Reporting to the Board / Audit & Risk Committee for Housing Associations

A CalQRisk Webinar

CalQRisk

Manage the effect of uncertainty on objectives

Presented By

Gerard Joyce, CTO, CalQRisk

19th July 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

- 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 and Not-for-Profit sectors
    - We work with housing associations across Ireland and the UK, we're an approved Sector Supplier with the National Housing Federation

Board Vs Audit & Risk Committee

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 assess the adequacy and effectiveness of risk management
  - Need to challenge and advise the 1st line
  - Need to ensure consistent implementation

Operational Vs Strategic

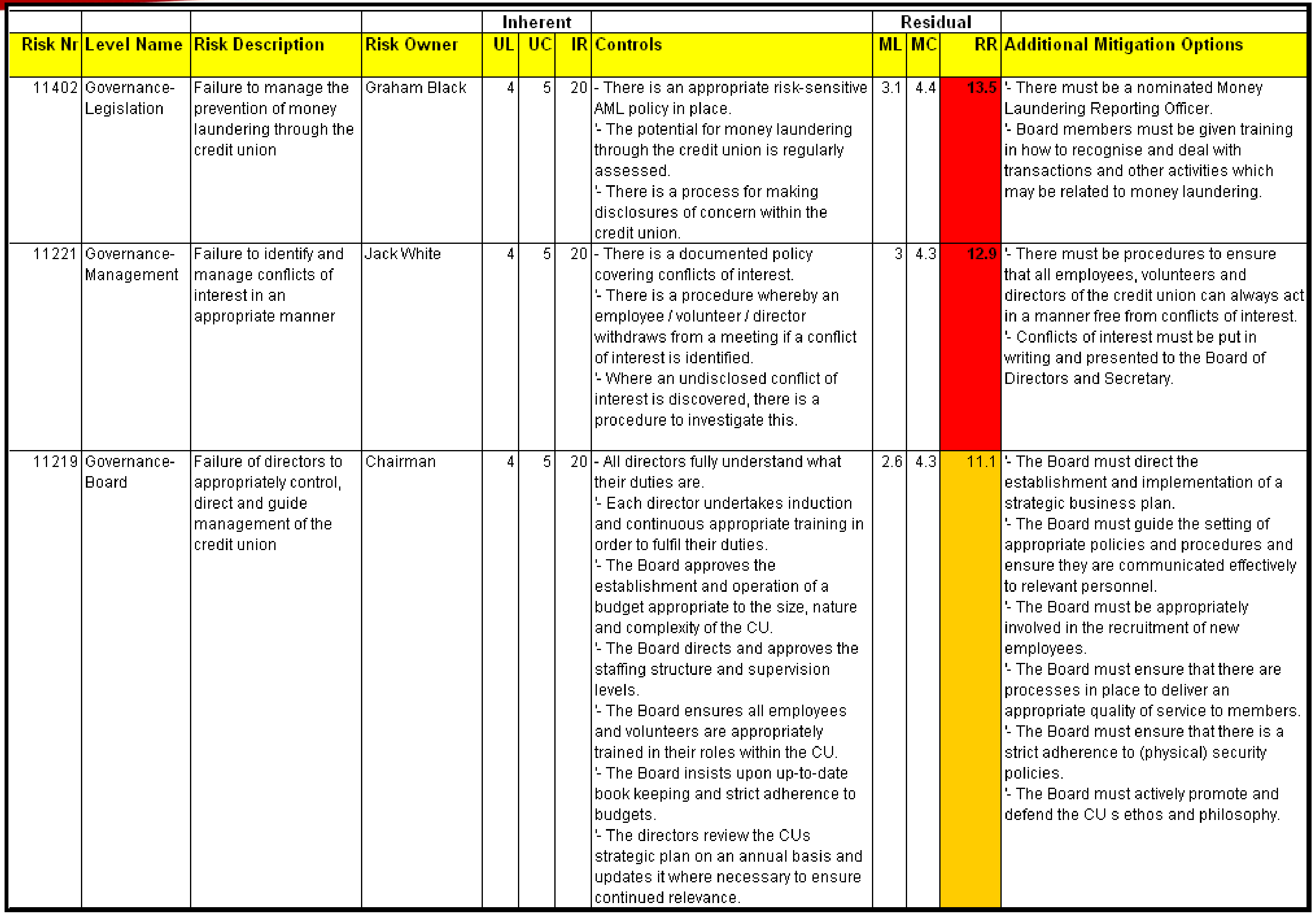
Operational

- More detail
- More risks
- Focus might be on operational area or category of risk

Strategic

- High Level
- Linked to Objectives / Strategic Plan / Specific Initiative
- Focus on Trends and Emerging risks

