CalQRisk

RISK MANAGEMENT & OPERATIONAL RESILIENCE

SCOPE AND PURPOSE

Everybody wants certainty, but uncertainty and change are more constant than ever. And yet, organisations are expected to maintain delivery of services through business disruptions. This is the essence of resilience and the subject of this guidance booklet.

Operational Resilience is becoming a key regulatory requirement in some sectors, particularly the broader financial sector, but consumers also have an expectation that businesses can continue to deliver services despite adverse events. They will walk if you cannot provide the service.

This booklet is written for those who are interested in making their business more resilient, while minimising the likelihood of a business interruption and optimising the recovery from one.

Resilience is not a replacement for Business Continuity, but an outcome of several key functions / processes in an organisation, Risk Management, Information Security, Incident Management, Business Continuity Management and Disaster Recovery. Understanding the risks that threaten the achievement of your objectives is key to prioritising actions that will optimise the resilience of your business.

ABOUT THE AUTHOR

Gerard Joyce is co-founder of CalQRisk with over 30 years' experience in various roles: engineering, IT management and Risk Management.

His broad experience in different functional areas coupled with his study and practice in Risk Management enables him to bring a deep understanding of the issues associated with Risk Management and Business Continuity. He is chairman of the National Standards Association of Ireland Risk Management Committee and a member of the ISO International Risk Management Technical Committee (TC262). He is also a member of the Institute of Directors Ireland.

GETTING STARTED: A 10-POINT PLAN

1. **Put resilience on the agenda of the Senior Management Team.**
   a. See section on "Governance" below for some ideas,
   b. Identify a champion who will drive the initiative. For larger organisations it would be good if there was a champion per function.

2. **Identify your business-critical services, the systems and third parties they depend on.**
   a. See section on "Risk Management" below for details.
   b. Conduct a detailed risk assessment on the "Service Disruption" risk. Identify any missing controls / protections / mitigation.
   c. Address the gaps identified.

3. **Assess your Information security risk (includes cyber-risk)**
   a. See section on "Information Security"
   b. Identify, Protect, Detect, Respond and Recover

4. **Develop a response plan to guide your response to a service disruption.**
   a. See section on "Incident Management" below.
   b. Keep plan generic, but consider: loss of building, loss of systems and loss of people and develop contingencies for each loss.

5. **Develop a Business Continuity plan that focuses on how you will deliver essential services following a severe disruption.**
   a. See section on "Business Continuity" below.
   b. Develop response plans to deal with specific incidents (e.g. cyber attack)
   c. See side panel: "Operational Resilience Vs Business Continuity"
   d. Communicate your plans to all relevant employees / third parties.

6. **Test your plans.**
   a. See side panel on "Exercising Plans" for suggestions on what and how to test.
   b. Update your plans after each test, you will always learn something from a test/exercise.

7. **Consider how you might recover from a Disaster. (e.g. fire, flood)**
   a. See section on "Disaster Recovery" below

8. **If an incident becomes a crisis, you will need a Crisis Management plan**
   a. See panel on "Incident Vs Crisis".

9. **Manage your Third Parties, they are a risk too.**
   a. See section on "Third Parties".

10. **Now assess how resilient you are, take the 21-question test.**
    a. See section on "Resilience Self-Assessment" below.

THE ELEMENTS OF RESILIENCE

Operational Resilience is an outcome of multiple functions or disciplines, all of which require detailed planning and control. They also need to be underpinned by robust Governance, that is, good oversight by the Board / senior management and appropriate management arrangements.

The five key elements are:

- Risk Management;
- Information Security (including Cyber-security);
- Incident Management (including Crisis Management);
- Business Continuity; and
- Business Recovery

Figure 1: The five pillars of resilience.

GOVERNANCE

The governance structure of most organisations generally consists of the executive board and / or senior management. If resilience objectives are to be achieved, then all the disciplines must be supported by this group. That support should be in the form of a stated policy (on resilience), assigned responsibilities, allocated resources; financial, human, and technological and review of

regular reports from each discipline

Key actions required at this level include:

- an understanding of the organisation's existing capabilities and a clear articulation of objectives with regards to resilience.
- agree Impact tolerances for disruption to critical services. (e.g. how long could you operate with no significant impact without your CRM (Customer Relationship Management) system?)
- agree plan to address the gaps in capabilities to achieve the desired level of resilience and resource this plan.

The policy and objectives for resilience must be communicated to all employees and third-party service providers on whom the organisation depends for delivery of critical services.

Resilience should be regularly tested through a range of severe but plausible scenarios (e.g., loss of building, loss of a utility, (power, water, etc.) server system failure, loss of people / individuals, etc.) Lessons learned from scenario exercises (See: Exercising below) will enable the organisation to improve plans and be better able to respond and adapt to unforeseen scenarios.

