Conducting a risk assessment on an outsourced service provider / contractor

A CalQRisk Webinar

Presented By: Gerard Joyce, CTO CalQRisk

Wednesday 8th February 2023

CalQRisk

Outline

- Introduction – Who we are
- A Risk-based Approach
- When
- Who
- What
- How
- Risk Assessment Vs Ongoing Due Diligence
- Evidence and Reporting

Who we are and what we do

- Experienced Risk & Compliance Professionals
- Members of IRM, IOB, CI (ACOI), IoD, ACCA, ISACA, ….
- We Make A Governance, Risk & Compliance Solution called CalQRisk
  - A cloud-based software solution
  - A single point of reference for risk and compliance status and control environment information
  - Contains a knowledgebase of risks and associated controls
- CalQRisk is used by 2,000+ users in regulated firms and others

  Including: Brokers, Fund Management Companies, Fund Administrators, Credit Unions, Charities, Sports Organisations, Housing Associations, Aviation, Public Sector Organisations, Solicitors, Schools, MATs and Colleges

66

" Coming together is a beginning,

staying together is progress, and

working together is success

Henry Ford

99

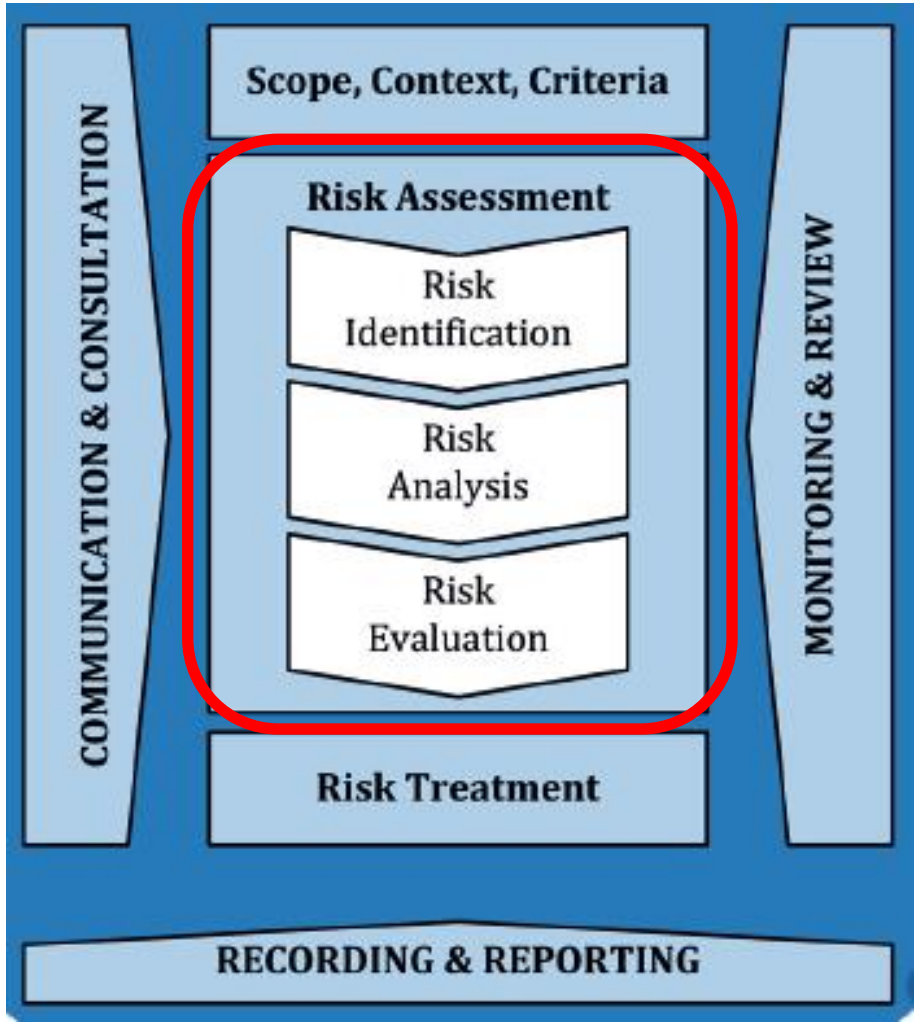
A Risk-based Approach

- Focus on what is important
- Know which are the most critical activities /functions that you have outsourced.
  - Have you “mapped” your processes?
  - Do you know which OSP/contractor is involved in each process?
  - Recovery cost / Cost to remedy
- Give the providers of these services the most attention