Risk Register



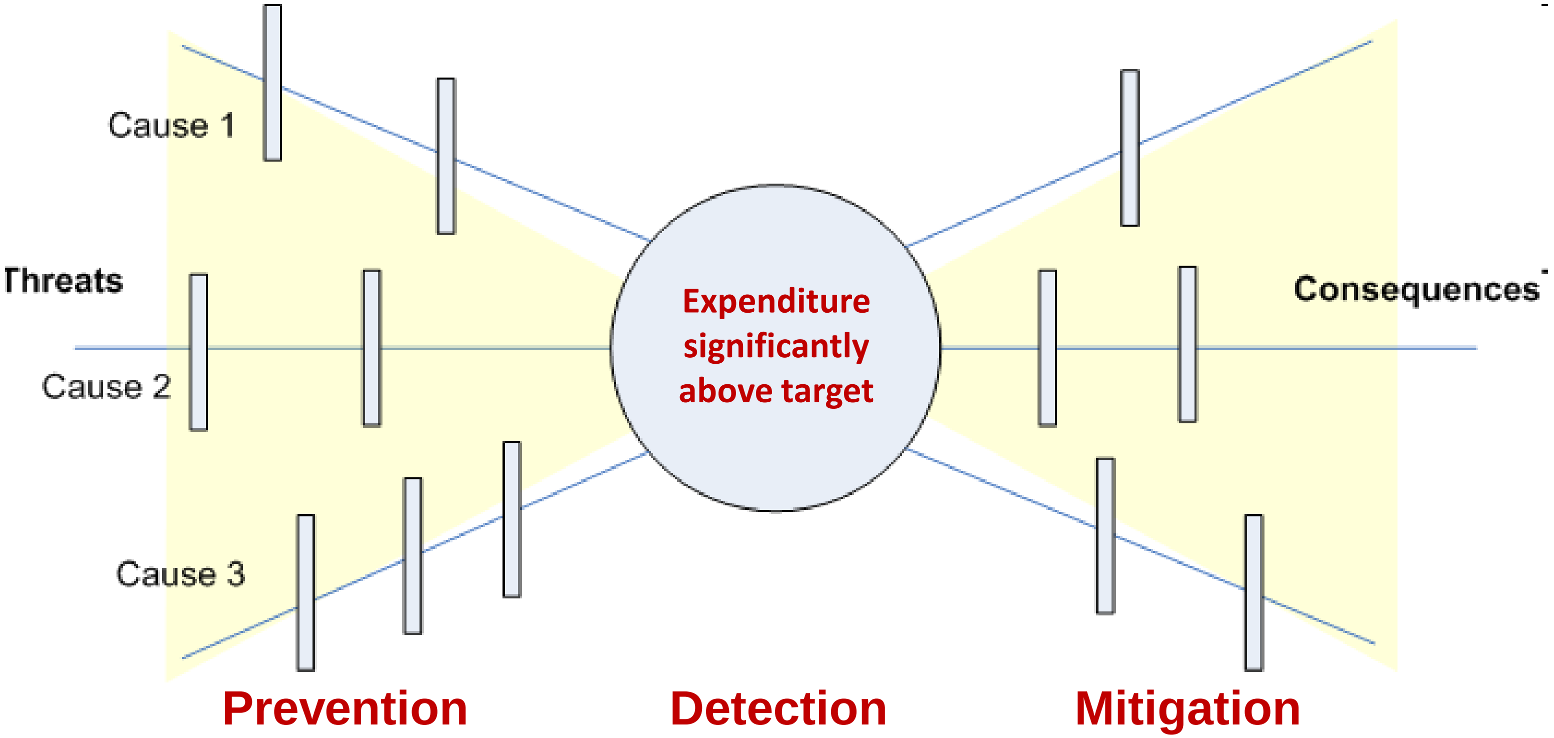
				Inherent				Residual			
Risk Nr	**Level Name**	**Risk Description**	**Risk Owner**	**UL**	**UC**	**IR**	**Controls**	**ML**	**MC**	**RR**	**Additional Mitigation Options**
11402	Governance-Legislation	Failure to manage the prevention of money laundering through the credit union	Graham Black	4	5	20	- There is an appropriate risk-sensitive AML policy in place. '- The potential for money laundering through the credit union is regularly assessed. '- There is a process for making disclosures of concern within the credit union.	3.1	4.4	13.5	'- There must be a nominated Money Laundering Reporting Officer. '- Board members must be given training in how to recognise and deal with transactions and other activities which may be related to money laundering.
11221	Governance-Management	Failure to identify and manage conflicts of interest in an appropriate manner	Jack White	4	5	20	- There is a documented policy covering conflicts of interest. '- There is a procedure whereby an employee / volunteer / director withdraws from a meeting if a conflict of interest is identified. '- Where an undisclosed conflict of interest is discovered, there is a procedure to investigate this.	3	4.3	12.9	'- There must be procedures to ensure that all employees, volunteers and directors of the credit union can always act in a manner free from conflicts of interest. '- Conflicts of interest must be put in writing and presented to the Board of Directors and Secretary.
11219	Governance-Board	Failure of directors to appropriately control, direct and guide management of the credit union	Chairman	4	5	20	- All directors fully understand what their duties are. '- Each director undertakes induction and continuous appropriate training in order to fulfil their duties. '- The Board approves the establishment and operation of a budget appropriate to the size, nature and complexity of the CU. '- The Board directs and approves the staffing structure and supervision levels. '- The Board ensures all employees and volunteers are appropriately trained in their roles within the CU. '- The Board insists upon up-to-date book keeping and strict adherence to budgets. '- The directors review the CUs strategic plan on an annual basis and updates it where necessary to ensure continued relevance.	2.6	4.3	11.1	'- The Board must direct the establishment and implementation of a strategic business plan. '- The Board must guide the setting of appropriate policies and procedures and ensure they are communicated effectively to relevant personnel. '- The Board must be appropriately involved in the recruitment of new employees. '- The Board must ensure that there are processes in place to deliver an appropriate quality of service to members. '- The Board must ensure that there is a strict adherence to (physical) security policies. '- The Board must actively promote and defend the CU s ethos and philosophy.