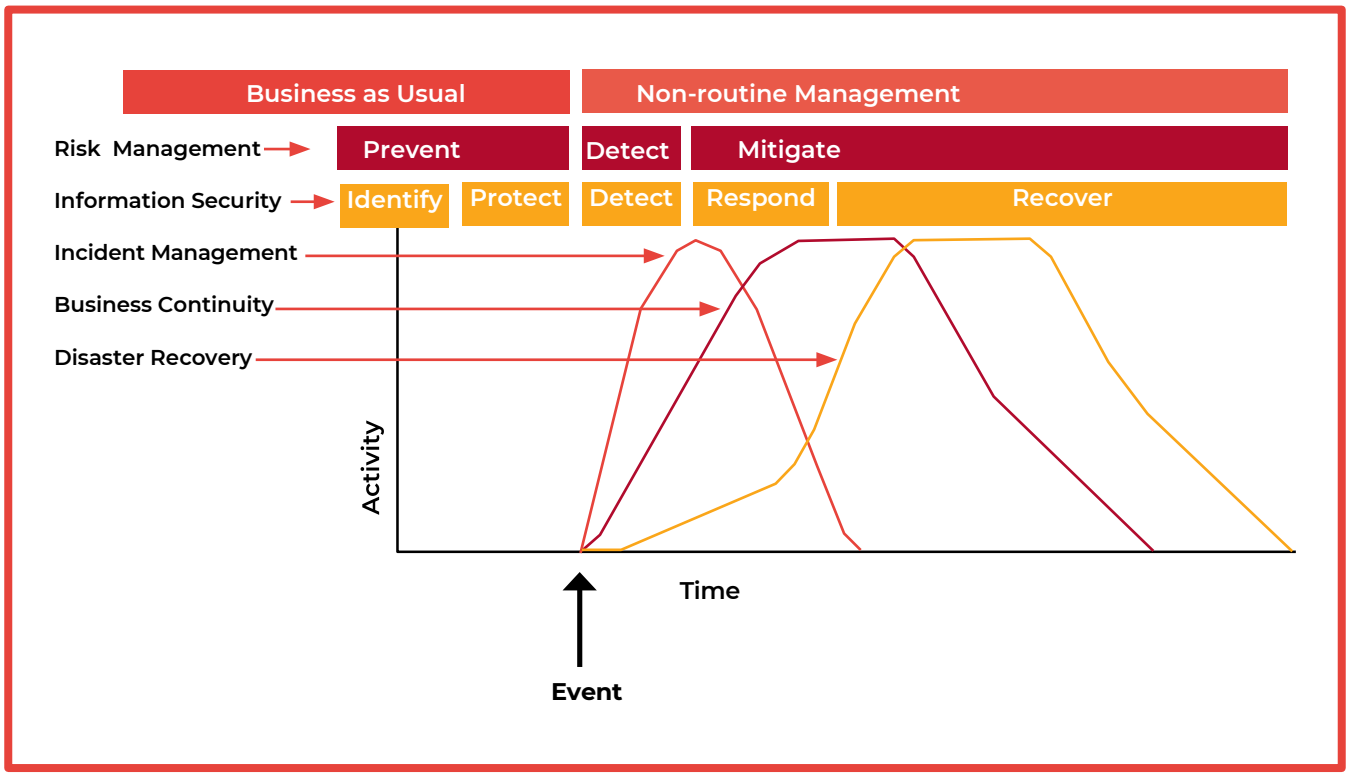

Figure 2: Key Elements of Resilience on Timeline

RISK MANAGEMENT

Depending on the size of your organisation you may already have a risk management discipline. If so, this should be leveraged to optimise resilience. The goal here is twofold; to gain a good understanding of what can cause a disruption and implement measures to prevent the occurrence of an undesirable event in the first instance; and understanding how critical services may be impacted and what mitigation can be put in place so that the impact is minimised.

The first risk assessment, to identify the causes of a disruption can best be achieved using a Fault Tree Analysis technique: Starting with (the Fault) “Service Disruption” ask, “what could cause that?”. For example: system failure, building loss, people loss, third-party failure, etc. Now ask what can cause each of those and work the detail of the next level (This is creating the Fault Tree).

See worked example below but consider your own environment and create your own fault tree. Every organisation is different, no one size fits all.

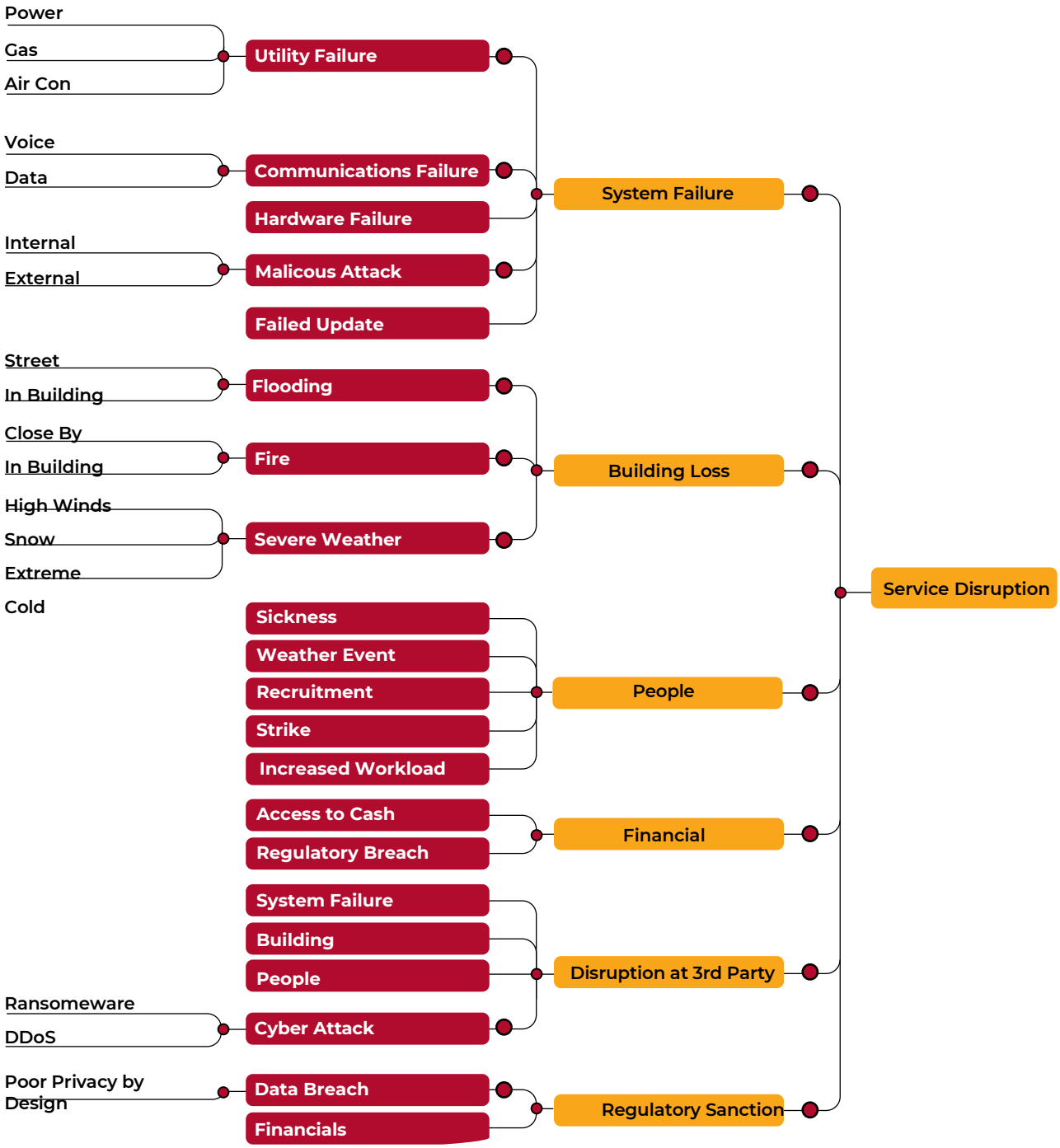

Figure 3: Worked Example of a Fault Tree Analysis of a Service Disruption

With a good understanding of what can cause a service disruption in your organisation you can now begin to consider what measures (controls) you can put in place to prevent disruption. For example; install a generator to supply power in the event of an electricity outage, cross-train employees so there is no dependence on any one individual for the delivery of a service.

The most resilient organisations regularly review this assessment and ensure that they are always aware of the prevailing situation. Controls may need to be improved / changed and plans may need to be "adapted" if the threat picture changes. While you may review risks on an annual basis you should also review relevant risks if there is a significant event or change in the business environment. e.g new regulations or collapse of an insurer.

The second risk assessment utilises a technique called a Business Impact Assessment (BIA). This is also a fundamental requirement for a sound business continuity plan.

