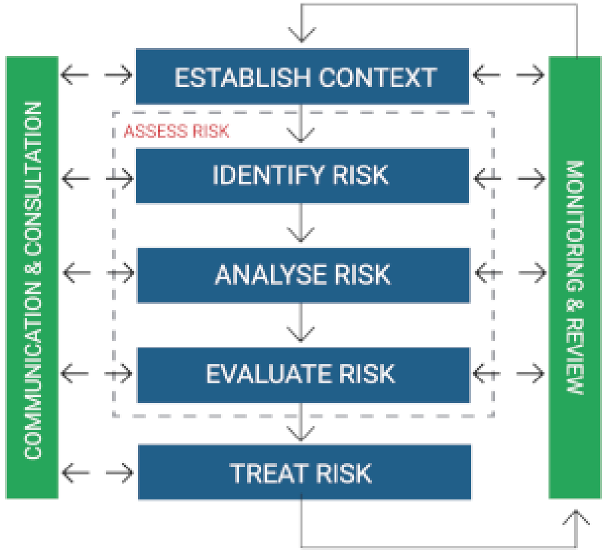
Risk Assessment

Or in a nutshell-identifying what is important to your business and selecting controls to protect it!



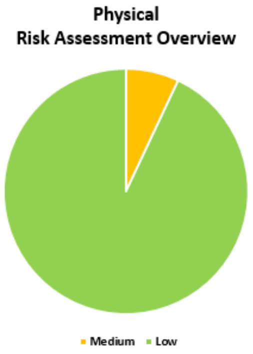
Risk Category	Risk Count
Catastrophic	0
Critical	0
High	0
Medium	24
Low	154

Risk Acceptance

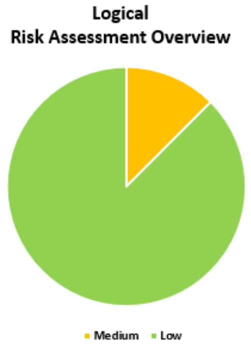


Risk Management Process

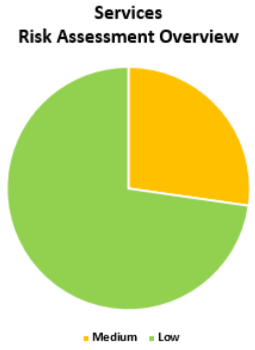
ISO 27005



- People
- Network infrastructure
- End user devices



- Network configurations
- Member data
- Employee data
- Data on endpoints
- Web presence
- Resilience
- Data protection



- Data centers
- Dark fiber providers
- Network management
- Security advisory
- Legal
- Financial services

Steppingstones to Compliance

- Develop a risk management policy. This should include a “risk acceptance statement- the level of risk the management team is willing to accept.
- Ensure it is approved by the Board/SLT.
- Identify your physical and logical assets and service providers which collectively support the delivery of important/critical services.
- Complete a risk assessment aligned with a recognised standard or approach, e.g. ISO 27005 or IEC 62443 3-2.
- Select controls from your chosen cybersecurity management framework to treat the risks identified.
- Upward reporting to support management oversight/accountability.

