CalQRisk
Manage the effect of uncertainty on objectives

Risk Management in the Public Sector

Speakers:

Gerard Joyce, CTO, CalQRisk

Aidan Horan, Director, IPA

April 6th, 2022

Outline

1. Introductions
2. Why Do Risk Management?
3. What is Risk Management?
4. Code of Practice for the Governance of State Bodies
5. The Risk Management Process
6. Risk Criteria / Risk Appetite
7. Roles and Responsibilities
8. Contemporary Topics – Aidan Horan
9. Q &A

Introductions

CalQRisk: Develop and supply software to support Governance, Risk and Compliance activity across many sectors.

Gerard Joyce: Co-Founder and CTO of CalQRisk

- Participated in the development of ISO 31000: International Risk Management Standard.
- Chairman of the Irish Risk Management Mirror Committee

Aidan Horan: Director with IPA

- Director in the consultancy, training and development directorate at the Institute of Public Administration (IPA) specialising in governance, risk and related services.
- Nominated as a non-executive member of a number of boards / committees.

Why Do Risk Management?

CalRisk
Manage the effect of uncertainty on objectives

Because*:*

- Objectives / Desired Outcomes
- Focus
- Forward Looking
- Process Identifies Opportunities
- Better / Informed Decision Making
- Improved Performance
- Effective Governance Demands It

What is Risk Management?

- Coordinated activities to direct and control an organisation with regard to risk (ISO 31000 Standard)

What is Risk?

- The Effect of Uncertainty on Objectives (ISO 31000 / Guide 73)

Public sector entities face a wide range of uncertain internal and external factors that may affect the achievement of their objectives. The effect of this uncertainty on their objectives is called risk

IFAC

Risks are not Events!

Code of Practice for the Governance of State Bodies

- First published in 1992, updated in 2001, 2009 and 2016 (DPER)
  - Role of the Board
  - Role of the Chairperson
  - Role of Board Members
  - Board Effectiveness
  - Codes of Conduct, Ethics,..
  - Business and Financial Reporting
  - **Risk Management, Internal Control, Internal Audit and Audit and Risk Committees**
  - Relations with the Oireachtas, Minister and parent Department
  - Remuneration and Superannuation
  - Quality Customer Service

Risk Management

CalQRisk
Manage the effect of uncertainty on objectives

Key Elements of Board's Oversight of RM:

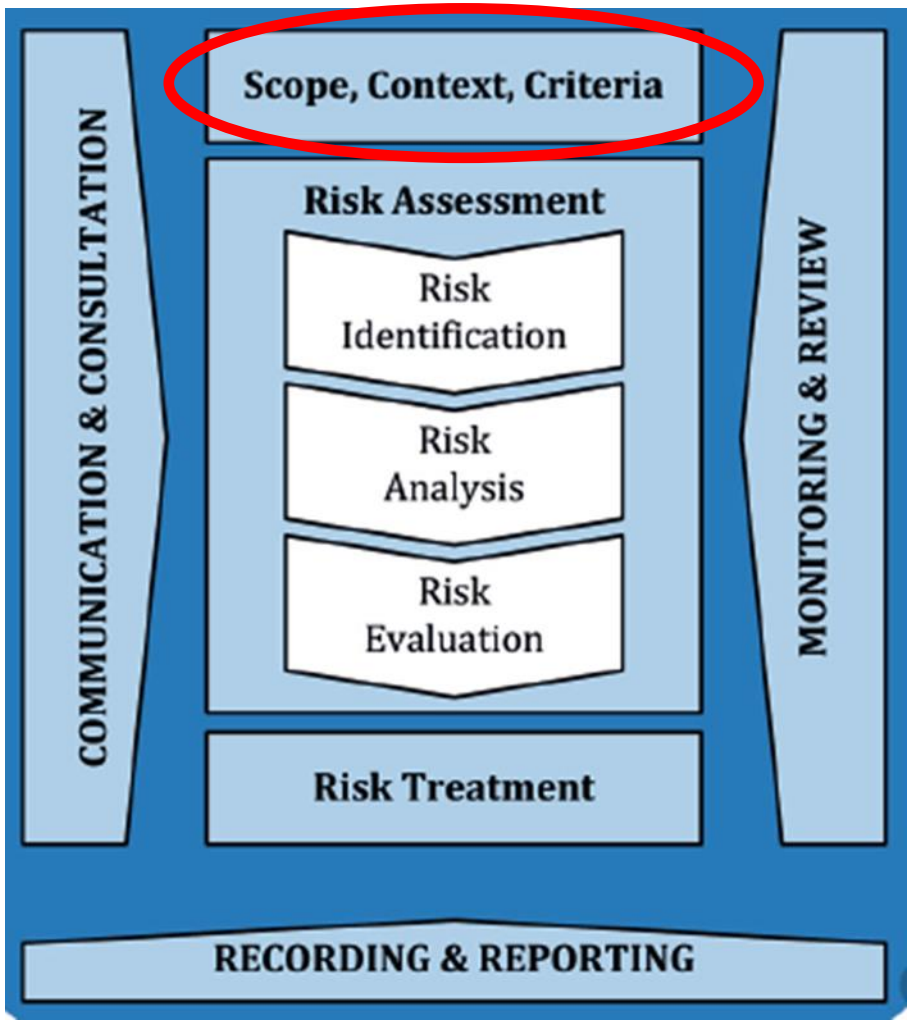
- Have Risk Management as a "Standing agenda item"
- Approve the Risk Management policy (including setting risk appetite)
- Review / approve management reporting on risk management
- Require external review of effectiveness of RM framework
- Confirmation in annual report of assessment / mitigation.
- Establish an Audit and Risk Committee
- Appoint a CRO

Internal Control

Board is responsible for ensuring:

- Clearly defined management responsibilities
- Risk identification process and evaluation of financial implications
- A budgeting system and means to compare actual with budget
- Procedures and practices to mitigate risks, e.g. segregation of duties
- Procedures for monitoring the effectiveness of controls
- Confirmation in annual report of review of effectiveness of the system of internal control

