So you want to be Resilient?

CalQRisk

Manage the effect of uncertainty on objectives

Presented by:
Gerard Joyce, CTO, CalQRisk
December 13th 2022

Outline

- Introduction
- What is Business Continuity
- What is Resilience
- The five key elements of resilience
- Building and Sustaining resilience
- Managing your Third Parties
- Reporting / Demonstrating Resilience
- 5 Things you can do now

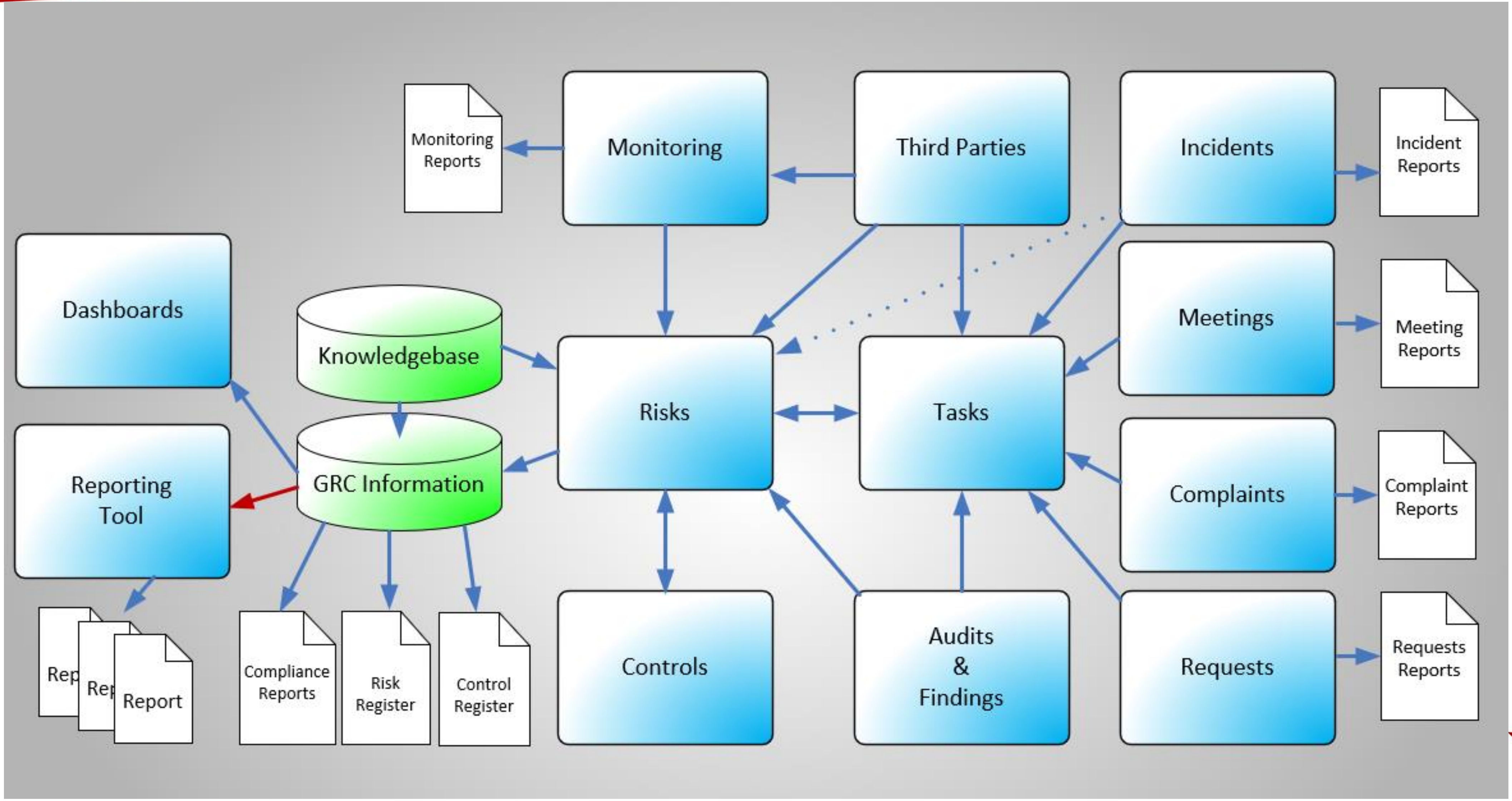
> **Survival is not Compulsory**
>
> *Kevin Knight (former ISO Risk Committee Chair)*

Introduction

- Experienced Risk & Compliance Professionals
- Members of IRM, CI (ACOI), IoB, IoD, ACCA, ISACA..
- Involved in the Development of Standards (ISO 31000)
- We supply a Governance, Risk & Compliance Software Solution called **CalQRisk**
- CalQRisk is used by 200+ regulated Organisations
  - Financial Services sector, Not-for-Profit sector

CalQRisk Platform

CalQRisk
Manage the effect of uncertainty on objectives



What is Business Continuity?