Steppingstone # 3

Risk Treatment/Mitigation

Standards Based Approach

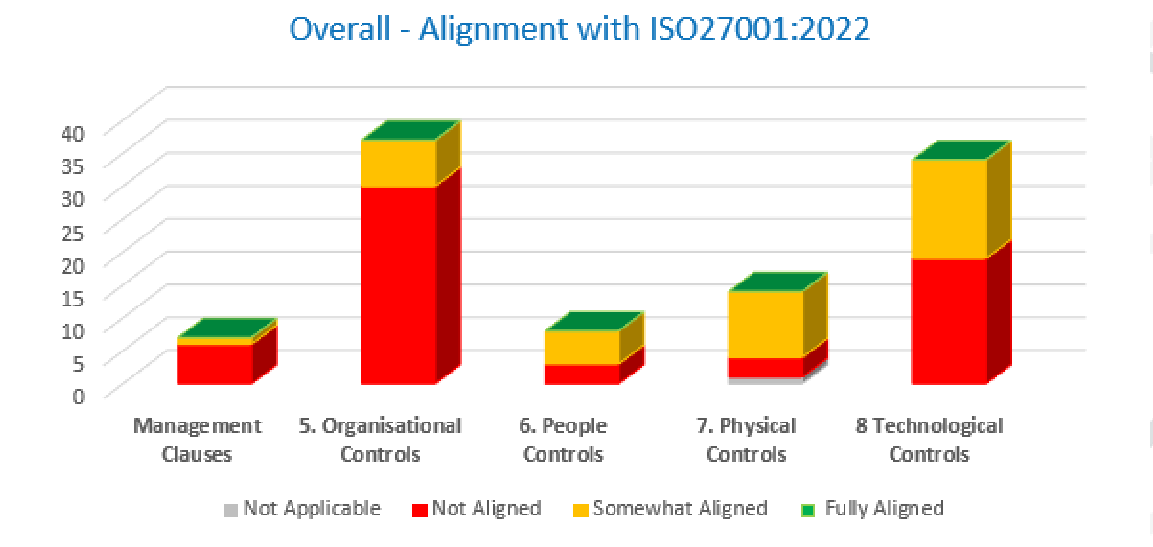
ISO 27001

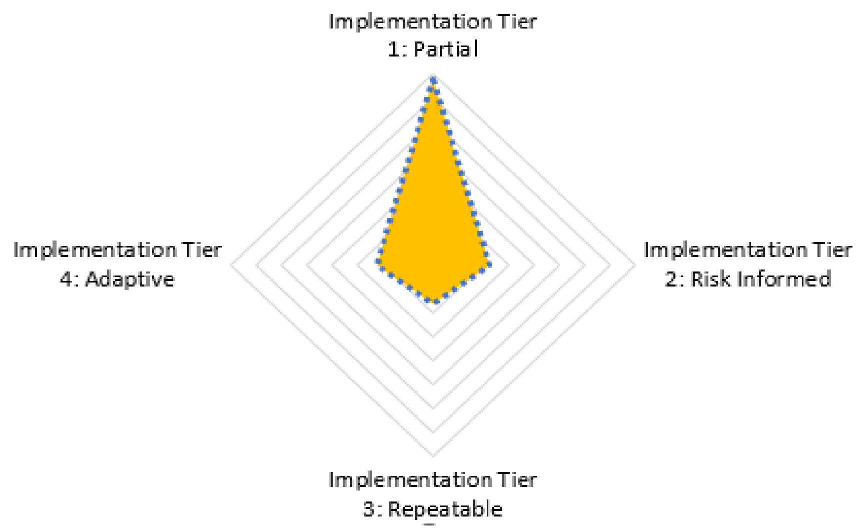
NIST Cybersecurity Framework

ISA/IEC 62443

Gap Analysis- Typical Profile

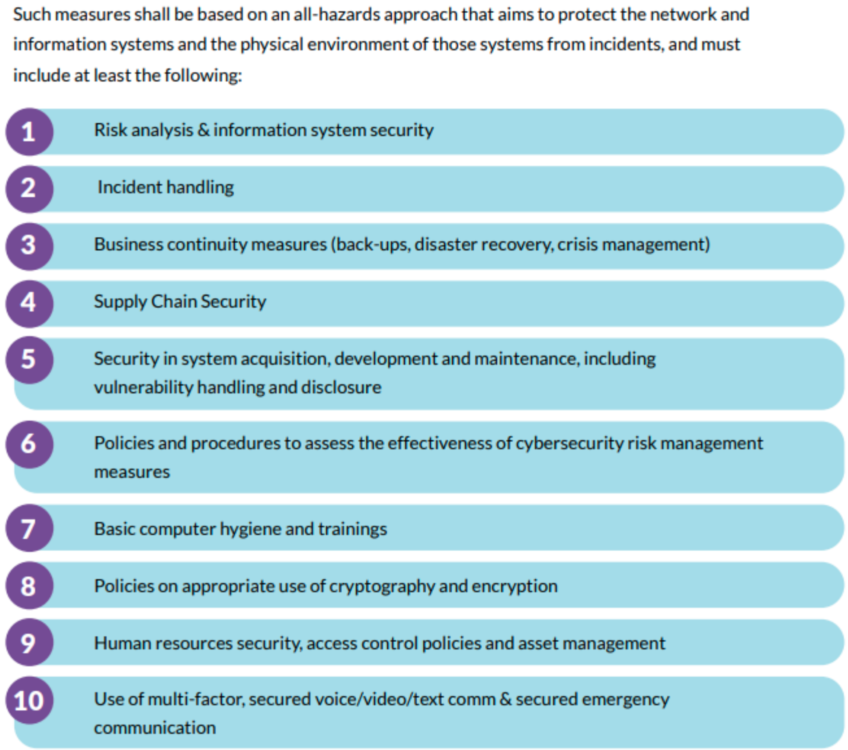
- Lack of cybersecurity governance
- Ad hoc management- no recognisable framework
- Little cybersecurity risk oversight and reporting
- No cybersecurity risk assessment methodology
- Lack of formal policies and procedures
- Ad hoc incident response management
- Immature business continuity management & DR
- No Manage third party security risk
- Lack of cyber assurance testing
- Lack of an internal audit function





