Summer School 2025
-
Rolling Up the Detail: What to Report in Risk Management

Gerard Joyce

CTO, CalQRisk

30th July 2025

CalQRisk

About Us

- Experienced Risk & Compliance Professionals
- We offer GRC software solutions and services
- Headquartered in Ireland
- Client base in financial services, insurance, public sector, housing and other sectors

NATIONAL FINTECH AWARDS 2023

2024 REGTECH 100
www.RegTech100.com

CalQRisk

66

If you can’t explain it simply, you don’t understand it well enough

Albert Einstein *(Physicist and Nobel laureate)*

99

AGENDA

- Purposes
- Performance and Progress Tracking
- Compliance Assurance
- Actions
- Summarising the data

CalRisk

Purposes

- To inform?
  - Progress (achieving business objectives)
  - Give assurance
  - Make aware
- To get a decision?
  - Describe problem
  - Offer solutions
- To Comply?
  - Demonstrate good Governance

CalRisk

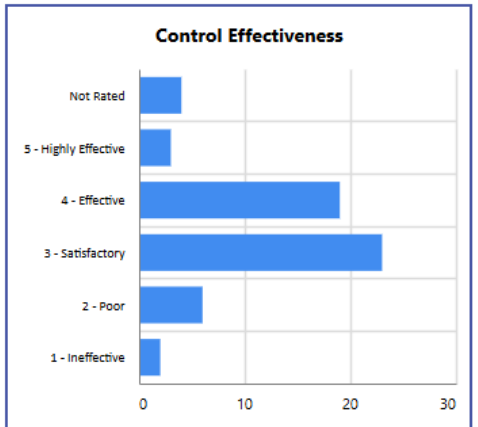
RM Performance and Progress Tracking

- Metrics
  - Top 10 Risks
  - Actions taken to mitigate risk
  - Key Risk Indicators (KRIs)
    - No. of Incidents / operational errors
    - No. of policy breaches / risk appetite breaches
    - Control Effectiveness
    - Audit Findings
- Plan
  - Going to do (next 30 days)
  - What you (the Board) can do to help

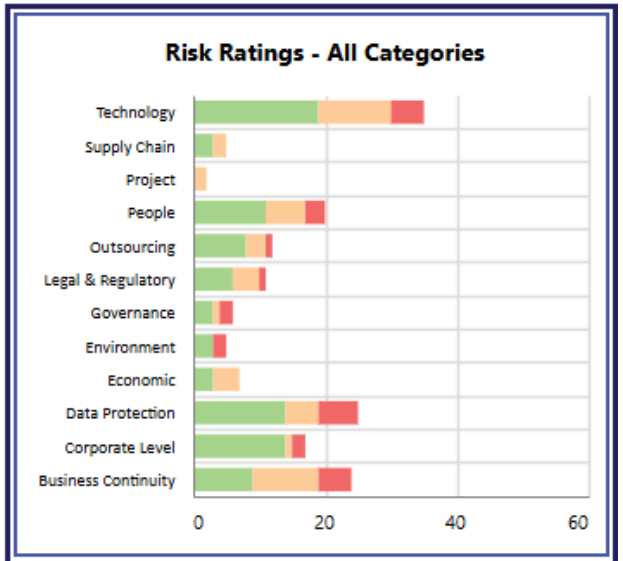
CalRisk

RM Performance and Progress Tracking

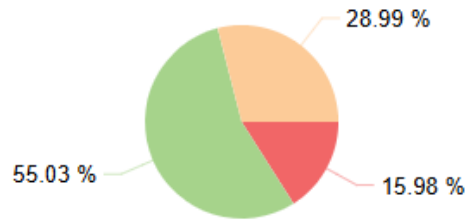
Risk ID	Category	Risk Description	Risk Owner	Controls in place	L	C	Score	Trend
71195	Corporate Level - Technology	IT systems unavailable for significant duration	Gerard Joyce	- UPS and Generator are in place. - Strong intrusion prevention system in place. - Anti-virus software kept up to date. - System vulnerabilities are patched as soon as patch is available. User Added Controls: Server logs are reviewed regularly. User Access is audited on a semi-annual basis Weekly WorldCheck completed There is a maintained Transaction Monitoring Programme in place. The organisation is expected to ensure that its disaster recovery and business continuity measures are tested and updated Review IT Policy	3.0	5.0	15.0	↑
138600	Corporate Level - Environment	Poor performance in relation to ESG	Paul O'Brien	- ESG policy is in place	4.0	3.5	14.0	○
71194	Corporate Level - Technology	Integrity of data held on IT systems compromised	Gerard Joyce	- Access to application data is strictly controlled. User Added Controls: Processes and mechanisms for installing and maintaining network security controls are defined and understood.	3.0	4.5	13.5	→
100209	Corporate Level - Legal & Regulatory	Regulatory Risk	Chris Hanlon	- Monthly compliance report User Added Controls: Weekly WorldCheck completed Conduct monthly compliance checks.	3.0	4.0	12.0	↓



	Q1	Q2	Q3	Q4	Total
Operational Errors	15	9	6		30
Policy breaches	5	2	1		8
Risk Appetite breaches	0	4	6		12
Audit Findings	8	3	1		12



