Independent Living Fund Scotland

Our Framework for Resilience

OWNER:	ILF Scotland SMT
AUTHOR:	ILF Resilience Hub
DATE DRAFTED:	Sep 2020
DATE APPROVED:	
VERSION:	1.3
STATUS:	Final

Revision History

Date	Version	Author	Comments
04 Aug	1.1	RJ	Update following feedback & drafting
18 Aug	1.2	RJ	Further refinement after feedback
17 Sep	1.3	RJ / JL	Annexes updated

Review/Approval Register

Name	Position / Role	Review / Approval
Paul Hayllor	Director of Digital & Information Services	Review
Harvey Tilley	Chief Operating Officer	Approval

Table of Contents

1. Introduction

Purpose

1.1 The purpose of the Resilience Framework is to enable ILF Scotland (ILFS) to build, sustain and continuously improve proactive and reactive resilience to protect the delivery of ILF Scotland's objectives.

1.2 This document sets out the scope, rationale and operational guidance for the Resilience Framework at ILF Scotland so that all responsible persons have a clear understanding of why this framework is in place and how it functions on a practical level.

Rationale

1.3 The Board approved Resilience Concept is at Fig 1 below. This framework presents the components as a mix of proactive and reactive measures, which are explained below.

Fig 1: ILFS Resilience Concept

Information

1.4 This component of the framework concerns the alignment and integration of resilience with ILFS's operating context, strategy and business objectives to ensure resilience is focussed on issues directly related to strategic priorities. It also governs the acquisition and use of extant and emerging information about ILFS's operating context. This includes fast moving threats requiring a rapid response, slow burning strategic threats and other changes to the environment.

1.5 The framework and associated policies establish accountabilities and responsibilities, information flows and outputs.

Direction

1.6 This component includes the arrangements to govern the performance of the framework and its constituent parts. It sets the direction for resilience and establishes and maintains what is to be done, why and how (including by whom and the competences they require).

1.7 Using the information flow (from the previous component), ILFS undertakes a resilience assessment (at least annually, or following a material change or a significant incident) to establish priorities and objectives for resilience (what is to be protected, what threats are faced, what degree

of impact is 'unacceptable', how will threats be mitigated and how will materialising risks be responded to).

1.8 Based on this understanding ILFS decides how it will resource the effort required, or use the realities of resourcing to make risk based business decisions and prioritise accordingly. The basis of resilience thus established subsequently guides the decision making process as to the overall approach to resilience informing management and board decisions.

Response

1.9 This component deals with the preparation of response plans that detail the strategic, tactical and operational level responses to disruption from minor incident to existential crisis. These plans are based on realistic analysis, a workable architecture and are grounded in the realities of response detailing how the response will be implemented within ILFS.

1.10 These plans are constantly improved to 'nest' well with each other internally and 'fit' with external partners' plans (government(s), suppliers and emergency services for example). ILFS response plans provide clarity as to how decisions are 'made' (how is the right information provided, situational awareness developed and shared) and how are decisions 'taken' (authorities and responsibilities).

Validation

1.11 ILFS sets objectives for resilience and maintains a continuous check on the performance of the framework to ensure that progress towards objectives is monitored. This is integrated with other existing management and improvement practices and provides the assurance evidence required (through audits, root cause analysis, reviews and exercises), identifies areas for improvement and governs the implementation of these improvements to satisfactory completion.

1.12 The validation component also 'houses' communications and the promotion of resilience and awareness raising activities. These pre planned, scheduled communications keep resilience front of mind and keep staff and external partners informed of ILFS's ongoing resilience efforts and response arrangements.

1.13 This component also houses training for staff to equip them with the knowledge and skills to effectively fulfil their roles. This competence is developed into a true capability by sustained participation in regular exercises of escalating complexity; the schedule of these exercises is developed and implemented through this component. The learning and improvement identified are governed by the management practices outlined above.

Scope

1.14 All ILF Scotland activities, processes and people are considered to be within scope. There are no exclusions. Specifically, the framework includes all risk, crisis, continuity and infosec activities, as well as the relevant governance and continuous monitoring and improvement processes.

