ISAO 100-1

Guidelines for Establishing an ISAO

Draft Document—Request For Comment

ISAO 100-1 v0.1
ISAO Standards Organization
July 22, 2016

Acknowledgements

This publication was developed by the Information Sharing and Analysis Organization Standards Organization (ISAO SO) with representatives from the private, professional, and government communities in an ongoing effort to produce a unified voluntary set of guidelines and guidance for information sharing. The ISAO SO and the Working Group leadership are listed below.

ISAO Standards Organization

Dr. Gregory B. White
ISAO SO—Executive Director
Director, Center for Infrastructure Assurance and Security, UTSA

Richard Lipsey,
ISAO SO—Deputy Director
Senior Strategic Cyber Lead, LMI

Brian Engle
Executive Director
Retail Cyber Intelligence Sharing Center

Working Group One—ISAO Creation

Frank Grimmelmann
President & CEO
Arizona Cyber Threat Response Alliance

Deborah Kobza
President & CEO
Global Institute for Cybersecurity & Research

Working Group Two—ISAO Capabilities

Denise Anderson
Executive Director
National Health Information Sharing & Analysis Center

Fred Hintermister
Manager
Energy Subsector Information Sharing and Analysis Center
North American Reliability Corporation

Working Group Three—ISAO Information Sharing

Kent Landfield
Director, Standards and Technology Policy
Intel Corporation

Michael Darling
Director, Cybersecurity and Privacy
PwC

Working Group Four—ISAO Privacy and Security

Rick Howard
Chief Security Officer
Palo Alto Networks

David Turetsky
Partner
Akin Gump Strauss Hauer & Feld LLP

Working Group Five—ISAO Support

Carlos Kizzee
Executive Director
Defense Security Information Sharing Exchange

Alex Crowther
Director of Research
Center for Technology and National Security Policy
National Defense University

Working Group Six—ISAO Government Relations

Michael Echols
Director, Cyber Joint Program Management Office
Cybersecurity and Communications,
Department of Homeland Security

David Weinstein
Chief Technology Officer
State of New Jersey

The ISAO SO leadership would also like to acknowledge those individuals who contributed significantly in the development of these guidelines:

(Names Under Consideration)

Table of Contents

Figures

Tables

Revision Updates

Item	Version	Description	Date

1 EXECUTIVE SUMMARY

These guidelines serve to address needs of newly forming Information Sharing and Analysis Organizations (ISAOs).

(*Note: An updated executive summary addressing the principles contained within these guidelines is planned for the final version. As this is a draft document that will continue to be edited and refined until its release in fall 2016, sections that appear in this version of the draft may not be included in the final release. Additional documents to be released will include more detailed discussions of various ISAO subjects.)*

2 INTRODUCTION

The importance of information sharing to computer security has been discussed for well over a decade. Early realization of its importance led to the creation of Information Sharing and Analysis Centers (ISACs) for critical U.S. infrastructure. In February 2015, the White House issued Executive Order (EO) 13691, "Promoting Private Sector Cybersecurity Information Sharing," which called for the Secretary of the Department of Homeland Security (DHS) to "strongly encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs)." These new entities could be "organized on the basis of sector, sub-sector, region, or any other affinity," which greatly expanded the number and type of information sharing organizations that will be developed. To help with their establishment, EO 13691 directed DHS to "enter into an agreement with a nongovernmental organization to serve as the ISAO Standards Organization" (ISAO SO).

In developing the standards, guidelines, and other documents that are needed to help entities create and operate ISAOs, the ISAO SO established a number of Standards Working Groups (SWGs). These groups were created to address specific areas pertinent to creating or operating ISAOs. When developing the various documents, the SWGs consider the two overarching efforts important to ISAOs: the sharing of cybersecurity information, and the analysis of the information that has been shared. The purpose of these efforts is ultimately to improve the national ability to "detect, investigate, prevent, and respond to cyber threats," while protecting the privacy and civil liberties of citizens.

To accommodate the expanded list of entities that can form ISAOs described in EO 13691, there will be different types of ISAOs with different objectives and capabilities. There will also be varying levels of organizations within the ISAOs, and there may be commercial entities that form to provide services to ISAOs. Some ISAOs may be formed on a very informal basis and may have little or no desire to collect and analyze the information in near-real time for its members. Other ISAOs may be highly interested in near-real time analysis and dissemination of actionable information to better protect its members and may have as an objective the ability to help respond to security incidents affecting its members.

