CalQRisk

GRC Summer School

There’s another spreadsheet gone!

August 2025

About Us

- Experienced Risk & Compliance Professionals
- We offer GRC software solutions and services
- Headquartered in Ireland
- Clients in various sectors across the EU and UK

FS AWARDS
CELEBRATING EXCELLENCE IN FINANCIAL SERVICES
In association with KPMG
2024 Winner
Compliance & Reg Tech Award
Presented by UCD Michael Smurfit Graduate Business School
24 OCTOBER 2024 | THE MANSION HOUSE | FSDUBLIN.COM

2024
REGTECH
100
www.RegTech100.com

NATIONAL FINTECH
AWARDS 2023
WINNER

Cyber insurance awards europe
★ 2025 ★
intelligent insurer
Proud to be a finalist
#CyberInsuranceAwardsEU
Awards Ceremony - February 5th, London

Agenda

- The Components of a GRC Programme
- The Challenges
- Sample Reporting
- Q&A

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, risk appetite and reporting cycles.

Defined incident management process which includes the logging of any risk loss events, control failures, 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.

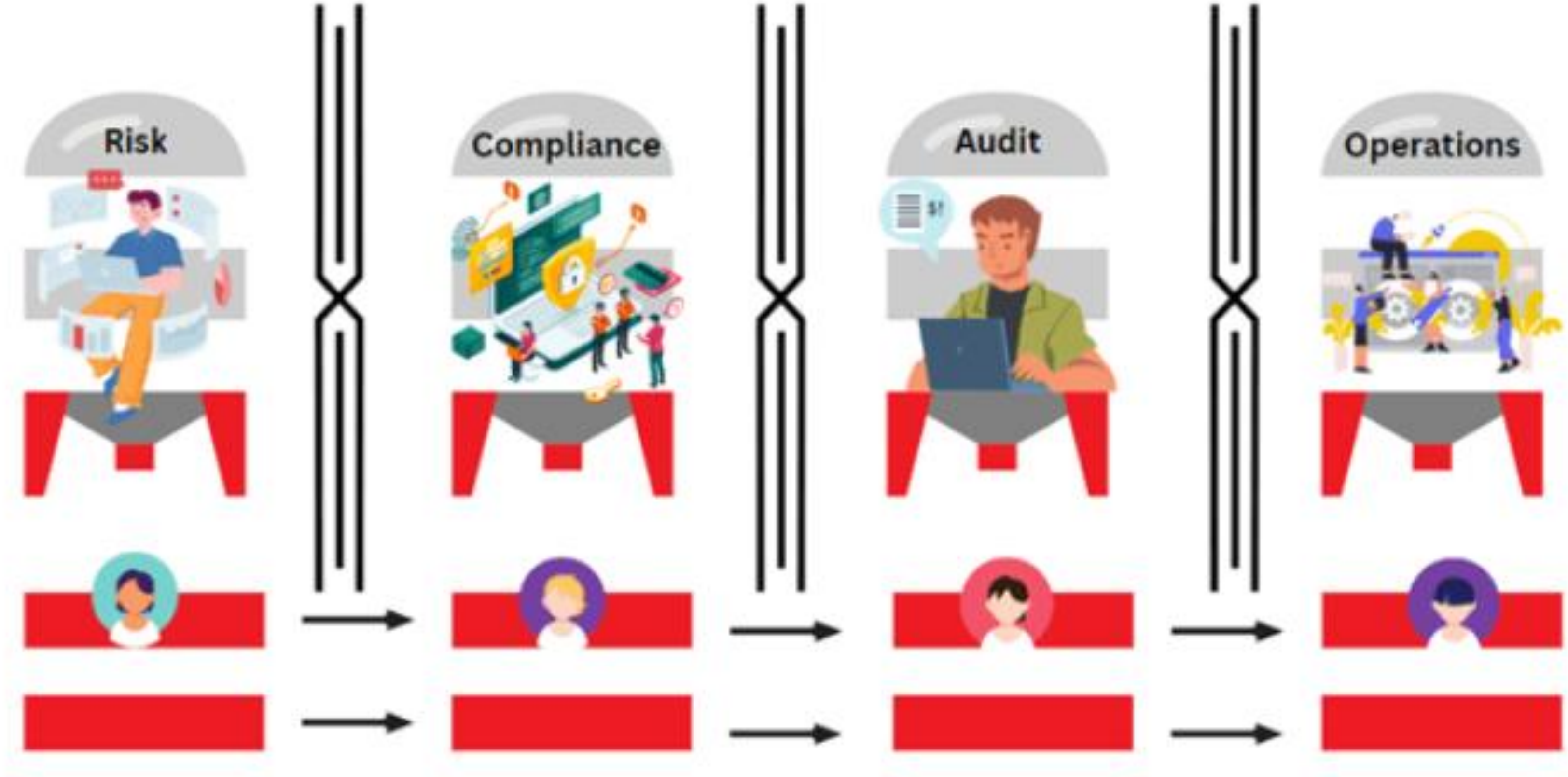
Documented compliance breach process including the tracking of corrective / preventative actions and reporting cycles.

