Reporting to the Board / Audit & Risk Committee for Multi Academy Trusts

A CalQRisk Webinar

CalQRisk

Manage the effect of uncertainty on objectives

Presented By

Gerard Joyce, CTO, CalQRisk

11th Oct 2022

Outline

- Introduction – Who we are
- Board Vs Audit & Risk Committee: Who should get what?
- Risk Registers: How many risks? How much detail?
- Trends: What should you include?
- Reporting Frequency and Detail to include
  - Monthly
  - Quarterly
  - Annually
- Takeaways

The majority of meetings should be discussions that lead to decisions.

Patrick Lencioni

Introduction

CalQRisk
Manage the effect of uncertainty on objectives

- Experienced Risk & Compliance Professionals
- Members of IRM, IoB, CI (ACOI), IoD, ACCA, ISACA
- Involved in the Development of Standards
- We supply a Governance, Risk & Compliance Software Solution called CalQRisk
- CalQRisk is used by 200+ regulated organisations
  - Financial Services, Educational Sector and Not-for-Profit sectors

Board Vs Audit & Risk Committee

CalRisk
Manage the effect of uncertainty on objectives

Board

- Responsible for Oversight, need assurance risk is being managed
- Need assurance that the organisation is compliant
- Need to know what is threatening the achievement of objectives

Audit & Risk Committee

- 2nd and 3rd Lines (of Defence) reporting in
  - Need to deliver “internal scrutiny”
  - Need to assess the adequacy and effectiveness of risk management
  - Need to ensure consistent implementation

Risk Register

Cal Risk
Manage the effect of uncertainty on objectives

RISK REGISTER

MAT Central 11/10/2022

				Pre-Control				Post-Control			
Risk Nr	Category	Risk Description	Risk Owner	L	C	R	Controls	L	C	R	Additional Mitigation Options
45486	Economic-Processes	Failure to prevent fraudulent activity in the procurement process	Tom Healy	5	5	25	- All purchases over a pre-defined amount require a formal purchase order. '- There is a formal procurement process in place that is monitored. '- There is a robust supplier validation and approval process in place. '- Some fraud detection procedures are applied randomly and at short notice to the procurement process.	3.3	4.5	15.1	'- There should be segregation of duties between those who enter purchase orders on the system and those who approve payment. '- Consider putting a procedure in place that ensures that goods or services received always match the purchase order.
77873	Governance-Academy	Failure to manage an effective governance framework	Chris Hanlon	4	4	16	'- The board of trustees has formally appointed, a named individual (the principal / chief executive / executive principal) as senior executive leader. '- There is a finance committee to which the Board delegates financial scrutiny and oversight, and which can support the board in maintaining the Trust as a going concern.	3.4	3.6	12.4	- Trustees should focus on ensuring clarity of vision, ethos and strategic direction. '- Trustees should focus on holding executive leaders to account for the educational performance of the organisation and its pupils, and the performance management of staff. '- Trustees should focus on overseeing and ensuring effective financial performance.
45485	People-Recruitment of School Staff	Failure to appropriately manage recruitment and vetting	Vicki Davies	4	5	20	- There is a policy in place for the safe recruitment and effective vetting of all staff. '- All relevant pre-employment checks are conducted on all shortlisted candidates. '- No person is employed before they have had an appropriate CRB check carried out. '- The school always receives written confirmation that all relevant vetting checks have been completed on agency staff. '- The school keeps and maintains a single central record of recruitment and vetting checks on all staff including volunteers.	2.7	4.1	11.4	'- The school must require personal / character references from all shortlisted candidates. '- Before a candidate is employed, their employment history should be scrutinised for consistency. '- There must be a risk assessment conducted before volunteers, for whom no DBS and Barred List is done, are recruited. '- The Head Teacher must produce a brief written assessment of each interviewed candidate. '- The designated Safeguarding Lead should be involved in the recruitment and vetting process