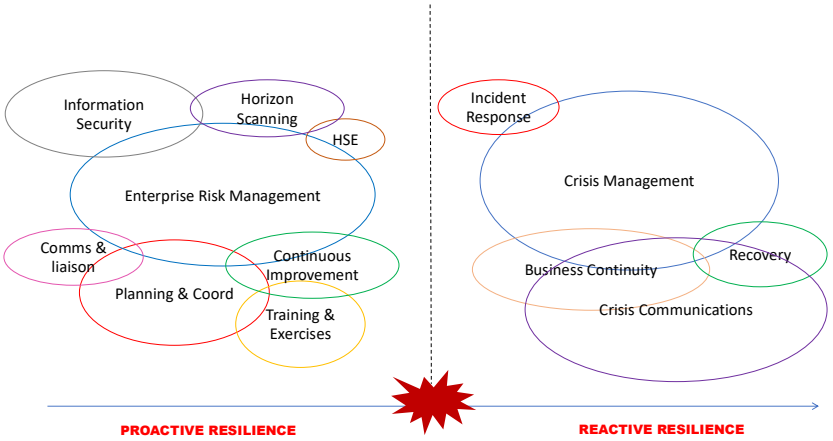

Fig 2: Scope & Components of Proactive & Reactive Resilience

Appetite & Thresholds

1.15 ILFS Risk Appetite and the Thresholds that determine acceptable levels of risk and the guidance for escalation are at in the ILFS Risk Policy.

Integration

1.16 This framework brings together all aspects of proactive and reactive resilience so that collectively ILFS achieves much greater business resilience (more than being good at individual components of it). This alignment and integration enables ILFS to embed resilience into its core business practices, protect ourselves appropriately, take acceptable risks and respond to any threat or disruption accordingly.

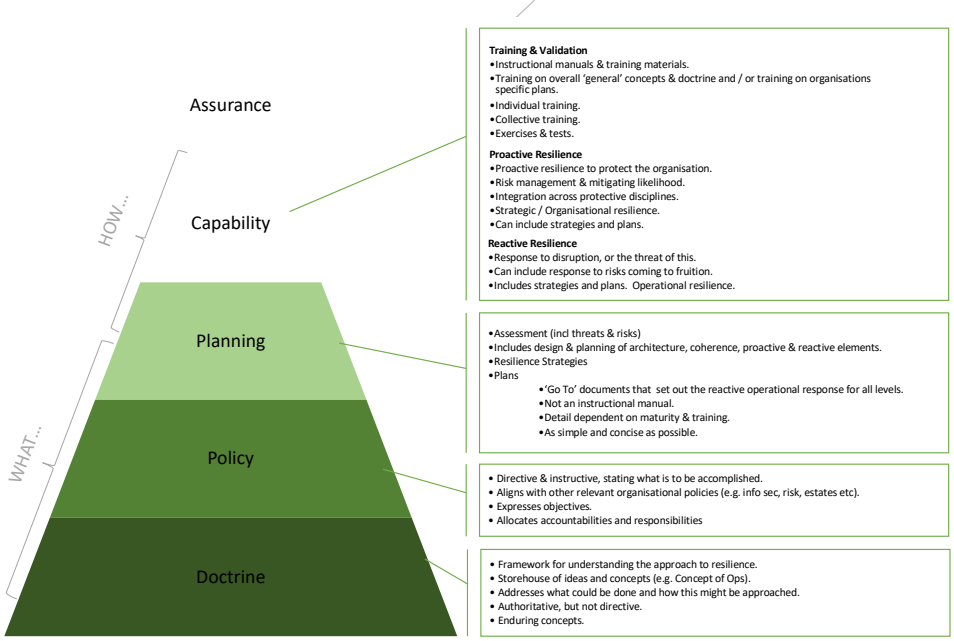

Fig 3: Integrating Resilience

1.17 Part 2 of this document deals with the operational (day to day) functioning of the Framework and the ongoing improvement of the framework's 'management system' and its components and protective disciplines.

2. Operating the Framework

Governance

2.1 Fig 3 below illustrates the structure and information flows within ILFS that govern the management and continuous improvement of all proactive and reactive resilience components. Senior Management are accountable to both the Audit and Risk Committee (and through them) the ILFS Governance Board, for the effectiveness of ILFS's resilience. The Resilience Hub are responsible for the day to day operation of the framework and all of its associated activities.