CalRisk
Manage the effect of uncertainty on objectives

"capability of the organization to continue delivery of services or products at acceptable predefined levels following disruptive incidents" Source ISO 22300

Business continuity processes are designed:

- to ensure that if a disruption does occur key systems and business processes are recovered within agreed timeframes
- to ensure one can maintain essential services during disruptions
- to assist staff in the event of an incident

What is Resilience?

The ability to deliver critical operations through disruption. (Basel Committee)

An outcome of multiple functions:

- Risk Management
- Information Security (includes Cyber Security)
- Incident Management (including Crisis Leadership)
- Business Continuity
- IT Disaster Recovery

The goal is to have as few as possible incidents and to keep the “outage” as short as possible

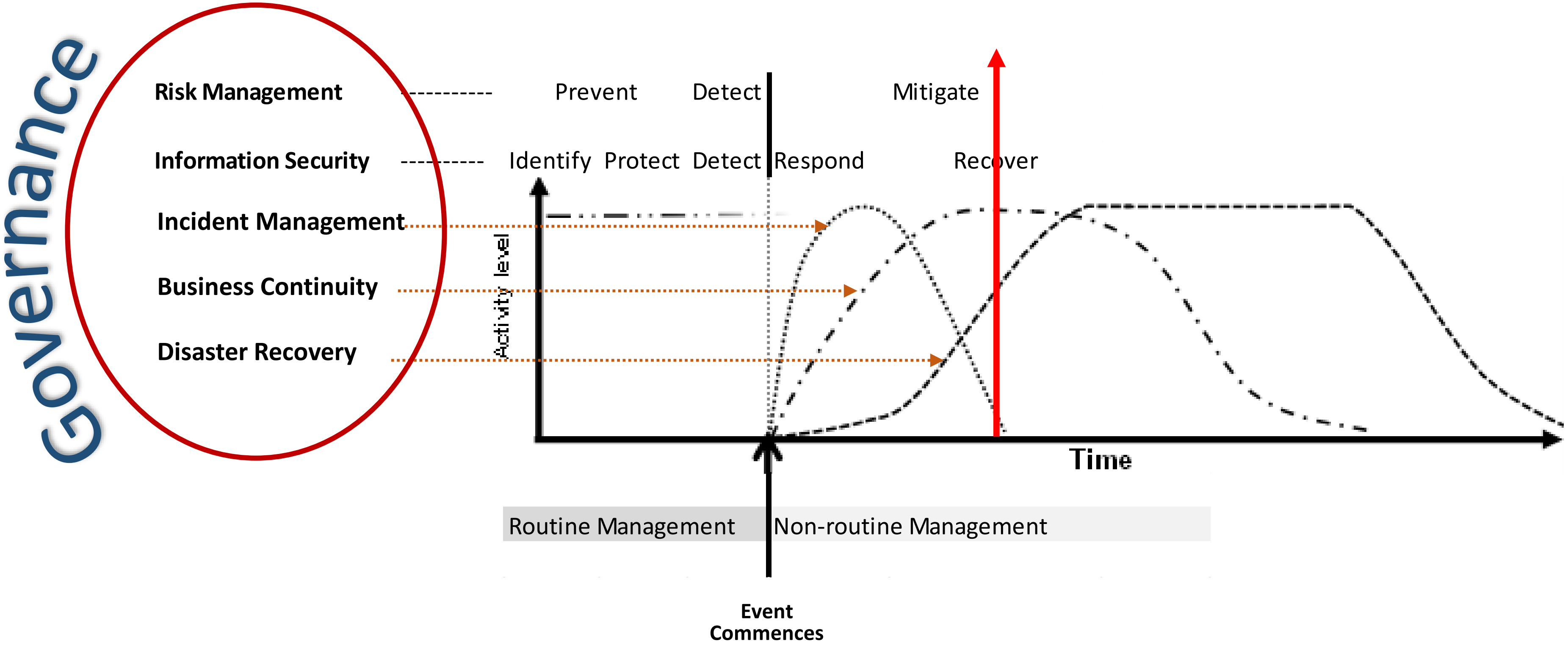
DORA

The Digital Operational Resilience Act (DORA)

This directive aims to reduce the vulnerabilities and strengthen the physical resilience of critical entities….

…. They need to be able to **prepare** for, **cope** with, **protect** against, **respond** to and **recover** from natural disasters, terrorist threats, health emergencies or hybrid attacks.