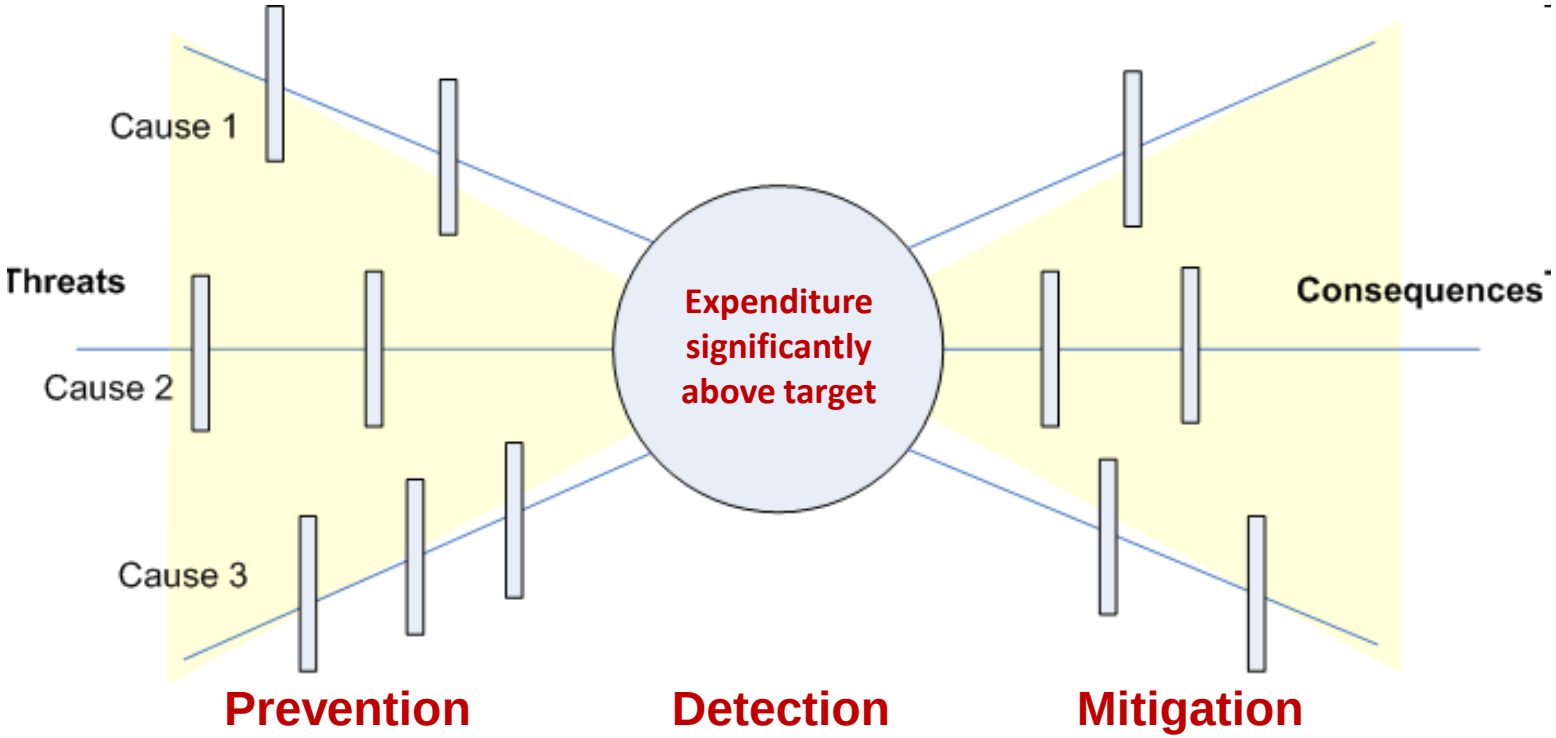
High Level Risks

15/07/2022

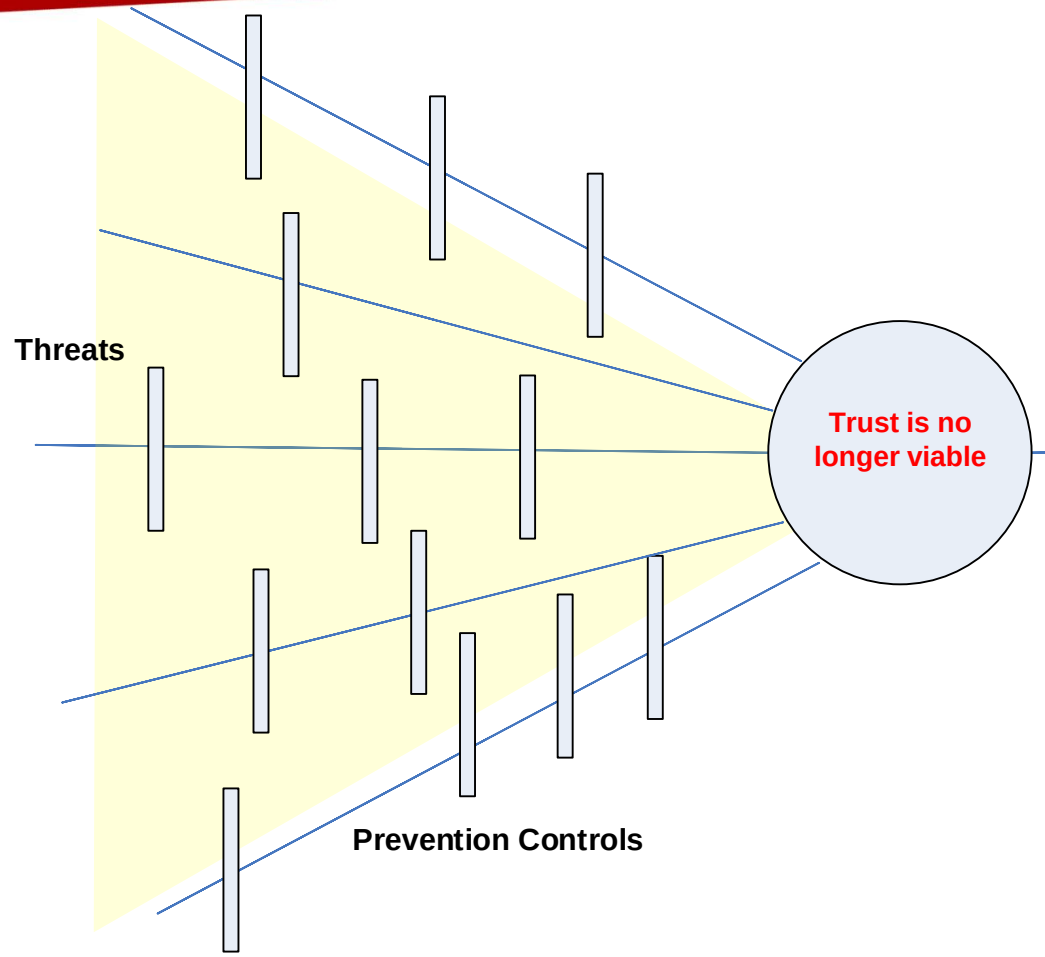
IQRisk
effect of uncertainty on objectives