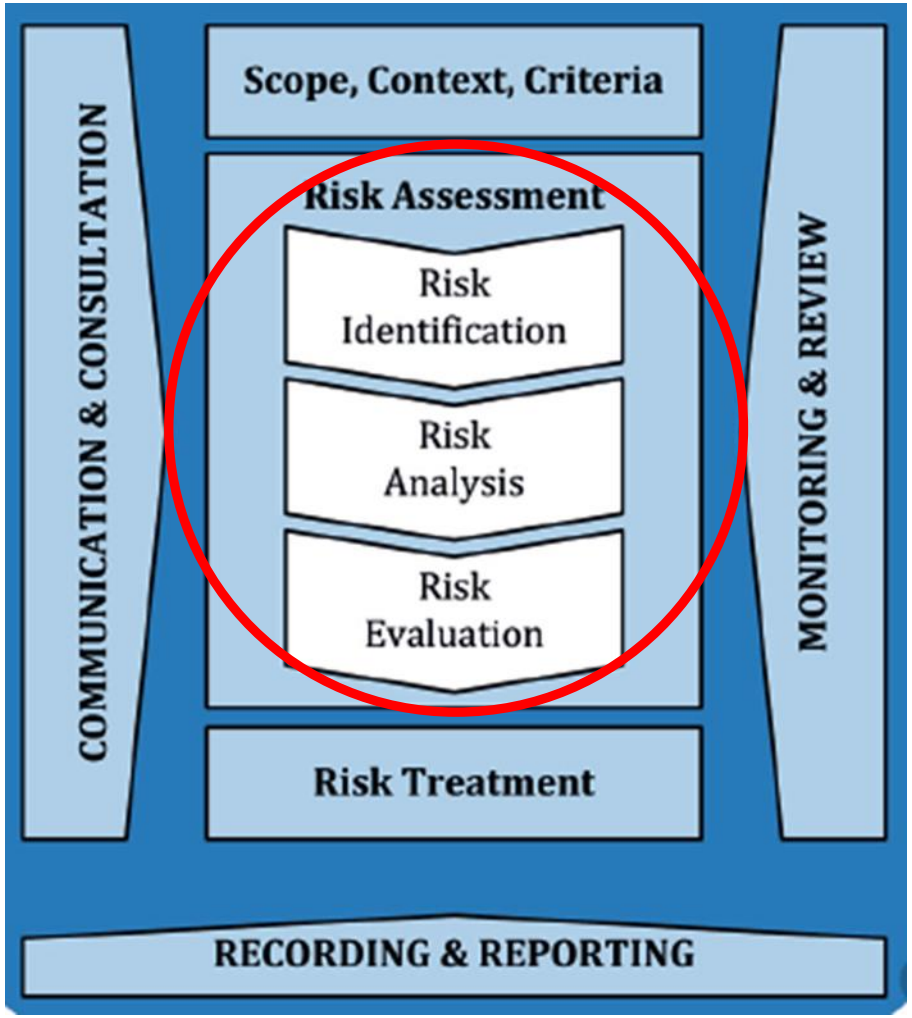
The Risk Management Process



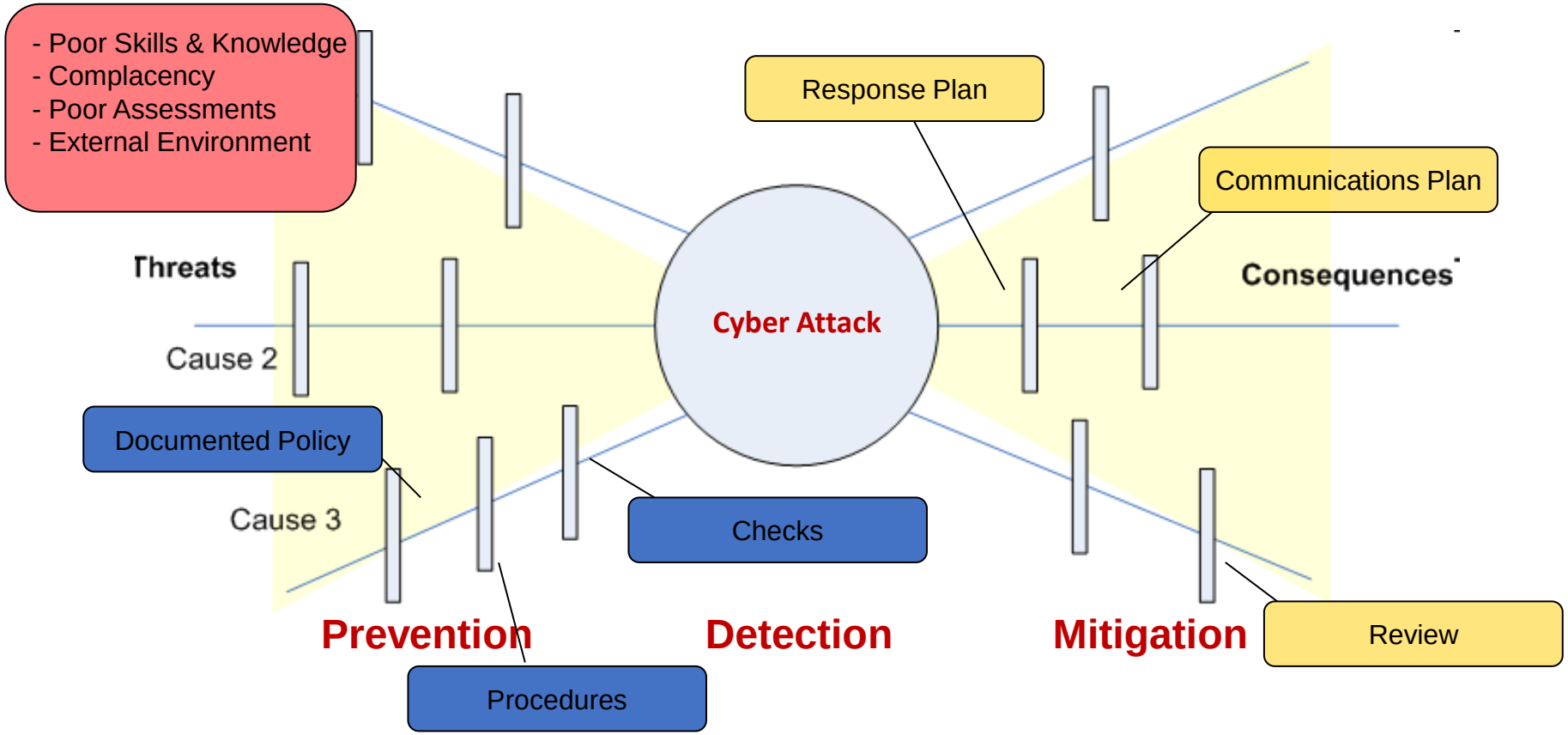
Establishing the Context

- the intended outcomes of the organisation
- the internal and external environment (structure, key third parties, standards and legal & regulatory requirements)
- the Risk Criteria used to evaluate the significance of risks
- the Risk Appetite as defined by the Board of Directors
- the stakeholders
- the scope of the risk assessment (Risk Assessment Framework)
- the Key Risk Indicators (KRIs)