Resilience Components



Governance

Risk Management ---------- Prevent Detect Mitigate

Information Security ---------- Identify Protect Detect Respond Recover

Incident Management

Business Continuity

Disaster Recovery

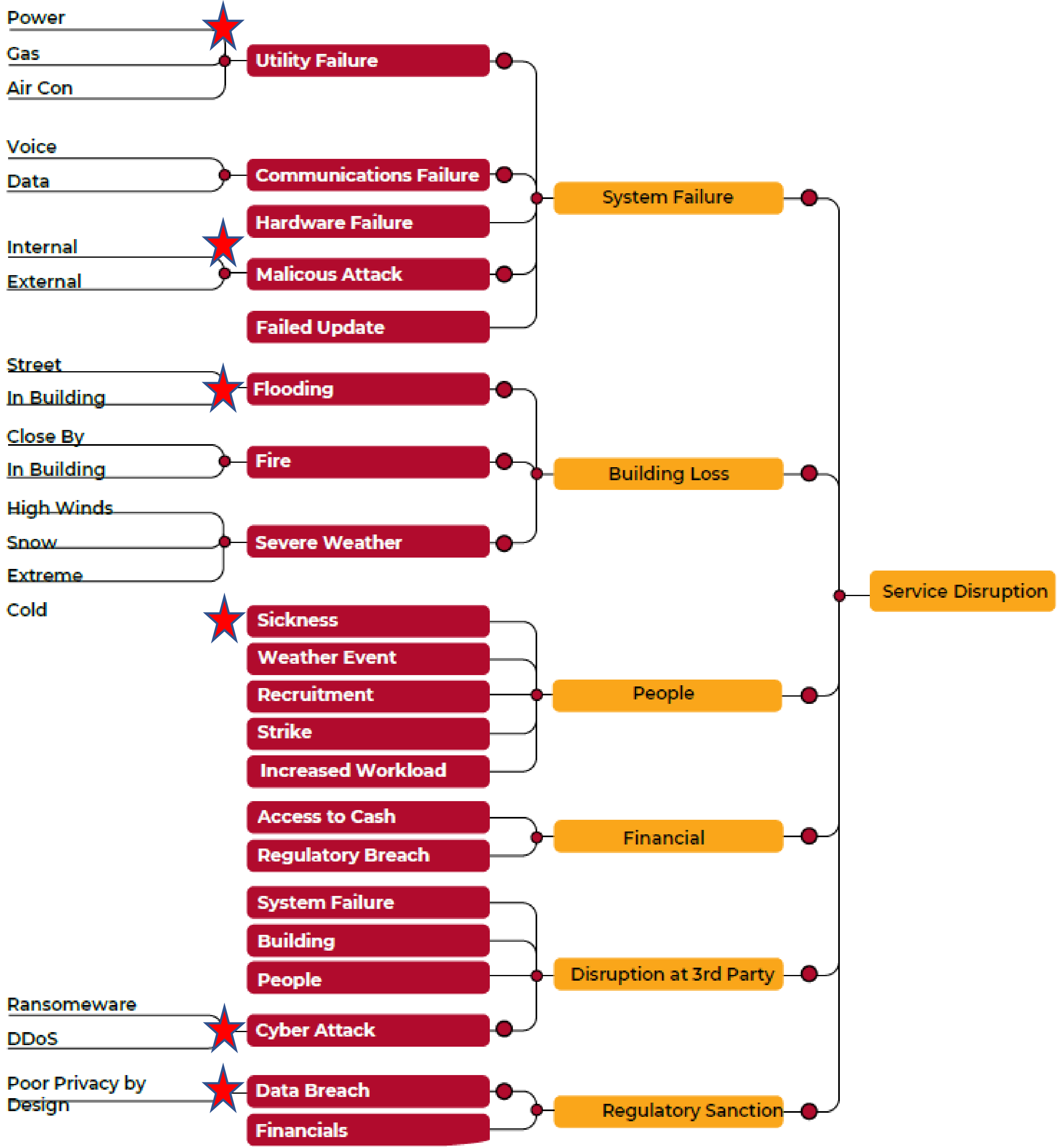
Routine Management | Non-routine Management