Sources	Lower Level risks	High Level Risk	Consequences	Owner
Mis-configuration, External hacker, Internal deliberate action	- Failure to have an appropriate Information Security policy () - 7.15 - Failure to appropriately manage information security () - 6.21 - Failure to appropriately manage information assets () - 6.91 - Failure to prevent unauthorised access to systems and information (Ennis HQ) - 8.59 - Poor Configuration Management () - 10.54	Confidentiality breach from IT failures RLoR: 9 Trend: Same	- Reputation damage, - Regulatory Sanction	Gerard Joyce
Controls:		**Associated Tasks:**		
- Information Security policy and procedures in place. - Access control policy in place - Patching programme ensures systems kept up-to-date.		21239 - Document procedure for configuring systems. - Gerard Joyce Due: 8/12/2021		
Comment: This is well managed and continuously monitored. No incidents in the past quarter.				
Poor project management can lead to cost overruns, poor cash planning, non-compliance can lead to heavy fines.	- Failure to deliver project on budget (Acme Development) - 10.22 - Deficient contractual arrangements and SLAs with OSPs, irrespective of criticality () - 14.64 - Non-compliance with NHF Code of Governance Principle 1: Mission and Values () - 6.26	Ineffective Treasury Management RLoR: 8 Trend: Same	Cash flow problems, Delayed payments, reputation damage	Chris Hanlon
Controls:		**Associated Tasks:**		
- Weekly Cash Flow update - Creditors and Debtors reporting weekly - Annual budgeting		26138 - Prepare outline budget for 2023 - Richard Joyce Due: 9/1/2022		
Comment: This is under control and closely monitored,				
Lack of knowledge in operation of equipment, poor practices, poor incident handling.	- Failure to manage the occupational health and safety of the enterprise stakeholders appropriately () - 18.31 - Injury of an employee due to an incident / accident at work () - 17.64 - Failure to manage the use of hazardous substances () - 6.26 - Injury from use of portable equipment () - 9.36	Poor Health and Safety programme RLoR: 8 Trend: Same	Death or Injury to employees or customers. claims, reputation damage	Harry Mooney
Controls:		**Associated Tasks:**		
- Robust H &S procedures in place. - All employees are well-trained in the use of equipment - 10% of employees have First Aid training		26139 - Conduct a full H&S audit of the new development. - Paul O'Brien Due: 8/19/2022		
Comment: Still some areas that need improvement, have plan to address gaps.				

Risk Assessment – Bow-Tie



From Objectives to Risks



Ensure safety of all in school community

Deliver school curriculum to the highest standard

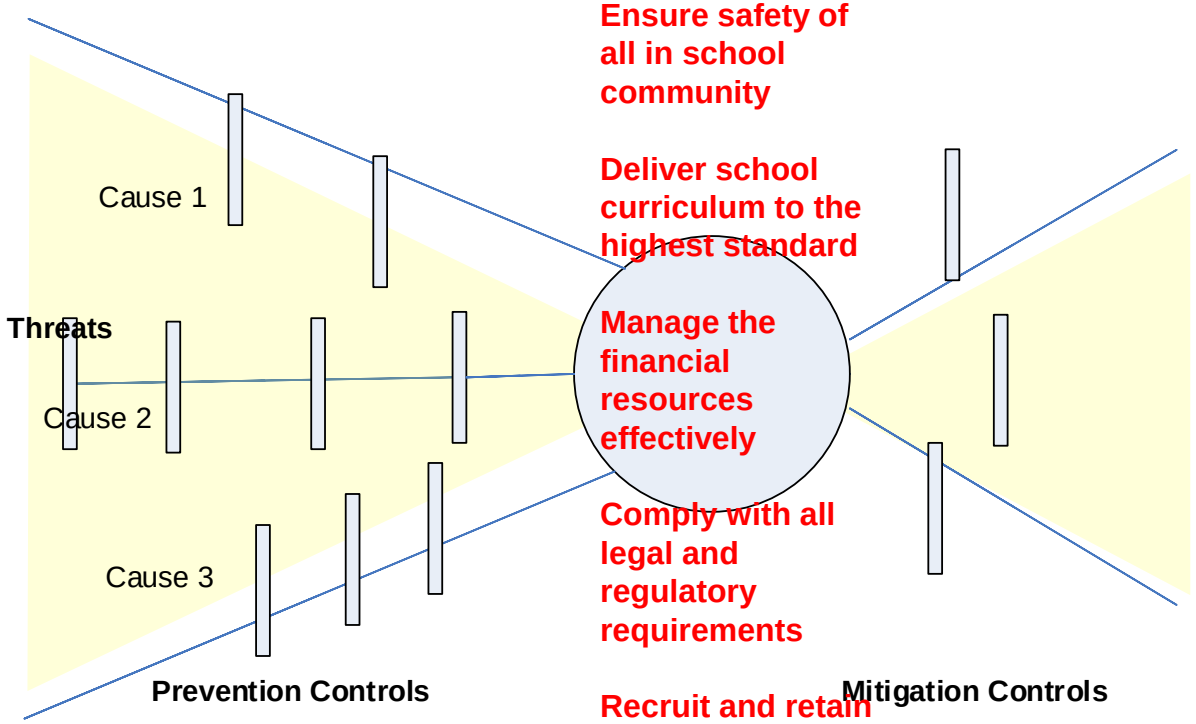
Manage the financial resources effectively