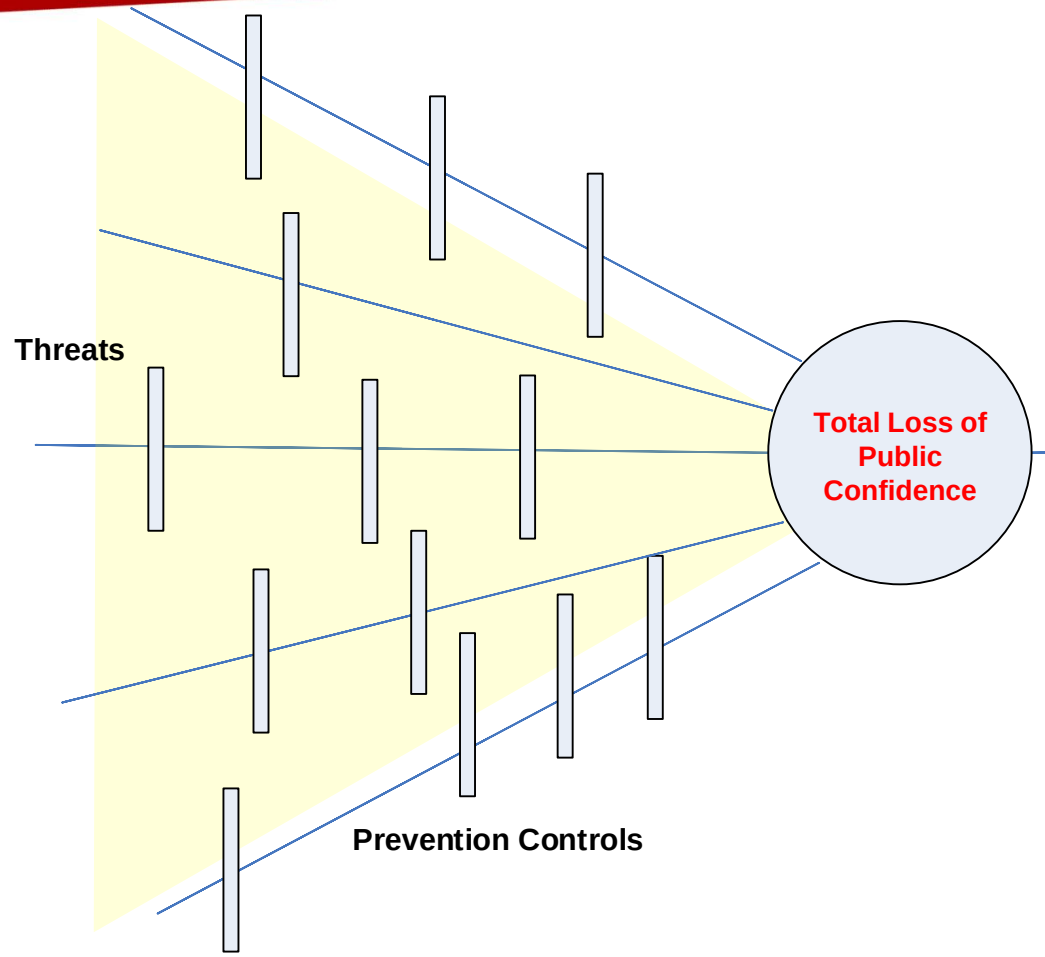
The Risk Management Process



Risk Assessment – Bow-Tie



From Objectives to Risks



Deliver quality service to service users

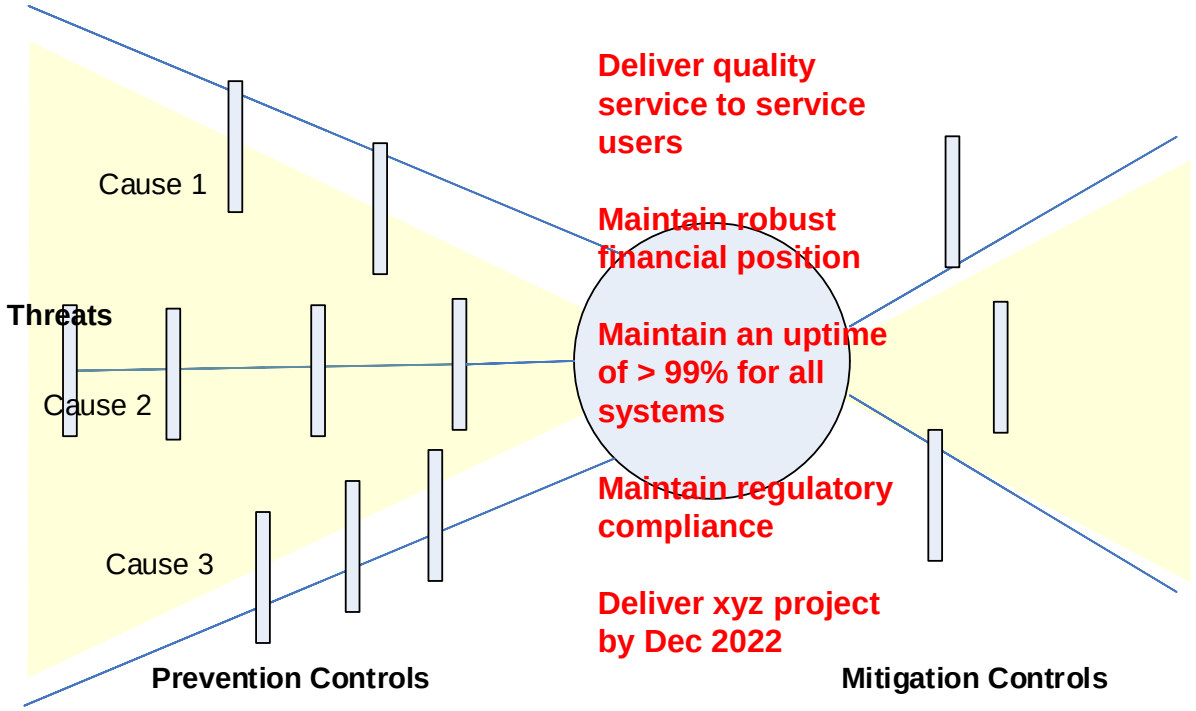
Maintain robust financial position

Maintain an uptime of > 99% for all systems

Maintain regulatory compliance

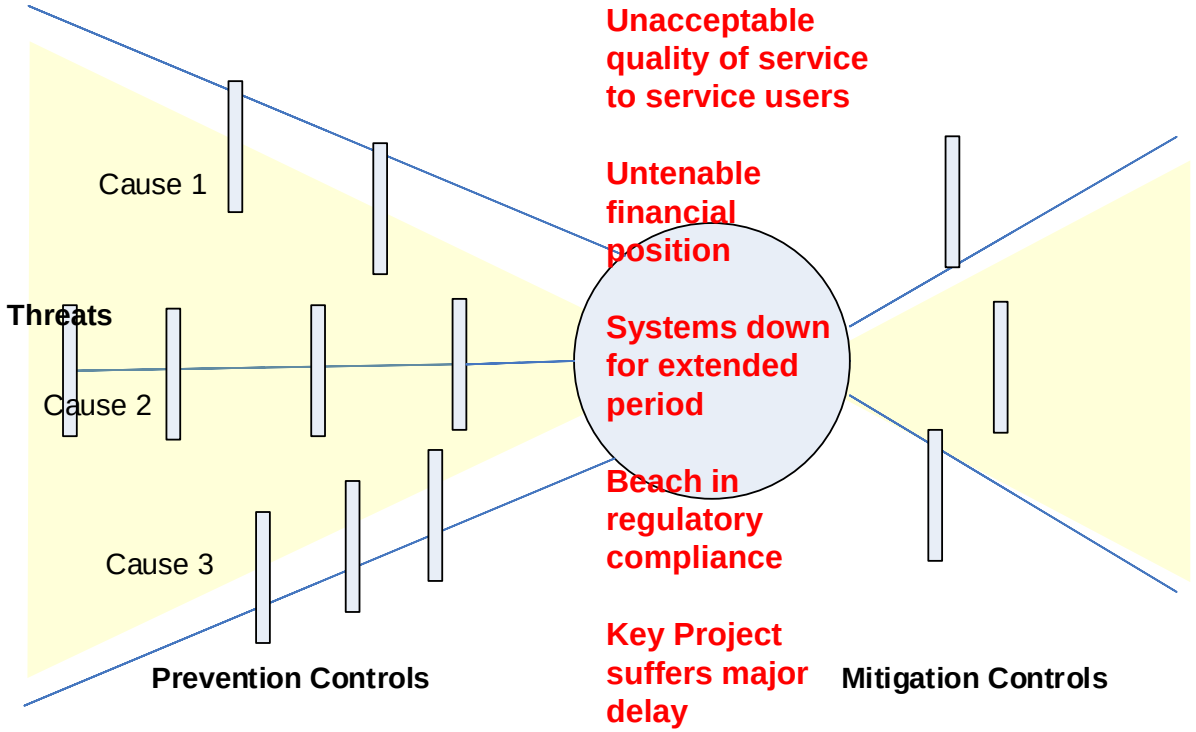