Event Commences

Disruptive Incidents

CalRisk

Manage the effect of uncertainty on objectives



Power
Gas
Air Con
Utility Failure

Voice
Data
Communications Failure

Hardware Failure

Internal
External
Malicous Attack

Failed Update

System Failure

Street
In Building
Flooding

Close By
In Building
Fire

High Winds
Snow
Extreme
Cold
Severe Weather

Building Loss

Sickness
Weather Event
Recruitment
Strike
Increased Workload

People

Access to Cash
Regulatory Breach

Financial

System Failure
Building
People

Ransomeware
DDoS
Cyber Attack

Disruption at 3rd Party

Poor Privacy by Design
Data Breach
Financials

Regulatory Sanction

Service Disruption

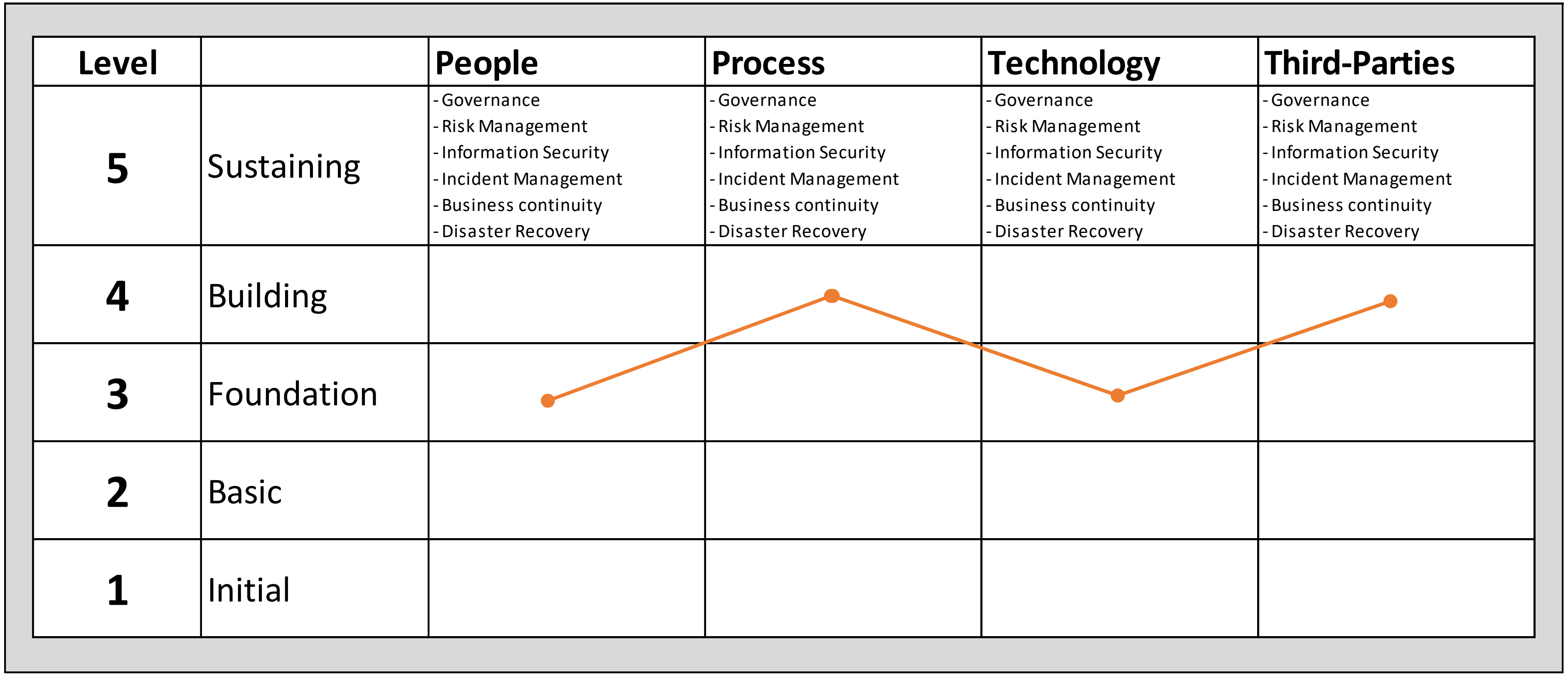
What is a Maturity Model?

Level	CQR	CMMI
5	Sustaining	Optimising
4	Building	Quantitatively Managed
3	Foundation	Defined
2	Initial	Managed
1	Ad hoc	Initial

Original Concept

A **maturity model** is a tool that helps people assess the current effectiveness of a person or group and supports figuring out what **capabilities** they need to acquire next in order to improve their performance

CalQRisk Maturity Model



Level		People	Process	Technology	Third-Parties
5	Sustaining	- Governance - Risk Management - Information Security - Incident Management - Business continuity - Disaster Recovery	- Governance - Risk Management - Information Security - Incident Management - Business continuity - Disaster Recovery	- Governance - Risk Management - Information Security - Incident Management - Business continuity - Disaster Recovery	- Governance - Risk Management - Information Security - Incident Management - Business continuity - Disaster Recovery
4	Building		●		●
3	Foundation	●		●	
2	Basic				
1	Initial				

Governance

	Foundation	Building	Sustaining
People	The Board and top management are committed to enhance organizational *resilience* At least one Board member has sufficient knowledge to provide oversight of Resilience arrangements. The behaviour of individuals is aligned with a shared vison and purpose.	All Board member have sufficient knowledge to provide oversight of Resilience arrangements. Adequate resources are provided to enhance resilience. Roles and responsibilities in the different disciplines have been established and assigned.	Board members have good understanding, board includes one specialist. Senior executive responsible. All management disciplines are coordinated to ensure optimum contribution to resilience. Vision and purpose is reviewed and revised in response to external and internal changes.
Process	Resilience Framework developed	There are appropriate governance structures in place to achieve effective coordination of organisational resilience activities. Framework is aligned to Risk Management framework. Priority is given to activities that reduce single-points of failure.	Framework developed, aligned, approved, reviewed and tested. Monthly updates received. Information used in decision making. Resilience arrangements are evaluated at least annually.
Technology	Knowledge and information is created, retained and applied through established systems and processes and shared in a timely manner with all relevant interested parties.	There are systems in place that support the effective implementation of organizational resilience activities.	Systems are utilised to enhance communication, coordination, and cooperation between management disciplines of the organisation to build a coherent approach to resilience.
Third-Parties	The organisation actively collaborates with relevant interested parties to support the delivery of the organization's purpose and vision. There is a robust outsourcing policy in place.	Key third-parties that are essential to the delivery of critical activities have been identified and resiliency requirements are extended to cover their operations.	Resiliency arrangements at all key third-parties are reviewed at least annually.