Comply with all legal and regulatory requirements

Recruit and retain the best staff

Maintain a < 8% vacancy level

From Objectives to Risks



Ensure safety of all in school community

Deliver school curriculum to the highest standard

Manage the financial resources effectively

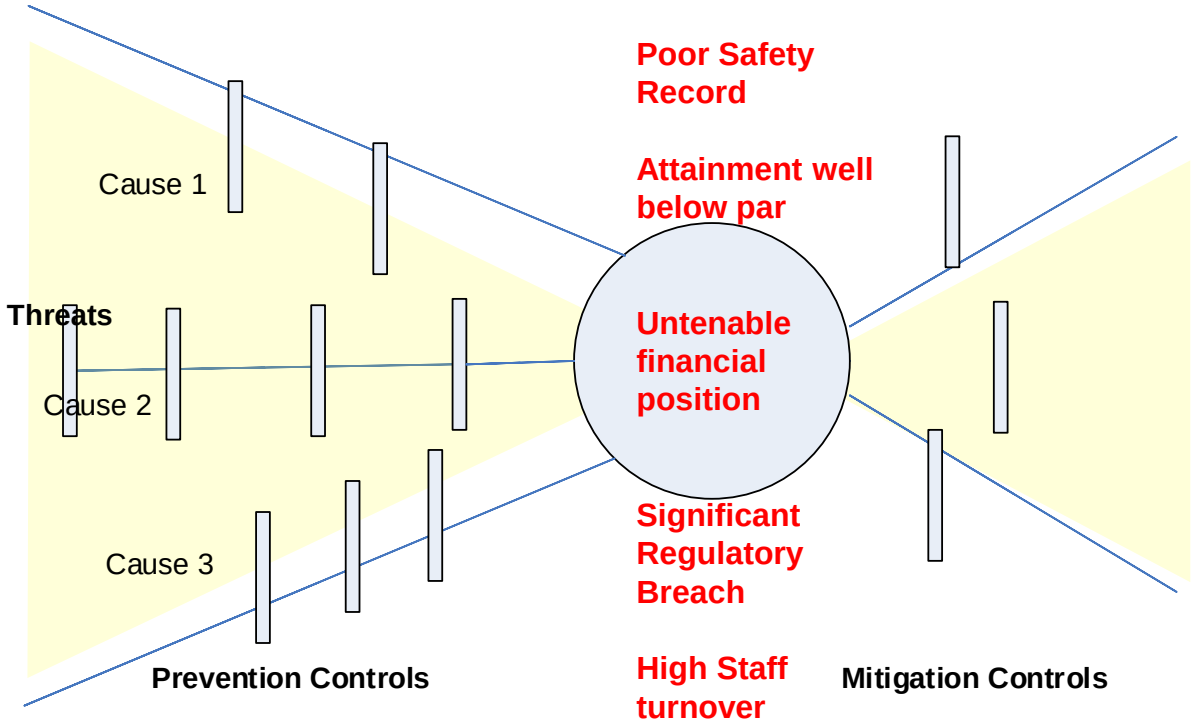
Comply with all legal and regulatory requirements

