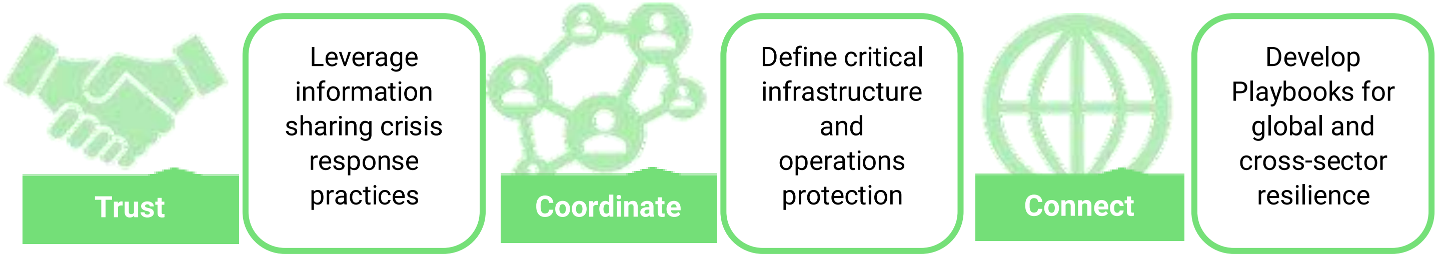
FS-ISAC

All-Hazards Framework

TLP White Version 2019 1.2, Date October 15, 2019

Table of Contents

Objectives of the Framework



Trust

Leverage information sharing crisis response practices

Coordinate

Define critical infrastructure and operations protection

Connect

Develop Playbooks for global and cross-sector resilience

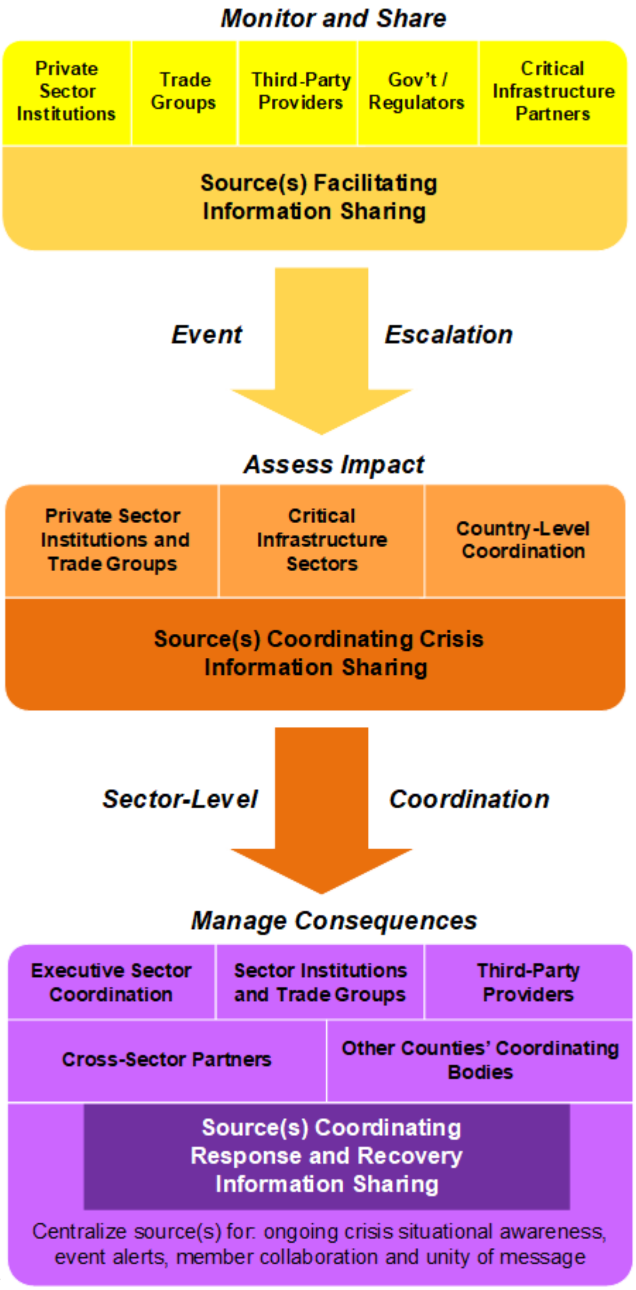
Use of Framework for Responding to a Crisis