The starting point here is to identify all your business activities / services. This exercise will ensure a good basis for determining what is critical, so it is best to be inclusive rather than exclusive at the start.

For each activity / service identify:

- The key responsible person.
- What systems (technology) are required to deliver this service (main dependency).
- What other dependencies (e.g. Internet, people, third-parties, facilities) are needed to deliver the service.
- The Maximum Tolerable Outage (MTO) that you have set for this service, that is how long can your organisation tolerate being offline / unable to provide the service?
- The Recovery Point Objective (RPO), date/time of last backup that is acceptable. Is it ok if you lose the last X hours of data you entered into systems? How big is "X"?
- The level of impact on your "Impact" scale that will be reached after 12, 24, 48, 72 hours.

See sample BIA form below. Examples of activities / services you should consider here include claims management, personal lines sales, accounts payable / receivable, etc.

Resp	Process / Service	Comments	System Dependencies	Other Dependencies	MTO	RPO	12	24	48	72
Mary White	Personal Lines New Business Sales	Need to be able to give quote while customer is on the phone. This accounts for 50% of our calls.	Quote server Relay system	Internet Power	2	1 Min	4	5	5	5
Joe Grey	Pay Employees	Every month, agree Wed, Pay Fri Sensitive	Sage	Internet Joe in HR	24	24 Hrs	2	3	3	4
Bob Morley	Investments and Liquidity Reporting	We measure this on a weekly basis	Local Financial Server	Network	48	24 Hrs	2	3	3	3

Figure 4: Sample Form to Record Details of a business Impact Analysis

One approach you could use to identify your key activities would be to start with the services you provide, ask what activity or process is involved in delivering that service and then ask who and what do we need to deliver the service / complete the activity.

From these two risk assessments you now have a greater understanding of what can happen, what the impact might be and (critically) what the dependencies are. (The people, processes and systems required to deliver your key / critical services.)

Whenever there is a change in the service or any aspect of its delivery then these assessments will need to be updated. Resilience is about constantly improving / updating controls / plans in response to “new information”, be that from a scenario exercise, an incident or from some external threat intelligence.

INFORMATION SECURITY (INCLUDING CYBER-SECURITY)

Organisations need to understand and approach information security as a risk management issue across the organisation, not just an IT issue.

It is about confidentiality and more. It's more than just keeping the bad guys out. It's more than firewalls and intrusion detection. It's more than just spyware and malware. It's also about protecting integrity, making sure that the customer data your decisions are based on is accurate and unaltered. (Integrity can be assured by using data validation and verification techniques and restricting access) It's also about availability, ensuring you and your customers can access applications and information as and when required. It's about people, their behaviour, sometimes careless and sometimes malicious. And it's also about prioritisation, what matters most, which information needs the most protection?

There are several published standards (See Standards and Guidance section below) that document a range of measures organisations need to implement to protect the information they hold. The NIST Cyber Security Framework (NIST CSF) has in recent years become popular because of its accessible language.

NIST categorises the required controls into five defined groups: **Identify, Protect, Detect, Respond and Recover.** Indeed, this is also the language that many regulators have begun to use. For this section we will broadly follow the NIST framework to outline the sequence of activities that will strengthen your defences against malicious and accidental incidents.

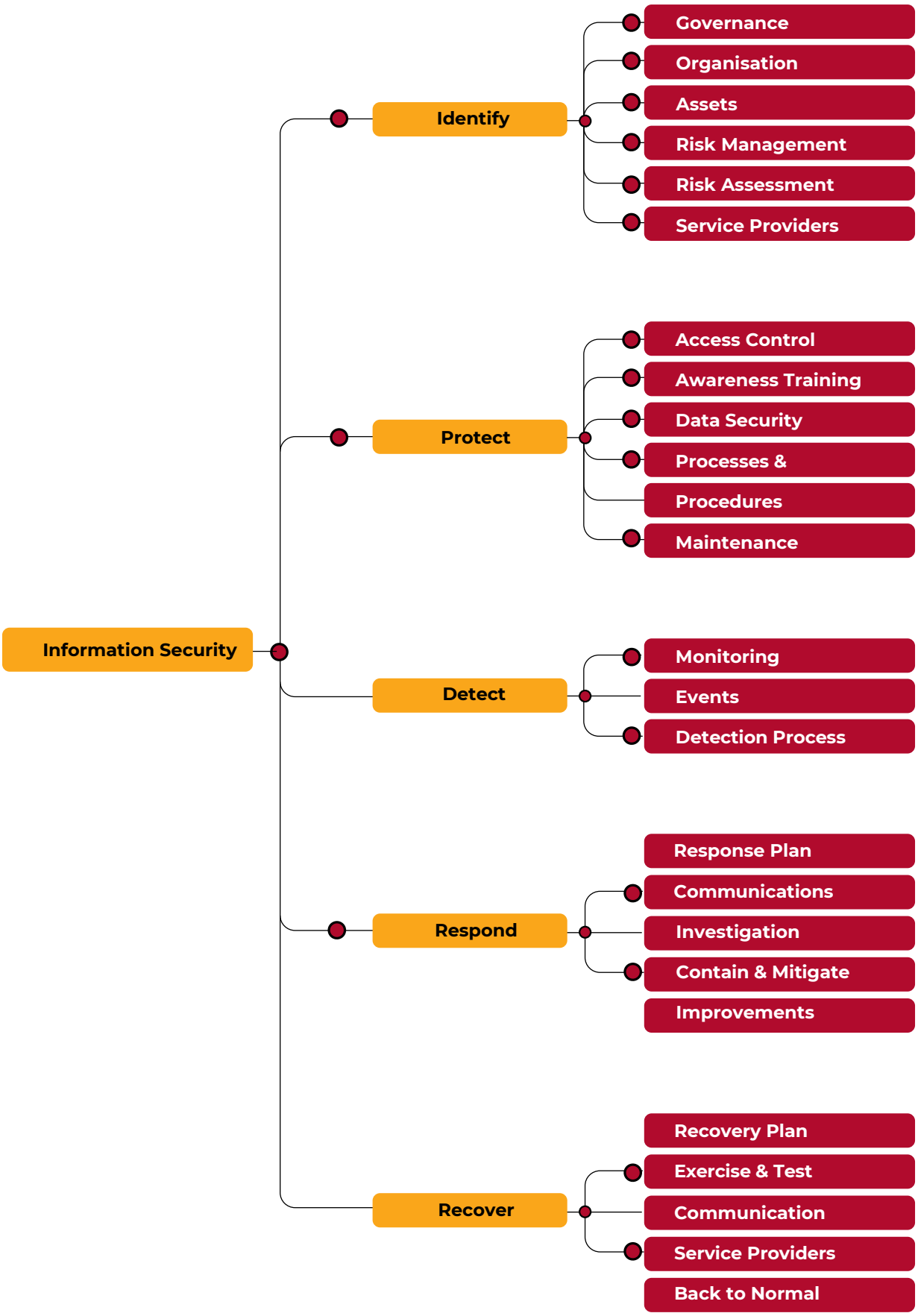

Figure 5: An Information Security Framework aligned to NIST CSF

Identify

Good Information Security demands that there are good governance arrangements in place: an information security policy, relevant procedures, assigned roles and responsibilities. Know what's important; what are the goals and objectives of the organisation. This will help later when you need to prioritise action.

