# How to Conduct a Third-Party Risk Assessment

*A CalQRisk Webinar*


Thursday, 14th July 2022

Presented by:
Gerard Joyce, CTO, CalQRisk

# Outline

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

# Who we are and what we do

CalQRisk
Manage the effect of uncertainty on objectives

- 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

" **Know what you're getting into, before you get into it**

Warren Buffett

# Risk Assessment Vs Due Diligence

CalRisk
Manage the effect of uncertainty on objectives


**Due Diligence**

- Mostly before you enter into an arrangement
- Authorisation, Capacity and Ability to meet your requirements
- Alignment with your risk appetite, culture, ethical values & behaviour
- IT Security

**Risk Assessment**

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

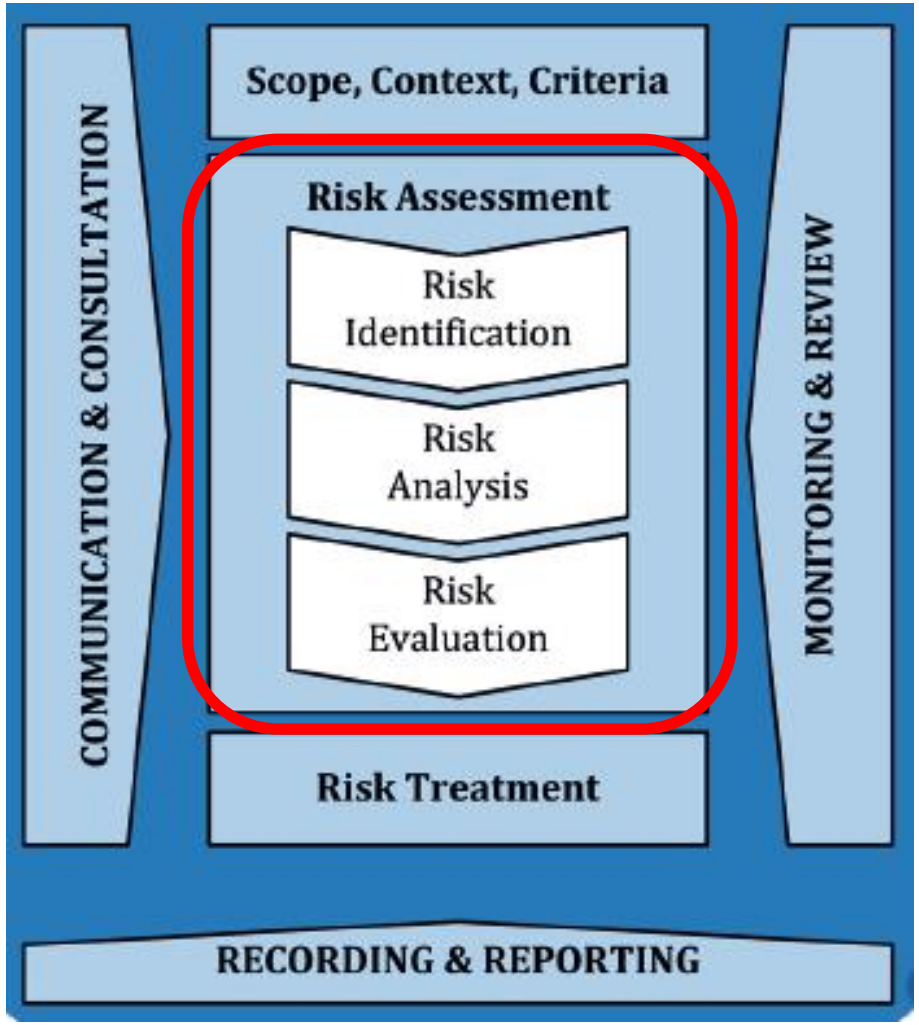
# A Risk-based Approach

- Focus on what is important
- Know which are the most critical activities and give the providers of these services the most attention
- Don’t overlook key suppliers of the non-service items