Deliver xyz project by Dec 2022

From Objectives to Risks



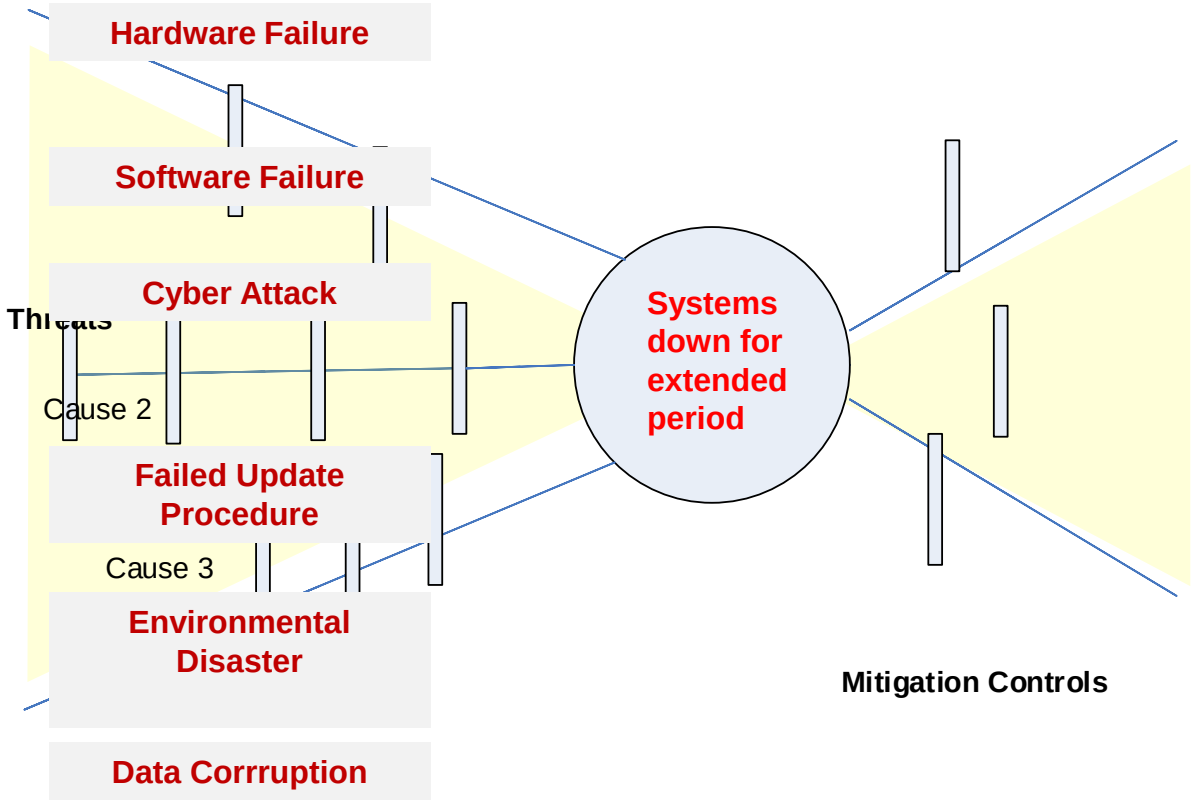
Objectives

From Objectives to Risks

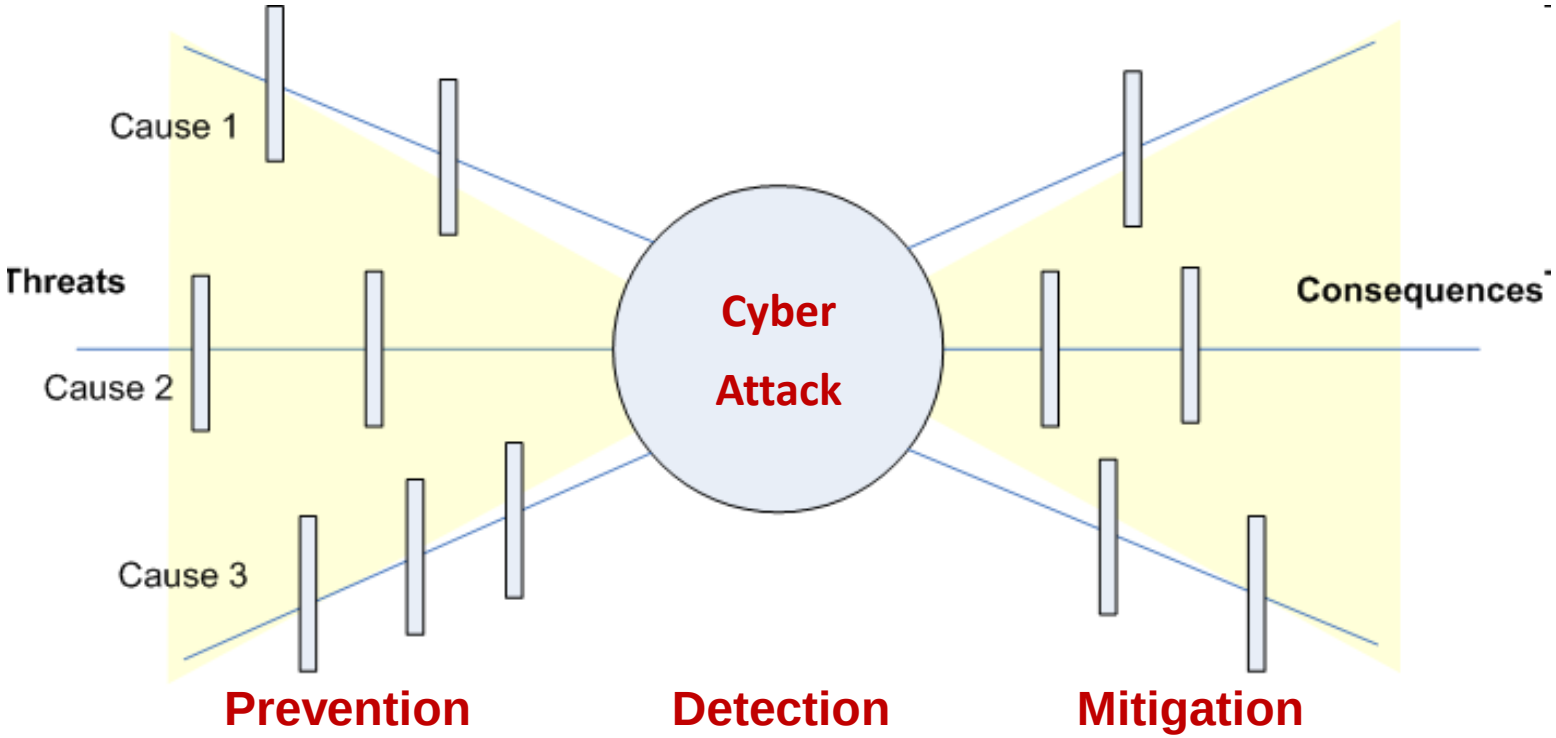


Risks

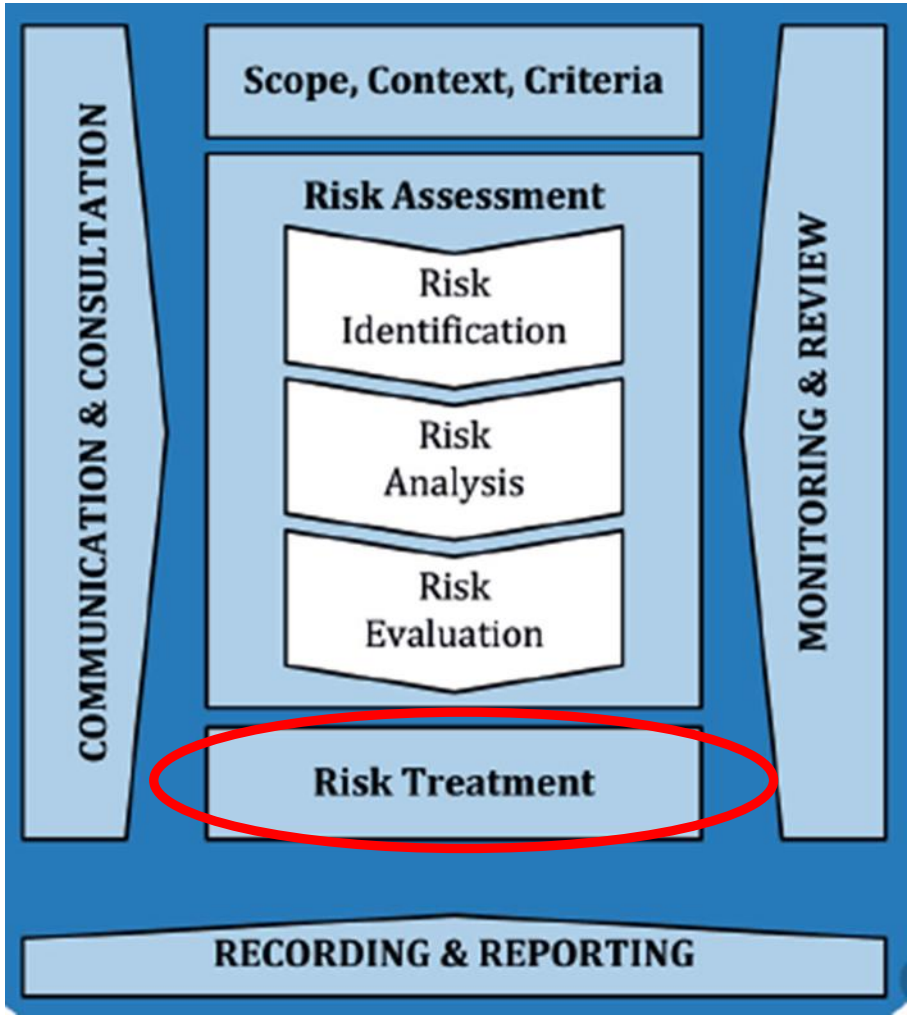
From Objectives to Risks



Risk Assessment – Bow-Tie



Risk Treatment



Brakes Allow a Car to go Fast

Risk Treatment

Risk Control (Minimise Exposure)