Recruit and retain the best staff

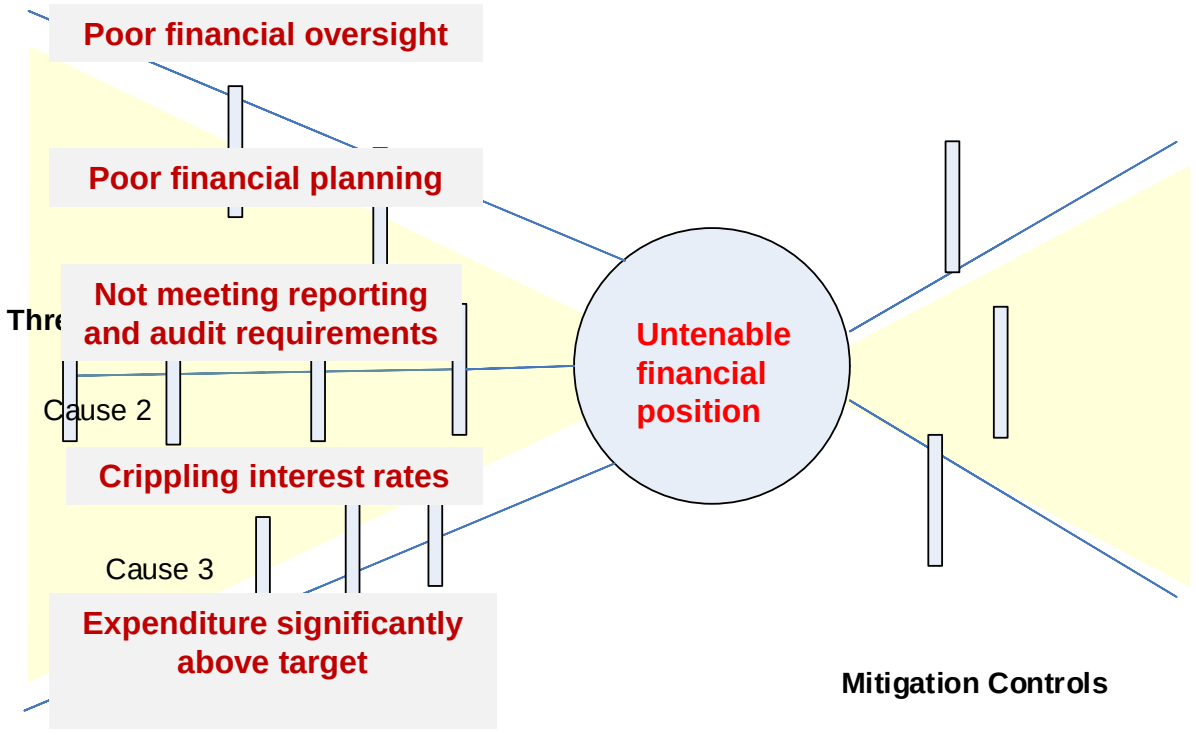
Maintain a < 8% vacancy level

Objectives

From Objectives to Risks



From Objectives to Risks



Trends

- Evidence of Good Governance at all levels in the organisation required
- ESG (Environmental, Social and corporate Governance) “Non-financial” factors
- **Environmenta**l: Climate change, Energy efficiency, pollution, waste management
- **Social**: Community relations, Diversity & inclusion, Human rights, Labour standards
- **Governance**: Board composition, Bribery and corruption, Compliance, Succession,..
- **Risk Appetite:** “The board is responsible for determining the nature and extent of the principal risks it is willing to take in achieving its strategic objectives.” UK Corporate Governance Code
- **Emerging Risks**: Trying to anticipate what’s coming, regulatory changes, market, skill shortages, recruitment,..

What I want to know as a Trustee

- What is our risk bearing **capacity**
- What **structures** and processes are in place
- Is **responsibility** assigned?
- Has **training** been carried out?
- How **effective** are controls / Have we had any ‘incidents’?
- Have there been any material **audit findings**?
- Are there any risks outside of our **risk appetite**? / KRIs?
  - What are we doing to **mitigate** these (and other) risks
- Are we **compliant** with all regulations / obligations
  - Are there any new regulations coming down the line?
- Is there anything the management team need from the Board to enable better management of risk?

What I want the Trustees to know

What I, as the Risk Management Officer, want the Trustees to know

- The top 10 risks that keep me awake at night
  - We are continuously monitoring these and seeking ways to mitigate further
- What we have done since the last board meeting to mitigate risks
- Where we have improved since the last board meeting
- The impact that their decisions are having / have had
  - Policy changes required
  - Control changes
  - New risks emerging
  - Stretching our resources
  - Risk appetite is too limiting
- The ‘loss events’ that we have experienced; these reflect the environment

What the R & A committee want

- Evidence that all relevant risks have been appropriately addressed through internal scrutiny
- Evidence that there are effective controls (financial and non-financial) in place
- Evidence that Risk Owners have the skills and knowledge to manage the risks under their responsibility
- Evidence that Risks are being managed within the organisation's risk appetite
- Details of plans to address known gaps / findings
- Details of plans to monitor any risks that are of concern

Compliance with the ATH

- Full gap analysis every September
- Findings sent to audit and risk committee / Board
- Action plan to address any gaps agreed, if necessary
- Compliance monitoring throughout the year e.g. thresholds, etc
- Summary report sent to audit and risk committee for every meeting

Frequency

- Monthly
- Quarterly
- Annually

Reporting - Monthly

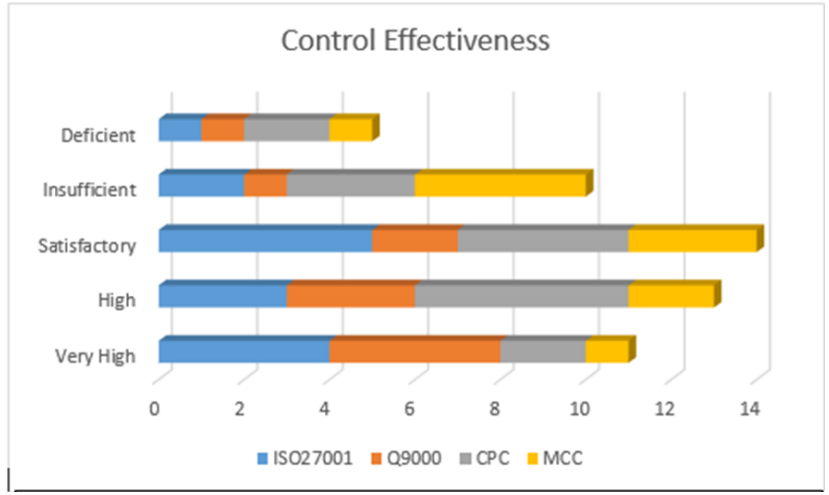
- You have max 15 mins to communicate your message(s)
- Use lots of graphics instead of lots of words
- If there's a theme to the board meeting, reflect that in your report
  - E.g Cybersecurity
- Are there regulatory requirements that need to be addressed?
- Are you responding to a previous request to investigate / risk assess
- Have you concerns, based on the trends you are seeing?
- Are you looking for approval for some action/initiative?