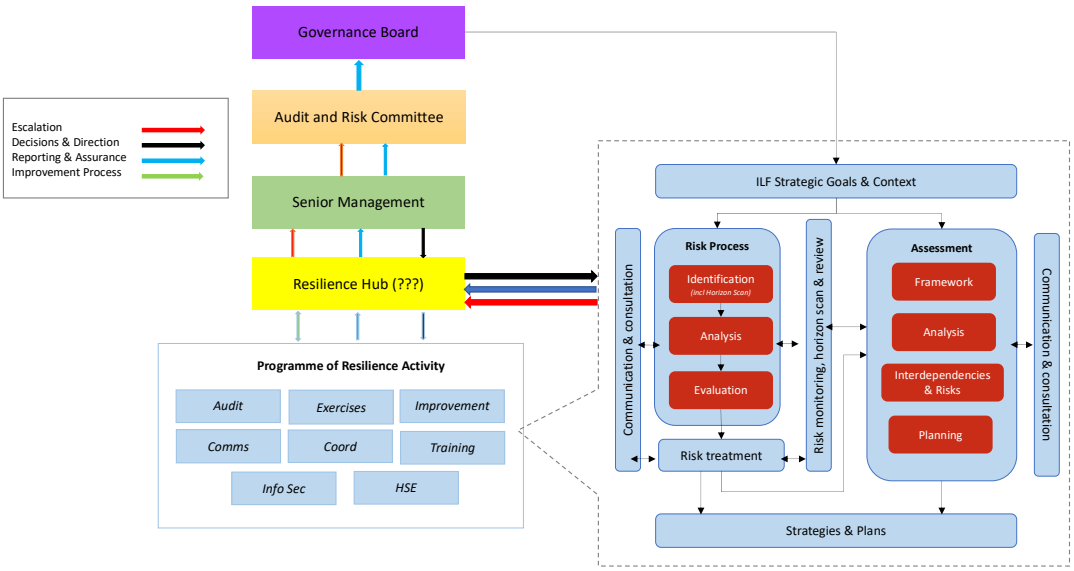

Fig 3: Governance & Architecture

Assurance & Reporting

2.2 The Resilience Hub and other relevant resilience roles will meet once per quarter to review resilience and agree (in detail) activities, objectives and priorities for enhancing resilience.

2.3 On a monthly basis the Resilience Hub will report to Senior Management on (a) the effectiveness of the Resilience Framework in delivering the objectives (see para 2.3) and (b) specific issues concerning resilience. This will 'nest' alongside the reporting of risk.

2.4 Senior Management (and above) will direct and / or approve resilience activity and will decide on risk acceptance and resilience enhancements. These will be governed through the process for continuous improvement (see paras 3.18 – 3.21).

2.5 Senior Management will take the necessary steps to assure themselves of effectiveness, capability and improvement using exercises, tests and audits as detailed in the schedule of resilience activity.

Resilience Framework Objectives

2.6 Objectives for the Resilience Framework will be set annually. The objectives for 2020 & 2021 for the ILFS Resilience Framework are:

a. By end 2020 undertake a full review of risk management processes within ILF Scotland and deploy updated risk management process.

b. Review and standardise all Business Impact Analysis by end May 2021.

c. Undertake resilience assessments across ILF Scotland by end May 2021.

d. By end Jan 2021 develop a timetable of exercise scenarios to undertake throughout the organisation.

e. By end Jan 2021 design a 12 month schedule of resilience activity (in outline) and 6 months (in detail). Sustain this schedule on a rolling basis, updated quarterly.

f. Design an internal schedule of communications to build awareness and understanding of resilience across ILF Scotland and engage stakeholders to make them aware of developments.

g. Undertake a validation exercise on the revised plans by Dec 2021.

h. All resilience staff training to be complete by June 2021, this is to include understanding the new framework and understanding individual roles within the framework.

i. Revise and validate all Incident, Crisis Management and Business Continuity Plans by Aug 2021.

j. Report to Senior Management monthly on resilience activity and performance on an ongoing basis..

k. Monitor the continuous improvement of resilience processes and improvements on an ongoing basis. Provide quarterly assurance reporting on performance (against these objectives (and other initiatives as required)) and on progress and completion of improvement actions to Senior Management.

l. Senior Management to undertake a resilience performance and improvement management review every quarter on an ongoing basis.