Additionally, an ISAO may initially form with limited objectives and target capabilities but then evolve over time to increase its ability to assist its members by adding additional capabilities and objectives. For example, an ISAO may initially be created to simply share cybersecurity-related information among security professionals in its member organizations; then increase the type and frequency of information it shares, and add the capability to analyze shared information to better detect and prevent cybersecurity attacks; then ultimately add a 24/7 operational capability to assist its members with ongoing cybersecurity incidents. Conversely, an ISAO may elect to maintain limited capabilities to best serve the needs and capabilities of its constituents. The goal of the ISAO SO is to be as inclusive as possible in finding a place for any individual or organization that wishes to be part of the overall U.S. information sharing effort.

These guidelines are designed to take into consideration the different types of ISAOs that may be formed and the capabilities each may incorporate. It presents an organized approach to the various topics pertinent to ISAOs while considering the immediate needs of emerging ISAOs.

3 THE ISAO ECOSYSTEM

EO 13691 clearly lays out the challenges addressed by the creation of a network of ISAOs. It states:

> In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies, and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.
>
> Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. The purpose of this effort is to encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.
>
> Such information sharing must be conducted in a manner that protects the privacy and civil liberties of individuals, that preserves business confidentiality, that safeguards the information being shared, and that protects the ability of the Government to detect, investigate, prevent, and respond to cyber threats to the public health and safety, national security, and economic security of the United States.

To address the challenges effectively will require more than just establishing a number of disparate information sharing organizations. It will require a coordinated effort that effectively identifies and considers the existence and ongoing formation of ISAOs to understand where information sharing is occurring and its impact. Additionally, it will require considering how the efforts of individual ISAOs can be combined into an overarching information sharing network for the United States to improve the cybersecurity resiliency of participants. The effort must be as inclusive as possible, appropriately incorporating information from multiple sources. Due consideration must be given to determining the amount of trust that can be placed in such information, which requires that the national effort address issues such as trust, reliability, and information overload.

4 WHAT IS AN ISAO?

According to 6 USC 131(5):

> *The term "Information Sharing and Analysis Organization" means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of--*
>
> *(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;*
>
> *(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and*
>
> *(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).*

The primary characteristic of an ISAO in the cybersecurity ecosystem is that the ISAO shares cybersecurity information related to cybersecurity risks and incidents, between and among its membership. This holds true across a wide range of ISAOs with varying constituent membership organizations. While not all members of all ISAOs may be critical infrastructure entities, and some ISAOs will be organized around models other than sectors of critical infrastructure, ISAOs that share information related to cybersecurity risks and incidents meet the intent of EO 13691.

5 ISAO CAPABILITIES AND CATEGORIES

5.1 INTRODUCTION TO CAPABILITIES

Although no single description of capabilities will fit all ISAOs, it is important to consider a description of the functions of a “fully capable” ISAO for supporting its members. This discussion will help emerging ISAOs determine the capabilities and objectives they wish to develop—keeping in mind that the initial set of objectives and capabilities may evolve as the ISAO matures.

A fully capable ISAO will provide a variety of services to support its members. These services, and the capabilities that are needed to provide them, should be designed to support ISAO members as they manage strategic and tactical cyber-related risks. The type of support can be grouped into three broad categories, with some overlap between them. These categories are:

- **Situational awareness:** ISAO members need to understand both the tactical and strategic aspects of the environment in which they are managing risks. This support includes activities to collect and share information, analyze it, and recommend what to do with it.
- **Decision-making:** ISAOs need to disseminate actionable information that will enable their members to make decisions related to their current security posture and allocation of security and IT resources. This support involves receiving information, establishing its relevance to the organization, assessing potential impacts, identifying potential actions, and selecting the best course of action.
- **Actions:** ISAO members ultimately will take actions based on received information and analysis. Organizations will develop detailed actions and assign responsibilities, implement the actions, and evaluate their effectiveness, providing feedback for further consideration.

For each type of support, individual members or organizations will have responsibilities addressing their own needs as well as responsibilities to the ISAO. The ISAO in turn also has responsibilities for each of these categories that address the ISAO membership as a whole.