The key activity at this stage is to identify all your assets that require protection, the IT systems, the PCs, laptops, tablets, mobile phones, everywhere that information may be stored. The data itself is an asset. Know what you have and know the physical facilities that require physical security.

Using the same Risk Management process you use elsewhere, assess the risks (Identify, analyse and evaluate). Use threat intelligence (what have others in your sector highlighted as the key risks / vulnerabilities?) to focus your efforts. When you have identified the gaps in your protection you need to draw up a plan of action to address these gaps.

Treat your critical third-party service providers as an extension of your organisation. Their information security should be at least as good as yours. Define "Criticality tiers" (levels of importance) and categorise all your third parties. The most critical will emerge.

The "Identify" phase is not a one-off exercise. As things change and you add more partners, more services, more systems, you will need to re-visit the identify phase and make sure it remains current.

Protect

Protecting your assets (identified above) and your information starts with "access control", defining who has access to what. Follow the "least privilege" principle and only give people access to what they need to do their job. (You will limit any damage caused if their credentials are stolen) If employees are accessing the company network remotely then it is wise to utilise two-factor authentication. (e.g., send a code to their mobile, which is then used to authenticate their login) Don't forget to limit people's physical access to areas where critical or sensitive data is stored.

A significant number of data breaches and cyber-attacks are successful because we humans are curious. We fall for the socially-engineered smooth-talk or phishing email and we click on that link we shouldn't have. So, be aware, be very aware! Organisations must regularly train their employees (minimum quarterly) to recognise suspect emails and to be constantly vigilant. This means all employees, from the Board of Directors down. Check that your critical third-party providers are also receiving regular awareness training.

Best practice and GDPR mandate that you implement appropriate security to protect data. Think CIA; confidentiality, integrity and availability. Is critical / sensitive data encrypted at-rest (where stored) and in-transit? Do you employ integritychecking mechanisms which ensure that files have not been tampered with? Do you have a UPS (Uninterruptable Power Supply) that can power critical systems when the electricity fails? Do you have a generator that can supply power to systems and the building, so you can continue to operate during longer periods of electricity outage? Have robust information security processes and procedures including:

- Ensure all systems (Servers, PCs, laptops, etc) are configured to a strong security standard.
- Back up your data at a frequency that reflects your RPO (Recovery Point Objective) requirements.
- Store a copy of your data off your network. (So that it is not affected by any incident that hits your network.) e.g. Off-network Cloudstorage.
- Test your back-ups. The most common reason that a data-restore fails is because the back-up was defective.
- Apply patches to your systems and applications as they become available. Do not leave vulnerabilities unaddressed. Keep your systems up to date.

What other protective technologies can /do you employ? Firewalls, to restrict access to /from approved lists, anti-virus software to detect and eradicate known malware, secure wireless access that restricts who can connect to your network. VPN (Virtual Private Network), that allows you to connect remotely to your network in an "encrypted tunnel" over the internet. Ensure your use of protective technology is appropriate for your organisation. Keeping up to date with threat intelligence for your sector will help you identify what is appropriate.

Detect

If you do have an intrusion, will you know? Many cyber-attacks include a reconnaissance phase where the bad guys are in your network looking around before stealing data or planting malware. Successful early detection is key to minimising damage. Continuous monitoring of the network activity to identify anomalous behaviour or unauthorised changes being made is critical to early detection. Your IT provider or in-house IT department can utilise network tools to detect and record unusual traffic on the network and generate "alerts" when anything unusual happens.

Note: Where IT has been outsourced to a third party, you should confirm the level of detection and continuous monitoring that is applied.

Service delivery may be affected by an intrusion in your network. So, be sure to investigate all reports of service disruptions / unusual events, in case the source is an as-yet-undetected rogue player in your network. Disruptions to service can also stem from system failures / hardware failures. These are often, but not always, preceded by warning events (e.g., high error rates.) Do your systems alert you when things are going/gone awry? 24 by 7?

When you do detect anomalies, intrusions or failures do you have a process to analyse and escalate if appropriate? Are roles and responsibilities for detection defined? Test your capability to detect intrusions / malicious acts on a regular basis.

Respond

When a cyber-attack or intrusion has been detected or a system has failed in some way, time to respond is crucial. Every minute delay is another minute of no service to customers. You need a plan. You need processes and procedures to follow and for everyone you depend upon for a quick return to normal service to know their role and responsibilities, long before a disruption.

If the "event" leads to a serious disruption you may need to invoke your Business Continuity plan. The decision process to invoke needs to be embedded in your response to any event.
Events of a particular nature, like a data breach or a cyber-attack, should have specific pre-planned actions associated with them, so that no time is lost in responding and disruptions can be kept to a minimum. For example, a personal data breach may require notification to the regulator and customers within a short period.

Response planning is covered in greater detail under the section "Incident Management" below.

Recover

Depending on the incident and the number of systems / devices affected, the recovery may be minutes, hours, days or weeks in duration. For the more significant disruptions the actions outlined in the business continuity and disaster recovery plans may take precedence.
Regardless of the nature or duration of the incident, it is imperative that an IT recovery plan is in place. The Business Impact Analysis, which you will have completed, will inform the prioritised plan to recover systems. Exercises and tests of these recovery plan elements should be carried out periodically to ensure that; 1) they work and 2) that individuals are familiar with their role. Where the recovery of a system requires the involvement of a third party this should also be tested (led by the person responsible for the system) in a "plausible scenario" in advance of any real incident.

Exercising Plans

Generally, there are two safe levels of plan-testing that you can and should conduct. They are:

- Component Testing; and
- Tabletop Walkthroughs

Component Testing
This involves testing of individual components of a bigger plan to identify missing information, test the timing and confirm it works. Examples of this are: IT procedures, like a data restore from backup, testing the "Call Tree" (to see if numbers are correct and up to date) or testing call diversion to mobiles. The advantages of these types of tests are: they are cost effective, there is minimal risk and it allows the owner to fine tune the details.

Tabletop Walkthroughs (Scenario Exercise)
These take more time in preparation and are built around a credible scenario. They are conducted around a large conference table with all incident response teams present. A facilitator gradually unfolds the plausible scenario, and the participants are prompted to react and say what they are going to do. (a form of role play)

Examples of scenarios are: a local power outage, a cyber attack, failure of a key system or failure of a key supplier. The exercise is usually conducted over a 2 hour period and involves multiple "injects", where the facilitator introduces new details / developments that force the individual teams to consider how they will respond.