Roles and Responsibilities

2.7 The Resilience Framework roles and responsibilities are:

Governance Board

- Set the tone and embody a culture of resilience across ILFS.
- Approve the resilience priorities, risk appetite and exposure for ILFS.
- Actively participate in major decisions affecting ILFS risk profile or exposure to risk.
- Through annual assurance and the A&R Committee's activity, monitor the management and implementation of the Framework.
- Ensure that significant risks are addressed to reduce the likelihood of adverse events occurring and the ability of ILFS to respond effectively and reduce impact.

Audit and Risk Committee

- Monitor and review the resilience, control, governance and associated assurance processes.
- Provide assurance to the Governance Board as to the effectiveness of resilience, the schedule of activity and operation of the ILFS Resilience Framework.
- Maintain an overview of the aggregated level of risk borne by ILFS and provide direction and approval for senior management's approach.

Senior Management

- Accountable to the Audit and Risk Committee for the effectiveness of ILFS resilience.
- Recommend the risk appetite and tolerances to guide resilience decisions.
- Accountable to the Governance Board for determining the ILFS resilience priorities, based on the ILFS Resilience Assessment process, at least annually.
- Responsible for ensuring the effective identification and escalation of risks.

- Accountable to the Audit and Risk Committee for the design and delivery of the ILFS Resilience Programme of Activities.
- Responsible for resilience decisions, including risk treatments, resourcing and giving direction to the Resilience Hub and other ILFS staff.
- Undertake monthly Management Reviews to monitor the functioning of the Resilience Framework and assess the effectiveness of ILFS proactive and reactive resilience.
- Agree corrective actions and prioritise as necessary. Monitor implementation.

Resilience Hub

- Responsible for recommending the ILFS resilience priorities.
- Responsible for the effective day to day operation of the Resilience Framework.
- Responsible for coordination of proactive and reactive resilience across ILFS.
- Responsible for the design and delivery of the schedule of resilience activity.
- Responsible for producing relevant reporting for monthly review by Senior Management.
- Responsible for the aggregation, further escalation and routine reporting of risk, in keeping with risk appetites and tolerances.
- Coordinating risk treatments with all other resilience priorities, strategies and plans.
- Recommend and coordinate the effective implementation (by appropriate, qualified staff) of corrective actions across all proactive and reactive components of resilience.

Responsible Owners / Champions (Management Team)

- Responsible for day to management of a component of ILFS resilience or a specific risk.
- Responsible for implementation of the tasks and activities determined by the Resilience Hub.
- Responsible for coordination of their activities with other responsible owners, with the Resilience Hub.
- Responsible for the ownership of specific risks.
- Responsible for escalating risks that exceed tolerance.

Staff

- Responsible for reading, understanding and complying with ILFS Resilience framework and Risk Management Policy.
- Responsible for identifying risks and reporting to the relevant member of the management team.
- Attending mandatory and any other relevant training courses.

Competences

2.8 The specific competences required for Resilience role holders are specified at Annex C. It is ILFS policy that all role holders will be qualified and remain current for their designated role. Full training records are held on You Manage.

3. Fitting Together the Components of Resilience

3.1 Figure 2 is reproduced here for ease of reference and indicates the components, relative priority and 'fit' of proactive and reactive resilience within ILFS.