5.2 VALUE PROPOSITION

Fundamental to the establishment of an ISAO will be the “value proposition” to be offered its participants, members, and collaborators. An ISAO must provide a tangible benefit in order for it to enroll members. ISAOs offer the following benefits to their members and other ISAOs:

- An informative set of cybersecurity threat indicators and best practices provided by ISAOs will make individual members more secure.

- ISAOs implemented in accordance with a consistent yet flexible framework can replicate and extend current trust relationships by establishing a common, shared set of values and expectations.
- Members enhance their knowledge about how to protect themselves from, detect, and react to cyber-attacks.
- By aggregating information from multiple organizations, ISAOs present a richer picture of malicious activity taking place around the country and the world. Member organizations can use this enriched information to improve their individual and collective security, blocking attacks they would not have seen otherwise.
- ISAO members can carry out effective and timely responses if they discover unauthorized intrusions.

5.3 INFORMATION SHARING CONCEPTS

Besides the value proposition, also fundamental to the establishment of an ISAO will be the categories of information to be collected, disseminated, and shared. The following guidance is provided to assist ISAOs in developing their information sharing policy considerations.

Before ISAOs can begin sharing with members or customers, it is important that they understand the needs of their members or customers. ISAOs are not formed in a vacuum. In many cases, the ISAO itself is formed by a community of like-minded organizations who have made the decision to collaborate with peers as a means to manage risk. In this case, the ISAO should be designed from the beginning by the members to meet the needs of the members.[1] In other instances, an ISAO is a for profit company providing services to paying customers. In such cases it is important for the ISAO company to understand and quantify its unique value proposition for its customers.

There are a variety of questions that an emerging ISAO will want to answer in order to determine its information sharing policy. The previous categories of information should be considered along with questions such as the following.[2]

- Which categories of information do the ISAO members want to share with each other?
- What information do ISAO members need to help enhance their situational awareness?
- Will the ISAO members provide to the ISAO raw data, analysis, or both?
- Will the ISAO provide its members raw data, analysis, or both?

[1] See ISAO Formation Section for more detail.

[2] Consult ISAO 100-2 for additional guidance.

- What information do ISAO members need to assist them in tactical decision-making?
- Do members expect to receive from the ISAO information related to defensive measures, mitigation activities, best practices, and/or incident coordination?
- Do members expect the ISAO to provide analysis such as trending analysis and insight on threat actor targeting and motivation

When organizations come together to create an ISAO, they do so with an understanding of what their information needs are. They are organizing for a specific purpose. It is appropriate that the ISAO's information sharing policies be informed by and designed to meet those purposes. For example, if a community forming an ISAO wants more information on effective practices to mitigate specific attacks, the ISAO would want to build policies that facilitate this purpose. Similarly, in a for-profit ISAO, it is important that the company providing ISAO services understand the specific market niche it is targeting and how the ISAO product and services add value to its customers. In either case, when developing information sharing policies, ISAOs may want to align their policies with the member objectives and customer needs.

For example, if an ISAO and its members choose to share information that will enhance member situational awareness, the burden is on the members or customers to clearly identify what information they need to enhance their situational awareness. If members are looking for contextual information, but the ISAO provides raw indicators instead, it will be difficult to meet the member or customer needs. Likewise, if members are looking for effective mitigation practices but the ISAO provides detailed malware analysis, members will not receive the desired information.

There are various types of information an ISAO and its members may want to share. The following is not an exhaustive list of types of information ISAOs may choose to share, and there is no expectation that an ISAO share all or any of the following information. An ISAO and its members or customers can choose to share or not share information based on what meets the mission of the ISAO and the needs of its members. Not all information is appropriate for all ISAOs or all members and customers.

Potential information that an ISAO and its members could choose to share includes:

- Malicious Internet Protocol (IP) addresses
- Malware analysis
- Automated sharing of raw threat indicators
- Effective cybersecurity practices for a specific community or incident
- Generic effective cybersecurity practices

- Big data analytics
- Attack trending and analysis
- Assessments on specific threat actors or campaigns
- Attacks specific companies have seen on their networks
- Aggregated attack information from multiple customers/members
- Information shared by for-profit ISAOs through managed security services
- Single-vendor vulnerability information
- Cross-platform or multi-vendor vulnerability information
- Vulnerability remediation tactics
- Information on a specific, ongoing or current cyber threat or attack
- Threat intelligence reports developed by other parties
- Open-source news reporting
- Presentations and discussions from subject matter experts
- Government alerts
- Vendor alerts
- Indicators of compromise.