High Level Risks

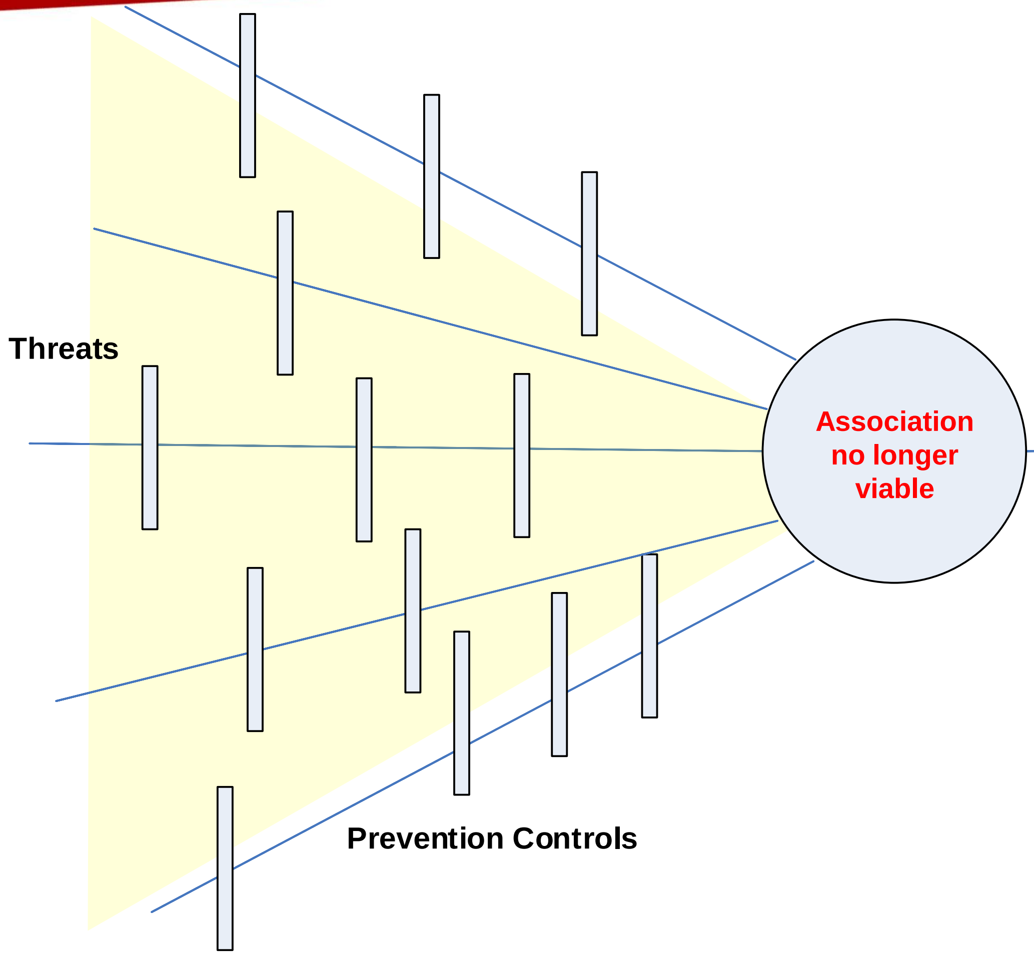
15/07/2022

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



Diversify into student accommodation

Deliver quality service to tenants

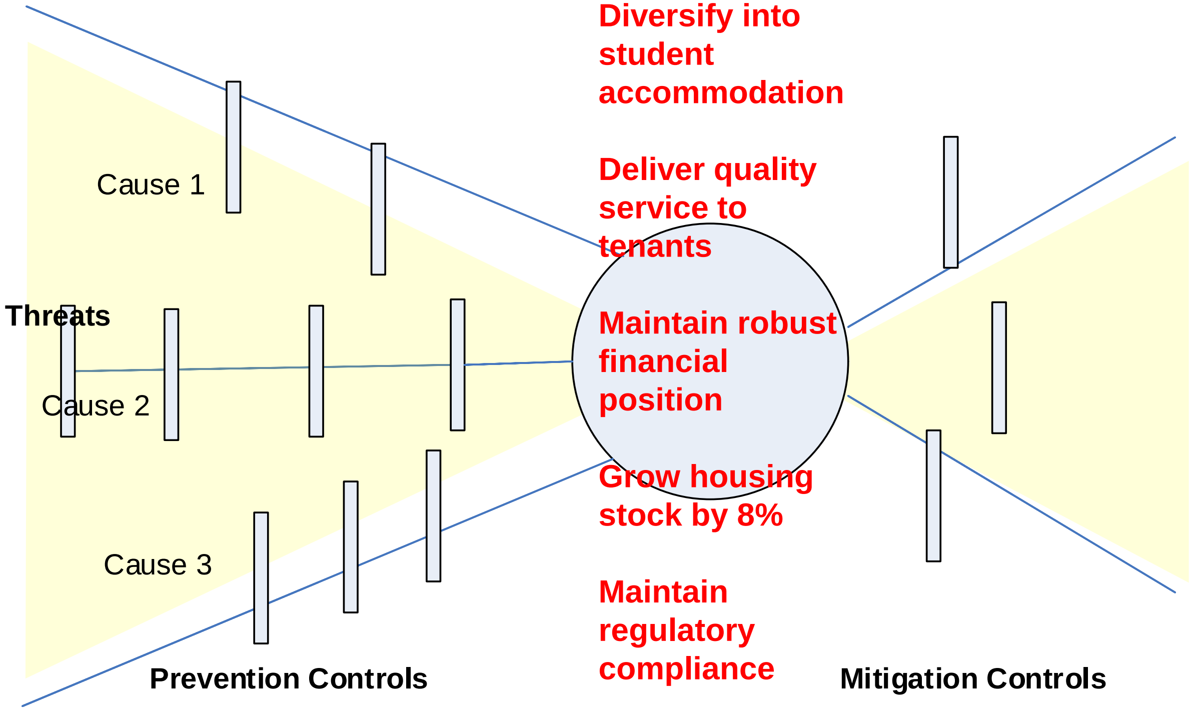
Maintain robust financial position

Grow housing stock by 8%

Maintain regulatory compliance

Protect the Health & Safety of Customers and Employees

From Objectives to Risks



Diversify into student accommodation

Deliver quality service to tenants

Maintain robust financial position

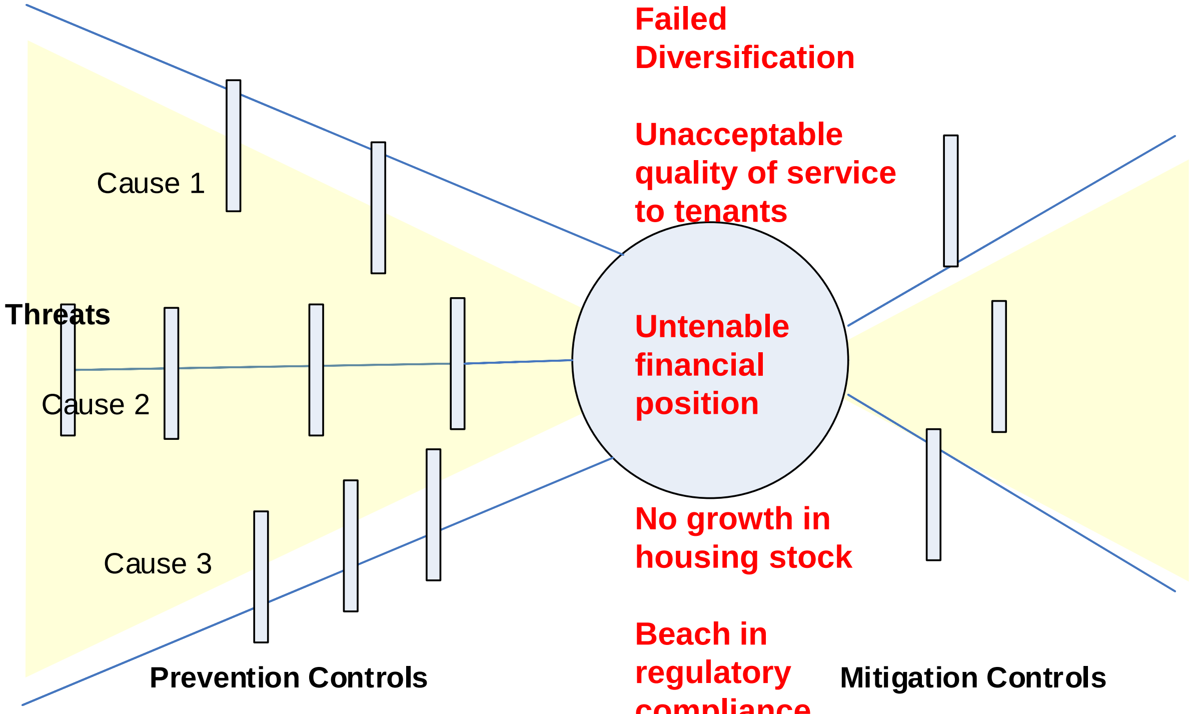
Grow housing stock by 8%

Maintain regulatory compliance

Protect the Health & Safety of Customers and Employees

Objectives

From Objectives to Risks



Failed Diversification

Unacceptable quality of service to tenants

Untenable financial position

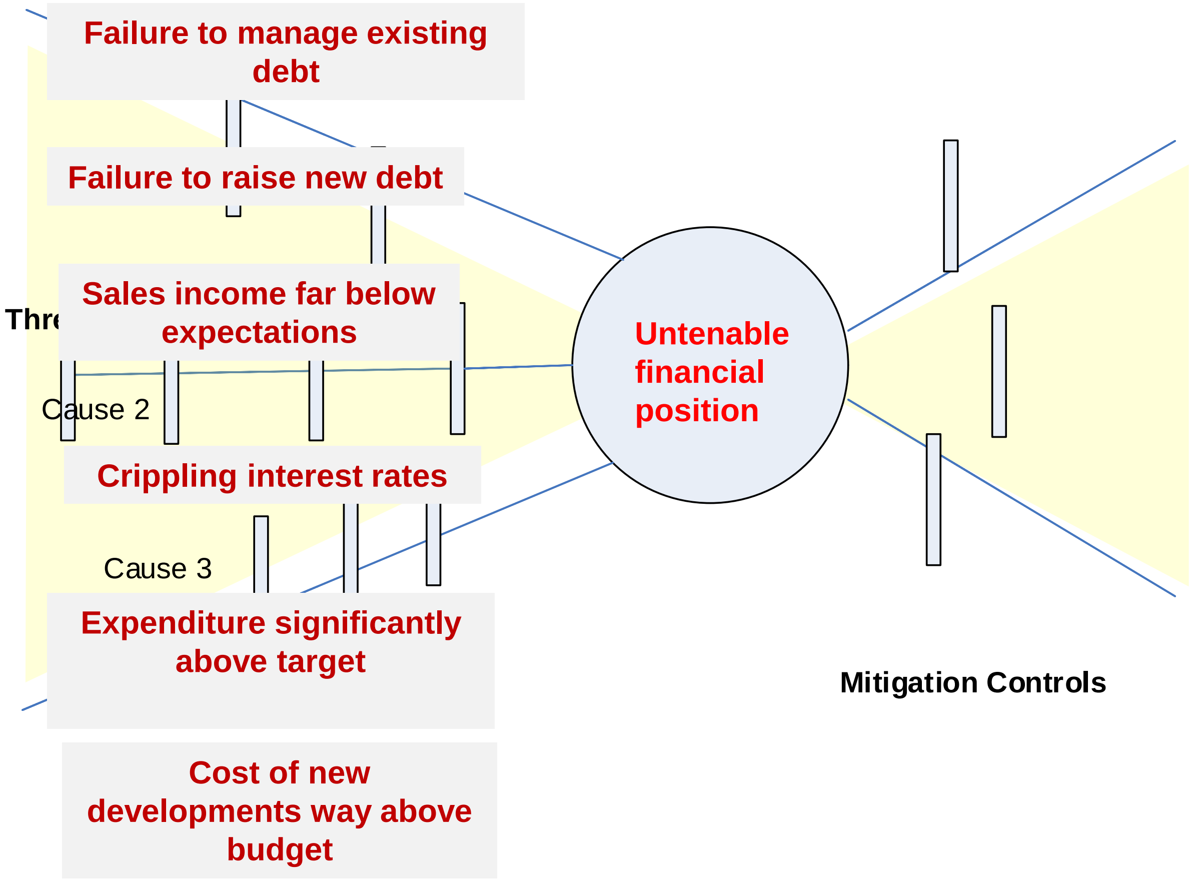
No growth in housing stock

Beach in regulatory compliance

Death or Injury

Risks

From Objectives to Risks



Failure to manage existing debt

Failure to raise new debt

Sales income far below expectations

Crippling interest rates

Expenditure significantly above target

Cost of new developments way above budget

Untenable financial position

Detailed Risks

Risks

Trends

- Evidence of Good Governance at all levels in the organisation
- ESG (Environmental, Social and corporate Governance) “Non-financial” factors
- **Environmental**: 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 establishes and documents its appetite for the risks the organisation faces in pursuit of its strategy.” (NHF CoP)
- **Emerging Risks**: Trying to anticipate what’s coming, regulatory changes, market, skill shortages, recruitment,..

What I want to know as a Director

CalQRisk
Manage the effect of uncertainty on objectives

- 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 Directors to know

What I, as the Risk Management Officer, want the directors 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 identified and analysed
- Evidence that there are effective controls 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 any incidents since last meeting
- Details of plans to monitor any risks that are of concern