There are four key objectives for these types of exercises:

- To familiarise employees with specifics of plans
- To establish if required resources will be available when needed
- To identify areas for improvement, training
- To develop teamwork

The advantages of Tabletop exercises are: minimal disruption to business (participants are away from their desks), no live systems are affected, and it is medium to low cost.
It is important that all lessons learned from exercises (and there will always be lessons learned) result in changes / updates to the individual plans.

INCIDENT MANAGEMENT

Most incidents lend themselves to pre-planned responses and so it is vital that one has an Incident Response Plan, to minimise the disruption resulting from the incident.

Crises, on the other hand, are less predictable and strategic in nature. They can occur suddenly without notice, emerge from poorly handled incidents or from latent problems within the organisation. Because of the potential for significant and lasting damage they require different skills and planning to handle successfully. See separate panel on “Incidents and Crises”.

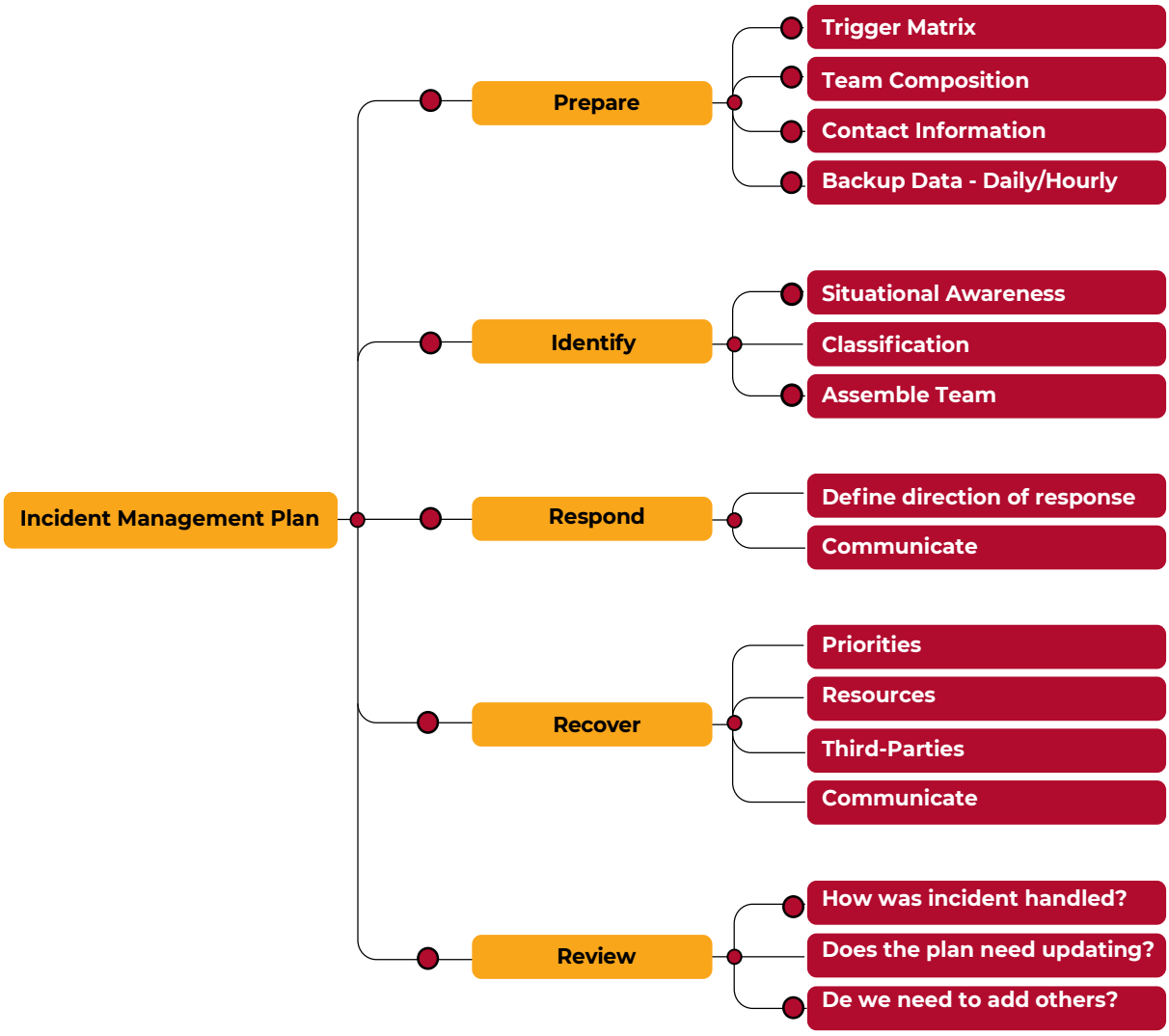

Figure 6: Outline of an Incident Management Plan

"Good Incident Management requires careful planning."

The rewards for this effort will be seen in:

- Shorter duration of disruptions
- Lower financial cost of disruptions
- Full compliance with regulatory requirements
- Positive reputation impact as the organisation is perceived as resilient

Incident Management plans should contain these five elements; **Prepare**, **Identify**, **Respond**, **Recover** and **Review**. We will look at each of these in more detail.

Prepare

Incident Management starts well before an incident occurs. You need to consider what types of incident are likely to occur and develop "trigger criteria" which if met will mean specific plans to address that type of incident are invoked (See Fig 3 above for suggestions on Incident Type).

Use the results of your Fault Tree Analysis of what can cause a disruption and use the high-level grouping to guide your planning. For example, if you suffer a building loss through fire, flood or severe weather event, your response will be different to that of a system failure.

For each incident type (keep this to five or six) consider what teams you will need to mobilise, what skills will be required to handle the incident and what financial resources may need to be automatically authorised in order to respond without delay.
Consider creating the following teams in advance of any incident:

- **Leadership**
  (The Gold Team, responsible for coordinating theresponse)
- **Operations**
  (Responsible for recovery of all business services)
- **IT Team**
  (Responsible for recovery of all systems)
- **HR & Facilities**
  (Responsible for people and building issues)
- **Legal and PR**
  (Responsible for regulatory and public relations)

Assign a "leader" for each team and an "alternate leader" if the leader is not available.
The size of your organisation will determine the number of teams that you define. In addition, you may involve a third-party to advise on Legal and PR aspects, where these skills are not retained inhouse.