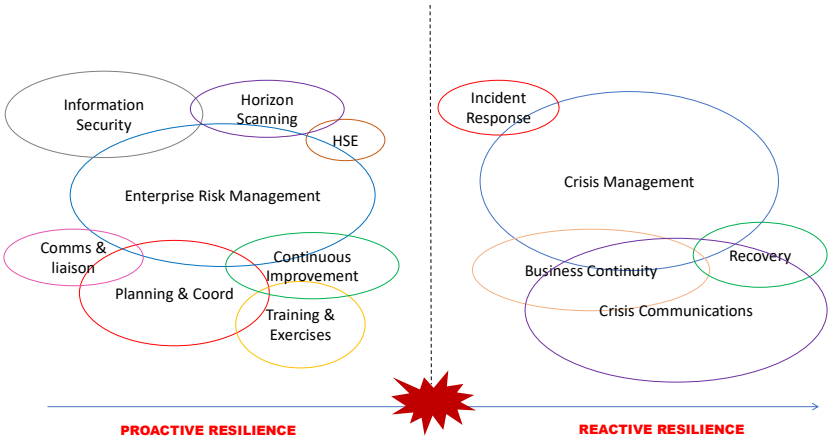

Fig 2 (Repro): Scope & Components of Proactive & Reactive Resilience

3.2 Each of these components and their responsible owner is described below.

Proactive Resilience

Horizon Scanning

3.3 This is the process of identifying potential threats that may disrupt ILFS's critical processes or present opportunities that can be exploited. This allows for future planning for key risks and opportunities that materialise over time.

3.4 Paul Hayllor is responsible for managing the horizon scanning process.

3.5 More information can be found in the ILFS Risk Management Policy and Aide Memoire.

Risk Management

3.6 Risk management allows organisations to manage the effect of uncertainties (positive or negative) on objectives. ILFS Risk Handbook sets out the risk management activities that follows a process of risk identification, assessment, evaluation (to understanding the degree of threat or opportunity), implement treatment(s), and monitor the risks and controls in place. All of this will be regularly communicated and assured as a key component of the ILFS Resilience Framework……

3.7 Nadeem Haneef is responsible for the effective management of risk within ILFS.

3.8 More information can be found in the ILFS Risk Management Policy and in the Risk Management Handbook.

Information Security

3.9 Information security is a set of practises that keep sensitive information and data secure from unauthorised access. ILFS Information Security Governance Handbook sets out the operational guidance to all staff to ensure good data and information management practices in order to be able to maintain and extend the trust and confidence of recipients and professional colleagues in ILF Scotland.

3.10 All staff regardless of employment contract are directed to read, understand and adhere to the contents of the Information Security Governance Handbook.

3.11 Paul Hayllor is accountable for the management of ILFS Information Security.

Health, Safety & Environment

3.12 ILFS has a responsibility for protecting health and safety of employees, stakeholders and all those with whom ILFS engages. Adherence to the ILFS Health and Safety Manual will reduce complications to health, safety and welfare, enabling everyone to carry out tasks safely and in that way it is a key contributor to resilience.

3.13 Aileen McNiven is responsible for the management of HSE at ILFS.

3.14 More information can be found in the ILFS Health & Safety Manual.

Planning & Coordination

3.15 Planning & Coordination includes the analysing of ILFS's objectives, strategy and key obligations to identify the key strategic Business Continuity requirements. This is carried out through a framework of analysis that assess the losses of key process and resources needed to deliver the key objectives and Business Continuity requirements, the impacts of threats posed to them and identify gaps to be addressed. This results in the development of Detailed Planning directions for Business Continuity Plans that consist of solutions to be implemented, the investment (time, effort, resources) to develop solutions, and which risks are being accepted. This planning includes collaboration and integration with suppliers and stakeholders.

3.16 Paul Hayllor is responsible for coordinating this activity.

3.17 More information can be found in ILF Scotland's business continuity planning direction documents.

Continuous Improvement

3.18 All proactive and reactive components of resilience and the Resilience Framework itself are subject to the ILFS continuous improvement process. Improvement activity is coordinated and driven by the Resilience Hub and governed by senior management, who are accountable to the Audit and Risk Committee for delivering ongoing continuous improvement. The process within ILFS is summarised at Fig 4.

3.19 Improvements identified that require effort by and engagement with suppliers and stakeholders are also subject to this process. This particularly applies to suppliers that are deemed critical for resilience or who support ILFS critical activities.