Other Components

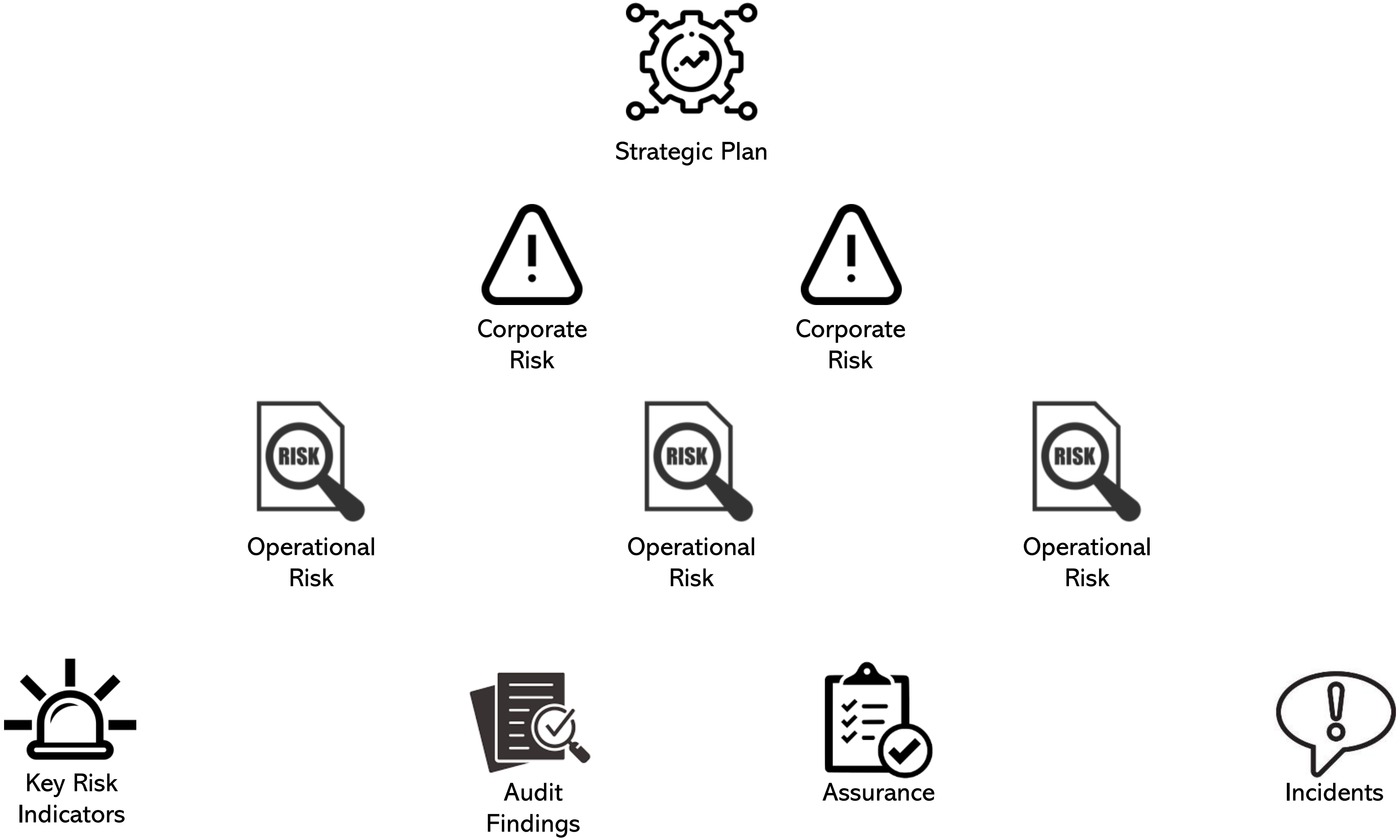
An independent audit process (internal or third party) providing assurance to the board and management team.