Incidents can happen outside of business hours and thus will challenge "Communication". Prepare lists of all contacts (names, email addresses, telephone numbers) you may need in an emergency. Have a list for employees and one for third-parties you may depend on. Store these in a place you can access in any emergency.
Your business data is your key asset, so you need to ensure that you are taking (minimum daily) backups and storing a copy off your network. (so it is not affected by any virus that gets on your network)

Identify

When an individual becomes aware of an incident or suspects something untoward is happening, they need to know who to call, especially if it is "out of hours". For example, this might be a help desk that is manned 24 by 7 (can be third party) or it might be the Operations manager / IT manager. That person needs to quickly get an appreciation of the unfolding scenario and decide if a formal incident response is appropriate.

The incident needs to be quickly "classified" and this will dictate the most appropriate response. Agree a classification matrix in advance so that this step can be taken without undue delay. Here is one example of how you might classify incidents and decide on next steps.

If any incident has the potential to cause serious financial or reputational loss to the organisation then the Leadership Team need to be advised and they will need to assemble.

Incident Type	Notify	Response
System Failure	IT Team	Identify systems affected. Assemble IT Team. Notify Operations of status.
Building	HR & Facilities Team	Identify issue. Assemble HR & Facilities Team. Notify Operations of status.
People	HR & Facilities Team	Clarify exact issue. Assemble HR & Facilities team. Notify other teams as appropriate.
Third Party	Operations Team	Identify Services affected. Assemble team.
Compliance Breach	Legal & PR Team	Confirm details. Assemble team.

Respond

Depending on the nature of the incident and the level of severity, the responsible team should define the direction of the response. Pre-defined procedures (For example: building evacuation, system shutdown, emergency medical response,..) may be invoked or full business continuity plan invocation may be appropriate.

It is important at this stage and at regular times during a prolonged incident (e.g. serious systems failure, flood) that the team leading the response communicate with other teams to advise on the status. The Legal and PR team could take the leading role in ensuring that appropriate communication is maintained with all stakeholders. (employees, customers, regulator, media, as appropriate) as their involvement in operations is minimal. Incident response plans should include Communication plans, so that the persons involved know who needs to be contacted, when.

Demonstration of concern, commitment and control in the communication is critical, especially if there is a high level of public interest.

It is also important that a member of each team is assigned the role of recording decisions and actions taken, preferably with a time noted. These logs of activity may become important later if there is a criminal case because of the incident or disciplinary action. They will also be valuable in the post-event review, when looking for areas that need improvement.

Recover

Depending on the nature of the incident and the duration of the event, recovery time may be minutes, or it may take hours / days. For the more complex incidents, the recovery phase may follow the priorities set in the business continuity plan. Recovery plans should take account of a potential lack of resources or unavailability of key personnel and ensure that there are options to address these deficiencies.

Depending on the incident, there may be a number of external parties that need to be communicated with during the course of the incident. It is important that information released to third parties is well managed to ensure it is timely and accurate. For example, if there is a personal data breach where the organisation must inform the regulator and customers, specific information needs to be shared.

As normal operations are restored, all stakeholders should be advised of the situation and, where appropriate, remind all employees how they should respond to comments / queries on social media / from journalists.

Review

When the incident has been resolved it is important to take some time to review 'how it was handled' and to see what lessons can be learned from the event. Did the response plans work? Did people know what to do? Were actions taken in a timely manner? Is there anything you would do differently next time?

Take these learnings into account when you review / revise your response plans. Share your experiences with peers and encourage them to share their experiences with you (Do this in a safe / secure sharing environment).

Incident Vs Crisis

Not every incident / event is a crisis, but they can have the potential to become a crisis if not handled appropriately. For example, a stolen laptop that is quickly excluded from connecting to the network remains an incident. If the laptop were to be used to connect to the network and steal personal customer data you could very quickly be in "crisis mode" and dealing with a very damaging event in public.
CEN / TS 17091 defines a crisis as an "*unprecedented or extraordinary event or situation that threatens an organization and requires a strategic, adaptive, and timely response in order to preserve its viability and integrity*". The standard includes a section on principles for crisis management which serve as a good guide for the management of any incident that has the potential to become a crisis. They are:

a) seek understanding of the situation.

b) achieve control as soon as possible.

c) communicate effectively, both internally and externally.

d) be prepared with clear, universally understood structures, roles and responsibilities.

e) build situational awareness by good information management and coordinated working.

f) have a clear and well-rehearsed decision-making and action-driving process in line with the core values and objectives of the organization.

g) implement effective leadership at all levels of the organization.

h) ensure people with specific crisis management roles are competent through appropriate training, exercising and evaluation of their knowledge, skills and experience.

BUSINESS CONTINUITY

Business Continuity (BC) is a key pillar in establishing a resilient organisation. This discipline has been around for many years and many organisations already have some level of business continuity planning in place. Some will see operational resilience as enhanced business continuity and may question the placing of BC under the Resilience umbrella. (See side panel: "Operational Resilience vs BusinessContinuity") But the focus is slightly different and to achieve high levels of resilience will require higher levels of competency in several disciplines.

Business continuity, by definition, is a focus on the "delivery of services or products at acceptable pre-defined levels following disruptive incidents," (ISO 22301). This capability is key for resilient organisations. In the following sections we will take a closer look at the key elements that make up good business continuity management.

Business Continuity Planning

It is typical that the Business Continuity programme includes plans for Incident response and disaster recovery. It makes good sense for these three elements to be coordinated by one individual. Before looking at the Business Continuity phase after an incident, we will look at Business Continuity Planning as a discipline and how it interrelates with the other disciplines. The details on Incident Management and Disaster Recovery are discussed in separate sections.

Business Continuity Governance

For an effective and successful business continuity programme there needs to be a commitment at Board and senior management level to develop the capability. Start with a BC policy that sets out the rationale for activity and the objectives for delivery of services in the event of a disruptive incident. Define the scope of the BC programme, what services are included and how does it relate to the strategic plan? Assign responsibility to one individual, who should report back on progress at periodic intervals. Make it a requirement that scenario exercises be conducted, and results reported to the board.

Embedding

If the objective is to be able to continue to deliver services despite a disruption, then this will require the whole organisation to be "on board" with the programme. Throughout the programme you will need to raise awareness of the issues (e.g. threats that can cause disruption, criticality of service delivery, etc.). Continuity needs to be part of the culture and considered when discussing all business activities. Those responsible for continuity need to collaborate with the related disciplines (risk management, information security, incident management, etc). Gaps in skills and competencies need to be identified (during planning and exercises) and addressed so that when disruption happens people know what to do and have the capability (e.g. IT recovery, paperbased information recording, dealing with the press, etc)

Analysis

This is where BC and risk management overlap. A healthy overlap. It starts with "Understanding your organisation". What are the organisational objectives? What are your obligations? What are the constraints? Conduct / use the Business Impact Analysis (BIA) carried out as part of your risk management activities to determine and rank the critical services and their dependencies.

Design

Use the BIA outcomes to inform BC strategy and guide selection of appropriate solutions. Identify recovery options under the headings:
Work Area, IT Systems, Operations and Data. For example, could you move some staff into another office location? Would a cloud-hosted system allow you to recover / restore in a shorter time frame (Vs in-house). If staff are out, can you borrow staff from another department / office?