In developing information sharing policies for ISAOs, it is important for members and customers to agree on the proper role of the ISAO itself. For example, depending on the needs and requirements of its members and customers, an ISAO could choose to do one or more of the following:

- Provide a platform for and facilitate member sharing.
- Deploy sensors to gather and share unique information beyond member information.
- Subscribe to a third-party service that provides threat intelligence feeds.
- Collect, aggregate, and disseminate open-source reporting.
- Collect, aggregate, and disseminate reporting from partner organizations.

Understanding the purpose of the individual ISAO, what it shares and how it functions will help potential and current members better understand and evaluate how the ISAO can add value to that individual organization. For example, if an ISAO is designed by its members to be a facilitator of sharing among members, it is not fair to expect that the ISAO will provide managed services or incident response capabilities. However, just because an ISAO may not provide value to one organization does not mean that it cannot or does not provide value to others.

Once it is understood as to the type of information that will be shared through the ISAO, it is important that members, customers, and the ISAO staff (if any) understand triggers for sharing information within the ISAO. It is not enough to say “share.” It is important to know what to share and when to share it.

Sharing among members and the ISAO may be done automatically from machine to machine. Sharing indicators in an automated fashion can enable information to be shared more rapidly and can also increase the volume of indicators that are shared. This technology is emerging and not fully deployed. But even in these cases, it is important that the machines understand what they should be sharing with their ISAO and ISAO members.

When humans are involved, the process can be slower, but the value of the data shared can be enhanced if the organization sharing the information provides information on how it identified and mitigated the attack or other context. Human-to-human sharing also can increase trust among participants, making them more willing to share. As such, there is value in both automated exchange and human exchange. ISAOs can choose to share information via automation, human interaction, or a combination of the two.

The ISAO members determine what information is shared, when it is shared, and how it is shared. They will make these decisions based on the mission of the ISAO and the capabilities of its members and customers. To help guide this decision making process of what to share, the ISAOs and their members and partners may want to consider the following potential (non-inclusive) examples:

- Share information only on attacks that disrupted a member’s business operations.
- Share information only on attacks that made it past members’ intrusion detection/prevention systems.
- Share vulnerability information on members’ products or services.
- Share vulnerabilities discovered in products or services provided by non-members.
- Share information on vulnerabilities that were successfully exploited in an attack on a member network.
- Share open-source news, including third-party threat reports.
- Share information on multiple attacks originating from the same source.
- Share all malicious indicators discovered throughout member enterprises.
- Share remediation advice on how to identify or mitigate a specific attack.

Once members and customers agree to and understand what information they wish to receive through an ISAO, they can begin to develop policies on what the ISAO can do with the information and how that information can be shared.

Some ISAOs may choose to enable sharing without attribution, while other ISAOs may choose to require attributing shared information with a specific member. Non-attribution could make a member feel more comfortable in sharing, but knowing who is sharing the information could provide greater confidence in its quality and accuracy. ISAOs are free to establish the policies that they determine best meet the needs of their organization, membership, and customers.

An ISAO and its members also may want to develop information sharing policies that consider the sensitivity of the information being shared. For example, the more sensitive the information, the more security an ISAO may choose to deploy. There are specific security and privacy practices, but it is important to emphasize that the ISAOs and their members may choose how to share information, based on its sensitivity and member capabilities.

Having information sharing policies also helps members understand how they can use the information that is shared within the ISAO and with other partners. ISAOs may want to consider establishing policies that detail how members can use and share information. This could include the following:

- How members can *share* the information they receive from the ISAO
- How members can *use* the information they receive from the ISAO—for example, can they use the indicators to protect their customers or just their enterprise?
- Whether the ISAO can share the information with other partners
- How shared information should be marked
- How to treat information that is shared over the phone or during virtual and in person meetings.