	Low	Medium	High
No. of Risks	93	49	27

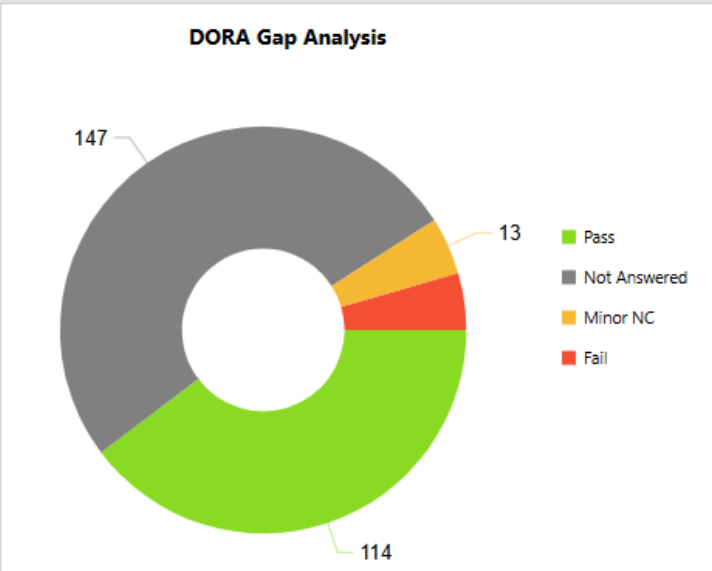


RM Compliance Assurance

- Non-Compliance is a risk
  - Regulations that apply
  - Effective Controls
  - Policies & Procedures

DORA Status Overview

Checklist Name	Count	% Pass
Article 14 - Communication	3	100.0%
Article 18 - Classification of ICT-related incidents and cyber threats	7	71.4%
Article 29 - Preliminary assessment of ICT concentration risk at entity level	7	0.0%
Article 45 - Information-sharing arrangements on cyber threat information and intelligence	5	100.0%
Article 6 - ICT risk management framework	18	77.8%
Article 8 - Identification	7	0.0%
Article 11 - Response & Recovery	15	0.0%
Article 28 - General principles	28	100.0%
Article 5 - Governance & Organisation	15	0.0%
Article 5 - Governance and organisation	15	60.0%
Article 6 - ICT Risk Management Framework	149	32.9%
Article 7 - ICT systems, protocols and tools	4	0.0%
Article 9 - Protection & Prevention	14	7.1%



RM Actions

- What evidence can you show that risk mitigation is happening
  - What Tasks have you completed in the past 30 days
  - What Action are you planning for the next 30 days
  - Focus on the Top 10 risks

Risk ID	Risk Description	Risk Owner	Score	Task ID	Task Description	Owner	Due Date	Status
71195	IT systems unavailable for significant duration	Gerard Joyce	15.0	21241	Organise a generator service and power failure test.	Paul O'Brien	27/07/2020	Closed
				41221	Set up a quarterly run-on-load on generator check.	Gerard Joyce	01/08/2025	Open
138600	Poor performance in relation to ESG	Paul O'Brien	14.0	41222	Procure a software application to support recording and reporting of Carbon Emissions.	Paul O'Brien	07/08/2025	Open
71194	Integrity of data held on IT systems compromised	Gerard Joyce	13.5	21240	Review and update list of individuals who have access to the Fin system database..	Fiona Kiely	27/07/2020	Closed
100209	Regulatory Risk	Chris Hanlon	12.0	41223	Review all relevant organisation policies to ensure the are aligned with regulatory requirements.	Fiona Kiely	14/08/2025	Open

CalRisk

RM Rolling up the Detail

- Too much detail will mean nothing is read
  - Present the risks at a higher level
  - Show how these relate to the Strategic Objectives

High Level Risks with Drill Down

Risk ID		Risk Description	Risk Owner	Inherent	Residual	Evaluation Comment	Control Effectiveness	Tasks
71194		Integrity of data held on IT systems compromised - Consequences: - Inaccurate reports, loss of data, - Reputation damage	Gerard Joyce	16	13.5	Working with IT and Operations to restrict the ability to enter data by user and by location.	4 - Effective	21240 - Review and update list of individuals who have access to the Fin system database.. - Closed
	31875	Failure to introduce new elements seamlessly ()	Josef Macdonald	20	10.4			41192 - Put a place in place to advise customer of any impairment in the service. - Open
	37011	Inadequate cyber protection at the network boundary ()	Tom Healy	20	7.1			
	37008	Failure to detect and respond to a cybersecurity breach in a timely manner ()	Tom Healy	20	5.9			36615 - Information security procedures should ensure that a single point of contact is created for the reporting and detection of security events. - Closed
	31880	Failure to ensure correct and secure operation of information processing facilities ()	Tom Healy	12	3.0	We are happy that this risk is well mitigated.		
58023		Inappropriate processing of personal data - Consequences: Data breach, reputation damage, sanction by regulator	Tom Healy	20	11.83		3 - Satisfactory	

Takeaways

- Focus on what's important and relevant
- Use graphics where possible
- Be prepared to give detail (if asked)
- Inform, give assurance, aid decision-making

Any questions?

Thank you

gerard.joyce@calqrisk.com

CalQRisk