Frequency

- Monthly
- Quarterly
- Annually

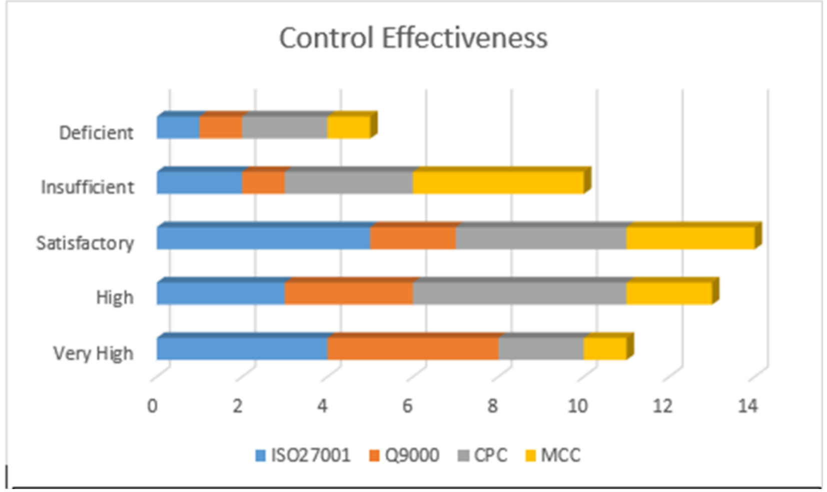
Reporting - Monthly

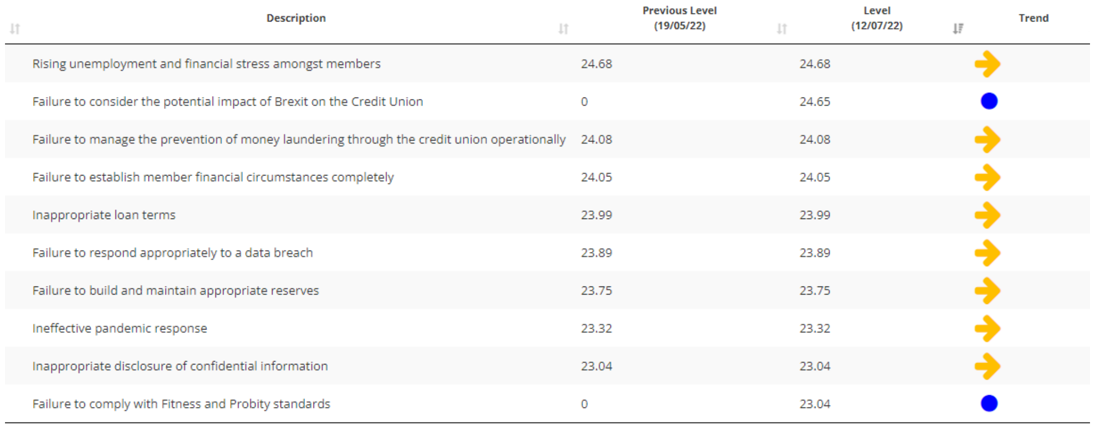
- You have max 15 mins to communicate your message(s)
- Use lots of graphics instead of lots of words
- If there’s a theme to the board meeting, reflect that in your report
    - E.g Cybersecurity
- Are there regulatory requirements that need to be addressed?
- Are you responding to a previous request 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

Include:

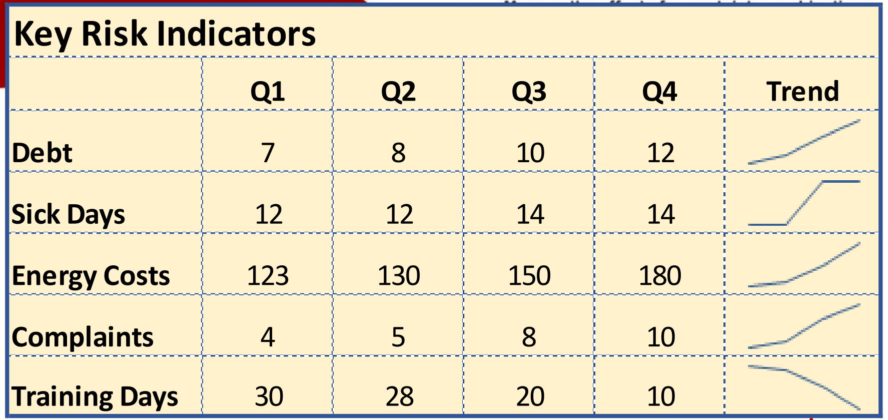
- Significant Risks
- Change / Trend since last report
- Any new risks / emerging risks
- Effectiveness of Controls
- Update on Tasks from previous reports
- Risk Events / Incidents that have occurred
- Deviations from risk appetite
- Key Risk Indicators (KRIs)





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



Key Risk Indicators	Q1	Q2	Q3	Q4	Trend
Debt	7	8	10	12	
Sick Days	12	12	14	14	
Energy Costs	123	130	150	180	
Complaints	4	5	8	10	
Training Days	30	28	20	10	

Exposure Indicators

Changes in the nature of the business 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, helpdesk calls
- Stress indicators at Third-Parties / Sub-contractors / Supply Chain