There are various ways to incorporate such policies. Some of these include:

- Asking members to sign a separate non-disclosure agreement
- Having a non-disclosure agreement included as part of the member agreement
- Describing the appropriate use of information in service level agreements or customer contracts
- Detailing how the information can be used in a concept of operations (CONOPS)
- Developing a separate, stand-alone, information use agreement within the ISAO.

5.4 CREATING AN ISAO

5.4.1 KEY STRATEGIC PLANNING FACTORS

DEFINING THE VALUE PROPOSITION

An ISAO's value proposition is a promise of value to be delivered. Creating an ISAO requires working with community stakeholders to define the ISAO's value proposition to improve cybersecurity for its constituents and membership partners – supported by the ISAO's goals and objectives.

- Who is the ISAO's target community? Critical Infrastructure, Industry, Business, Government? Local, Regional, Statewide, National, International? If international, consider whether sharing information with international partners will present challenges from a legal and/or "safe-sharing culture" point of view.
- Will the ISAO be limited to one critical infrastructure sector or sub-sector, multiple sectors, or support an industry or business community?
- What is ISAO's vision? How do the ISAO stakeholders and members picture the ISAO one year after formation, after five years, etc.? For each timeline milestone, where will the ISAO be in terms of size, geographic scope, products, services and activities?
- What goals does the ISAO intend to achieve? Goals may range from raising awareness locally through information sharing of basic threat intelligence information among individuals, to high-speed real-time sharing of technical threat intelligence on an automated, global basis across an entire sector. Goals may also evolve over time as the ISAO grows in size and resources.
- How will the ISAO improve the cybersecurity position of the sharing partners and members of the ISAO? What information sharing problem will the ISAO solve?
- What types of cybersecurity information will the ISAO be sharing (i.e. warning fellow members of the types of emerging cyber threats in a particular sector, industry or business; and/or sharing of technical details of cyber threat intelligence from basic Internet protocol address information to technical indicators of malicious software code that members can use to detect problems on their systems).
- How does the ISAO intend to share information, at least initially? For example, informally and on a person-to-person basis, manually through online portals, or via automated information sharing platforms. The ISAO may start with informal sharing and mature into exploring what technologies exist to allow for rapid sharing of threat indicators.
- How will the ISAO maintain sustainability? What funding models support the ISAO – Grant(s), Corporate Sponsorship, Membership Model, etc.

- How will the ISAO identify, engage and encourage member and stakeholder participation and collaboration?
- Has the ISAO identified target community leaders to champion the ISAO throughout the community, encouraging participation? Is the targeted community already sharing information?
- What does the ISAO have to offer the community of sharing partners to enhance the protection of critical infrastructure, industry, business or government?
- What are other similar ISAOs currently providing and how can you coordinate, collaborate and work together?
- What is the ISAO planning to do differently than other ISAOs? What solution can you bring to information sharing that is unique to the ISAO?
- Is internal and external collaboration part of the ISAO's natural workflow?
- Has the ISAO defined strategic information sharing partners? Have the mutually beneficial objectives of partner strategic alliances been defined?
- What will the ISAO's value-added actionable content be: threat information (threat observables, indicators, incidents, adversary tactics/techniques/procedures, exploit targets, courses of action, campaigns, threat actors), incident analysis, analytics, vulnerabilities?
- How will the ISAO ensure that information shared is actionable?
- Does the ISAO plan to acquire analytic capability to apply to information that is shared for members, and share analytics with others external to the ISAO?
- How will the ISAO work with other partners to enhance the value of the information received? Will the ISAO openly share with other ISAOs?
- Does the ISAO have special expertise in cybersecurity and information sharing?
- How will the ISAO share information with its members?
- What core set of services with the ISAO offer that adds value to the ISAO's members? For example, will it act as a hub to share cyber threats and defensive measures, will it analyze data and turn it into "actionable" intelligence, or both?
- Beyond the core set of information sharing services, what additional services does the ISAO desire to provide to enhance the core ISAO services, thereby adding further value to members?
- What is the plan for future ISAO service offerings?

5.4.2 BUILDING A TRUSTED COMMUNITY

Trust is an essential component of the ISAO's information sharing relationship with internal (staff/members) and external partners.