Operational Resilience Vs Business Continuity

At first glance you might think Operational Resilience is just Business Continuity (BC) by another name, but there is a difference. BC focuses on the plan to deal with disruptions (usually severe) and ensuring the organisation can maintain essential services at pre-defined levels, within an acceptable timeframe.

Operational Resilience is focused on outcomes. The organisation continues to deliver critical services through the disruption. This certainly requires good Business Continuity planning, but it also requires effective operational risk management where risks are identified, and measures are put in place to prevent undesirable events from happening in the first instance. It also requires the continuous monitoring of the environment / business context for changes that may require a corresponding change to a process / procedure. When disasters do happen, they are never exactly as expected, so BC plans have to be adapted. This ability to respond and adapt before, during and after an event is agility, the ability to see opportunities and threats and respond quickly. The most resilient organisations are agile.

Evaluate your recovery options to identify the best fit. (Consider up-front cost, ongoing cost, effort to implement, and effectiveness of solution). Working with the risk management discipline identify opportunities to harmonise / standardise mitigation measures.

Implementation

Draw up BC plans at strategic, tactical, and operational level. Establish the command, control and communications systems that direct the response to an incident and ensure they are in harmony with the detailed BC plans. Assign roles and responsibilities and ensure that all identified training is carried out. Note, cross-training of individuals in key processes (critical services) before any disruption will give you more options in a disruption.

Collaboration with other disciplines is key to an effective implementation. Some plans may be developed for specific scenarios, but all plans should be "flexible", they will need to be adaptable to the current incident. Flexible plans equal "agility".

Validation

Dwight D Eisenhower once said, "In preparing for battle I have always found that plans are useless, but planning is indispensable." Incidents are never exactly as you expect, and so business continuity plans will always be "less than perfect". However, by exercising your plans through plausible, but severe, scenario exercises you will not only make them better, but you will improve individuals' competencies and ability to think on their feet.

It is in the preparing and exercising of plans that the competency to handle any disruption is developed. By testing your plans through scenario exercises (see section on Exercising Plans below) you will find out if they meet the objectives. You will know if they are effective, and you will learn things that enable you to make them better.

Getting to a Continuity State

You have developed your BC plans and tested them and now you have a real business disruption. How does all the planning now deliver "continuity"?

Your Business Impact Analysis (BIA) tells you what business services are critical and sets the priorities for the various teams responsible for their restoration. But first you need to gather facts. These will be available from the teams that are handling the incident as it is unfolding. Depending on the nature of the incident
one or more of the following plans may need to be invoked.

- Building evacuation and move to recovery site / remote working from home/ hot spot
- Switching one or more IT systems to the backup systems if available
- Data breach response plan
- Cyber-attack response plan

- Switching to a paper-based process / processes
- Diverting landline telephone numbers to mobile phones
- Switching Internet traffic to back-up connection / ISP (possible mobile connection)
- Emergency Communications plan. (Employees, Customers, others)
- Switch to alternative power (electricity) source (Mobile generator)
- Arrange alternative water supply (by truck)
- Arrange supply of replacement production / process equipment (e.g. photocopier)
- Suspend non-critical operations and re-deploy resources to critical services
- Switch supply of critical materials to alternative supplier (pre-identified / qualified)
- Retrieve backed-up data from remote location (may need to be physically transported)
- Retrieve archived paper records from remote storage
- Third Party provider substitution / re-establish service in-house
- Delayed delivery communications plan
- Loss of significant portion of business sudden contraction plan
- Sudden increase in business activity - Pivot plan

When the plans were written certain assumptions about the nature of the incident were assumed. Now that you are handling the incident in realtime you may need to adjust the plan to reflect the actual circumstances. You may decide to re-prioritise the restoration of certain services because of the circumstances. This is normal. And this capability to adapt plans is the agility that resilient organisations display.

While in the continuity state and providing services at somewhat reduced levels, there will be an ongoing need for good communication with employees and customers, and possibly the regulator. Ensure that there are regular updates to relevant stakeholders. Use the scenario exercises to determine the most appropriate frequency of communication to each cohort of stakeholders.

DISASTER RECOVERY

At this stage of a disruption, you have successfully recovered to your "continuity state". If the incident was minor then you may have recovered completely to "normal operations". But if the incident was major (a fire, flood, ransomware attack) then the recovery may take a little longer.

You have had a disaster and are now limping along providing minimal services at an acceptable level. It is important to return to full service quickly and restore the confidence of your customers in you. A long-drawn-out recovery can damage the longerterm viability of an organisation as customers may begin to look elsewhere for a more resilient provider.

It is difficult to plan for disasters. It is uncomfortable because we have to acknowledge the possibility that we may lose everything. By considering these uncomfortable but remote disasters you will identify measures you can put in place today that will significantly increase your chances of survival. Think of the "upside". You suffer a disaster but emerge stronger and better. You are now more attractive as a supplier of a service because you are perceived as resilient.

In the design phase of your business continuity planning, when you understand all the requirements to deliver the services you provide, you need to imagine a few disaster scenarios and start identifying your options, e.g., how would you find and move into a new premises? How would you quickly eradicate malware and restore all PCs and servers after a cyber-attack? What would you do if a key supplier went out of business? At one level, this is mitigation of those risks with the most severe consequences. And possibly a very low likelihood.

Eisenhower was right - "planning is indispensable".

Not only that, but by forcing yourself to consider the doomsday scenarios you will see options and possibilities for changes to how you operate today that reduce "singlesource" dependencies, that reduce the likelihood of a disaster or enable contingencies that you hadn't previously considered. All of this will ultimately make you more resilient.

Here are some contingency plans that you might add into the mix:

- Enter a reciprocal arrangement with a neighbour, supplier, to share office space in the event of a disaster.
- Large scale disasters often impact the mobile network, so consider having a secure area on your website when you can post communications for your employees.
- Talk to your equipment suppliers (of IT and office equipment), see if you can get an agreement to supply temporary or new equipment in a short time scale in the event of a disaster. You may have to pay a small fee to secure this option.
- Consider dual sourcing key services (i.e. source from two suppliers) when in growth mode or integrating merged entities.

THIRD PARTIES

There is increasing reliance on outsourced service providers across all industry sectors. The financial regulator has expressed concern, resulting from recent thematic reviews, that organisations are failing to put appropriate arrangements in place to govern and manage their third parties.

As the resilience of your organisation is to some extent dependent on the resilience of one or more of your third-party service providers, it is imperative that you ensure the measures you deem important / necessary to be resilient are also present in your outsourcing partners. A good outsourcing policy is the cornerstone of outsourcing arrangements. Here we look at some aspects an outsourcing policy might include.