Causal Indicators

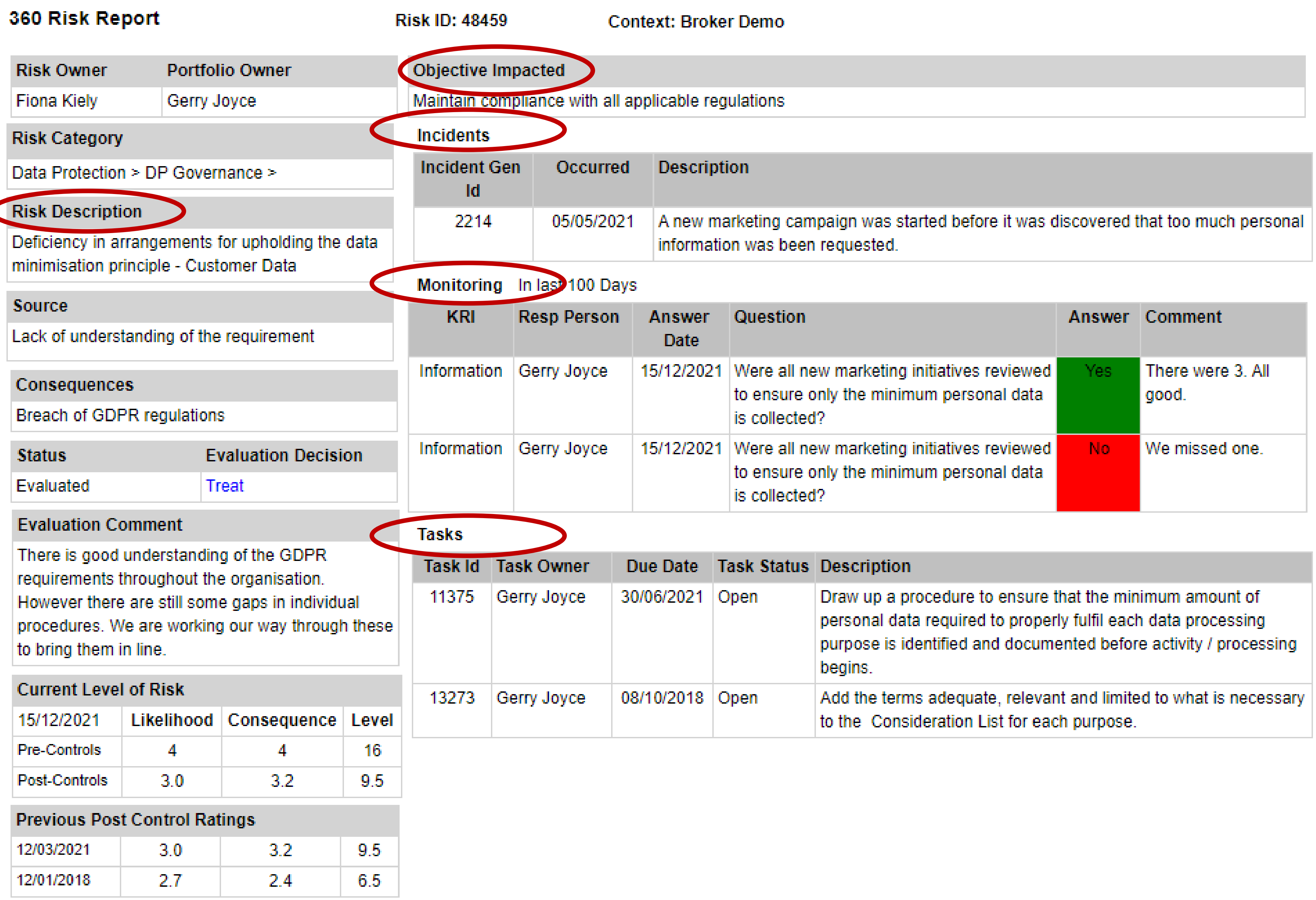
Drivers of some key risks to the business

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

Failure Indicators

Poor performance and failing controls

- Complaints, 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.

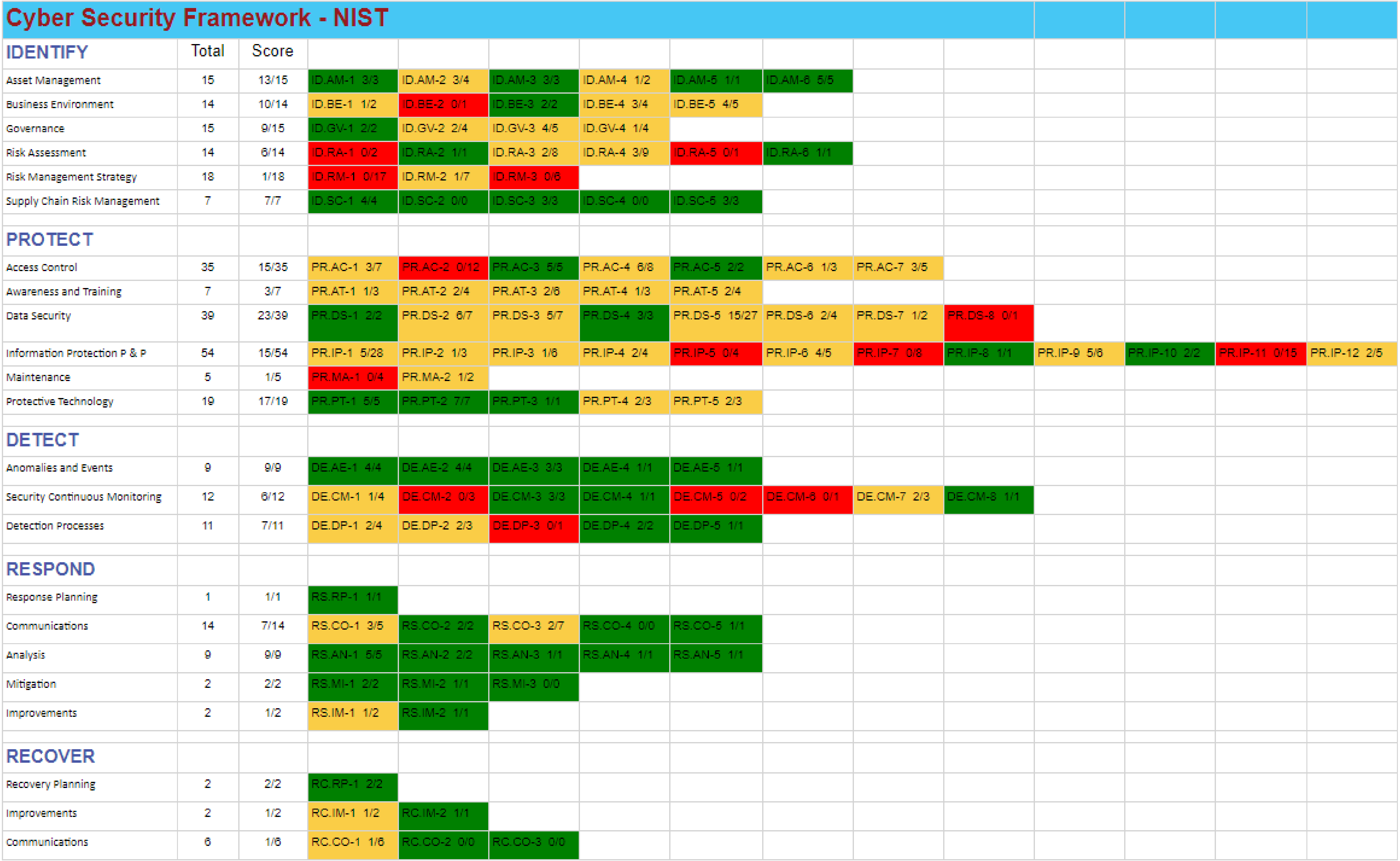
Monitoring In last 100 Days

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.