Purpose of Framework	The FS-ISAC All-Hazards Framework ("Framework") outlines the key elements of trusted information sharing to evaluate and respond to physical and cyber crises. The key elements include trusted information sharing to gain situational awareness; analysis of threats, vulnerabilities, impact to critical processes, and infrastructure; and coordination with government agencies and other stakeholders. The Framework is voluntary, country-neutral and adaptable for use by different critical infrastructure sectors. The objective is to enhance sector, regional, national and global resiliency. This does not replace institution obligations to meet regulatory communication requirements. The Framework provides instructions and recommends content for developing a Playbook Appendix.
How to Use the Framework and Appendices	• Use the FS-ISAC All-Hazards Framework to develop country, sector or event specific Playbook Appendix. Playbook Appendices use trusted information sharing crisis response practices, define coordination of critical infrastructure, operations activities and seek to connect global and cross-sector resilience organizations. • Articulate the coordination activities within a country or region, identify stakeholders who lead coordination and define stakeholder participation in trusted information sharing global activities. • Identify roles and decisions made by trusted sharing communities, private sector and public sector organizations when they collaborate during crisis events. • Include various skills and complementary peer communities such as: technical, security, business operational, critical business lines and suppliers. • Include Framework crisis response information sharing in company response plans.
Definition of a crisis	A "crisis" is defined as a large-scale disruption that impacts, or have the potential to impact, the security, stability, operations and/or reputation of critical infrastructure sectors, business services and critical national functions. When developing a Playbook Appendix, public and private sector partners discuss and assess the severity of threats and events to determine if they reach a "crisis" threshold.

***FS-ISAC Traffic Light Protocol** (TLP) WHITE – TLP: P WHITE information may be distributed without restriction, subject to copyright controls.*

Stages of Information Sharing All-Hazards Framework Model

The following diagram represents the three stages of information sharing during an event. The first is monitor and share. The second is assess impact. The third is manage consequences. Use the All-Hazards Framework model to achieve different goals. It is a collaborative tool that identifies information sharing stakeholders and practices. Use this model as a roadmap for developing a country playbook appendix and as a tool for exercises to facilitate information sharing awareness and training.


Monitor and Share
Private Sector Institutions
Trade Groups
Third-Party Providers
Gov't / Regulators
Critical Infrastructure Partners
Source(s) Facilitating Information Sharing
Event
Escalation
Assess Impact
Private Sector Institutions and Trade Groups
Critical Infrastructure Sectors
Country-Level Coordination
Source(s) Coordinating Crisis Information Sharing
Sector-Level
Coordination
Manage Consequences
Executive Sector Coordination
Sector Institutions and Trade Groups
Third-Party Providers
Cross-Sector Partners
Other Counties' Coordinating Bodies
Source(s) Coordinating Response and Recovery Information Sharing

Centralize source(s) for: ongoing crisis situational awareness, event alerts, member collaboration and unity of message

Uses for the All-Hazards Framework

To Identify and Guide Sharing Activities

- ☑ List trusted sharing activities for each stage of crisis response;
- ☑ Identify crisis alerts, calls, trusted sharing guidance; and
- ☑ Identify how crisis collaboration, impact assessment and mitigation occur.

To Develop Playbook Appendix

- ☑ Collect and review existing public/private Playbooks;
- ☑ Document crisis response entities that engage during each stage of crisis response;
- ☑ Use crisis stakeholder tables to define crisis roles, responsibilities and decisions;
- ☑ Develop draft Playbook appendix;
- ☑ Exercise Playbook with stakeholders; and
- ☑ Continue to enhance document.