Risk Management Pillar

	Foundation	Building	Sustaining
People	Individual managers taking responsibility for risks in their area or responsibility.	Senior manager with responsibility for RM appointed. Resources identified in annual budget. Consistent understanding of risk among managers. Risk treatment prioritisation agreed at senior level.	All senior managers support RM policy. Individuals are aware of their roles and responsibilities. Training programme in place to maintain skills. People encouraged to report incidents / near misses. Company-wide understanding of interdependencies.
Process	Risk Management policy is in place. Risk Management process applied in key areas. Risk Management priorities are informed by the organisational objectives.	Company-wide agreement on Risk Criteria. Agreed risk management process applied across the organisation. Risks are collated and a single report is presented to senior management. Risk information, including control effectiveness, is used in decision-making.	Risk Management is embedded in Strategic Planning. Business processes have been mapped and interdependencies have been identified. Gaps in controls have been identified and remediation has been implemented. Maximum tolerable duration of impacts agreed, aligned with risk appetite.
Technology	Individuals maintaining risk information within their own area.	Central register of risks is maintained with a consistent method of measurement of likelihood and context.	Risk Identification and assessment captured in database. Risk register maintained and updated regularly. Regular reports generated from single source of information. Priorities identified. Treatments recorded. Progress tracked.
Third-Parties	All outsourcing partners have been identified and the service they provide has been categorised. (Critical / non-critical)	Risk assessments are carried out on an annual basis on all critical third-parties.	Outsourcing policy documented and applied. Risk assessment carried out on all proposed third-party engagements. Business processes have been mapped and dependencies on third-parties have been identified. Third-party operations are reviewed at least annually.

Information Security Pillar

	Foundation	Building	Sustaining
People	Responsibilities for information processing facilities are clearly defined and allocated. Staff screening is conducted upon employment. Contractors are screened same as employees. All employees, at all levels, are given basic information security awareness training.	Further screening is conducted when senior or privileged roles are filled. Information security awareness training is refreshed on an annual basis.	Senior executive appointed with responsibility for information security. All roles and responsibilities defined and allocated. Checks carried out on all employees throughout their employment at regular intervals. Information security awareness is checked via questionnaires / online tools.
Process	A comprehensive Information security policy is in place. Operating procedures for information processing facilities have been documented. There is an effective process in place that ensures technical vulnerabilities are identified and addressed in a timely manner.	Security strategy documented. Policies and procedures developed. Event information from critical systems is collected and analysed in real time. Vulnerability remediation is validated and assured. Remote access requires strong authentication.	The organisation operates a strategic programme of threat intelligence-led end-to-end penetration tests. Control effectiveness is assessed. Baseline patterns of network activity have been recorded and documented. MI is used to inform decision making.
Technology	Inventory of information assets is maintained. Baseline security standards are documented and applied. Data and systems are backed up and encrypted. The organisation proactively monitors access to ingress/egress points. Firewalls are regularly updated.	Systems are checked at set intervals for compliance against baseline standards Copies of data are retained off the network / off-site. Information security is considered as part of all changes to critical systems. The corporate network is segregated effectively and protected from externally facing systems.	All assets are monitored on an continuous basis for compliance with agreed standards. End of life assets identified and effectively managed. Information security is considered as part of all changes to all systems. Effectiveness of security controls is independently assessed on an annual basis.
Third-Parties	All data that is stored on third-party systems has been identified and classified. Agreements with third-parties include information security requirements. Third-parties understand their roles and responsibilities.	Third-parties are routinely assessed to confirm they are meeting their contractual obligations. Third party access to critical infrastructure and information is understood, and proportionate controls have been implemented.	Any changes in relationships with third-parties is captured in updated agreement. Third party access to infrastructure and information is identified and documented.

Incident Response Pillar

	Foundation	Building	Sustaining
People	A communications plan exists which is designed to be used for all incidents. Individual roles during an incident have been defined and allocated.	A stakeholder map has been developed for use in a cyber incident. Scenario tests have been conducted to familiarise individuals with their roles.	Incident communications plans are tested annually. Alternates have been identified for each critical role in responding to an incident. Information is shared with external stakeholders.
Process	An incident response plan is in place. Cyber threat intelligence is used to inform situational awareness and contextual understanding. Defined thresholds exist to help determine the response to an incident. Processes are in place to carry out investigations following an incident where required.	The incident response plan has been tested for different scenarios. Cyber threat intelligence is actionable, timely and used to support specific stakeholders. Thresholds and responses are documented and agreed with stakeholders. Processes are in place to carry out forensic analysis.	The firm conducts a lessons learned exercise as part of the incident review process. Thresholds are reviewed on a regular basis or after an event/incident. Protective and detective controls are specifically engineered to facilitate the investigative process.
Technology	Event information from critical systems is collected in real time. Alerts from detection systems are actioned during business hours. Successful remote access to critical systems is monitored and malicious activity is flagged.	The integrity of event information is protected. Detection systems are linked directly to the incident response process. Available 24/7 All remote access attempts to critical systems are monitored.	Automated alerting from all systems. Protective and detective controls are specifically engineered to facilitate the investigative process. All remote access attempts to all systems are monitored.
Third-Parties	The roles of third-parties in an incident response have been documented and allocated.	Scenario exercises have been conducted in partnership with key third-parties.	Third-parties who can assist with communications, forensic analysis and legal issues have been identified and are ready to respond if / when required.