nage the effect of uncertainty on objectives

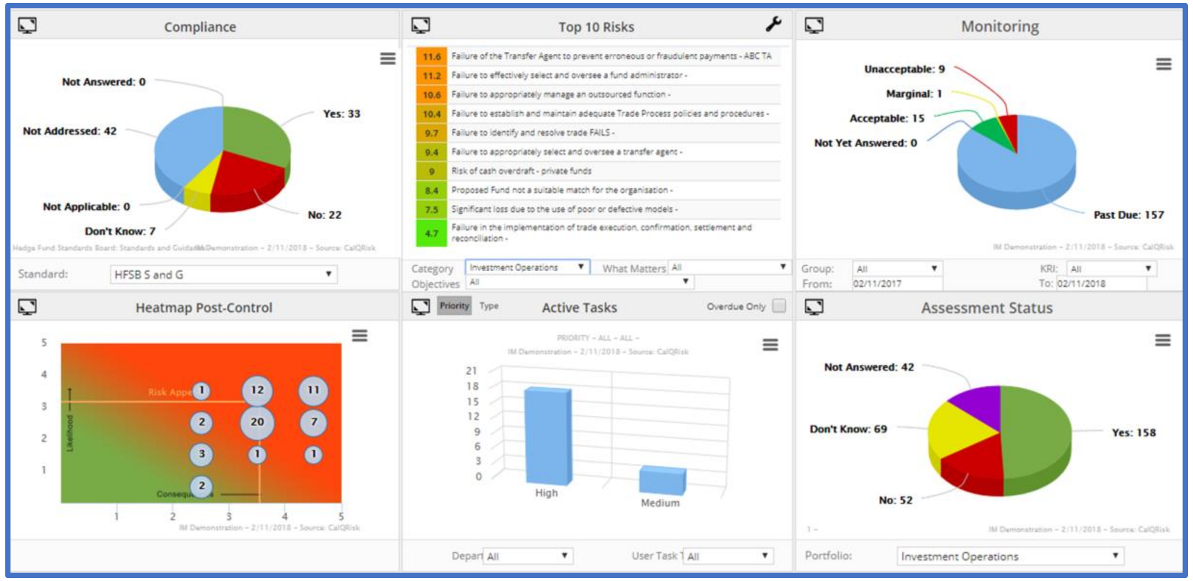


Cyber Security Framework - NIST

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	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 1/6	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									

sk objectives

Reporting - Quarterly



Top 10 Risks

11.6	Failure of the Transfer Agent to prevent erroneous or fraudulent payments - ABC TA
11.2	Failure to effectively select and oversee a fund administrator -
10.6	Failure to appropriately manage an outsourced function -
10.4	Failure to establish and maintain adequate Trade Process policies and procedures -
9.7	Failure to identify and resolve trade FAILS -
9.4	Failure to appropriately select and oversee a transfer agent -
9	Risk of cash overdraft - private funds
8.4	Proposed Fund not a suitable match for the organisation -
7.5	Significant loss due to the use of poor or defective models -
4.7	Failure in the implementation of trade execution, confirmation, settlement and reconciliation -

Standard: HFSB S and G

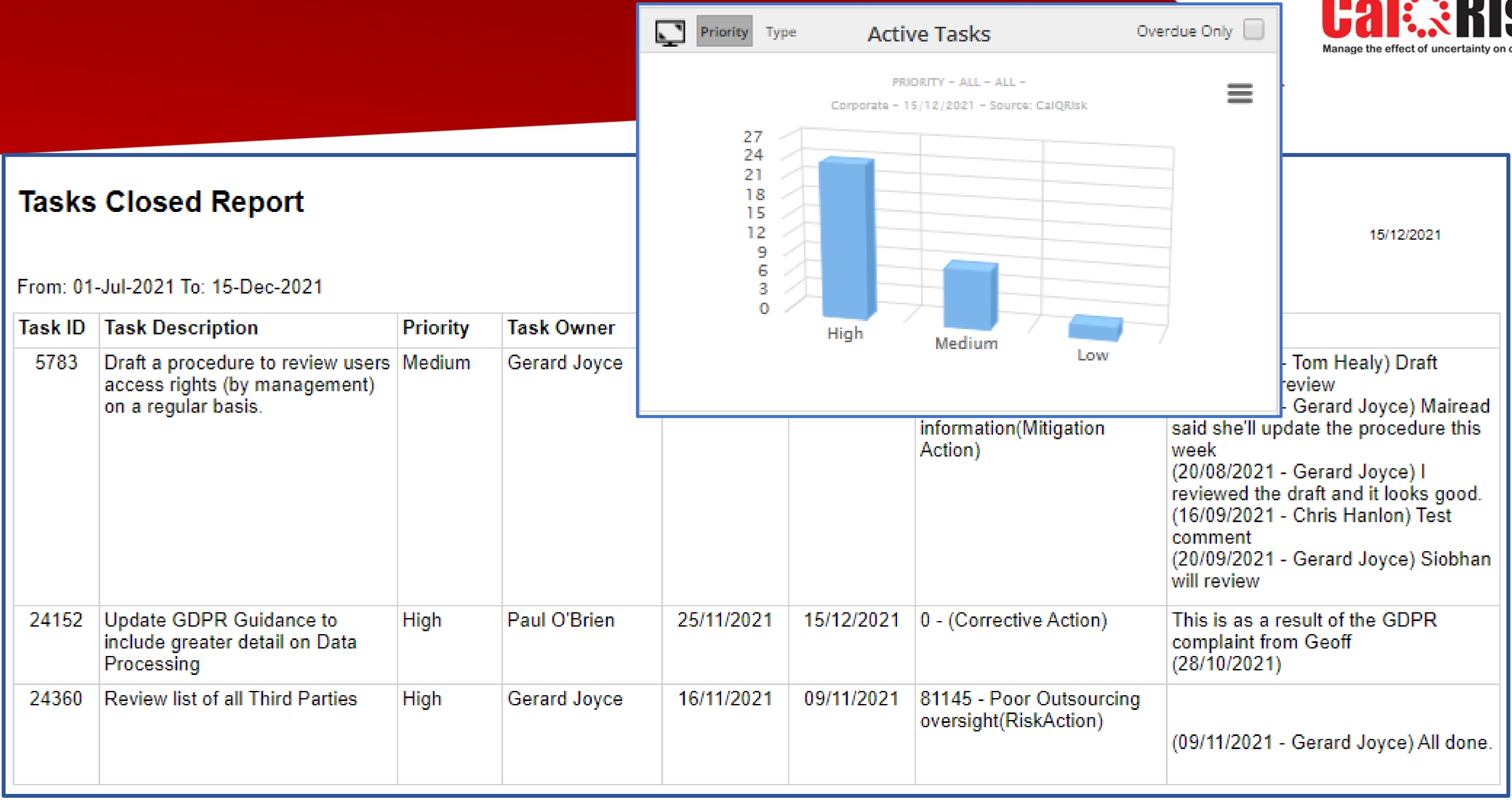
Category: Investment Operations
What Matters: All
Objectives: All

Group: All
KRI: All
From: 02/11/2017
To: 02/11/2018

Depart: All
User Task T: All

Portfolio: Investment Operations

- 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, ..

