GRC & The Golden Thread

Chris Hanlon, CEO, CalQRisk

27th June 2023

CalQRisk

Agenda

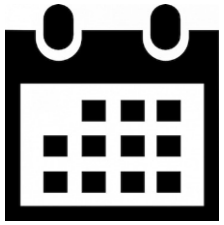
- GRC Programme Components
- Practical steps – tying the components together
- Reporting
- Q&A

About Us

- Experienced Risk & Compliance professionals
- Various backgrounds – Insurance, Asset Management, NFP, etc.
- Involved in international standards – e.g. ISO 31000
- GRC solution used across the UK and Ireland

Governance

A board, committee and management structure that is suitable to the size and complexity of the organisation.



Policy Management Framework with a defined list of policies, clear ownership for each policy, established review dates / cycles and clear approval processes.

Tracking of the Key Performance Indicators (KPIs) as per the strategic plan.

Risk

Defined risk management process which includes risk categorisation, risk impact matrix / risk criteria, risk assurance and reporting cycles.

Defined incident management process which includes the logging of any risk loss events, control failures, near misses, etc. while also ensuring any corrective / preventative action(s) are put in place.

The tracking of Key Risk Indicators (KRIs) across the organisation, including documented contingency plans should there be a KRI breach.

Compliance

Defined compliance assurance process in place with a documented compliance plan, assurance / testing process and reporting cycles.

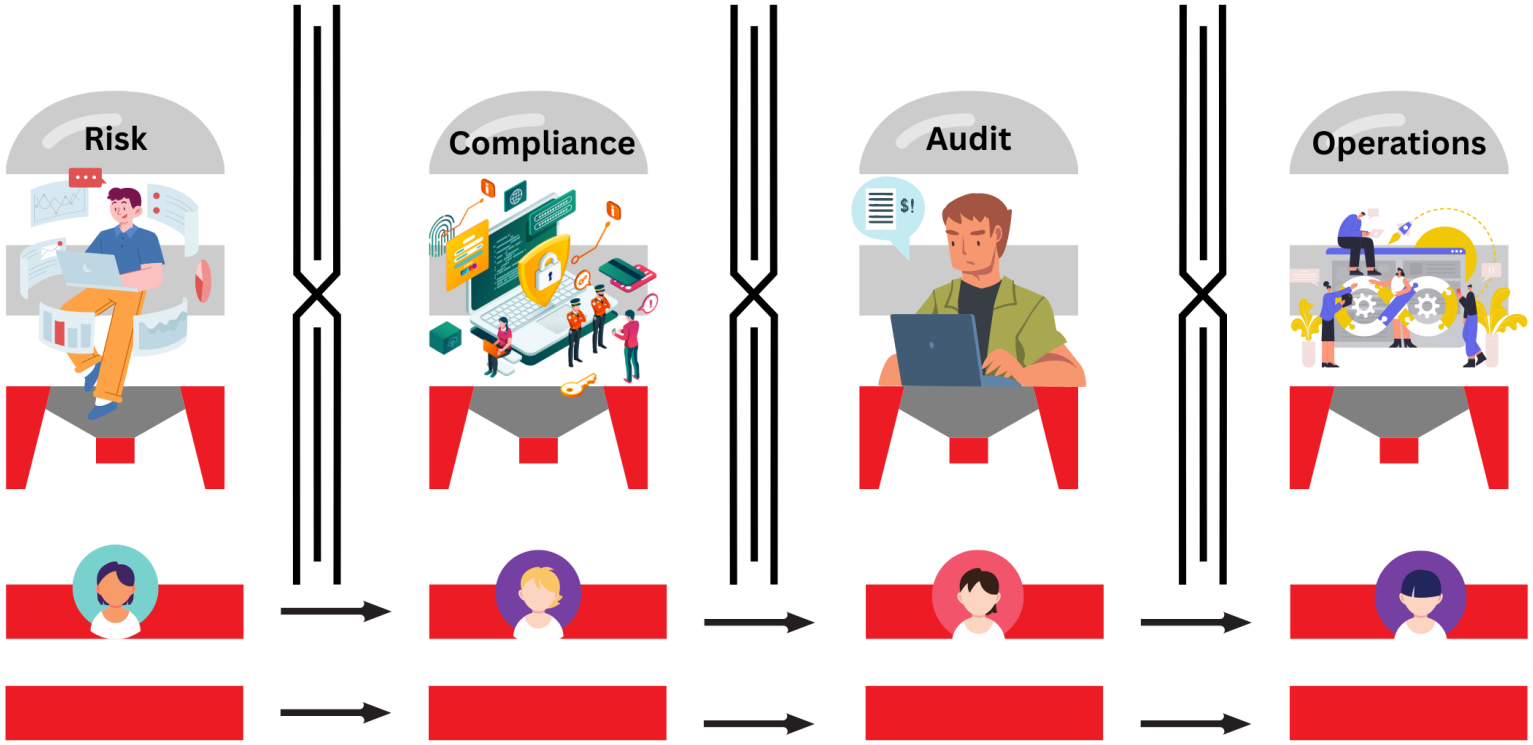
Documented compliance breach process including the tracking of corrective / preventative actions and reporting cycles.