- Terminate (Avoid)
- Treat (Reduce)
  - Pre-loss (Prevention)
  - Post-loss (Mitigation)

Risk Financing (Fund Losses)

- Tolerate (Retain)
- Transfer
  - Insurance
  - Contract

Risk Appetite

Amount and type of risk that an organization is prepared to pursue, retain or take. (ISO Guide 73)

- Set by the Board of Directors
- For all who make decisions in the organisation
- For those stakeholders who need assurance

The limits for risk taking

Risk Appetite – The What

- **Reputational risks**: We have adopted a cautious stance for reputational risks, with a preference for safer delivery options, tolerating a cautious degree of residual risk and choosing the option most likely to result in successful delivery, thereby enhancing our reputation for delivering high quality, cost-effective services to the public.
- **Financial risks:** We have adopted a cautious stance for financial risks with reference to core running costs, seeking safe delivery options with little residual risk that only yield some upside opportunities. The Board will receive ongoing assurance through the annual governance statement that policies and procedures are in place in line with guidance

Source: Risk_Appetite Guidance Note Aug 2021

Risk Appetite – The How

CalQRisk
Manage the effect of uncertainty on objectives

We only allow Finance department staff to use the company credit card

Statements

- Start with each risk category or objective
- For each Objective clarify Primacy and Flexibility
- Will Do / Will not do
- State what you will tolerate / not-tolerate

We will cancel any events or activities that we cannot deliver in compliance with our safeguarding obligations

Members of the Board may only serve for x Terms

Any expenditure greater than €5,000 will require Board approval

We will apply full public procurement compliance to all suppliers/third party providers

Limits

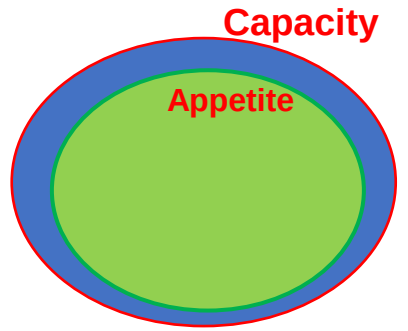
- Disaggregation of overall appetite
- Constraints
- Probably expressed in many policies already

Meeting our legal and regulatory obligations will take priority over other business objectives.

Our core systems will have a minimum uptime of 99.5% during operating hours (7 x 12). (Implies max 25 min downtime in any one week)

If you have zero-tolerance of non-compliance with legal obligations: Say it!

Risk Appetite – The How



Risk Capacity

is the maximum amount of risk which the organisation is technically able to assume before breaching constraints determined by capital, liquidity, borrowing capacity, regulations, reputation and operational environment.

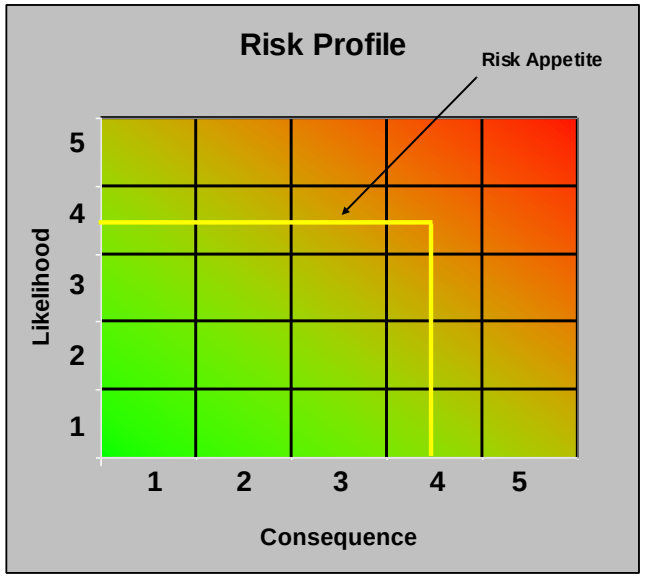
Risk Management Capability

the ability to manage risk exposures within desired risk limits. (Understanding, measurement, skills & knowledge, controls and oversight, culture..)

Risk Criteria

Terms of reference against which the significance of a risk is evaluated. (ISO Guide 73)

- Defined by the Risk Officer
- Approved by the Board of Directors
- Must be consistent with the Risk Appetite