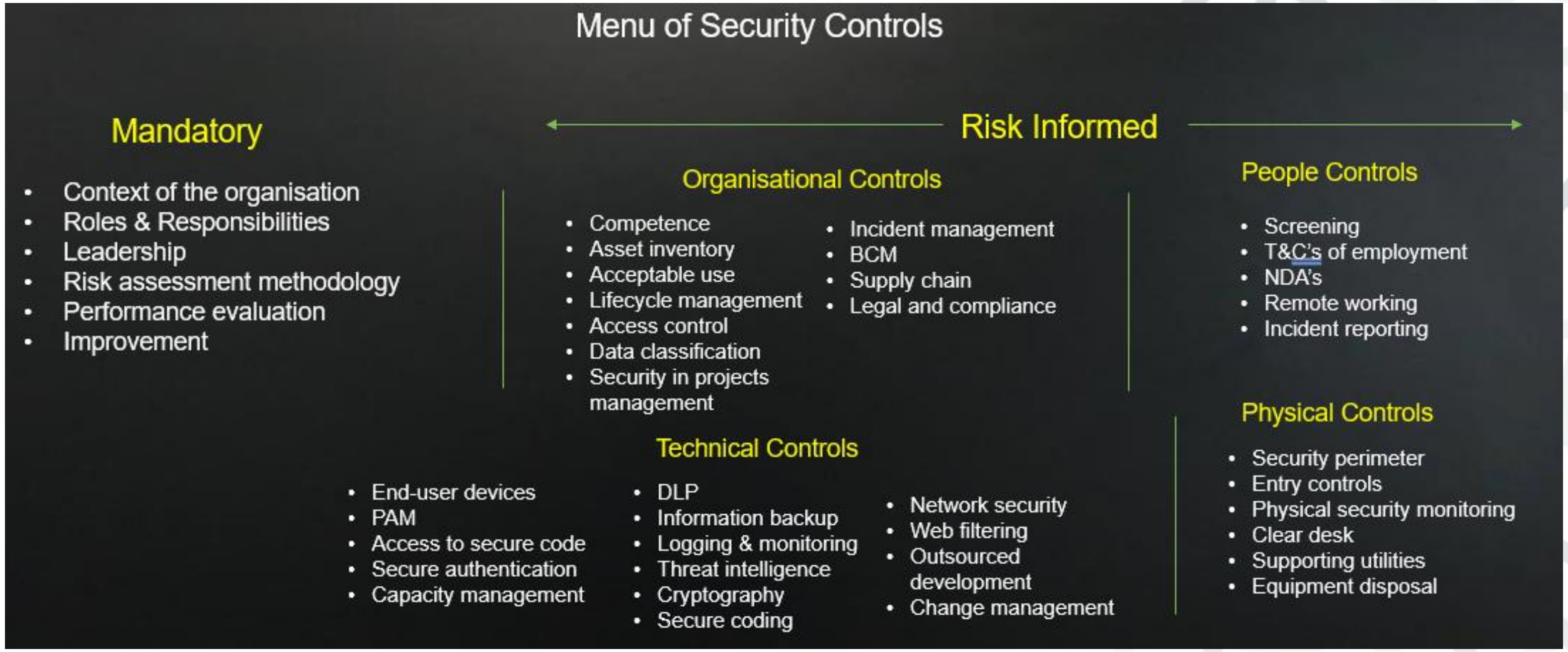
Security Control Selection
(Link to your Risk Assessment)