Business Continuity Pillar

	Foundation	Building	Sustaining
People	The CEO is actively involved in the BC planning process. Senior management is involved in the design of the Business Continuity management programme. There is a remote working policy in place.	HR policies address the business need for the provision of essential services and continuity of operation. Roles and responsibilities for implementation of the Business Continuity programme are clearly assigned. There are established communication channels for employees working from home.	The Business Continuity Management programme is fully supported by senior management. Strategies for maintaining core skills and knowledge that are essential for critical activities / processes have been identified. Individuals and alternates have been identified for key roles in a BC scenario.
Process	Critical Services identified and prioritised. Business Continuity solutions have been developed for all mission critical activities / processes.	Business Continuity plan in place and aligned with resilience framework. Impact tolerances developed, approved and tested using scenario testing. A significant number of employees have been involved in a BC exercise.	Plans are reviewed, tested and updated annually. Command and Control capability has been tested.
Technology	An IT recovery strategy for mission critical applications has been developed. The organisation's policy on access control is maintained in a BC scenario.	Procedures to restore individual systems are documented and tested. Recovery priorities are defined and are related to organisation objectives.	Process maps are reviewed whenever new IT systems are introduced. Recovery priorities and times are reviewed annually.
Third-Parties	Dependencies on third parties for delivery of critical services identified.	Key suppliers are aware of relevant parts of the organisation's Business Continuity programme. Potential vulnerabilities from reliance on third-parties have been identified.	Arrangements with third-parties have be verified to have at least equivalent resilience conditions. Arrangements reviewed and tested annually.

Disaster Recovery Pillar

	Foundation	Building	Sustaining
People	Key individuals who have a role to play in any disaster recovery have been identified.	Roles and responsibilities for return to normal are documented. Alternative means of communication have been planned for.	Restoration activities are coordinated with internal and external parties.
Process	Documented plans / procedures for recovery from a damaging event are in place. Recovery strategies have been developed based on the outcomes of a Business Impact Analysis. Protection from natural disasters, malicious attack or accidents was taken into consideration in the design and siting of facilities.	The key risks that could have damaging consequences for IT have been identified and are actively managed. Recovery procedures have been reviewed and tested in the past 12 months. Insurance cover limits are in line with plans. The Business Continuity Plan includes details on salvage, recovery and restoration.	Recovery strategies and plans are updated after each lessons learned review.
Technology	Equipment and systems that would be needed in the event of a damaging incident has been identified and plans are in place to ensure it/they are available at short notice. The network is appropriately segmented in order to minimise the impact of any malicious attack.	All data and system configurations are backed up and stored off-site. Network diagrams that may be needed for a re-build are securely stored off-site.	Critical systems have been replicated in an alternative hosting location and can be brought on line within required time limits.
Third-Parties	Proactive relationships exist with critical third parties. Third-parties that may be required in a damaging event have been identified and contact details are in the DR plan.	Recovery activities are clearly understood by third-parties.	Recovery activities have been tested with third-parties in the past 12 months.

Scenario Testing / Exercises

- What
  - Based on a credible scenario
  - Unfolded as exercise progresses
  - Round-table format

- Objectives
  - To familiarise staff with specifics of plans
  - Establish if required resources will be available when needed
  - To identify areas for improvement
  - To develop teamwork