Risk Criteria

CalRisk
Manage the effect of uncertainty on objectives

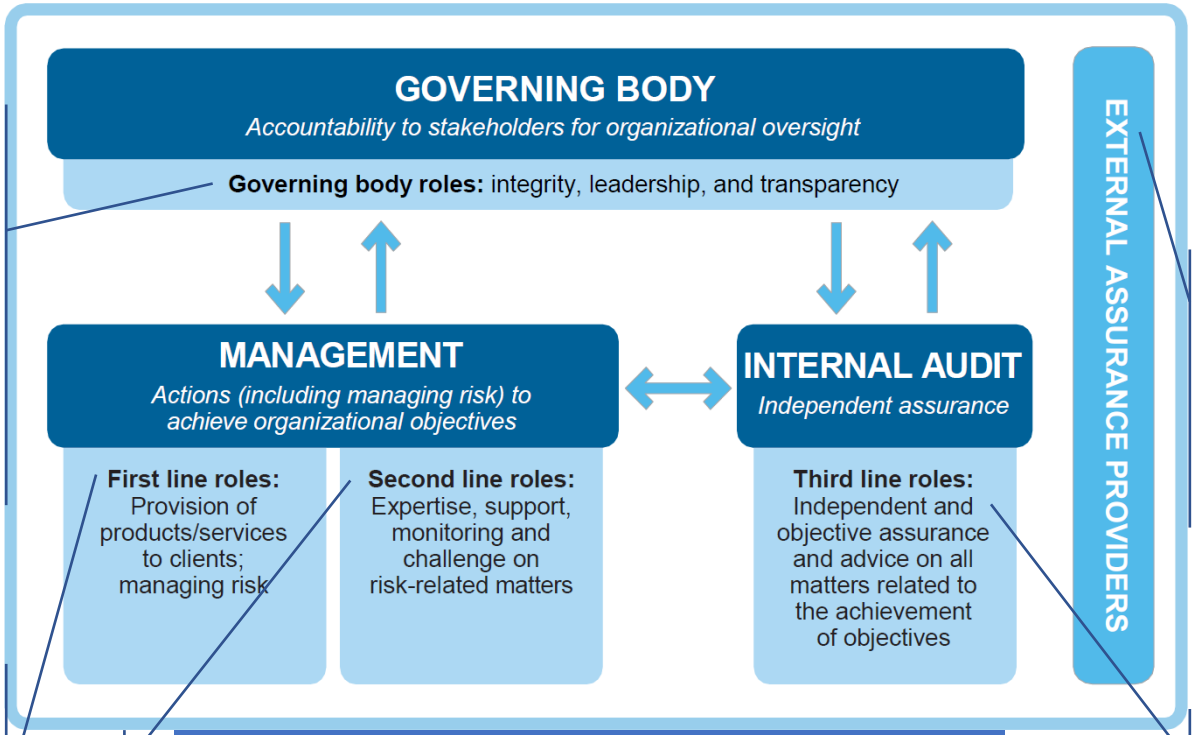
Risk Criteria

CONSEQUENCES					
Criteria	5 Substantial	4 Significant	3 Moderate	2 Minor	1 Negligible
Governance	3 significant Audit Findings and several Directors departing				
Approvals / Compliance	Breach of 3 compliance obligations				
Reputation	Sustained National and Local Multi-Media adverse publicity	Sustained Local Media adverse publicity	Once-off National multi-media adverse publicity	Once-off Local Multi-media adverse publicity	A single complaint
Operations	Unable to provide any service for 1 week				
People	Departure of 6 key managers in one month				
LIKELIHOOD					
	5 Very High	4 High	3 Medium	2 Low	1 Very Low
	Once per quarter or more often	Once in a year	Once in 3 years	Once in 10 years	Once in 30 years, or less frequent

Roles and Responsibilities

CalRisk
Manage the effect of uncertainty on objectives

4 Oversight
Define Objectives
Establish Structures
Provide Resources
Set Risk Appetite
Establishes Internal Audit



5 Expertise
e.g. Pen Testing
Satisfy reg requirements
Independence

1 The Doers
The Risk Owners
Identify and control risks
Implement Processes
Report on plans and outcomes
Ensure compliance

2 CRO, CCO
Expertise
Advise First Line
Challenge (respectfully)
Ensure Consistent Implementation
Monitoring
Reporting Adequacy and Effectiveness

3 Quality Control
Independent
Adequacy and Effectiveness
Advise

Thank You

gjoyce@calqrisk.com

Our Guest Speaker

Aidan Horan, IPA

Risk Management in the Public Sector

Contemporary Topics

Aidan Horan
Governance Team @IPA
ahoran@ipa.ie

Governance – Risk – Assurance

A sound system of internal control provides assurance that an organisation will not be hindered in achieving its objectives or in the orderly and legitimate conduct of its business, by circumstances which may be reasonably foreseen.

IPA
AN FORAS RIARACHÁIN
INSTITUTE OF PUBLIC
ADMINISTRATION

Governance
Forum

2022

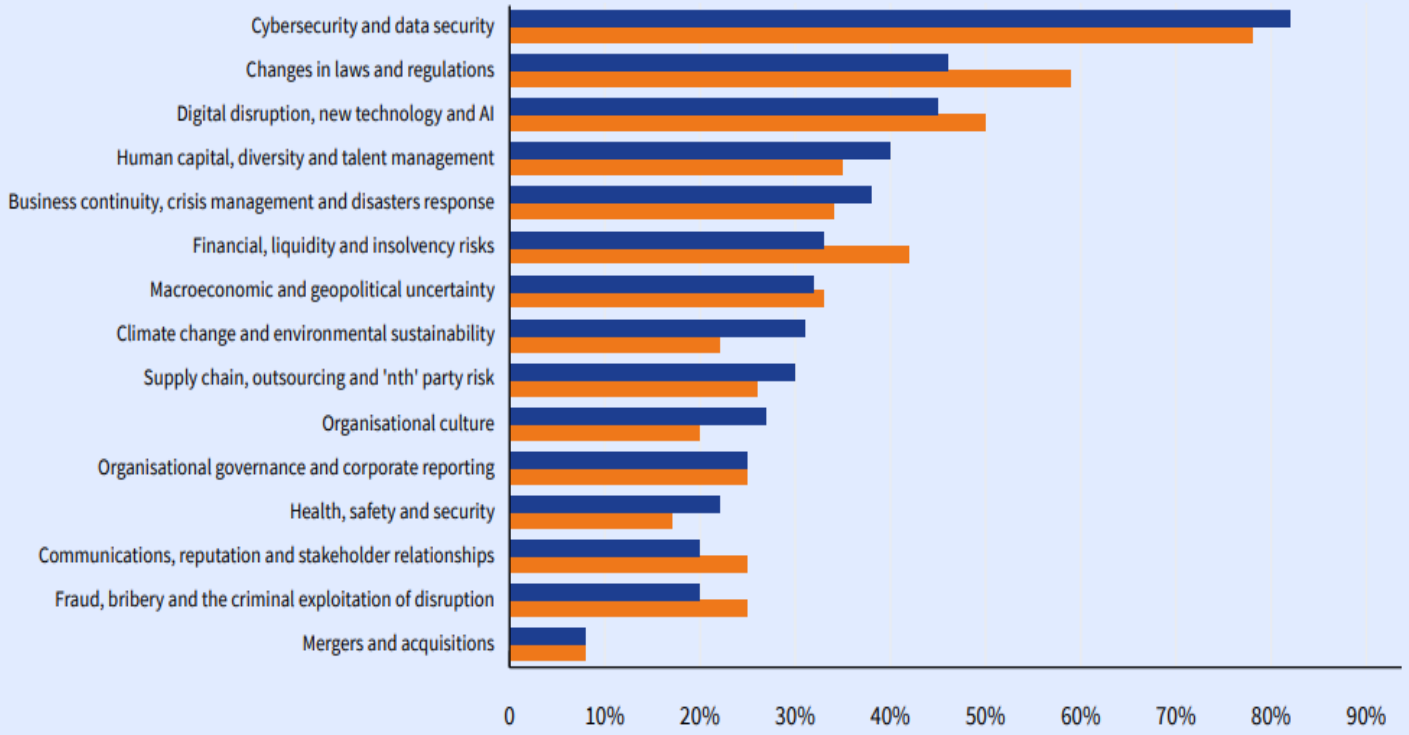
RISK IN FOCUS

Hot topics for internal auditors

Read more

ECIIA

What are the top five risks that your organisation currently faces?



Baseline Cyber Security Standards align with the NIST Framework[2]

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

The NIST 1.1 CSF is a framework of cyber security guidance published by the U.S. National of Institute of Standards and Technology and is available to download from their website.

It is designed as a comprehensive framework for businesses and organisations to identify, assess and address the cyber security risks they face. NIST encourages any organisation or sector to review and consider the Framework as a helpful tool in managing cybersecurity risks.

An Roinn Caiteachais
Phoiblí agus Athchóirithe
Department of Public
Expenditure and Reform

Blended Working Policy Framework for Civil Service Organisations

Prepared by the Department of Public Expenditure and Reform
gov.ie
March 2022

I am delighted to present to you the ***Blended Working Policy Framework*** for the Civil Service.

