SFJCCAA2

Manage and share information for decision making in resilience and emergencies

Overview

This standard is about effective information management, which involves assessing data integrity, addressing uncertainty, ensuring secure and ethical information handling, and sharing information appropriately. Information should be shared by default where possible to support coordination and decision-making, but must also be governed by legal, operational, and security considerations. Management and sharing processes, agreements, and protocols should be continuously monitored and adapted to remain fit for purpose in dynamic environments.

This standard applies to working with public, private, and voluntary sector organisations across the resilience cycle.

Performance criteria

You must be able to:

1. collaborate to assess and improve information management, sharing structures, processes, and products in line with legislation, policies and guidance
2. identify and gather data, information and intelligence to support evidence-based decision making
3. verify the integrity of data, intelligence, and information for the intended purpose and the phase of the resilience cycle
4. work collaboratively with data and intelligence specialists to create the systems, protocols and information products needed
5. analyse information to identify facts, patterns and trends
6. evaluate and manage uncertainty in information across the resilience cycle
7. present, map, or visualise information to meet user needs, clearly communicating any limitations
8. identify the need for, develop and implement information sharing policies, procedures and agreements in line with legislation, policies and guidance so that information can be shared effectively during response and recovery
9. manage and share information safely, securely, and ethically, ensuring it is proportional to the need and in accordance with information sharing agreements
10. implement and operate within governance processes to ensure information management adapts to changing needs and remains efficient, legal, ethical, and secure.

Knowledge and understanding

You need to know and understand:

1. internal and external partners and stakeholders, their information needs and preferences
2. how data, information, and intelligence are used to support rigorous decision-making and collaboration across the resilience cycle
3. ethical and accountable approaches to information handling
4. factors that influence the validity and reliability data, information and intelligence
5. methods for managing and communicating uncertainty and limitations in data, information, and intelligence
6. the benefits and risks of using digital and AI systems to manage information
7. legislation, regulations, policies and guidance for information management and sharing
8. types of sensitive information and the restrictions on them, including national security, public safety, commercial sensitivity, and personal data
9. risk management in information management and sharing, including security classification, vetting, data minimisation, and disposal across the resilience cycle
10. data sources and analysis techniques relevant to role and resilience cycle phase
11. the benefits and limitations of information management systems, agreements, and protocols
12. principles of designing and implementing information systems and protocols for effective information management
13. governance structures and standards for improving information management and sharing
14. the role of reflective practice in evaluating performance, identifying areas for improvement and professional development

Glossary

Data, information, and intelligence

• Data: Unprocessed facts and figures.

• Information: Processed data with context.

• Intelligence: Information that has been thoroughly analysed and combined from multiple sources to provide deeper insights.

Information integrity

The accuracy, reliability, and consistency of information. Information integrity in resilience and emergencies enables effective decision-making.

Uncertainty management

The identification, assessment, and mitigation of uncertainties in data and information, including addressing gaps, inconsistencies, and source reliability. It also involves managing the consequences of inherent uncertainties, especially in risk-based information, to support informed decision-making.

Communicating uncertainty

Methods for transparently conveying uncertainty in information as a means of ensuring stakeholders understand limitations and manage risks associated.

Types of uncertainty

Categories of uncertainty affecting resilience decision-making, including data uncertainty, model uncertainty, situational uncertainty, and behavioural uncertainty

Information governance

The policies, standards, and processes that ensure information used in resilience and emergencies is handled responsibly, accurately, securely, and in compliance with relevant regulations.

Sensitive Information

Information which, if disclosed to the public would, or would be likely to (a) adversely affect national security, (b) adversely affect public safety, (c) prejudice the commercial interests of any person; or is information that is personal data, within the meaning of section 1(1) of the Data Protection Act 2018, disclosure of which would breach that Act.

Information Sharing Agreements (ISAs)

Formal agreements defining how data is shared between organisations, including its purpose, security measures, and responsibilities. The ICO recommends ISAs to ensure accountability under UK legislation.

Data Minimisation

A legislative principle requiring organisations to collect and process only the minimum

necessary personal data. This reduces data breach risks and ensures compliance with data protection laws.

Risk communication

The exchange of risk-related information among stakeholders to support awareness, preparedness, and informed action. It involves using effective methods to disseminate information and facilitate discussions, ensuring a shared understanding.

Defensible decisions

Decisions based on transparent, evidence-based reasoning, ensuring accountability and justification under scrutiny. These decisions clearly reference the evidence upon which they are based.

Evidence-based decisions

Decisions that rely on data, validated information, and tested models to ensure credibility and effectiveness. These decisions are transparent about the evidence used, making them defensible under scrutiny.

Links to other NOS

SFJCCAA3

SFJCCAA2

Manage and share information for decision making in resilience and emergencies

Developed by	Skills for Justice
Version Number	3
Date Approved	31 Mar 2025
Indicative Review Date	31 Mar 2029
Validity	Current
Status	Original
Originating Organisation	Skills for Justice
Original URN	SFJCCAA2, SFJCCAA3
Relevant Occupations	Associate Professionals and Technical oc, Health Professionals, Police Officers, Public Services and Care, Resilience and Emergencies Professional: Fire Officer
Suite	Resilience and Emergencies
Keywords	co-operation; exchanging information; emergency; emergencies; emergency management; activity; exercise