When to do a Risk Assessment

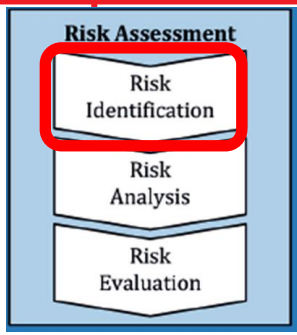
- Prior to entering an arrangement
- Whenever there is change in the arrangements
- Whenever there is change in the environment (regulatory, political,..)
- Whenever there are changes to the circumstances of the Service Provider / Contractor
- Whenever there is a serious incident / risk event

The Risk Assessment Process



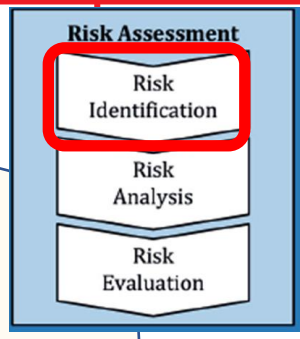
Source: ISO31000

Who is “in Scope”?



- Service Providers (IT, Facilities, Payroll, Payments, Delegates..
- Contractors (Trades, Project Mgmt, …

What are the Risks?



Extended Enterprise

OSP 1 (IT Services)

Our Co

Information Security

OSP 2 (Collections)

OSP 3 (Back Office)

Concentration Risk

OSP 4 (Payroll)

Sensitive Data

Offshoring Risk

EU

OSP 2-1 (Collections)

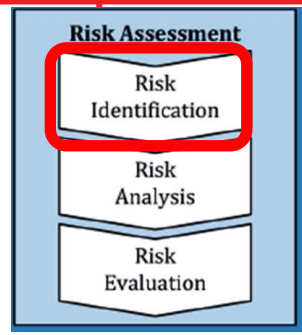
Country Risk

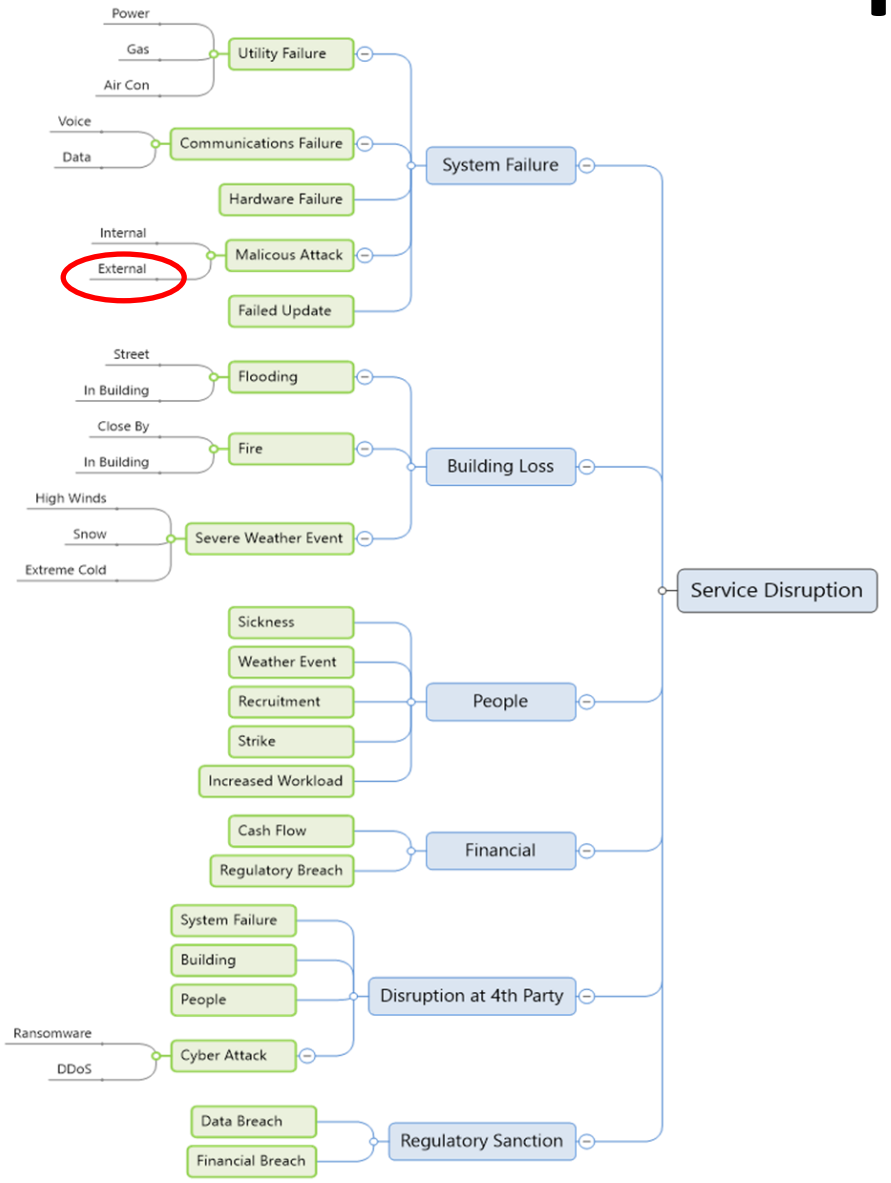
Regulatory Environment, Political, Physical Climate, Culture, Employment Conditions…