Identify	• Define SMART objectives for resilience. • Resilience activity identifies a problem / improvement with a component or the framework. • Record on the improvement register. • Associated risk(s) enter risk management system.
Assess	• Define the problem / issue. • Determine root cause(s). • Identify possible fix(es).
Plan	• Present improvement options for decisions. • Agree resourcing. • Assign responsibilities & timelines. • Update improvement register.
Action	• Responsible staff implement action(s) to improve. • Report progress, other findings or issues. • Demonstrate 'success'.
Check	• Periodic management review and other checks (audit etc) to assure effectiveness of framework & improvement actions. • Regular reporting to governance.

Fig 4: Continuous Improvement

3.20 Nadeem Hanif is accountable to Senior Management for continuous improvement of resilience. Joanne Leitch is responsible for coordinating and managing day to day improvement activity.

3.21 More information can be found through the Resilience Hub.

Training & Exercises

3.22 Resilience related training equips our people with skills and knowledge, whilst regular exercising provides an opportunity for our reactive resilience teams to practice and improve performances. These activities help us identify areas for improvement and are a great opportunity to test effectiveness of people, plans and processes, and shine a light onto any in specific capability gaps. As a matter of policy ILFS sets specific objectives for training and exercising and progress towards these objectives is measured on an ongoing basis.

3.23 Joanne Leitch is responsible for the management and coordination of resilience training and exercises.

3.24 More information can be found in the ILFS Resilience Programme of Activity.

Communications & Liaison

3.25 ILFS will communicate internally and externally as an ongoing aspect of developing resilience and managing risk. This includes liaison with internal departments, resilience leads, all resilience disciplines, all staff as well as our suppliers and stakeholders.

3.26 This includes all resilience activities and the assessment component of planning that is undertaken at least annually or after a significant incident. It also includes all efforts to generate interest in and engagement with resilience and to sustain awareness across ILFS and with our suppliers and stakeholders.

3.27 Normal internal communications channels and the Resilience Programme of Activity contain further details.

Reactive Resilience

Response Architecture

3.28 The architecture that structures reactive resilience and response arrangements is detailed in the ILFS Business Continuity Plan.

Incident Management

3.29 Incident management is the escalation process in the event of any incident that needs an ILFS response. ILF Scotland Business Continuity Plan lays out this process of identifying, reporting and responding to incidents to recover from them.

3.30 Paul Hayllor is responsible for the maintenance and currency of incident response processes. In response to an incident arising, the appropriate member of the senior management is responsible for the management of the ILFS Incident Management process, as set out in the Business Continuity Plan.

3.31 Further information can be found in the ILF Business Continuity Plan.

Business Continuity

3.32 Our Business Continuity enables ILFS to manage the impacts of any disruption to our priority activities to deliver a good enough service in enough time and avoid unacceptable impacts. ILFS Business Continuity Plan sets out the operational guidance for incident and BC responses.

3.33 Paul Hayllor is responsible for the management of this process and Business Continuity Plan.

3.34 More information can be found in the ILFS BC Plan.

Crisis Management

3.35 Crisis management enables ILFS to deliver a coordinated overall response to a major incident that threatens the delivery of our objectives, reputation or the existence of ILFS. The ILFS Business Continuity Plan provides a framework that includes a relevant command and control structure; escalation and activation of this structure; information flows; management of the incident; stand down and recovery; identification of key roles and responsibilities, and; guidance that enables the ILF senior teams to make critical decisions during a crisis.

3.36 Harvey Tilley, Chief Operating Officer, is responsible for ensuring ILFS crisis management capability and plans remain current.

3.37 Further information can be found in the ILFS Business Continuity Plan.

Crisis Communications

3.38 Crisis Communications governs how ILFS will communicate with key internal and external parties in a crisis using traditional and social media, and all internal channels. It also includes measures to allow ILFS to protect our reputation during disruption.

3.39 Holly Child is responsible for ensuring ILFS crisis communication capability and plans remain current.

3.40 Further information is in the ILFS Crisis Communications Plan.

Recovery

3.41 Recovery describes the trajectory and coordination of activities to return ILFS to a normal / new normal state of operations after BC measures have been stood down. It is included as a specific component of BC / CM planning.

3.42 The ILFS Crisis Management Team will govern Recovery \planning and allocate responsibilities at the appropriate time in ILFS crisis response.