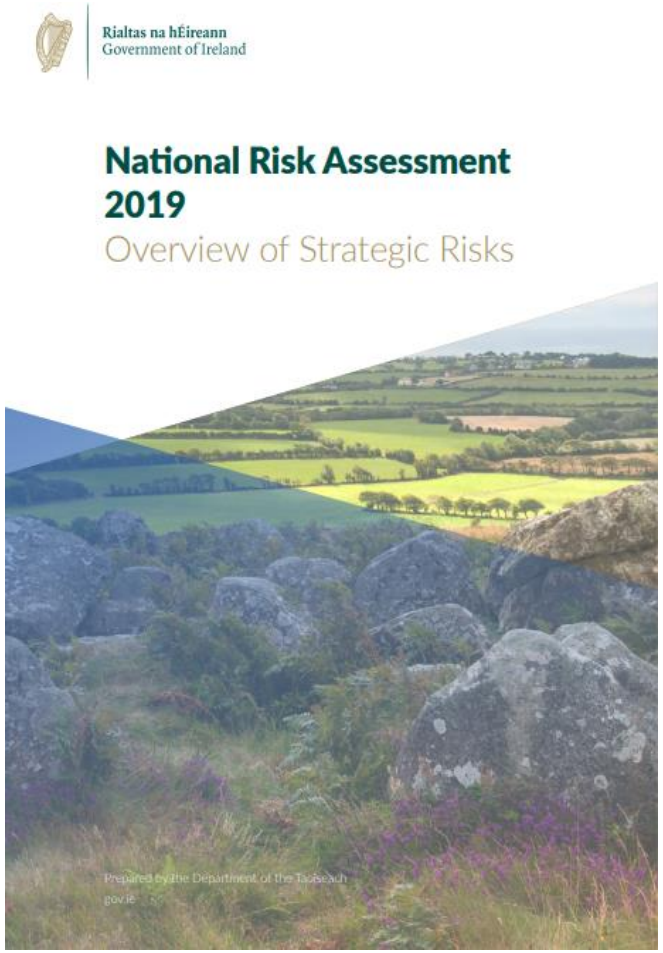
Over the last couple of years, the pandemic brought about a sudden and seismic change in the working arrangements for everyone. Despite the challenges, civil servants adapted swiftly and with great success to this new working environment which required so many to work remotely. In doing so, their efforts have helped to ensure the continuity in the provision of key services to the public.

Many lessons were learned around how remote and blended working applied in practice, often in very difficult circumstances. This Framework harnesses those lessons and provides guidance to Departments and Offices which will bring a level of consistency and transparency while allowing organisations the flexibility to tailor their policy to meet their business needs.

The Government has mandated public sector employers to move to 20% remote working and this Framework supports that commitment by providing for a longer term approach to blended working across the Civil Service. This move to blended working also supports commitments in the National Remote Working Strategy, Our Rural Future, the Climate Action Plan and the National Planning Framework.

I fully support the principles set out in the Framework which aim to address opportunities and risks for both employers and employees:

1. Support the Business Needs of the Organisation
2. Leadership and Management
3. Be an Employer of Choice
4. Transparency and Consistency
5. Health and Safety


Rialtas na hÉireann
Government of Ireland
National Risk Assessment 2019
Overview of Strategic Risks
Prepared by the Department of the Taoiseach
gov.ie


1.2. List of Risks 2019
Strategic Geopolitical Risks
1. Departure of the UK from the EU
2. Instability in Northern Ireland
3. Future direction and stability of the EU
4. Changing distribution of global influence and move away from a rules-based system
5. Terrorist incidents and armed conflicts
6. Economic Impact of Brexit
7. Risk of Overheating
8. Public Expenditure Pressures
9. Global Slowdown, including changes to international trading environment
10. International Tax changes
11. Reliance on multinational corporations and sectoral concentration
Strategic Economic Risks
Strategic Social Risks
12. Capacity of Higher and Further Education System
13. Skilled Labour Shortages
14. An Ageing Population including pensions and health system challenges
15. Impact of Social Media on Public Debate
16. Social cohesion including perceptions of Regional and Rural imbalances
17. Migration and Integration
18. Climate Change & Biodiversity
19. Ensuring an affordable, sustainable and diverse energy supply
20. Delivery of Public Infrastructure
21. Food safety
22. Supply and Affordability of Housing
Strategic Environmental Risks
Strategic Technological Risks
23. Cyber security
24. Disruptive technology trends
25. Anti-Microbial Resistance
26. Major Pandemics
27. Nuclear contamination

Rialtas na hÉireann
Government of Ireland

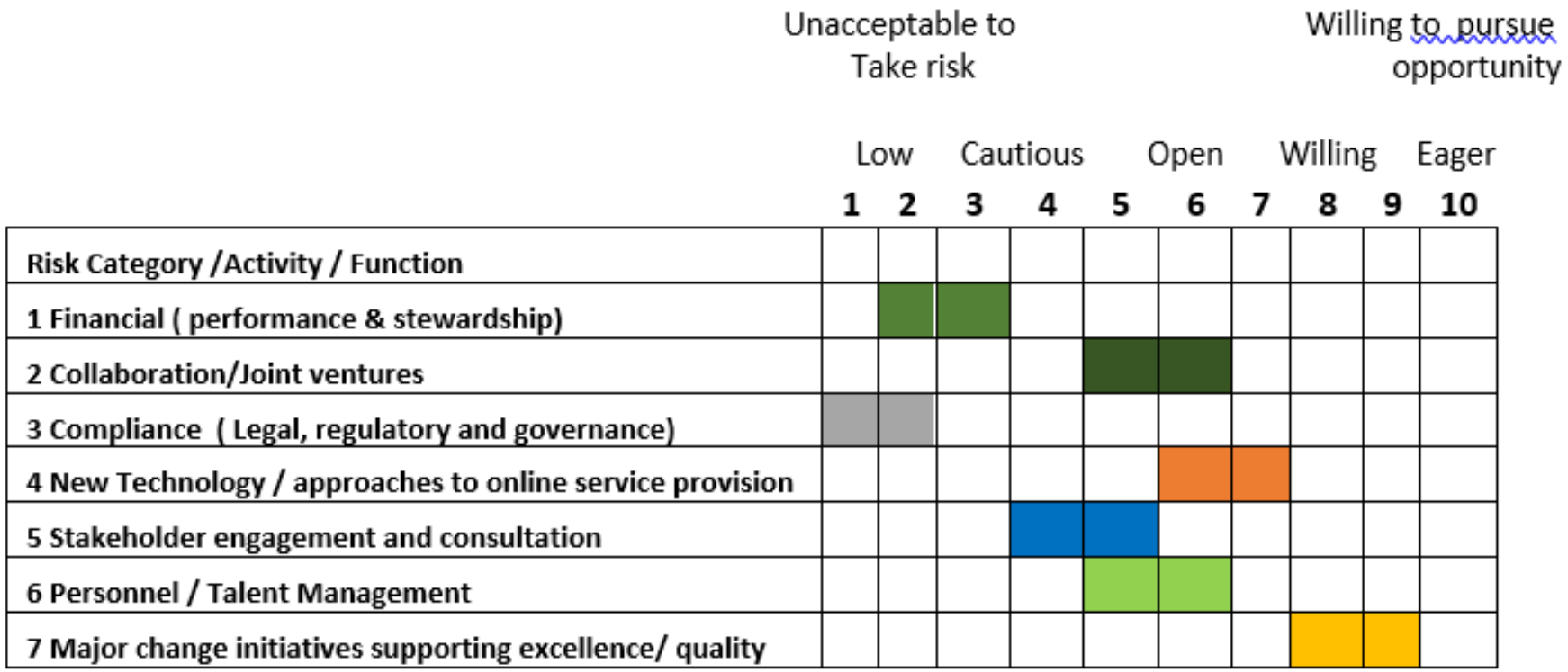
National Risk Assessment 2021/2022

Overview of Strategic Risks

Table 1: Strategic risks – 2021/2022

Geopolitical Risks	Rise of a multipolar world Future direction of the European Union Ireland's relationship, post-Brexit, with the United Kingdom Armed conflict, terrorism and hybrid threats
Economic Risks	Economic scarring Public finances and the financial system Labour shortages, supply chain and capacity constraints Inflation Vulnerabilities arising from Ireland's enterprise mix Changes to international trading relationships Disruption to a secure and sustainable energy supply
Social Risks	Social cohesion Housing and sustainable development Migration and integration Demographic change Digital exclusion
Environmental Risks	Climate change Biodiversity loss Extreme weather events and other natural disasters Pandemics Antimicrobial resistance
Technological Risks	Food safety Data flows, storage and security Disruptive technology Cybersecurity Nuclear contamination