Common Risks

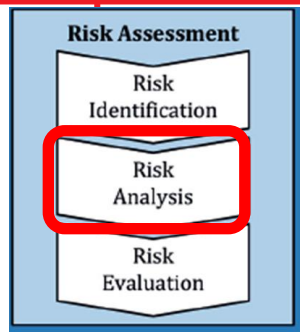
- Financial Distress
- Legal & Regulatory
- Contract & SLA
- Service Disruption
- Data Backup / Recovery
- Reputational

What can cause a Service Disruption





Business Impact Analysis Technique



Overview

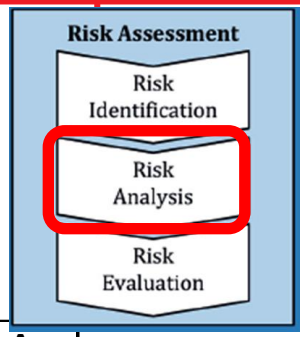
- Analyses how incidents and events could affect an organisation's operations
- Critical functions / activities are ranked and dependencies identified
- Provides understanding of capability needed to manage a disruptive incident
- Undertaken using questionnaires, interviews, workshops.

Use

- Used to determine the criticality and recovery timeframes of processes and associated resources so that appropriate response plans can be put in place.
- Helps organisations determine and select appropriate business continuity strategies to enable an effective response.

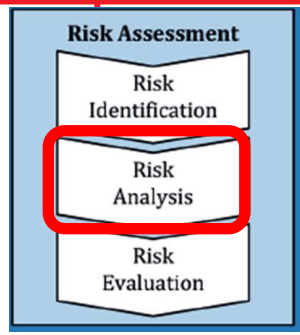
Source: ISO31010

Business Impact Analysis



Resp	Process	Comments	System Dependencies	Other Dependencies	MTO	RPO	12	24	48	Agg
Mary White	Sales / Customer Service	Customers are very demanding. Reputation damage after 24 hrs	CRM system	Acme CRM Services Internet Email	12	12	4	5	5	14
John Brown	Billing run	Total sales get posted to Billing db in the nightly run	Fin system Billing db	Internet Remote Desktop Gateway	12	1 min	3	4	5	12
Joe Grey	Pay Employees	Every 2 weeks, Agree Wed, Pay Fri Sensitive.	Sage	Payroll Co Internet ROS 1 person from 3	24	24	2	3	3	8
Bob Morley	Cash Management	AR, AP Use Bank portal Unable to pay would have reputational impact, possibly perceived as "non-compliance".	Internet Finance system	Email	48	n/a	2	3	3	8

Risk Analysis



Reduce - Pre-loss

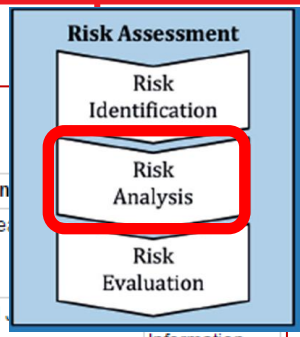
- Policies, Procedures
- Education & Training
- Design
- Communication
- Performance Measurement
- Maintenance, Review
- Alerts
- KRIs