3.43 Further information is available in the Business Continuity Plan.

Appendix Summary

Annex A – Policies

The following policies are relevant to the Scope of Resilience within ILFS. To view the policies listed below please log into YouManage, they are all published under Documents/Policies and Procedures. A copy is also located within G:\??

- Data Protection Policy
- Learning & development Policy
- Lone Working Policy
- Password Guidance
- Health & Safety Manual 2019

The following policies all exist in the current Information Governance Handbook which can be found within the same section of YouManage.

- Information Security Policy
- Desk & Workspace Policy
- Internet & Communications Policy

The policies and plans below are located within the ILF Scotland network, please see hyperlinks below:

- Risk Policy
- Business Continuity Plan
- Incident Management Plan
- Cyber Security Policy

The Framework is included as part of the staff induction pack

- Staff Induction Pack

Annex B – Definitions

- **Accident**: Unplanned, unexpected and undesirable happening, which results in or has the potential for injury, harm, ill-health or damage. (HM Government (2009) Emergency Response and Recovery).
- **Activity**: set of one or more tasks with a defined output (ISO22301)
- **Business Continuity:** Capability of the organisation to continue delivery of products or services within acceptable timeframes at predefined capacity during a disruption. *(ISO 22301)*
- **Business Impact Analysis**: Process of analysing the impact over time of a disruption on the organisation. *(ISO 22301)*
- **Command and Control**: Activities of target-orientated decision-making, assessing the situation, planning, implementing decisions and controlling the effects of implementation on the incident. (ISO 22300 Societal Security – Vocabulary).
- **Common Recognised Information Picture (CRIP)**: Statement of shared situational awareness and understanding, which is briefed to crisis decision makers and used as the accepted basis for auditable and defensible decisions (developed from PAS 200 Crisis Management – Guidance and Good Practice).
- **Co-ordination**: way in which different organizations (public or private) or parts of the same organization work or act together in order to achieve a common objective (ISO 22300 Societal Security – Vocabulary).
- **Crisis**: Inherently abnormal, unstable and complex situation that represents a threat to the strategic objectives, reputation or existence of an organization.
- **Crisis Management**: A strategic level activity, led by a Crisis Management Team, to manage a crisis and deal with issues arising (both during and after) in order to bring the situation under control.
- **Disruption**: incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to the organisations objectives.
- **Emergency**: Event or situation that threatens serious damage to human welfare, or to the environment, or war or terrorism which threatens serious damage to national security (HM Government (2009) Emergency Response and Recovery).
- **Incident**: Event that can be, or could lead to, a disruption, loss, emergency or crisis. (ISO22301).
- **Information Management**: The collection, collation, assessment and dissemination of appropriate information to enable decisions and action. *(EPS Ltd)*
- **Management System**: set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives. (ISO22301).
- **Prioritised activity**: an activity to which urgency is given in order to avoid unacceptable impacts to the business during a disruption. (ISO22301)
- **Process**: a set of interrelated or interacting activities which transforms inputs into outputs. (ISO 22301
- **Product and service**: output or outcome provided by an organization to interested parties.
- **Requirement**: need or expectation that is stated, generally implied or obligatory.

- **Recovery Time Objective**: Period of time following an incident within which product or service must be resumed, activity must be resumed, or resources must be recovered. *(ISO 22301)*
- **Resilience:** The ability to absorb and adapt to volatility, uncertainty, complexity, ambiguity and disruption, while continuing to deliver objectives.
- **Risk:** The effect of uncertainty on objectives.

Annex C - Competences

For each defined role set out in this framework there will be a set of core competencies. These are identified below and act as a guidance for the role.

Role	Competencies
Governance Board	• Leadership on management of risk & resilience • Influence & Communication • Decision making • Protect organisation reputation
Audit & Risk Committee	• Risk Management • Assurance and influence
SMT	• Risk Analysis & Management • Governance & Organisation • Influence Resilience Hub outcomes • Reporting
Resilience Hub	• Understanding organisation priorities & strategy • Relationship management • Risk Analysis & Management • Information Management • Report Writing • Exercise & Test planning and delivery
Responsible Owners	• Risk Management & Ownership • Report Writing • Communications Skills
Staff	• Risk Identification & Reporting • Communication Skills • Familiarisation of Risk & Resilience Framework