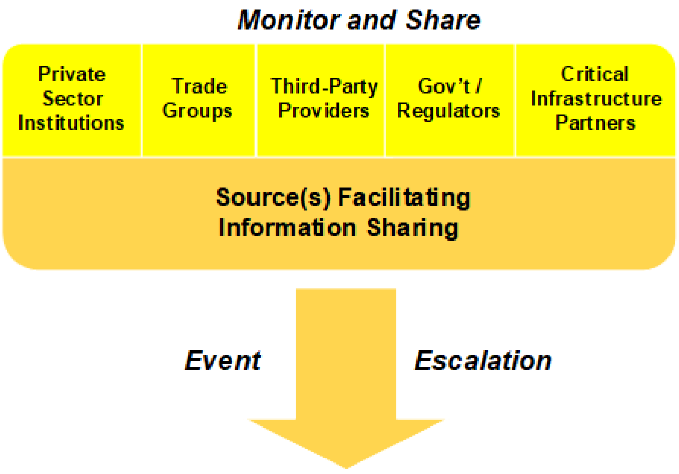
To Identify Trusted Sharing During Exercises

- ☑ Identify crisis response stakeholders during exercise planning;
- ☑ Ask questions during the exercise, to identify when trusted sharing is taking place;
- ☑ Identify stakeholder roles and decisions;
- ☑ Identify gaps in clarity of collaboration and decision making; and
- ☑ Document exercise results using Framework templates.

Stage 1: Monitor and Share

Information sharing stakeholders include trusted information sharing organizations, industry trade groups, critical infrastructure partners, government, regulators and third-party vendors, and other organizations. During the Monitor and Share stage stakeholders work to determine:

- ☑ Which sector organizations are contributing to trusted information sharing to protect the sector?
- ☑ What critical functions and organizations are impacted? Where are sources of accurate situational awareness?
- ☑ What organizational risks exist?
- ☑ Is there potential for systemic or cross-sector impacts?
- ☑ What sector messaging is developed and by whom?


Monitor and Share
Private Sector Institutions
Trade Groups
Third-Party Providers
Gov't / Regulators
Critical Infrastructure Partners
Source(s) Facilitating Information Sharing
Event
Escalation

Information sharing communities encourage sector participants and third-party providers to share event status reports within their trusted information sharing communities, trade groups, and with government.

Components of a Playbook Appendix

Instructions for Reporting Events

Include in the Playbook Appendix instructions for sector participants to report cyber and physical events. Identify where information is coordinated and available to guide awareness and fact validation for trusted public-private sharing stakeholders. This section of the Playbook Appendix may include the following:

- ☑ Specify a trusted communication protocol, such as Traffic Light Protocol.
- ☑ Identify how sector participants should communicate cyber and physical critical events.
- ☑ Provide contact information for government and/or private sector reporting.
- ☑ Identify a central reporting organization for trusted information sharing.
- ☑ Describe how sector participants contact the centralized contact
- ☑ Describe crisis coordination communities.
- ☑ Describe how trusted communities are activated during a crisis.
- ☑ Include instructions or tools to use for crisis coordination.

Reasons to Collaborate through Information Sharing

To ask about an event or report an incident; with reference or anonymous request.

To inquire if public messaging for the event has been determined or to validate messaging.

To request that information sharing groups reach out to government or their global network for situational awareness and fact

To validate the facts of an event and request situational awareness or alerts.

To ask for assistance with other critical infrastructure such as: electricity, communications, transportation, etc.

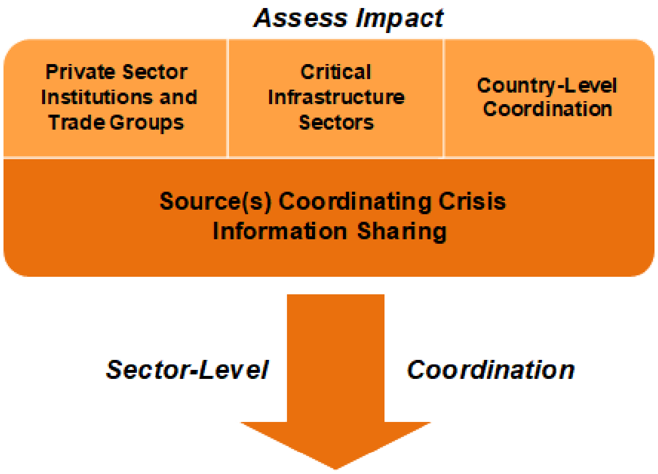
To ask if trusted communities are activated for the event; or ask questions of the peer community.