Reporting - Monthly

CalQRisk
Manage the effect of uncertainty on objectives

Include:

- Significant Risks
- Change / Trend since last report
- Any new risks / emerging risks
- Effectiveness of Controls
- Update on Tasks from previous reports
- Risk Events / Incidents that have occurred
- Deviations from risk appetite
- Key Risk Indicators (KRIs)



Description	Previous Level (19/05/22)	Level (12/07/22)	Trend
Rising unemployment and financial stress amongst members	24.68	24.68	→
Failure to consider the potential impact of Brexit on the Credit Union	0	24.65	●
Failure to manage the prevention of money laundering through the credit union operationally	24.08	24.08	→
Failure to establish member financial circumstances completely	24.05	24.05	→
Inappropriate loan terms	23.99	23.99	→
Failure to respond appropriately to a data breach	23.89	23.89	→
Failure to build and maintain appropriate reserves	23.75	23.75	→
Ineffective pandemic response	23.32	23.32	→
Inappropriate disclosure of confidential information	23.04	23.04	→
Failure to comply with Fitness and Probity standards	0	23.04	●

Key Risk Indicators

Exposure Indicators

Changes in the nature of the macro environment

- Interest rates, unemployment rate, debt financing, energy costs

Stress Indicators

Significant rise in the use of resources (people / material)

- Sick days, accidents, system downtime, complaints.
- Stress indicators at Third-Parties / Sub-contractors / Supply Chain

Causal Indicators

Drivers of some key risks to the business

- Number of open positions, training completed, equipment age, skills lost

Failure Indicators

Poor attainment and failing controls

- Attainment levels, incidents, audit findings, data breaches, policy breaches, fraud

360 Risk Report

Risk ID: 48459 **Context: Broker Demo**

Risk Owner	Portfolio Owner
Fiona Kiely	Gerry Joyce

Risk Category

Data Protection > DP Governance >

Risk Description

Deficiency in arrangements for upholding the data minimisation principle - Customer Data

Source

Lack of understanding of the requirement

Consequences

Breach of GDPR regulations

Status	Evaluation Decision
Evaluated	Treat

Evaluation Comment

There is good understanding of the GDPR requirements throughout the organisation. However there are still some gaps in individual procedures. We are working our way through these to bring them in line.

Current Level of Risk

15/12/2021	Likelihood	Consequence	Level
Pre-Controls	4	4	16
Post-Controls	3.0	3.2	9.5

Previous Post Control Ratings

12/03/2021	3.0	3.2	9.5
12/01/2018	2.7	2.4	6.5

Objective Impacted

Maintain compliance with all applicable regulations

Incidents

Incident Gen Id	Occurred	Description
2214	05/05/2021	A new marketing campaign was started before it was discovered that too much personal information was been requested.

Monitoring In last 100 Days

KRI	Resp Person	Answer Date	Question	Answer	Comment
Information	Gerry Joyce	15/12/2021	Were all new marketing initiatives reviewed to ensure only the minimum personal data is collected?	Yes	There were 3. All good.
Information	Gerry Joyce	15/12/2021	Were all new marketing initiatives reviewed to ensure only the minimum personal data is collected?	No	We missed one.

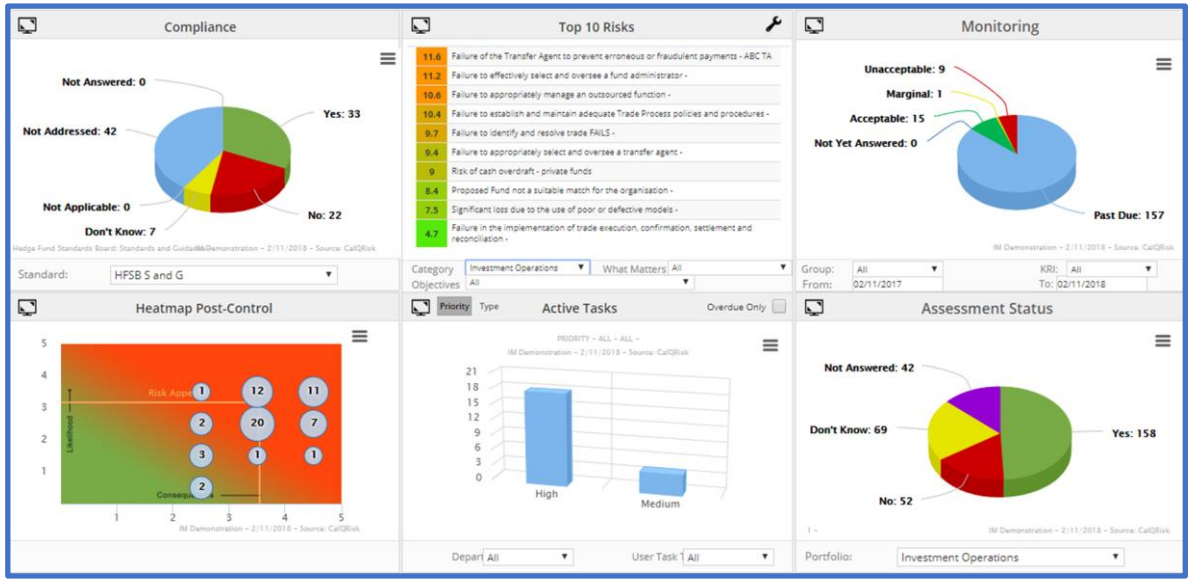
Tasks

Task Id	Task Owner	Due Date	Task Status	Description
11375	Gerry Joyce	30/06/2021	Open	Draw up a procedure to ensure that the minimum amount of personal data required to properly fulfil each data processing purpose is identified and documented before activity / processing begins.
13273	Gerry Joyce	08/10/2018	Open	Add the terms adequate, relevant and limited to what is necessary to the Consideration List for each purpose.