ISO 27001



Such measures shall be based on an all-hazards approach that aims to protect the network and information systems and the physical environment of those systems from incidents, and must include at least the following:

1. Risk analysis & information system security
2. Incident handling
3. Business continuity measures (back-ups, disaster recovery, crisis management)
4. Supply Chain Security
5. Security in system acquisition, development and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk management measures
7. Basic computer hygiene and trainings
8. Policies on appropriate use of cryptography and encryption
9. Human resources security, access control policies and asset management
10. Use of multi-factor, secured voice/video/text comm & secured emergency communication



Menu of Security Controls

Mandatory

- Context of the organisation
- Roles & Responsibilities
- Leadership
- Risk assessment methodology
- Performance evaluation
- Improvement

Risk Informed

Organisational Controls

- Competence
- Asset inventory
- Acceptable use
- Lifecycle management
- Access control
- Data classification
- Security in projects management
- Incident management
- BCM
- Supply chain
- Legal and compliance

People Controls

- Screening
- T&C's of employment
- NDA's
- Remote working
- Incident reporting

Technical Controls

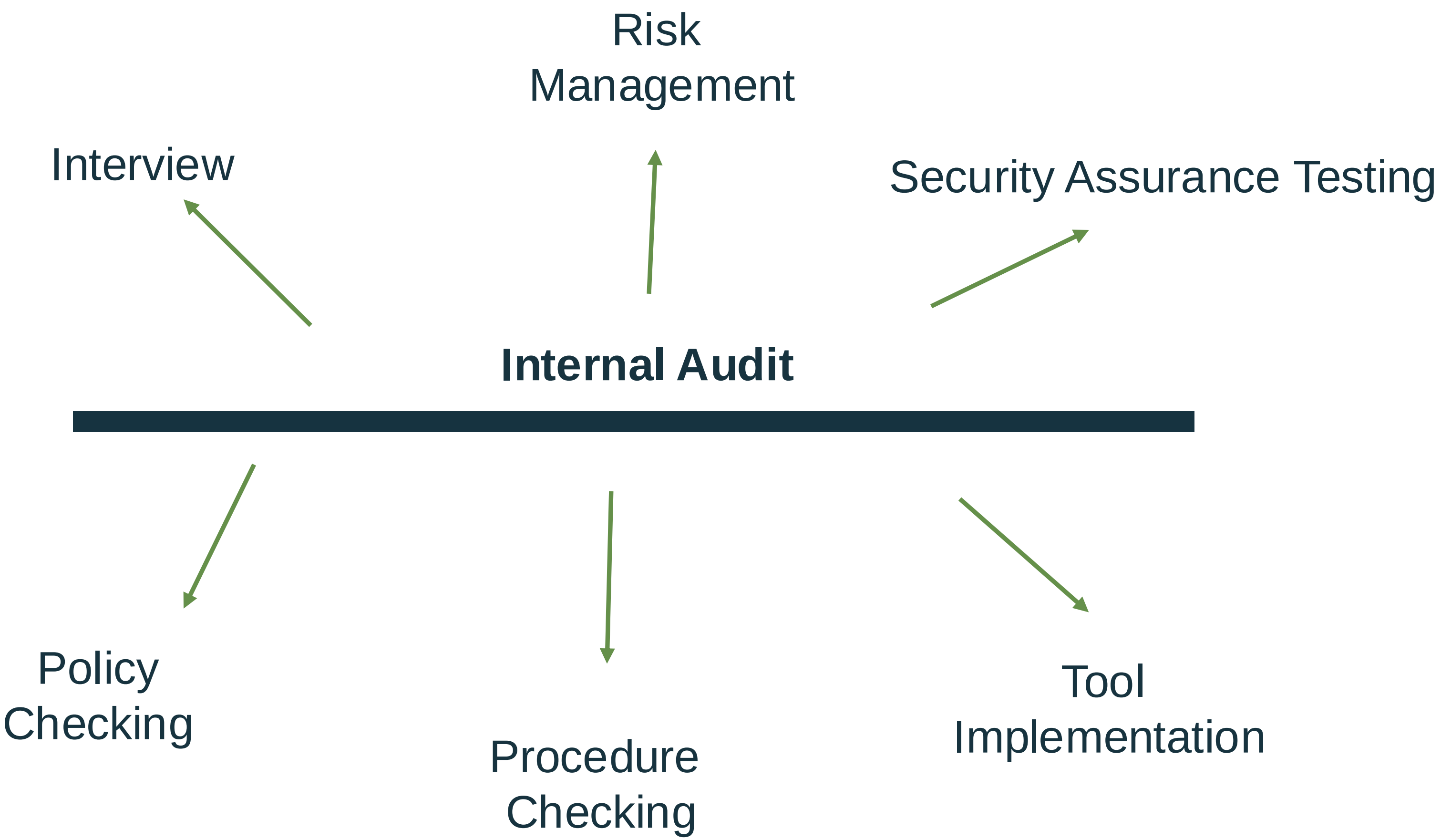
- End-user devices
- PAM
- Access to secure code
- Secure authentication
- Capacity management
- DLP
- Information backup
- Logging & monitoring
- Threat intelligence
- Cryptography
- Secure coding
- Network security
- Web filtering
- Outsourced development
- Change management