Reduce - Post-loss

- Incident Response Procedure
- Education & Training
- Communications Plan

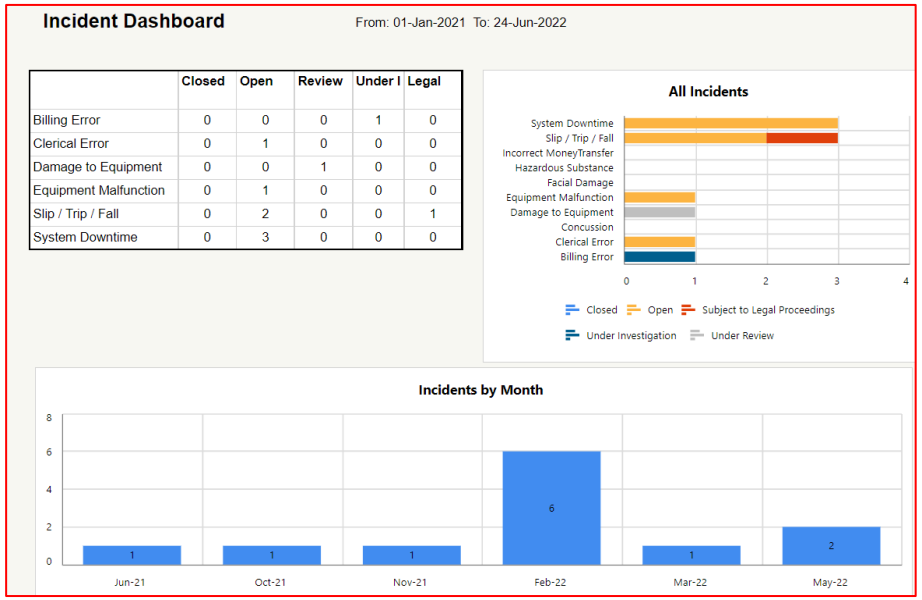
How do you Analyse the Risks?

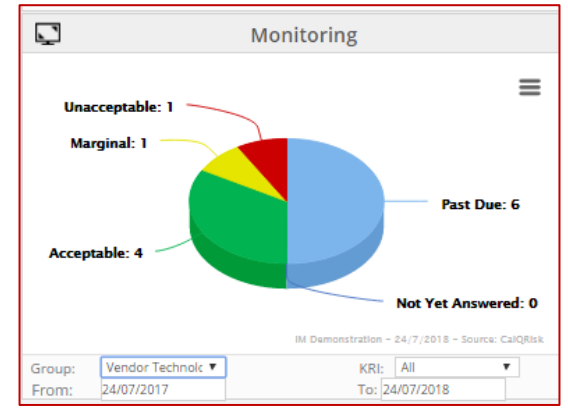
- Physical Audits
- Questionnaires
  - By key area of interest
  - What controls are in place
- Performance Review
  - Service Levels
  - Incidents / Risk Events
- Continuous Monitoring
  - Maintaining Standards