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

The Traditional Approach



An Integrated Approach



Strategic Plan

Corporate Risk

Corporate Risk

Operational Risk

Operational Risk

Operational Risk

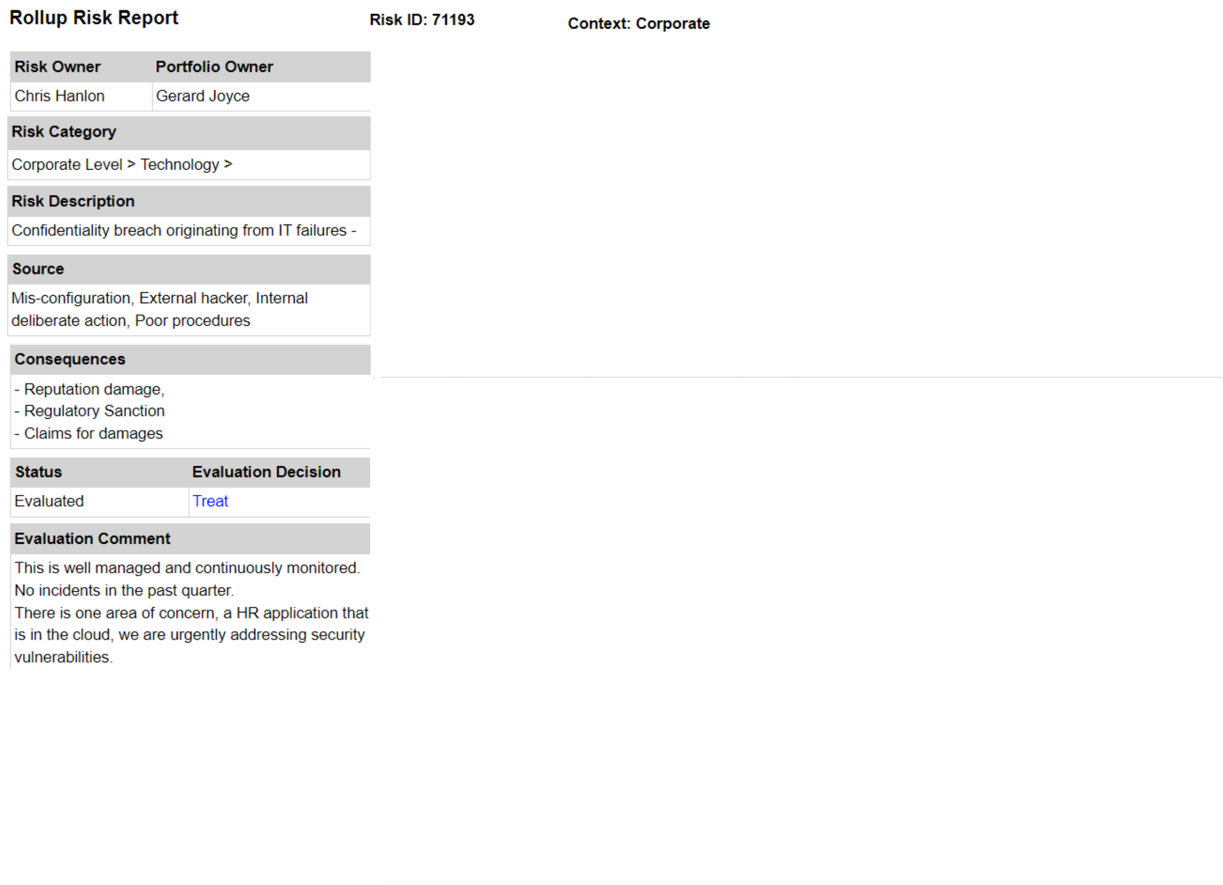
Key Risk Indicators

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

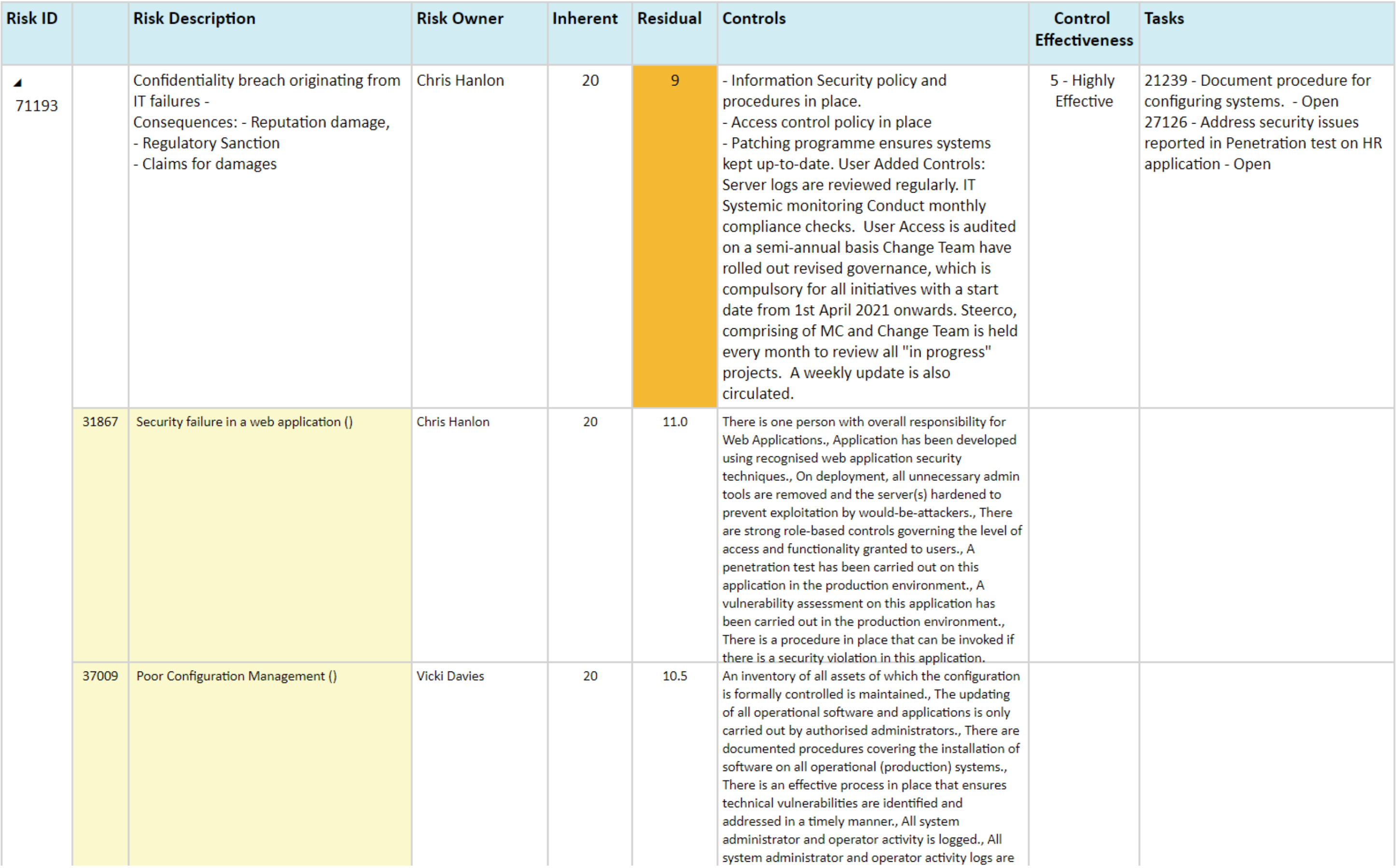
- Reputation damage,
- Regulatory Sanction
- Claims for damages

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.

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		

CONTACT US

ADDRESS

2C Western Business Park,
Shannon, Co.Clare, Ireland

E-MAIL

enquiries@calqrisk.com

TELEPHONE

+353 61 477 888

WEBSITE

www.calqrisk.com