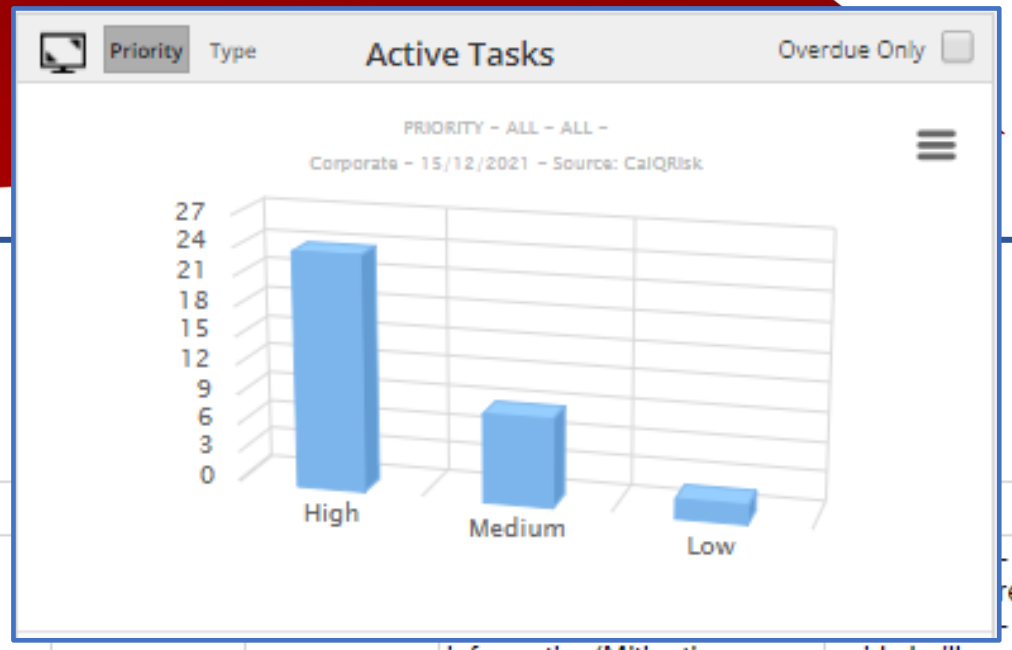
Cyber Security Framework - NIST

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	9/15	ID.GV-1 2/2	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	15/35	PR.AC-1 3/7	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 3/5					
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	54	15/54	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 5/6	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	17/19	PR.PT-1 5/5	PR.PT-2 7/7	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	2	2/2	RC.RP-1 2/2											
Improvements	2	1/2	RC.IM-1 1/2	RC.IM-2 1/1										
Communications	6	1/6	RC.CO-1 1/6	RC.CO-2 0/0	RC.CO-3 0/0									

Reporting - Quarterly



- Monthly Report +
- You have 30 minutes
- Report
  - Page 1: Summary
  - Page 2: Graphics
  - Page 3+: Detail (Risks, Tasks, Risk events, Compliance, ...)
- Significant changes from previous quarter
- Control Effectiveness: pick one / two areas. (e.g. Financial, Cyber security)
- Emerging Risks: Changes in regulations, Changes in sector, ..