# 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 Third Party

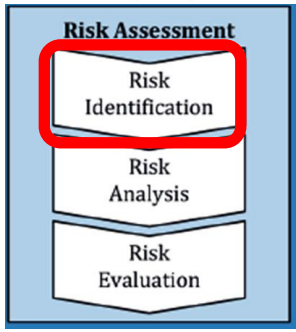
# The Risk Assessment Process




Source: ISO31000

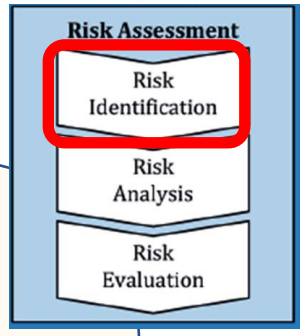
# Who are your Third Parties?

CalQRisk
Manage the effect of uncertainty on objectives




- Service Providers (IT, Facilities, Payroll, Payments, Delegates..
- Agents
- Suppliers (Utilities: Power, Gas, Internet, Communications,..
- Contractors (Trades, Project Mgmt, …

# What are the Risks?




Extended Enterprise

OSP 1 (IT Services)

Our Co

Supplier X (Fuel)

Supply Chain Risk

Information Security

Concentration Risk

Sensitive Data

OSP 2 (Collections)

OSP 3 (Back Office)

OSP 4 (Payroll)

Offshoring Risk

EU

OSP 2-1 (Collections)

Country Risk

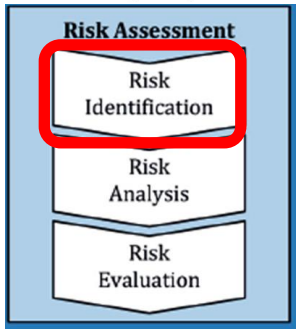
Regulatory Environment, Political, Physical Climate, Culture, Employment Conditions…