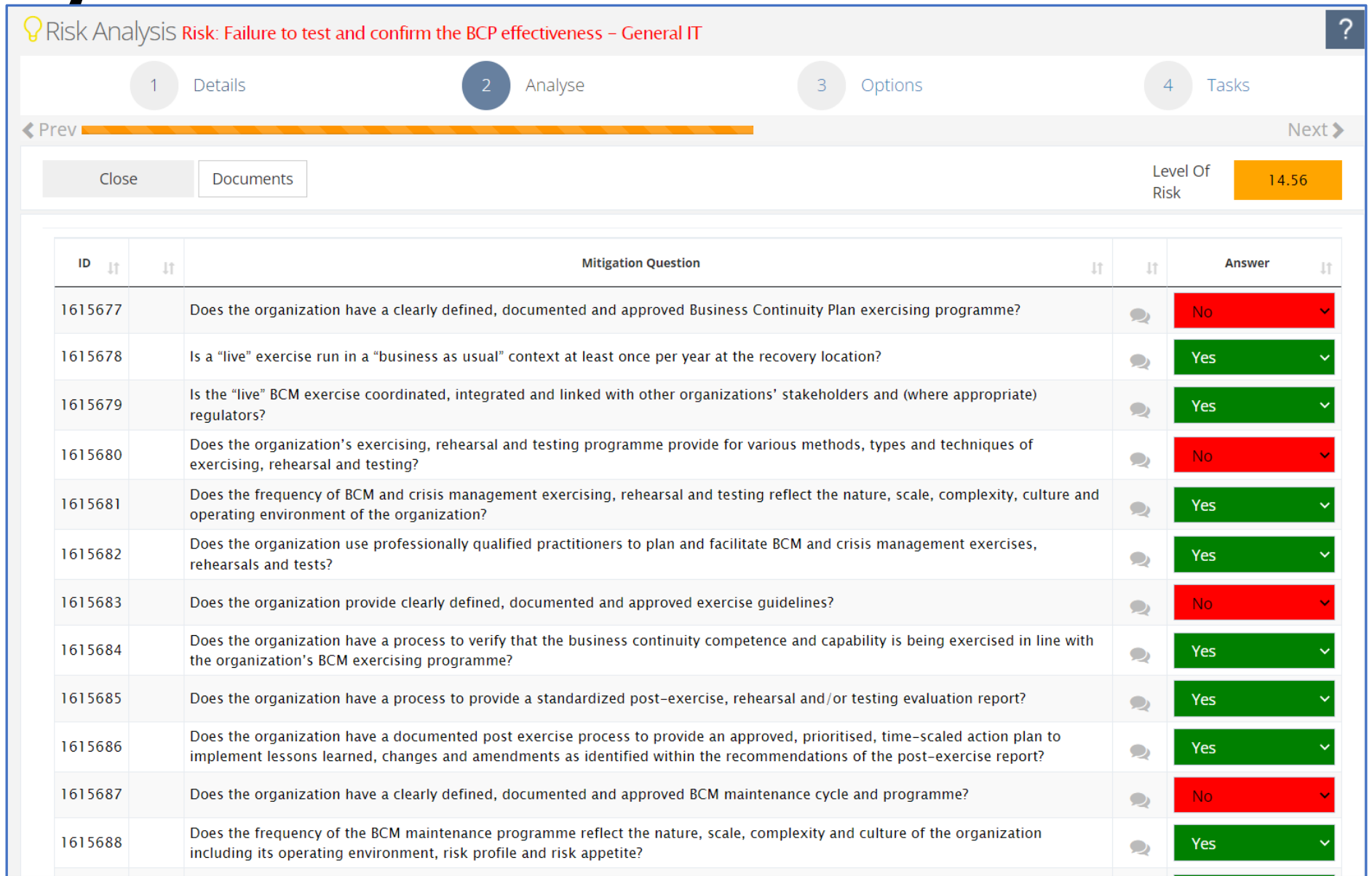
Monitoring IM Demonstration

Control Id	Ask Date	Control Question	Value	Answer Date	Comment	Respon	
25445	01/06/2017	Is there one individual in charge of information security at the firm? (If yes, write name in Comment box)	Yes	15/01/2018	Gerry Joyce	Tom He	
50850	24/07/2018	Is your Information Security Management process modelled on a recognised standard? (Please describe any NIST /ISO standard used to model IS architecture)	Yes	24/07/2018	ISO 27001	Gerard	Information Security
50855	24/07/2018	Do you have the right to audit your critical service providers? (Please enter date of last audit in the comment box)	No	24/07/2018	They supply certified copies of audits	Gerard Joyce	Client Information Security
50857	24/07/2018	Do you actively identify relevant best practices regarding cybersecurity for your business model? (If yes, explain how)	Yes	24/07/2018	Subscribe to several online advisory sites and maintain up-to-date knowledge of best practice in that way.	Gerard Joyce	Client Information Security