Stage 2: Assess Impact

During the Assess Impact stage sector participants collaborate to identify critical functions that are disrupted and at risk. Information sharing communities identify impact from: technical and operational interdependencies, needed resources, supply chain and global functions.

Cyber security impact assessment includes trusted sharing of threat and vulnerability information. Stakeholder experts in technology and critical business processes collaborate. Impacted organizations may dynamically form trusted communities to achieve collective assessment, response and recovery.

When cyber or physical events threaten critical functions, the potential for systemic impact and broad consequences exists which require cross-sector and cross-country collaboration.


Assess Impact
Private Sector Institutions and Trade Groups
Critical Infrastructure Sectors
Country-Level Coordination
Source(s) Coordinating Crisis Information Sharing
Sector-Level
Coordination

Components of a Playbook Appendix

Sector Event Escalation Thresholds

When building a Playbook, identify and include thresholds which stakeholders use to guide crisis assessment of cyber and physical events. Sector stakeholders agree on thresholds for crisis escalation, guidelines for crisis collaboration and rules for engagement.

- ☑ Consider process for private sector and government to agree on public messaging.
- ☑ Include timeline of crisis response information sharing and define when groups engage.
- ☑ Define how crisis teams activate.
- ☑ Identify partners who will be contacted to validate event impact to critical functions.
- ☑ Define the critical stakeholders, trade groups and government organizations who participate in sector impact assessment.
- ☑ Identify partners who can contribute to analysis of systemically important impacts for the sector.

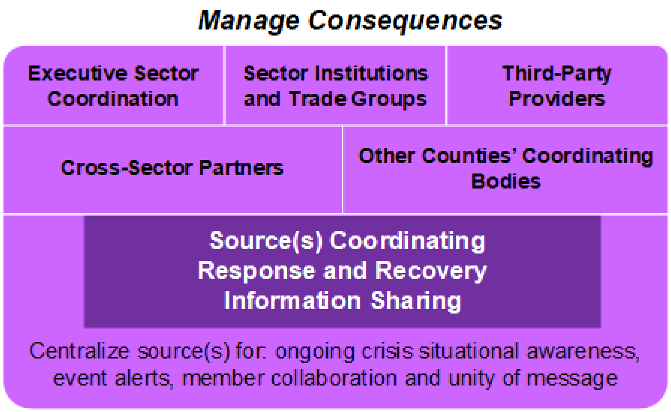
Impact Assessment Information Sharing components

- ✓ **Likelihood:** that an incident occurs
- ✓ **Geographic Importance:** impact to critical infrastructure
- ✓ **Critical Supporting Service:** critical sector supply chain disrupted
- ✓ **Impact Landscape:** number of stakeholders impacted
- ✓ **Dependent Sector:** disruption to lifeline or critical infrastructure sectors
- ✓ **Risk Complexity:** identified potential for cascading disruption
- ✓ **Member Importance:** escalation by sector stakeholders
- ✓ **National Importance:** impact to national critical functions
- ✓ **Systemic Risk:** domino effect with global consequences

Stage 3: Manage Consequences

When a cyber or physical event escalates to disrupt a critical business services or supply chain, trusted crisis management teams engage for response and recovery activities and to collectively manage the consequences of the crisis. Information sharing activities may include:

- Identify government coordination routines and meetings which engage the private sector.
- Identify private and public sector sources where response and recovery coordination are taking place.
- Identify priorities for consequence management.
- Identify global coordination stakeholders.
- Define how subject matter experts will engage, including impacted third-party suppliers.
- Identify technology coordination taking place between impacted stakeholder.
- Identify sources where public messaging will be coordinated.