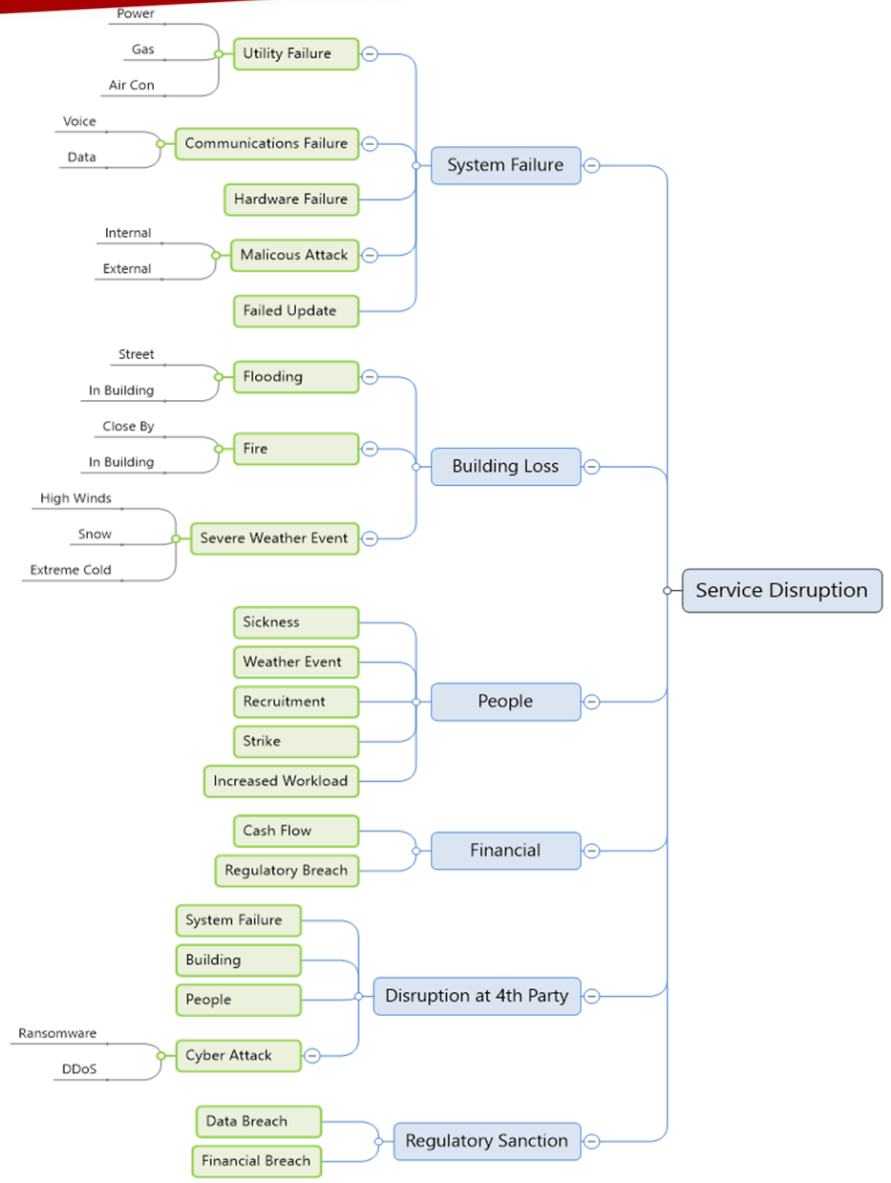
**Common Risks**

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

# What can cause a Service Disruption

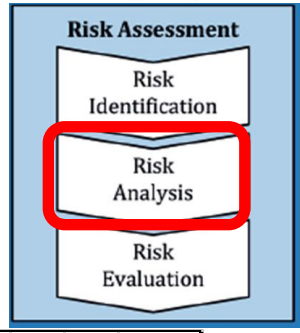
CalRisk
Manage the effect of uncertainty on objectives



# Business Impact Analysis

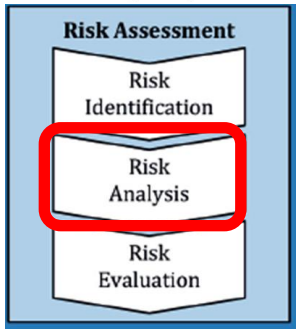
CalRisk
Manage the effect of uncertainty on objectives




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

# Risk Analysis

CalRisk
Manage the effect of uncertainty on objectives




**Reduce - Pre-loss**

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

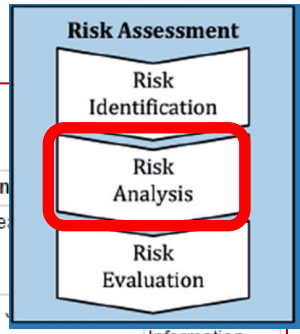
**Reduce - Post-loss**

- Incident Response Procedure
- Education & Training
- Communications Plan

# How do you Analyse the Risks?

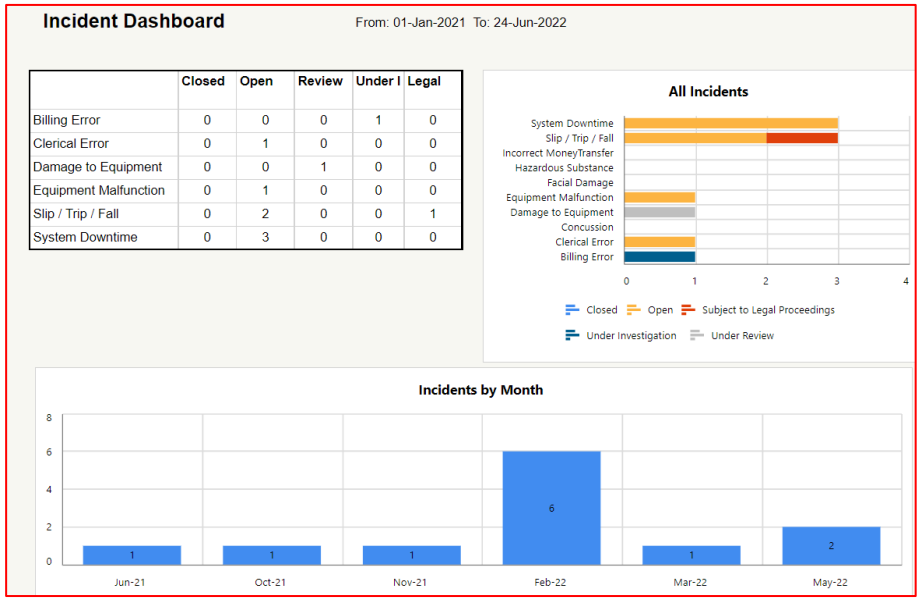
CalQRisk
Manage the effect of uncertainty on objectives