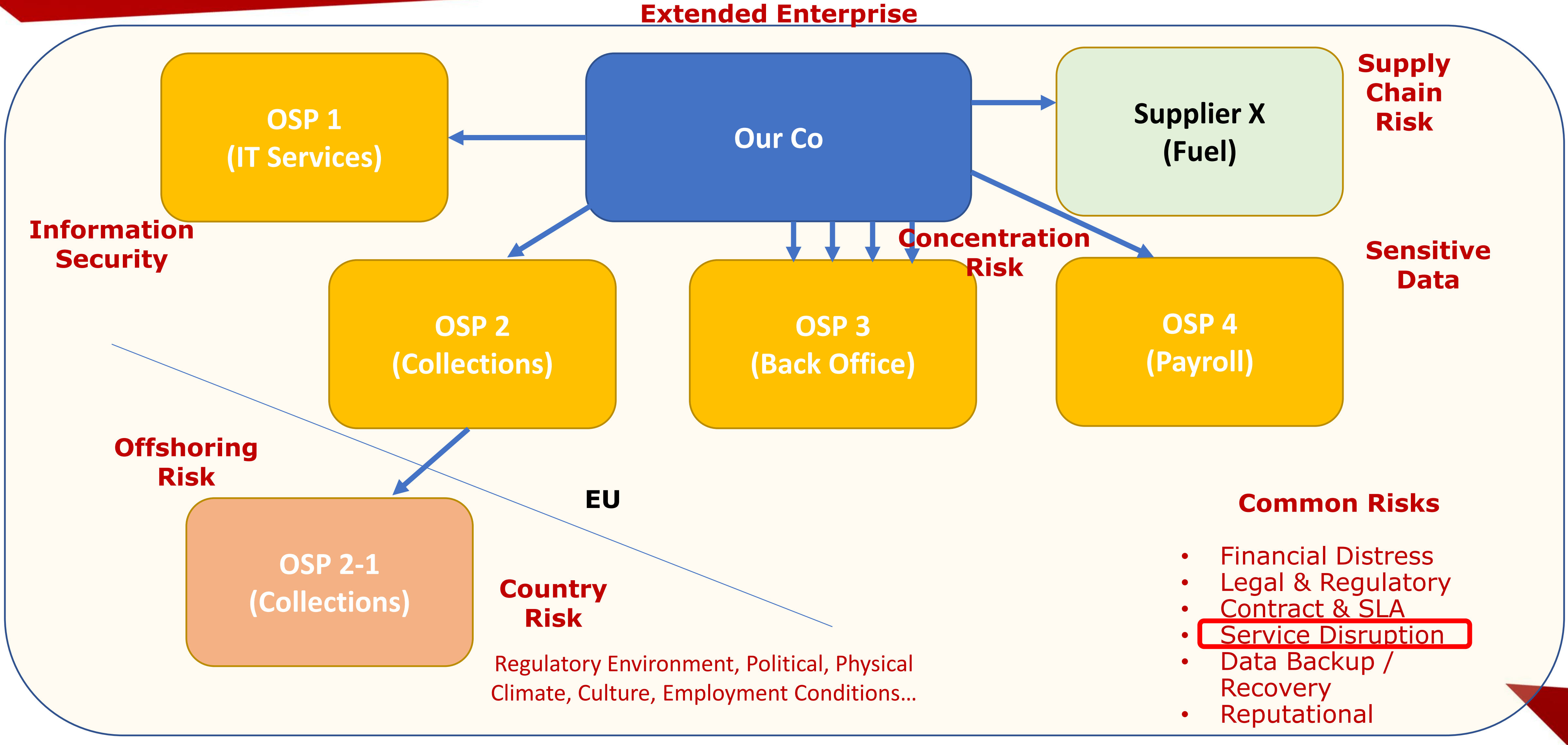
- Examples
  - Power failure
  - Cyber attack
  - Telecommunications failure
  - Key system failure
  - Key supplier affected by a disaster

- Advantages
  - Minimal disruption to business
  - No live systems affected
  - Medium-low cost

Your Third Parties

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

What are the Risks?



Extended Enterprise

Supply Chain Risk

Information Security

Concentration Risk

Sensitive Data

Offshoring Risk

Country Risk

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

Common Risks

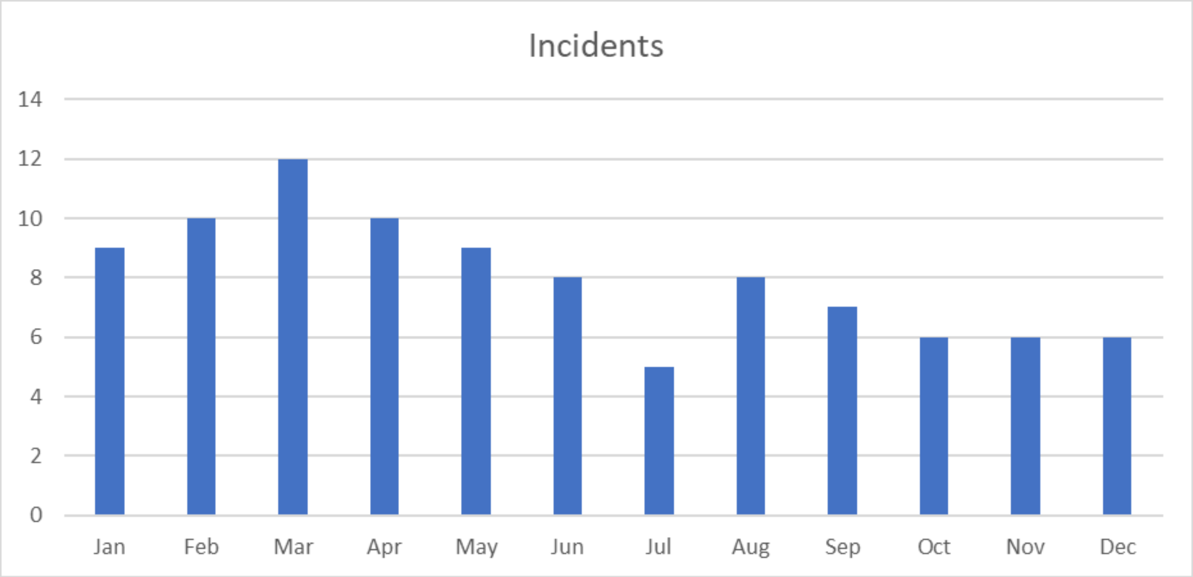
- Financial Distress
- Legal & Regulatory
- Contract & SLA
- Service Disruption
- Data Backup / Recovery
- Reputational