Other Components

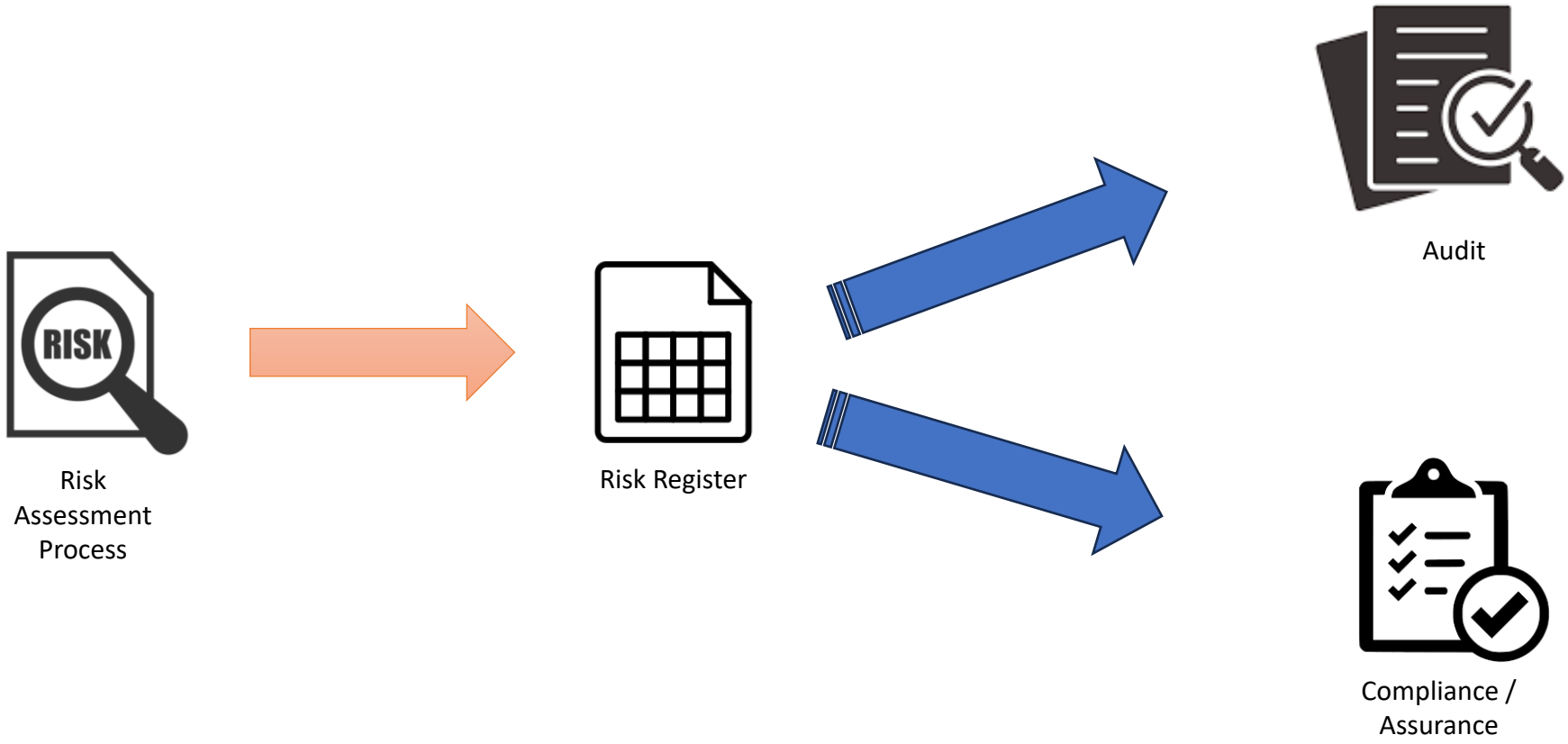
An independent audit process (internal or third party) providing assurance to the board and management team.

A proactive programme to manage third parties / outsourced service providers.

The Traditional Approach



Applying the Golden Thread



Applying the Golden Thread

Strategic Plan

Corporate Risk

Corporate Risk

Operational Risk

Operational Risk

Operational Risk

Key Risk Indicators

Audit Findings

Assurance

Incidents

Reporting

Rollup Risk Report **Risk ID: 71193** **Context: Corporate**

Risk Owner	Portfolio Owner
Chris Hanlon	Gerard Joyce

Risk Category

Corporate Level > Technology >

Risk Description

Confidentiality breach originating from IT failures -

Source

Mis-configuration, External hacker, Internal deliberate action, Poor procedures

Consequences

- Reputation damage,
- Regulatory Sanction
- Claims for damages

Status	Evaluation Decision
Evaluated	Treat

Evaluation Comment

This is well managed and continuously monitored.
No incidents in the past quarter.
There is one area of concern, a HR application that is in the cloud, we are urgently addressing security vulnerabilities.