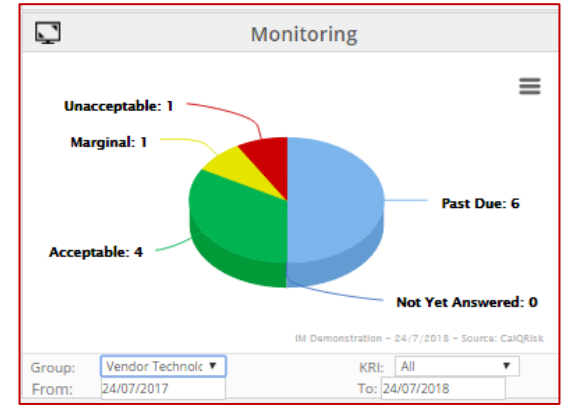
- Physical Audits
- Questionnaires
  - By key area of interest
  - What controls are in place
- Performance Review
  - Service Levels
  - Incidents / Risk Events
- Continuous Monitoring
  - Maintaining Standards




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

CalQRisk
Manage the effect of uncertainty on objectives


Risk Analysis Risk: Data Processing contract / legal agreement not appropriate – Payroll Co Ltd ?

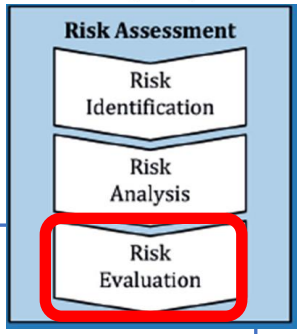
1 Details 2 Analyse 3 Options 4 Tasks

Prev Next

Close Documents Level Of Risk 6.3

| ID | | Mitigation Question | | Answer |
|---|---|---|---|---|
| 1182001 | i | Is there a formal, contract, or other legally binding act, in place with the data processor? | | Yes |
| 1182002 | i | Is the contract / legal agreement documented in writing or electronic form? | | Yes |
| 1182003 | i | Are all outsourced data processing activities governed by the contract / agreement? | | No |
| 1182004 | | Does the contract / legal agreement clearly document the services to be provided and the expected level of service? | | Yes |
| 1182005 | | Has the contract / legal agreement been formally reviewed by competent, qualified professionals? | | Yes |
| 1182006 | | Are informal alterations, modification or exemptions from **any** of the terms of contracts forbidden? | | Yes |
| 1182007 | | Is there one competent person with overall responsibility for the supervision of this contract? | | Yes |
| 1182008 | | Have formal communication channels between the organisation and the processor been established and communicated to all relevant personnel? | | Yes |
| 1182009 | i | Does the contract / agreement preclude the processor from engaging another processor without your (the contractor's) prior specific or general written authorisation? | | No |
| 1182010 | i | Does the contract / legal agreement stipulate that the processor must inform you (the contractor) of any intended changes concerning the addition or replacement of other processors, thus giving you the opportunity to object to such changes? | | Yes |
| 1182011 | i | Does the contract / legal agreement set out the subject-matter and duration of the processing? | | Yes |
| 1182012 | i | Does the contract / legal agreement set out the nature and purpose of the processing? | | No |
| 1182013 | i | Does the contract / legal agreement set out the type of personal data and categories of data subjects? | | Yes |
| 1182014 | i | Are your rights and obligations as a data controller set out in the contract / legal agreement? | | 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 |

# Evidence

- List of Third Parties that you regularly deal with
- List of Risks associated with each Third Party
- Description of the Controls in place to manage the risks
- SLA Adherence
- Results of regular Monitoring
- Plans to maintain knowledge and understanding up to date
- Regular Communication

# Questions ?

CalQRisk
Manage the effect of uncertainty on objectives

**Thank You**

gjoyce@calqrisk.com