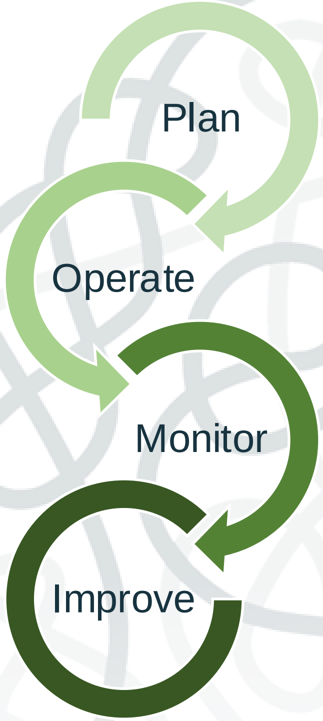
Physical Controls

- Security perimeter
- Entry controls
- Physical security monitoring
- Clear desk
- Supporting utilities
- Equipment disposal

NCSC
National Cyber
Security Centre

Ongoing Improvement





-

Process of Continuous Improvement

Steppingstones to Compliance

- Complete gap analysis against your chosen risk management framework to get an objective understanding of the current “state of the nation”.
- Understand your security control gaps. These can be technical and/or administrative in nature.
- Select and implement appropriate technical security controls to secure your critical services. (See Steppingstone 2 - Risk Assessment)
- Document and implement security policies appropriate to your organisation size, complexity and risk profile.
- Monitor the effectiveness of control implementation.
- Implement process of continuous improvement