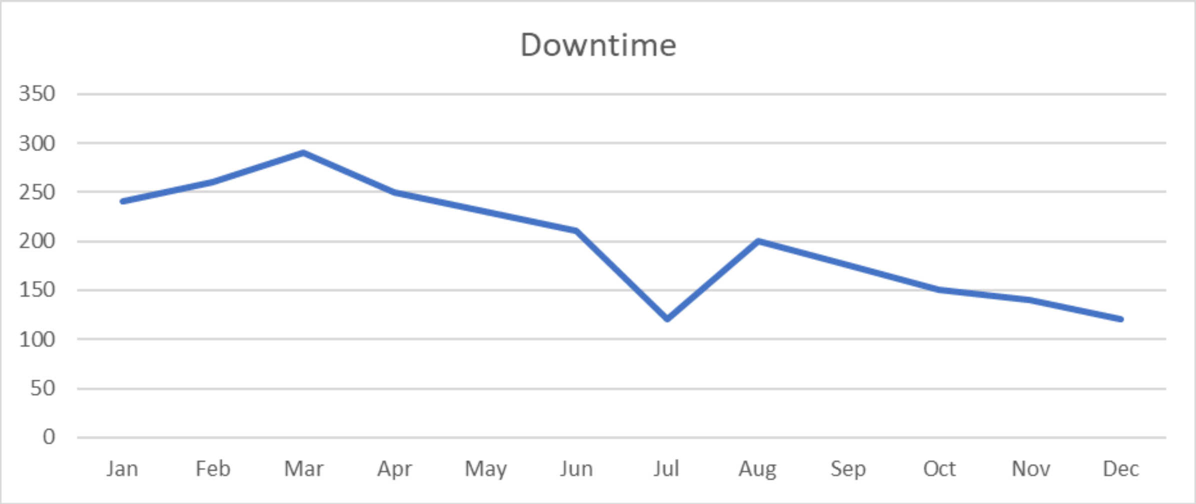
Manage your Third-Parties

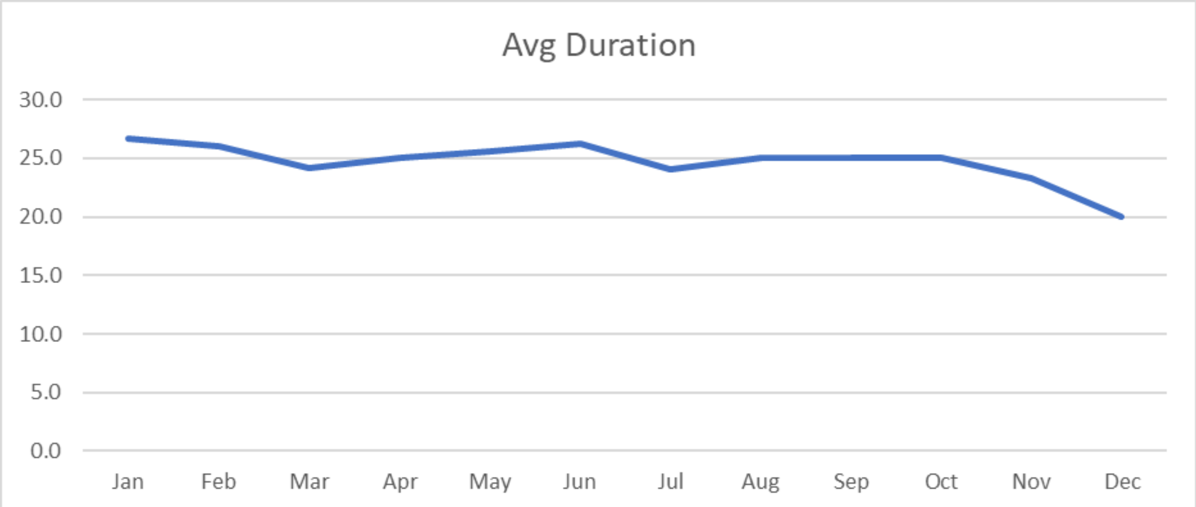
- Maintain a list of Third Parties that you regularly deal with
- Identify those that are critical to your operations
- Identify the risks associated with each Third Party
- Identify and document the Controls in place to manage the risks
- Monitor adherence to Service Level Agreement
- Be aware / informed of all Incidents
- Involve your Third-Parties in your Business Continuity testing
- Communicate regularly with your Third-Parties

Reporting

Disruptive Incidents







5 Things you can do now

1. **Put resilience on the agenda** of the Senior Management Team
2. **Identify your business-critical services**, the systems and third parties they depend on
3. Develop a **response plan** to guide your response to a service disruption
4. Test your plans
5. Start **Managing your Third Parties**, they are a (source of) risk too

Q & A

Cal Risk
Manage the effect of uncertainty on objectives

Thank You

gjoyce@calqrisk.com