Manage Consequences

Executive Sector Coordination

Sector Institutions and Trade Groups

Third-Party Providers

Cross-Sector Partners

Other Counties' Coordinating Bodies

Source(s) Coordinating Response and Recovery Information Sharing

Centralize source(s) for: ongoing crisis situational awareness, event alerts, member collaboration and unity of message

Components of a Country Playbook Appendix

Coordination and Consequence Management

The All-Hazards Playbook appendix recommends the use of playbook templates. The Manage Consequences section of the Playbook Appendix may include the following content:

☑ Document private sector and government roles and responsibilities during a crisis.
☑ Where able, identify decisions and ownership.
☑ Include cross-sector partnerships for trusted sharing of intelligence and crisis collaboration.
☑ Define how cross-sector supply chain failures will be identified and joint course of action will be identified.
☑ Utilize trusted sharing to Identify critical needs and gaps for remediation; and prioritize them.
☑ Deconflict meetings taking place with other stakeholders.
☑ Generate transaction availability reporting to assist in critical infrastructure recovery.
☑ Convene meetings to obtain situational awareness update from impacted parties. manage the coordination of information sharing and recovery efforts.
☑ Participate in trusted sharing crisis calls, alerts and surveys.

Event Closure

After the crisis subsides, information sharing stakeholders facilitate an after-action assessment to identify areas of sector collaboration improvement and direct changes to improve the *All Hazards Playbook Appendix*. Once the crisis ends, the crisis coordination teams return to steady-state responsibilities for cyber and physical threat information sharing. The Crisis Management teams stand down and are closed.

Crisis Response Information Sharing and the NIST Cyber Security Framework

The FS-ISAC All-Hazards Framework and Playbook Appendices promote the development of trusted peer networks to create a collective defense against all-hazards events. During a crisis event, trusted groups engage to share vital situational awareness, including information and control activities defined by the NIST Cyber Security Framework (CSF). What follows is a partial list of alignment between the frameworks.

Function	NIST CSF Category	NIST CSF Subcategory	CRIS Framework Objectives
IDENTIFY (ID)	**Business Environment**	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	During crisis response, trusted stakeholders join in critical infrastructure impact assessment to protect dependent services at risk.
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	
	Risk Assessment	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	Trusted sharing communities collaborate on risk assessment, impact risk analysis and ongoing crisis vulnerabilities.
		ID.RA-4: Potential business impacts and likelihoods are identified	
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	
PROTECT (PR)	**Protective Technology**	PR.AC-1: Identities and credentials are managed for authorized devices and users	Security solutions are shared for crisis mitigation, response & recovery.
DETECT (DE)	**Anomalies and Events**	DE.AE-2: Detected events are analyzed to understand attack targets and methods	Anonymous and trusted Information sharing communities engage in early detection of anomalies and events. Skilled subject matter experts share knowledge to expand sector awareness and protection.
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	
		DE.AE-4: Impact of events is determined	
	Detection Processes	DE. DP-4: Event detection information is communicated to appropriate parties	
RESPOND (RE)	**Response Planning**	RS.RP-1: Response plan is executed during or after an event	Provide guidance to develop sector and country coordination response plans. Use the Country Playbook appendix to define country and regional operational information sharing activities. Stakeholders coordinate their crisis response activities and agree on event facts and public messaging. Public and private sector stakeholder participate in trusted information sharing to achieve situational awareness for cybersecurity and consequence management.
	Communications	RS.CO-1: Personnel know their roles and order of operations when a response is needed	
		RS.CO-2: Events are reported consistent with established criteria	
		RS.CO-3: Information is shared consistent with response plans	
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	
	Analysis	RS.AN-2: The impact of the incident is understood	
RECOVER (RC)	**Recovery Planning**	RC.RP-1: Recovery plan is executed during or after an event	Develop Country Playbook appendix and use during exercises and actual events. Revise the document to incorporate improvements from exercise and actual events.
	Improvements	RC.IM-1: Recovery plans incorporate lessons learned	
	Communications	RC.CO-1: Public relations are managed	