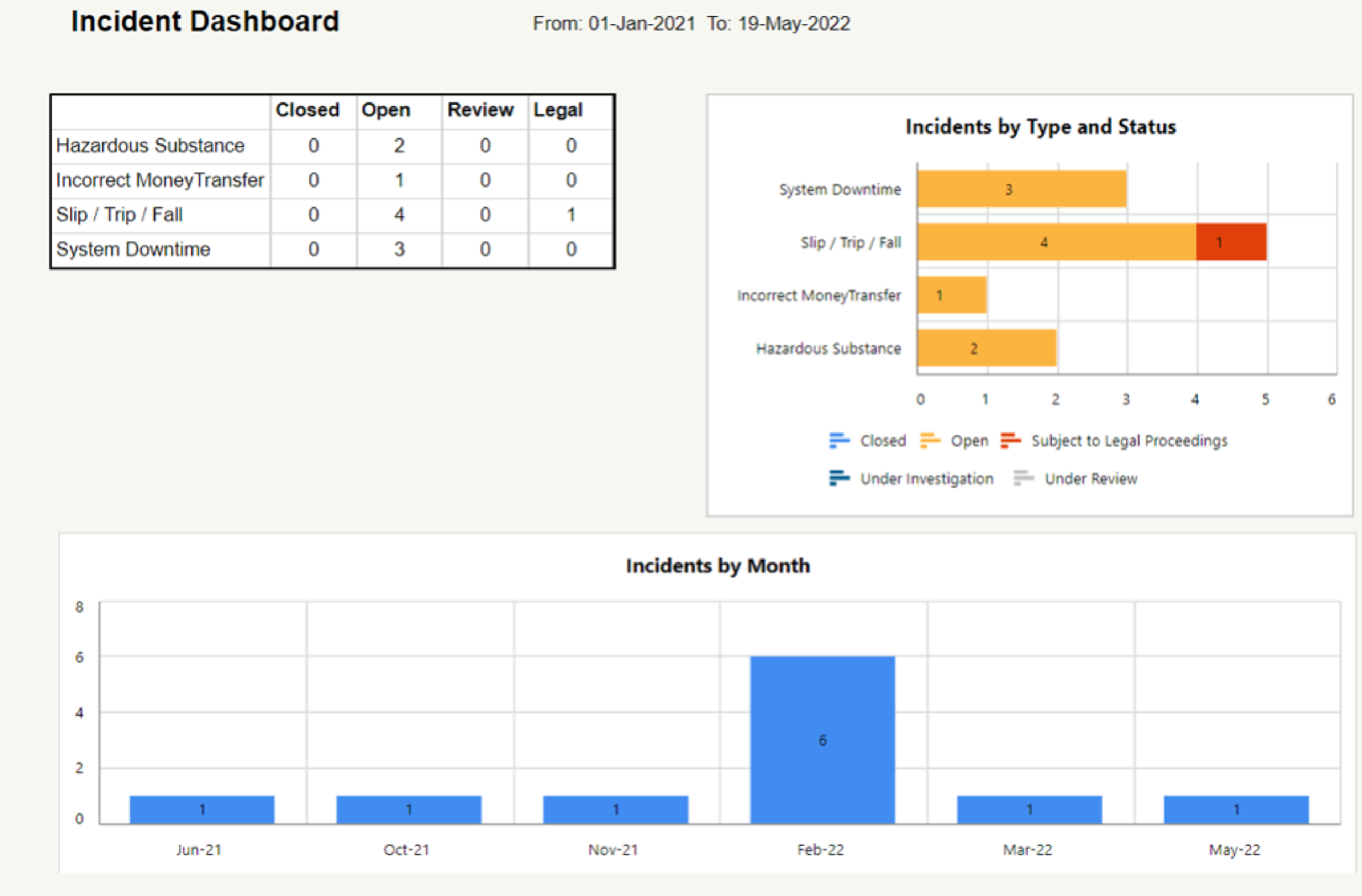


Tasks Closed Report

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

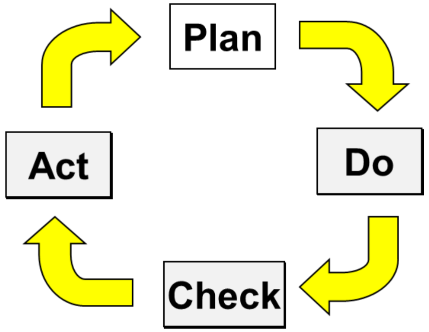
	Closed	Open	Review	Legal
Hazardous Substance	0	2	0	0
Incorrect MoneyTransfer	0	1	0	0
Slip / Trip / Fall	0	4	0	1
System Downtime	0	3	0	0

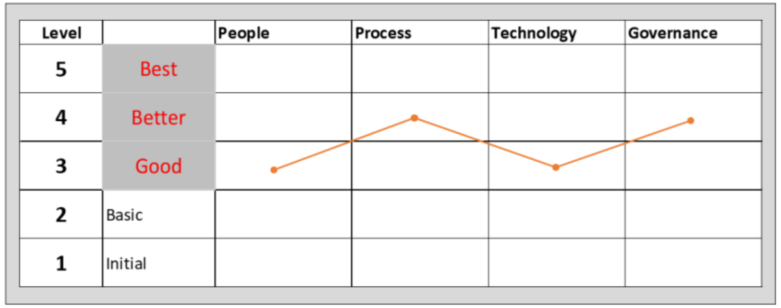
Incidents by Type and Status

Incidents by Month

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





Level		People	Process	Technology	Governance
5	Best				
4	Better				
3	Good				
2	Basic				
1	Initial				

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