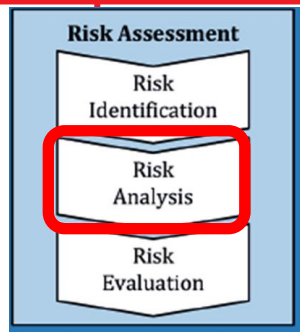




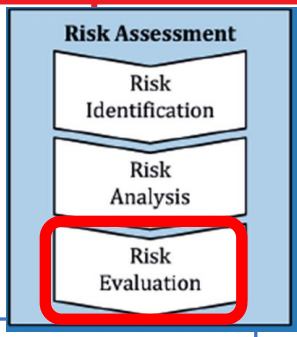
Analyse the Risks



ID		Mitigation Question		Answer
1615677		Does the organization have a clearly defined, documented and approved Business Continuity Plan exercising programme?		No
1615678		Is a "live" exercise run in a "business as usual" context at least once per year at the recovery location?		Yes
1615679		Is the "live" BCM exercise coordinated, integrated and linked with other organizations' stakeholders and (where appropriate) regulators?		Yes
1615680		Does the organization's exercising, rehearsal and testing programme provide for various methods, types and techniques of exercising, rehearsal and testing?		No
1615681		Does the frequency of BCM and crisis management exercising, rehearsal and testing reflect the nature, scale, complexity, culture and operating environment of the organization?		Yes
1615682		Does the organization use professionally qualified practitioners to plan and facilitate BCM and crisis management exercises, rehearsals and tests?		Yes
1615683		Does the organization provide clearly defined, documented and approved exercise guidelines?		No
1615684		Does the organization have a process to verify that the business continuity competence and capability is being exercised in line with the organization's BCM exercising programme?		Yes
1615685		Does the organization have a process to provide a standardized post-exercise, rehearsal and/or testing evaluation report?		Yes
1615686		Does the organization have a documented post exercise process to provide an approved, prioritised, time-scaled action plan to implement lessons learned, changes and amendments as identified within the recommendations of the post-exercise report?		Yes
1615687		Does the organization have a clearly defined, documented and approved BCM maintenance cycle and programme?		No
1615688		Does the frequency of the BCM maintenance programme reflect the nature, scale, complexity and culture of the organization including its operating environment, risk profile and risk appetite?		Yes



Reporting: Risk Register



Third Party Risks

Third Party		Risk ID	Risk Description	Level	Risk Owner	Last Assessed
92	General IT Service Providers	81213	Personal identifiable data breach (General IT)	6.0	Eimear Farrell	20/10/2021
		81292	Failure to test and confirm the BCP effectiveness (General IT)	15.0	Tom Healy	20/10/2021
102	COM IT	31881	Failure to prevent unauthorised access to systems and information (Ennis HQ)	8.6	Gerard Joyce	20/06/2022
		81214	Personal identifiable data breach (COM IT)	9.0	Eimear Farrell	20/10/2021
		81217	Failure of a suppliers supplier (PC Services)	6.3	Tom Healy	20/10/2021
110	Payroll Co Ltd	47043	Failure to test and confirm the BCP effectiveness (Payroll Co Ltd)	7.2	Tom Healy	11/07/2022
		58026	Data Processing contract / legal agreement not appropriate (Payroll Co Ltd)	6.3	Tom Healy	11/07/2022
		81222	Failure of a Cloud service provider to deliver service (Payroll Co Ltd)	12.2	Tom Healy	11/07/2022
		81293	Inappropriate processing of personal data (Payroll Co Ltd)	11.0	Tom Healy	11/07/2022
230	Sample Contractor	58023	Inappropriate processing of personal data (Customer Data)	9.3	Tom Healy	28/06/2022
		90672	Data Processing contract / legal agreement not appropriate (Sample Co)	7.1	Tom Healy	12/07/2022

Regulator Reporting

Internal Reference No.	Start Date of the contract	Date of next contract renewal	End date of contract	Notice period for the institution (in Months)	Notice period for service provider (in Months)	Category of Service	Category of the outsourcing service provider	Description of the outsourced function	Transfer or processing of personal data	Location(s) of the data	Country/countries of provision of services	Critical or Important	Reasons for criticality or importance	Last date of assessment of criticality or importance
10	**170**	**180**	**190**	**200**	**210**	**220**	**IE080**	**230**	**240**	**250**	**260**	**270**	**280**	**290**