Tasks Closed Report

15/12/2021

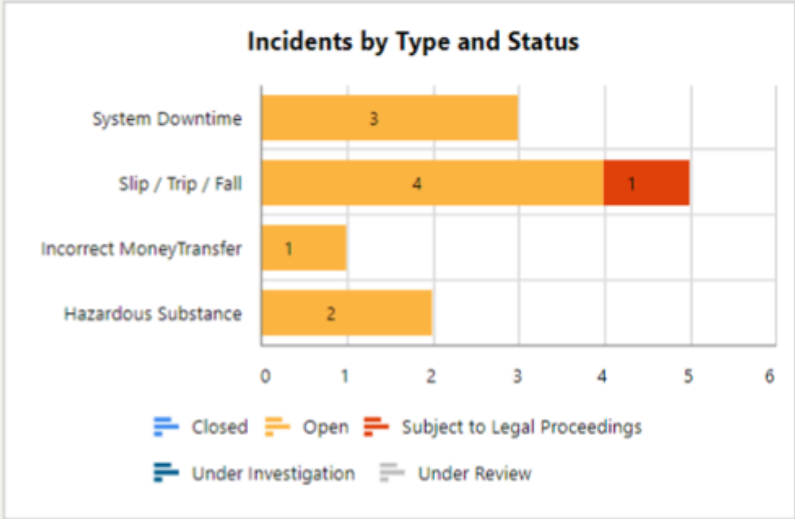
From: 01-Jul-2021 To: 15-Dec-2021

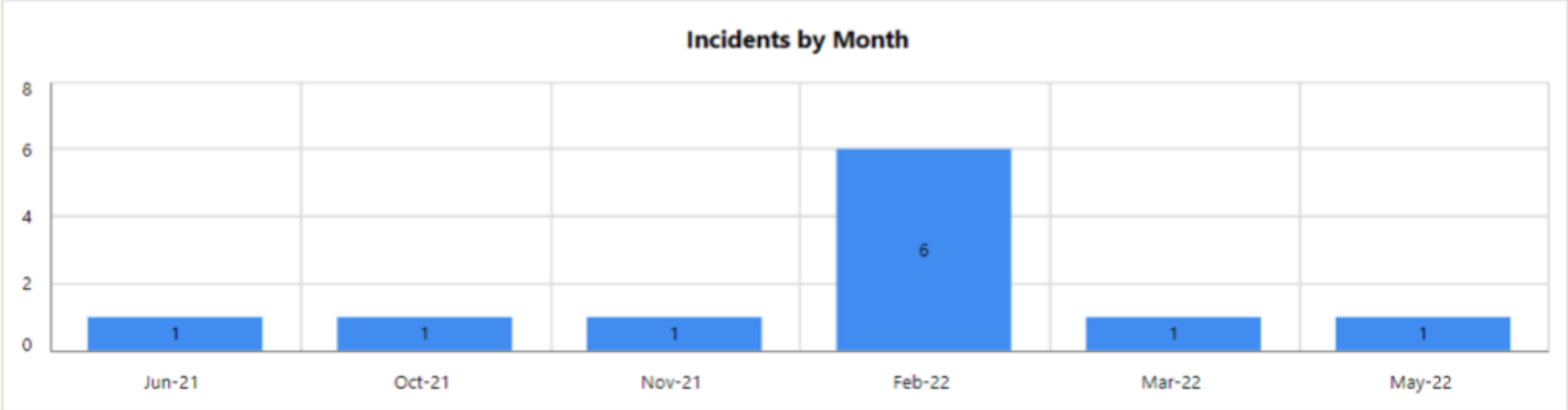
Task ID	Task Description	Priority	Task Owner				
5783	Draft a procedure to review users access rights (by management) on a regular basis.	Medium	Gerard Joyce			information(Mitigation Action)	- Tom Healy) Draft review - Gerard Joyce) Mairead said she'll update the procedure this week (20/08/2021 - Gerard Joyce) I reviewed the draft and it looks good. (16/09/2021 - Chris Hanlon) Test comment (20/09/2021 - Gerard Joyce) Siobhan will review
24152	Update GDPR Guidance to include greater detail on Data Processing	High	Paul O'Brien	25/11/2021	15/12/2021	0 - (Corrective Action)	This is as a result of the GDPR complaint from Geoff (28/10/2021)
24360	Review list of all Third Parties	High	Gerard Joyce	16/11/2021	09/11/2021	81145 - Poor Outsourcing oversight(RiskAction)	(09/11/2021 - Gerard Joyce) All done.

Incident Dashboard

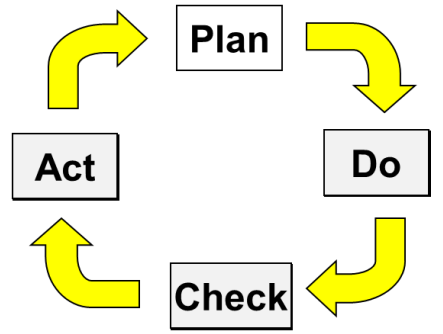
From: 01-Jan-2021 To: 19-May-2022

	Closed	Open	Review	Legal
Hazardous Substance	0	2	0	0
Incorrect MoneyTransfer	0	1	0	0
Slip / Trip / Fall	0	4	0	1
System Downtime	0	3	0	0

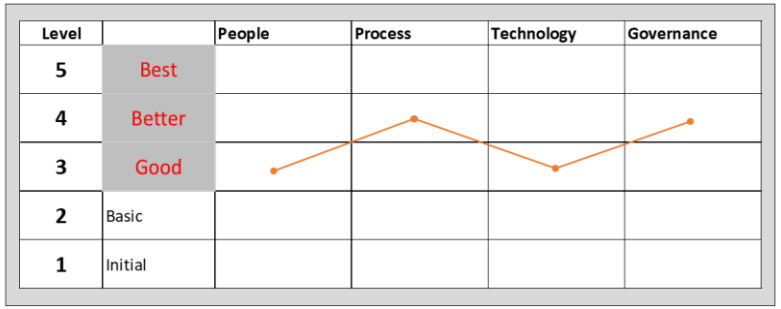




Reporting to the Board - Annually



- Quarterly Report +
- You have 60 mins
- Review of Risk Management (Framework)
- Full Risk Profile (by Category ?)
- Risk Management Maturity
- Achievements over the past 12 months
- Key Risk Drivers / Events
- Priorities for the next 12 months
- Any changes expected as a result of changes in the Strategic Plan



Takeaways

- Have different report formats for Monthly, Quarterly, Annual reports
- Make sure that the recipients of the report are getting what they need
- Only include detail where requested / required to support a proposal
- Supply text in pre-meeting documentation / Use Graphics in the meetings
- Communicating with the Board is key to the success of your RM efforts
- Consider giving the Board access to live data

Q&A

CalQRisk
Manage the effect of uncertainty on objectives

Thank You

Gerard Joyce

gjoyce@calqrisk.com