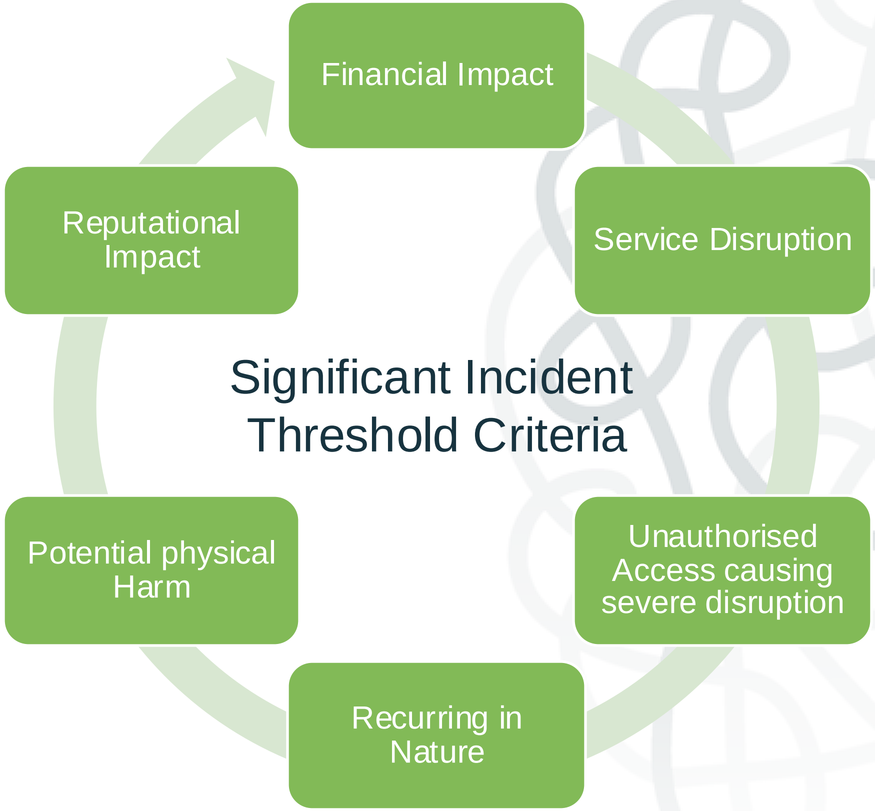
Steppingstone # 4

Incident Response Management & Reporting

What is a Significant Incident?

Any incident that has a significant impact on the provision of any service listed in the sectors or sub-sectors in annexes I and II of the law and which:

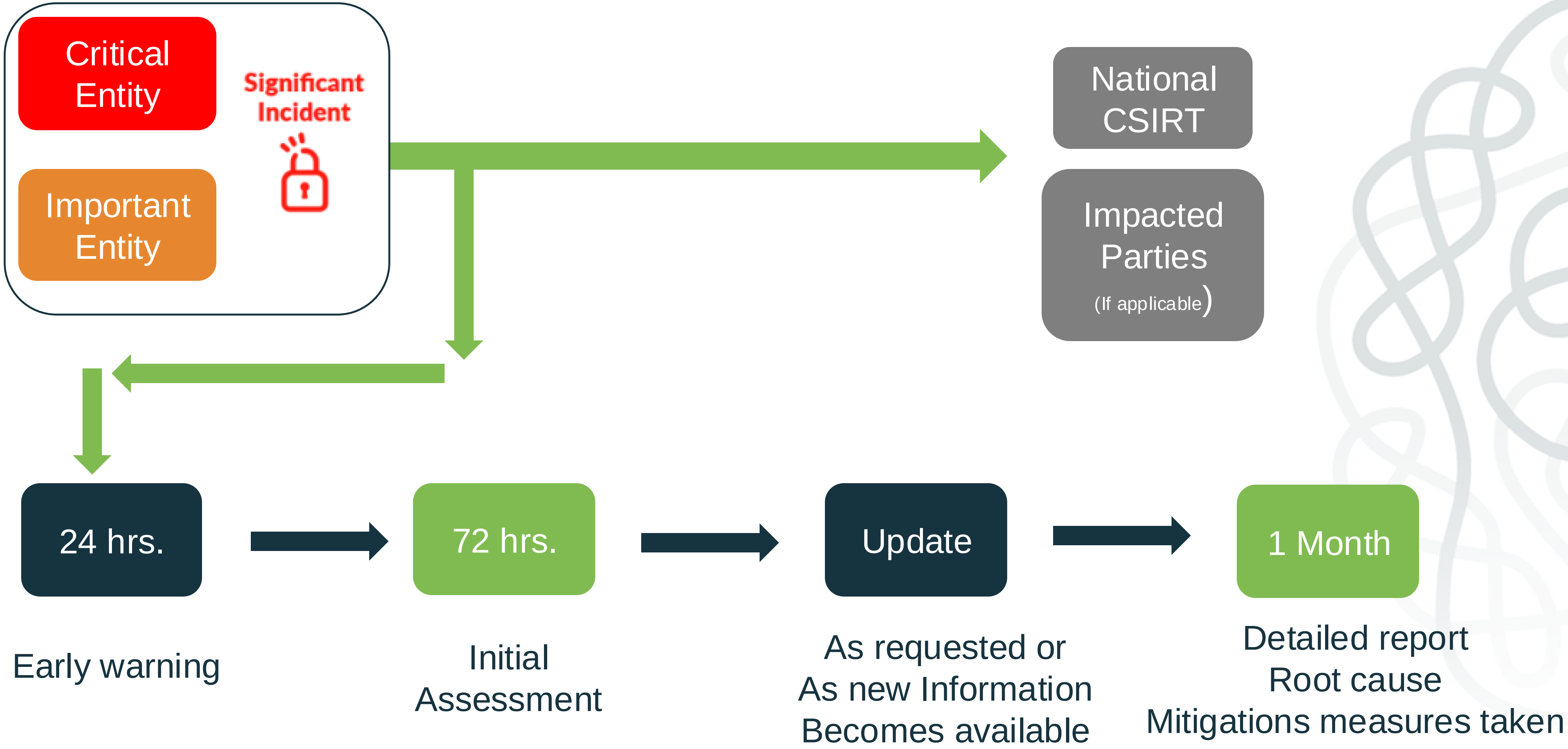
- has caused or is likely to **cause severe operational disruption** to any of the services provided in the sectors or sub-sectors listed in annex I and II or financial loss to the entity concerned; or
- has affected or is capable of affecting other natural or legal persons by **causing considerable material, personal or non-material damage**."