Current Level of Risk

26/06/2023	Likelihood	Consequence	Level
Pre-Controls	4	5	20
Post-Controls	3.0	3.0	9.0

Previous Post Control Ratings

19/06/2023	3.0	3.5	10.5
30/05/2023	3.0	3.5	10.5

Objective Impacted

Maintain compliance with all legal and regulatory requirements

Linked Risks

ID	Risk Owner	Category	Level	Description
31870	Chris Hanlon	Technology/IT	6.9	Failure to appropriately manage information assets -
31881	Julie Scarlett	Technology/IT	10.5	Failure to prevent unauthorised access to systems and information -
31866	Gerard Joyce	Technology/IT	3.9	A mobile device (phone, tablet, laptop) being lost or stolen -
31867	Chris Hanlon	Technology/IT	11.0	Security failure in a web application -
31877	Tom Healy	Technology/IT	4.5	Failure to dispose of equipment legally and securely -
37009	Vicki Davies	Technology/IT	10.5	Poor Configuration Management -

Monitoring

KRI	Resp Person	Answer Date	Question	Answer	Comment
Breaches	Outsourced Provider	27/03/2023	What was the uptime of the xyz system in the last 30 days?	95.00	>
Breaches	Jess Clarke	04/04/2023	What was the uptime of the xyz system in the last 30 days?	90.00	>
Breaches	Chris Hanlon	26/06/2023	Were access rights reviewed and confirmed this quarter?	Yes	>
Breaches	Chris Hanlon	26/06/2023	What was the uptime of the xyz system in the last 30 days?	98.50	>
Data Processing	Julie Scarlett	16/03/2023	Have all users changed their passwords in the last three months?	Yes	>
Data Processing	Outsourced Provider	27/03/2023	Have all users changed their passwords in the last three months?	Yes	>
Data Processing	Jess Clarke	18/04/2023	Have all users changed their passwords in the last three months?	Yes	> Confirmed with IT
Data Processing	Chris Hanlon	26/06/2023	Have all users changed their passwords in the last three months?	No	>

Tasks

Task Id	Task Owner	Due Date	Task Status	Description
21239	Gerard Joyce	11/11/2022	Open	Document procedure for configuring systems.
27126	Gerard Joyce	21/10/2022	Open	Address security issues reported in Penetration test on HR application

Reporting

Risk ID		Risk Description	Risk Owner	Inherent	Residual	Controls	Control Effectiveness	Tasks
◢ 71193		Confidentiality breach originating from IT failures - Consequences: - Reputation damage, - Regulatory Sanction - Claims for damages	Chris Hanlon	20	9	- Information Security policy and procedures in place. - Access control policy in place - Patching programme ensures systems kept up-to-date. User Added Controls: Server logs are reviewed regularly. IT Systemic monitoring Conduct monthly compliance checks. User Access is audited on a semi-annual basis Change Team have rolled out revised governance, which is compulsory for all initiatives with a start date from 1st April 2021 onwards. Steerco, comprising of MC and Change Team is held every month to review all "in progress" projects. A weekly update is also circulated.	5 - Highly Effective	21239 - Document procedure for configuring systems. - Open 27126 - Address security issues reported in Penetration test on HR application - Open
	31867	Security failure in a web application ()	Chris Hanlon	20	11.0	There is one person with overall responsibility for Web Applications., Application has been developed using recognised web application security techniques., On deployment, all unnecessary admin tools are removed and the server(s) hardened to prevent exploitation by would-be-attackers., There are strong role-based controls governing the level of access and functionality granted to users., A penetration test has been carried out on this application in the production environment., A vulnerability assessment on this application has been carried out in the production environment., There is a procedure in place that can be invoked if there is a security violation in this application.		
	37009	Poor Configuration Management ()	Vicki Davies	20	10.5	An inventory of all assets of which the configuration is formally controlled is maintained., The updating of all operational software and applications is only carried out by authorised administrators., There are documented procedures covering the installation of software on all operational (production) systems., There is an effective process in place that ensures technical vulnerabilities are identified and addressed in a timely manner., All system administrator and operator activity is logged., All system administrator and operator activity logs are		

Q&A

CalQRisk Overview

"With the CalQRisk solution, we are able to have a system in place to collate the risk information required into a single database, have complete overview to manage and monitor the risks with risk owners across the organisation, and provide constructive and fit-for-purpose reports to many key stakeholders in a shorter period of time"

Rola Haddad, Senior Internal Audit Specialist, Red Kite Housing