Policy Objectives:

- Ensure that all outsourced activity is compliant with legal and regulatory requirements;
- Ensure that there are appropriate processes in place to support a robust outsourcing programme;
- Ensure that the orderliness of the conduct of business is not impaired; and
- Ensure that all roles and responsibilities are clearly identified and assigned

Framework for Setting Control Objectives

To ensure that outsourcing is addressed in a comprehensive and thorough manner, control objectives should be specified in detail for the following principal activities:

- Outsourcing Decision-Making Process;
- Outsourcer Selection Process;
- Outsource Agreements;
- Business Continuity; and
- Notification to the Central Bank / Regulatory Authority

Outsourcing Performance Supervision and Reporting

Consider monitoring the performance of all outsourced service providers under the following headings:

- Financial Condition of Service Provider
- Governance, Risk Management and Compliance of Service Provider
- Quality of Service and Support

Maintain an outsourcing register of all third-party arrangements. The regulator will want to see this. And maintain a clear understanding of your service provider's "third-parties". (Some times referred to as "sub-outsourcing"). It will also be expected that you conduct periodic due diligence on your critical service providers and not just before entering into an outsourcing arrangement.

Other Actions that may need to be taken in the event of a disruption

Plans will include checklists of things to do and people to contact, but in the heat of the battle and when you are focused on restoring an acceptable level of service things will be forgotten or overlooked. Here's another checklist of things that you might need to take care of in times of disruption.

- Make contact with insurance provider and advise of disruption
- Review any planned meetings / travel arrangements and reschedule
- Check for any critical reports that need to be submitted in the short-term
- Check payroll arrangements and reassure employees that they will be paid
- Check your Revenue obligations and advise / plan for any delays.
- If you have had to vacate the building, redirect your post

Resilience Self-Assessment

How resilient are you? Answer the 21 questions below and see how high you score.

1. Do you have a documented Risk Management policy?
2. Do you have a documented Information Security policy?
3. Do you have an Incident Response Plan?
4. Do you have a Business Continuity Plan?
5. Do you have a Disaster Recovery plan?
6. Has your Board of Directors mandated the development of a plan for greater resilience?
7. Have you conducted a Business Impact Analysis / Assessment in the past 12 months?
8. Have you determined your critical business services?
9. Have you identified all business-critical IT systems?
10. Have you established acceptable Impact Tolerances for all critical services?
11. Have you identified all Third Parties on whom you depend?
12. Are you capturing and analysing incidents, near misses, good catches, and complaints?
13. Have you exercised your resilience plans using a plausible, severe scenario in the past 12 months?
14. Did you involve your key third parties in your response exercises?
15. Do you have specific plans to direct your response to a cyber-attack?
16. Are individuals' roles in a disruptive incident clearly defined and assigned?
17. Do you have the contact details of all employees and a call cascade plan in place?
18. Do you have the contact details of all key third-party service providers in an accessible place?
19. Do you keep a backup copy of your data off your network?
20. Have you tested your data restore procedure in the past 12 months?
21. Do you ensure that there is no over-dependence upon single individuals for any key task?

STANDARDS AND GUIDANCE

A standard is a repeatable, harmonised, agreed and documented way of doing something. Standards are usually developed by standards bodies, like NSAI / ISO, while involving experts from the relevant sector. Guidance documentation is usually produced by a regulator or sector representative body.

When the guidance comes from a regulator it is usually with the expectation that it will be applied with proportionality to the size and complexity of your organisation. For example, Consumer Protection Code. It may also be a non-binding, sector-specific guidance document that describes current bestpractice and how to apply it to your organisation.

At the time of writing these are the current international standards that are published on the broad subject. They are usually revised every 5-7 years so check for the most current version.

ISO 31000:2018 Risk Management – Guidelines.
This is not a certifiable standard; it offers guidance on how to structure your risk management efforts.

ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements.
This is a certifiable management system standard and is the most popular standard covering Business Continuity.

ISO 22316:2017 Security and resilience — Organizational resilience — Principles and attributes.
This is not a certifiable standard but a companion standard to the 22301. It describes the attributes that an organisation should aspire to have to become more resilient.

ISO27001:2018 Information technology — Security techniques — Information security management systems.
This is a Management System standard, which is certifiable. It details the controls necessary for the protection and management of information technology and the information stored / processed.

ISO/IEC 27035:2016- — Information technology — Security techniques — Information security incident management.
This is a companion standard to the 27001 and comes in several parts. Part 1 describes the principles of incident management and Part 2 contains guidelines for incident response planning. Part 3 is guidance for incident response operations.

CEN/TS 17091:2018 Crisis management - Guidance for developing a strategic capability.
This Technical Specification provides guidance on good practice for crisis management.

BS 65000:2014 Guidance on organizational resilience.
This standard describes the nature of resilience and ways to build and enhance organizational resilience. An updated version, reflecting the lessons learned from the Covid pandemic is expected in early 2022

NIST Cybersecurity Framework.
This Framework is voluntary guidance, based on existing standards, guidelines, and practices for organisations to better manage and reduce cybersecurity risk. In addition to helping organisations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organisational stakeholders.

CIS Controls.
The Center for Internet Security is an independent non-profit organisation (US-based). Their set of recommend cyber security controls is often cited as a requirement by insurance companies offering cyber insurance.

The BCI Good Practice Guidelines.
The Good Practice Guidelines (GPG) 2018 Edition is a guide for business continuity and resilience professionals. The GPG Is used as an information source for individuals and organizations seeking an

understanding of business continuity as part of their awareness-raising campaigns and training schedules.

You should also check with your regulator(s) to ensure that you are aware of the most up to date guidance / requirements. At the time of writing this booklet the following guidance documents (some of them Consultation Papers) reflect the current thinking of various bodies, on Operational Resilience.

Basel Committee Principles for Operational Resilience.

In this 12-page document the Committee seeks to promote a principles-based approach to improving operational resilience.

European Commission Digital Operational Resilience for the financial sector Act (DORA).

This 102-page proposal is part of wider work ongoing at European and international level to strengthen the cybersecurity in financial services and address broader operational risks.

Central Bank of Ireland Cross Industry Guidance on Operational Resilience.

This guidance document was issued in Dec 2021 and acts as the Central Bank of Ireland's guidance document for all firms it regulates.

Central Bank of Ireland Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks - 2016.

This paper sets out the CBI's guidance in relation to information technology and cybersecurity governance and risk management by regulated firms in Ireland.

Prudential Regulation Authority Operational Resilience.

Impact tolerances for important business services – PS 6/21. This PRA Policy Statement provides feedback to responses to Consultation Paper 29/19. It also contains the PRA's final policy.

Bank of England / PRA / FCA Operational Resilience.

Impact tolerances for important business services. This paper is issued jointly by the Prudential Regulation Authority, the Financial Conduct Authority and the Bank of England and focuses on areas of commonality.

CalQRisk