What is a Significant Incident?

- Change Control
- Asset configuration management
- Component failure
- Lack of adequate security hygiene
- Misaligned contract Requirements
- Single points of failure
- Software vulnerabilities
- Underperforming supplier
- Lack of standardized processes
- Human error
- Lack of continuity management
- Lack of system documentation
- Lack of incident response
- Cyber attack

Significant Incident Reporting



Critical Entity

Important Entity

Significant Incident

National CSIRT

Impacted Parties (If applicable)

24 hrs.

Early warning

72 hrs.

Initial Assessment

Update

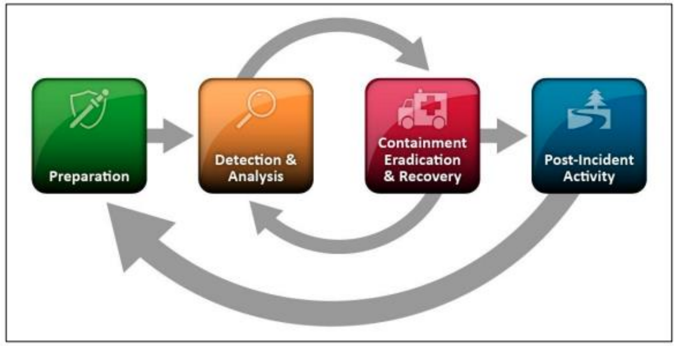
As requested or
As new Information
Becomes available

1 Month

Detailed report
Root cause
Mitigations measures taken

Steppingstones to Compliance

- Adopt a recognised incident management Framework
- Develop and implement an incident management policy and supporting incident management plans
- Define incident related roles and responsibilities, both technical and management level.
- Develop a significant incident classification procedure.
- Develop a significant incident reporting procedure.
- Maintain incident logs to record actions taken
- Maintain an incident register (recurring incident ID)
- Ensure lessons learned processes are completed and remediations tracked to completion.
- Develop Mandatory Vulnerability Disclosure Policy and procedure
- Don’t forget GDPR!