Start date of the contract / written agreement	**170 (Refer to worksheet R01)**	Date	Date of entry into force of the agreement (dd/mm/yyyy) as stipulated in the contract / written agreement. For Not Applicable values report 01/01/4444 For Not Available values report 01/01/6666 For the first submission, only include contracts / written agreements with a start date before the reference date (31/12/2021) The column cannot be left blank.
Date of next contract / written agreement renewal	**180 (Refer to worksheet R01)**	Date	Date (dd/mm/yyyy) of contract renewal as stipulated in the contractual agreement / written agreement or as planned by the parties. For Not Applicable values report 01/01/4444 For Not Available values report 01/01/6666 The column cannot be left blank.
End date of the contract	**190 (Refer to worksheet R01)**	Date	Date (dd/mm/yyyy) as stipulated in the contractual agreement / written agreement. For Not Applicable values report 01/01/4444 For Not Available values report 01/01/6666 The column cannot be left blank.
Notice period(s) for the institution	**200 (Refer to worksheet R01)**	Decimal	Notice period(s) for terminating the contract / written agreement by the outsourcing entity/entities in months. This field allows decimal values only. So for example populate 1 for one month or 1.5 for one and a half months' notice period etc.

From CBI Guidance Note: Outsourcing Register Template

Risk Assessment Vs Ongoing Due Diligence

Risk Assessment

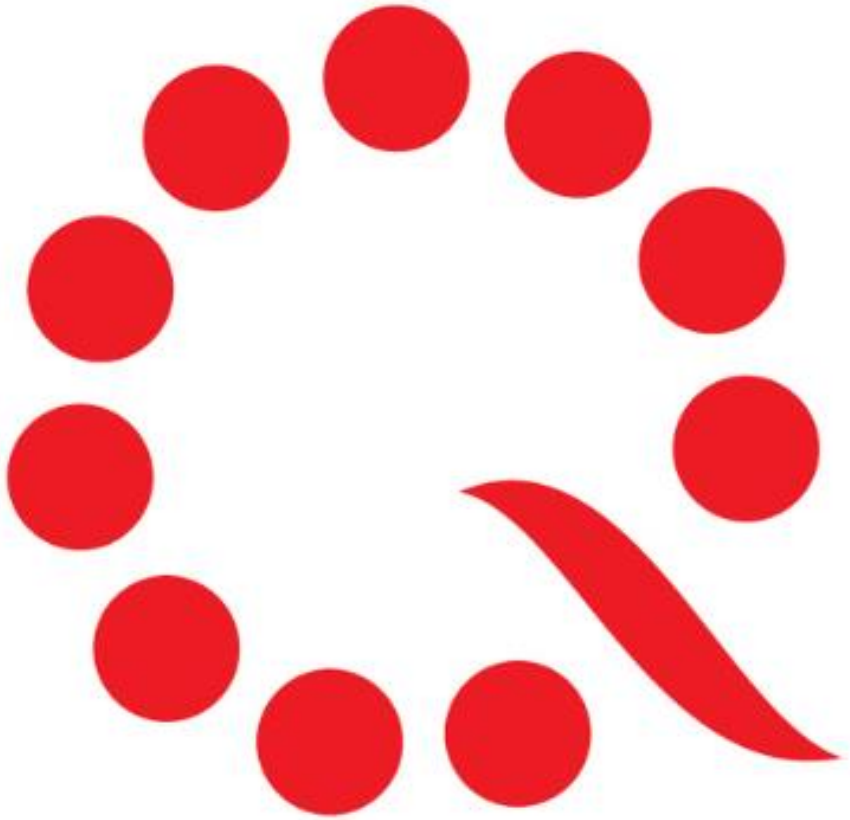
- Part of Risk Management Framework
- Focus is on what could threaten your objectives
- Treat the Service Providers as an extension of your organisation

Ongoing Due Diligence / Monitoring

- Monitor relevant Key Risk Indicators (e.g. # Incidents, Uptime)
- Ability to meet your requirements.. Key Performance Indicators
- Financial standing
- Business Continuity testing

Takeaways

- List critical activities and their dependencies
- List of Service Providers / contractors that you regularly deal with
- Identify "4th Parties" that are involved
- Identify the Risks associated with each SP / Contractor
- Understand the Controls in place to manage the risks
- Monitor SLA Adherence
- Monitor for any changes in the environment
- Update your risk assessments



Questions ?

gjoyce@calqrisk.com

Linkedin.com/company/calqrisk

Twitter.com/calqrisk

CalQRisk