Illustration / Example



Risk Management in the Public Sector

Contemporary Topics

Thank you

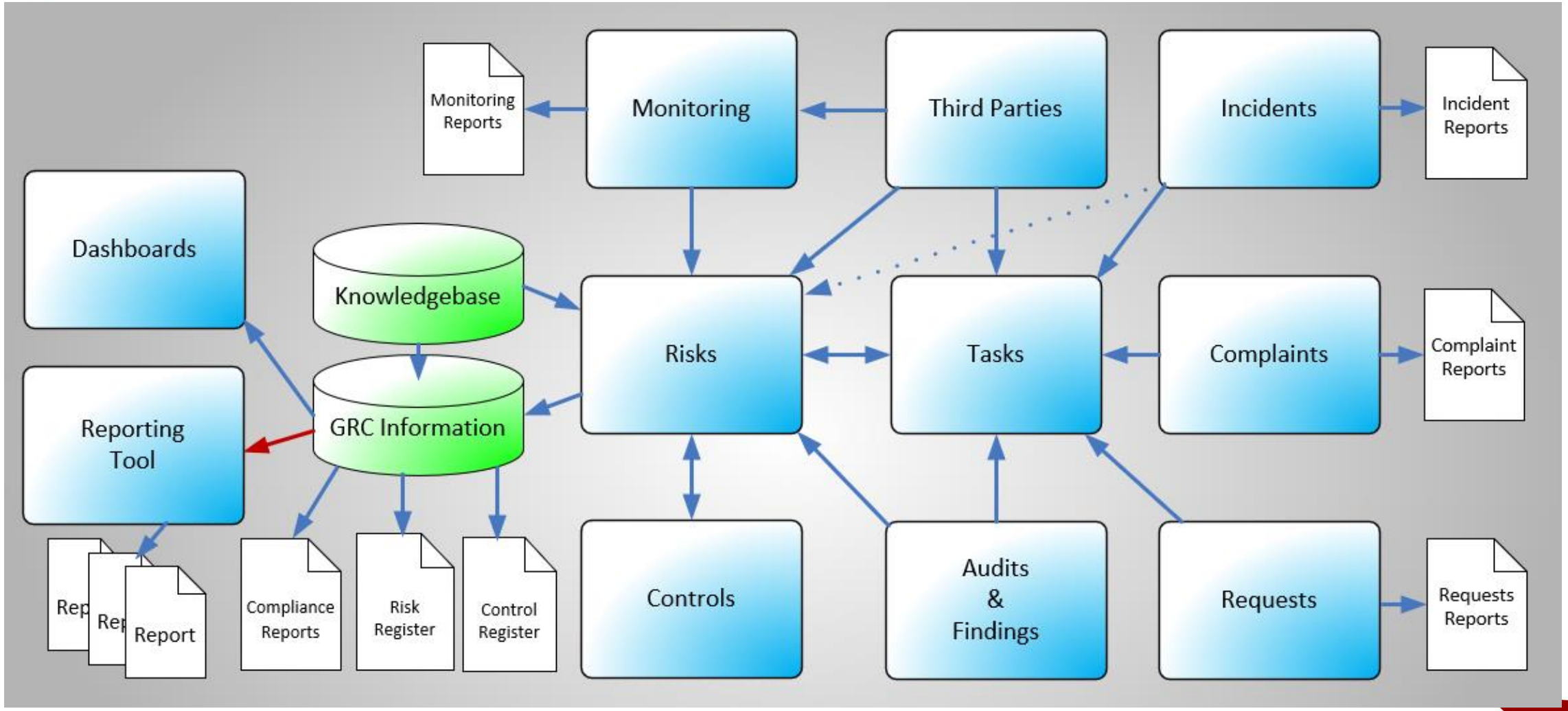
Aidan Horan

Governance Team @IPA

ahoran@ipa.ie

Questions & Answers

CalQRisk Platform



NIST Compliance Report

CalRisk
Manage the effect of uncertainty on objectives

Cyber Security Framework - NIST															
IDENTIFY	Total	Score													
Asset Management	15	13/15	ID.AM-1 3/3	ID.AM-2 3/4	ID.AM-3 3/3	ID.AM-4 1/2	ID.AM-5 1/1	ID.AM-6 5/5							
Business Environment	14	10/14	ID.BE-1 1/2	ID.BE-2 0/1	ID.BE-3 2/2	ID.BE-4 3/4	ID.BE-5 4/5								
Governance	15	8/15	ID.GV-1 1/2	ID.GV-2 2/4	ID.GV-3 4/5	ID.GV-4 1/4									
Risk Assessment	14	6/14	ID.RA-1 0/2	ID.RA-2 1/1	ID.RA-3 2/8	ID.RA-4 3/9	ID.RA-5 0/1	ID.RA-6 1/1							
Risk Management Strategy	18	1/18	ID.RM-1 0/17	ID.RM-2 1/7	ID.RM-3 0/6										
Supply Chain Risk Management	7	7/7	ID.SC-1 4/4	ID.SC-2 0/0	ID.SC-3 3/3	ID.SC-4 0/0	ID.SC-5 3/3								
PROTECT															
Access Control	35	14/35	PR.AC-1 2/7	PR.AC-2 0/12	PR.AC-3 5/5	PR.AC-4 6/8	PR.AC-5 2/2	PR.AC-6 1/3	PR.AC-7 2/5						
Awareness and Training	7	3/7	PR.AT-1 1/3	PR.AT-2 2/4	PR.AT-3 2/6	PR.AT-4 1/3	PR.AT-5 2/4								
Data Security	39	23/39	PR.DS-1 2/2	PR.DS-2 6/7	PR.DS-3 5/7	PR.DS-4 3/3	PR.DS-5 15/27	PR.DS-6 2/4	PR.DS-7 1/2	PR.DS-8 0/1					
Information Protection P & P	55	15/55	PR.IP-1 5/28	PR.IP-2 1/3	PR.IP-3 1/8	PR.IP-4 2/4	PR.IP-5 0/4	PR.IP-6 4/5	PR.IP-7 0/8	PR.IP-8 1/1	PR.IP-9 5/7	PR.IP-10 2/2	PR.IP-11 0/15	PR.IP-12 2/5	
Maintenance	5	1/5	PR.MA-1 0/4	PR.MA-2 1/2											
Protective Technology	19	16/19	PR.PT-1 5/5	PR.PT-2 6/7	PR.PT-3 1/1	PR.PT-4 2/3	PR.PT-5 2/3								
DETECT															
Anomalies and Events	9	9/9	DE.AE-1 4/4	DE.AE-2 4/4	DE.AE-3 3/3	DE.AE-4 1/1	DE.AE-5 1/1								
Security Continuous Monitoring	12	6/12	DE.CM-1 1/4	DE.CM-2 0/3	DE.CM-3 3/3	DE.CM-4 1/1	DE.CM-5 0/2	DE.CM-6 0/1	DE.CM-7 2/3	DE.CM-8 1/1					
Detection Processes	11	7/11	DE.DP-1 2/4	DE.DP-2 2/3	DE.DP-3 0/1	DE.DP-4 2/2	DE.DP-5 1/1								
RESPOND															
Response Planning	1	1/1	RS.RP-1 1/1												
Communications	14	7/14	RS.CO-1 3/5	RS.CO-2 2/2	RS.CO-3 2/7	RS.CO-4 0/0	RS.CO-5 1/1								
Analysis	9	9/9	RS.AN-1 5/5	RS.AN-2 2/2	RS.AN-3 1/1	RS.AN-4 1/1	RS.AN-5 1/1								
Mitigation	2	2/2	RS.MI-1 2/2	RS.MI-2 1/1	RS.MI-3 0/0										
Improvements	2	1/2	RS.IM-1 1/2	RS.IM-2 1/1											
RECOVER															
Recovery Planning	3	2/3	RC.RP-1 2/3												
Improvements	3	1/3	RC.IM-1 1/3	RC.IM-2 1/2											
Communications	10	1/10	RC.CO-1 1/7	RC.CO-2 0/2	RC.CO-3 0/1										