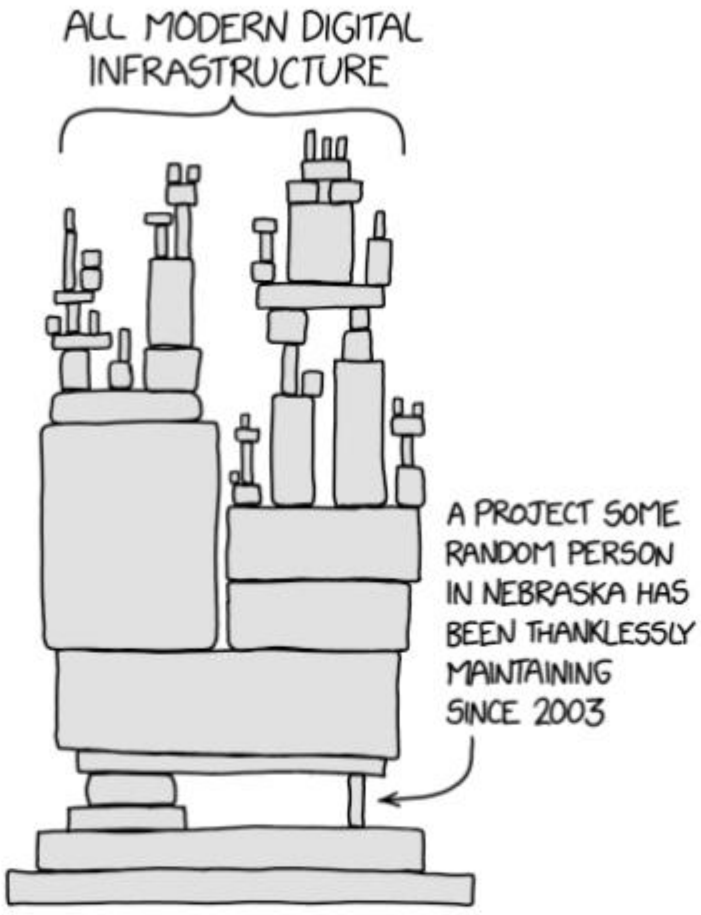


Steppingstone # 5

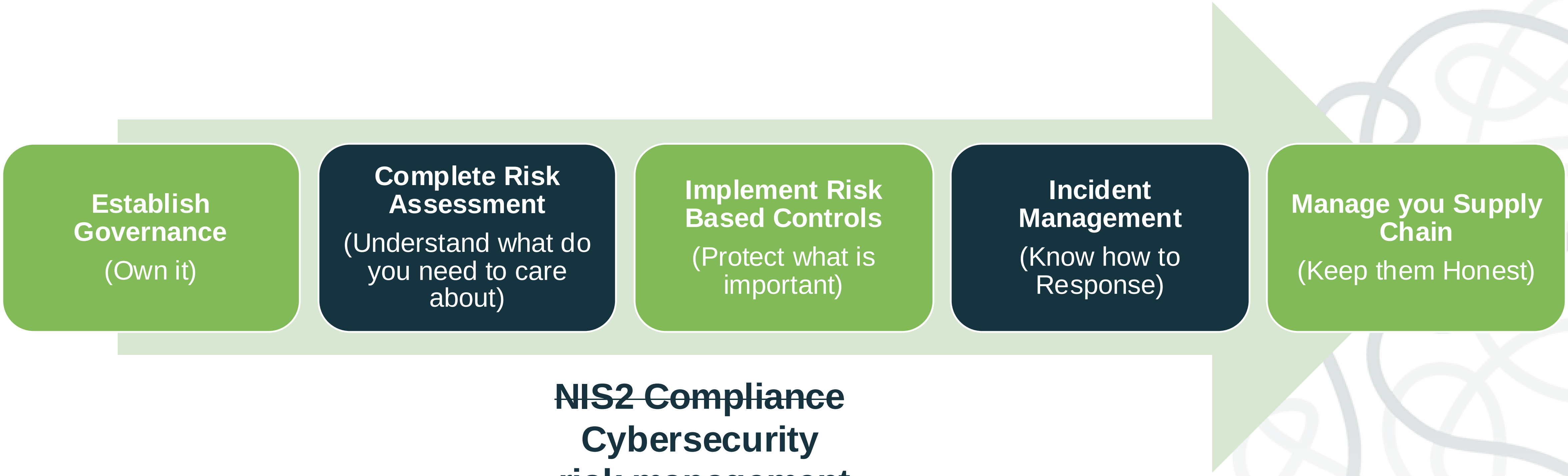
Supply Chain Management

Steppingstones to Compliance

- Map your suppliers, identify and evaluate direct and indirect suppliers.
- Risk assessment - understand their criticality
- Classify each.
- Review supplier contracts to ensure accountability
- For Critical suppliers-
  - Complete security risk management due diligence- measure suppliers' alignment with recognised standards
  - Risk based approach based on criticality of supplier
  - Ensure ongoing supervision – supplier compliance
- Develop supplier incident reporting procedures
- Plan for business continuity
- Consider Cybersecurity requirements in projects


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

In Summary
Steppingstones to Compliance



Establish Governance

(Own it)

Complete Risk Assessment

(Understand what do you need to care about)

Implement Risk Based Controls

(Protect what is important)

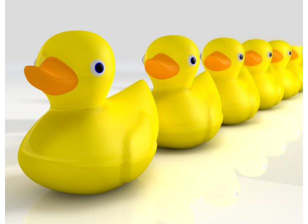
Incident Management

(Know how to Response)

Manage you Supply Chain

(Keep them Honest)

~~NIS2 Compliance~~
Cybersecurity
risk management
Program



Time- Low
Effort - Low

Time- High
Effort - High

Thank you

INEX

INTERCONNECTING NETWORKS
AND PEOPLE FOR OVER 25 YEARS