- Will trust be based informally on existing relationships, or more formally established via membership or information sharing agreements, confidentiality agreements, information sharing policies and protocols, or a combination of these? A formal agreement and/or written policies may facilitate a "safe sharing" culture among members.
- Will new members be subject to vetting and due diligence by existing members before they are granted access to information?
- How will members be accountable to one another and ensure the information being shared is not used inappropriately? Who will monitor compliance with the membership or information sharing agreements, confidentiality agreements and/or information sharing policies and protocols?

ISAOs must establish a basis of trust among sharing partners and members (internally and externally). To establish and sustain the ISAO's culture of trust, ISAOs should consider defining:

- **Trust Model Planning**—A plan with measurable goals to create a trust model for the ISAO.
  - ISAO member—new member trust expectations
  - How will transparency be ensured among sharing partners?

- **The Sharing Model**—People-to-people, organization-to-organization, organization-to-government, restricted, or open membership sharing
- **Sharing Model Scope**—Local, regional, state, national, international
- **Sharing Model Platform**—Automated or manual
- **Partner and Member Vetting**—Requirements and process. National? International?
- **Information Sharing**—Based on informal or existing relationships, or more formally established—membership/information sharing agreements, confidentiality/non-disclosure agreements, information sharing policies and protocols, or a combination?
- **ISAO Information Sharing Agreement**
  - Information sharing rules (protocols), rules of behavior, secure access to information
  - Risks and consequences when information sharing rules are broken

5.4.3 ISAO MEMBERSHIP

ISAO membership includes establishing a membership model consisting of the following:

- **Membership requirements**—Criteria for membership consideration
  - Membership requirements—Minimum set of requirements been defined for membership?
  - Members—Individuals, organizations, or both
  - Members—Limits on membership
  - Membership requirements adherence policy—Monitoring process
- **Membership model**—Cost to join the ISAO
  - Membership value/return on investment (ROI)—ISAO provided products and services
  - Membership cost
- **Member nomination and recruiting**
  - Member identification, nomination and recruiting strategy
  - New member outreach plan—Tactics used to reach potential new members

- **Membership vetting policies and processes**
  - Membership vetting policy—Including assessment and probation in the event of member issues
  - Membership acceptance voting rules
  - Membership vetting process—Including assessment, approval (by management or member voting)
- **New member tactical onboarding considerations**
  - Membership/information sharing agreement process—Signing, recording, storage of membership/information sharing agreements
  - New membership onboarding—Training. Who receives training and how will it be delivered?
  - New member introductions process—To all members and ISAO management/staff/board of directors
- **Membership retention**
  - ISAO-to-member communication to ensure that the ISAO meets members' expectations

5.4.4 ISAO MARKETING AND COMMUNICATIONS

Whether an ISAO is established for the public or private sector, the ISAO should define and have resources to implement a marketing and communications strategy.

MARKETING PLAN—DEFINE, DEVELOP, MAINTAIN AND MEASURE

- Essential marketing policies and processes—Who will define, develop and maintain the plan?
- Leveraging the ISAO's value proposition:
  - ISAO's foundational value proposition positioning statement—This includes how the positioning statement will be used in recruiting members, internal member communications, and external communications
  - Goals and objectives
  - Envisioned capabilities
  - Value and benefits the ISAO is Intending to deliver
  - Differentiation from other ISAOs

- Tactical marketing tools—Reaching the ISAO's audience
  - Marketing communications policy—Rules, responsibilities, authorities, activities, budget
  - What tactical marketing tools will the ISAO use to communicate externally (events, online, documentary materials, public relations, advertising, private recruitment, etc.)?
  - Sponsor advertising policies—Does the ISAO accept sponsor-recognized advertising?

COMMUNICATIONS PLAN (STRATEGY)

- **External communications** (exclusive of threat intelligence information sharing)
  - Communications policy—Rules, responsibilities, authorities, and activities for external communications
  - External communications governance methods and approaches—What methods and approaches will be used to communicate governance matters bi-directionally with other ISAOs, the ISAO governing body, strategic alliances and with government organizations?
  - Communication tactical tools—What tactical tools will the ISAO use to communicate externally (listserv, portal, newsletters, email, news feeds, calendars, etc.)?
- **ISAO member communications** (exclusive of threat intelligence information sharing)
  - Member communication policy—Roles, responsibilities, authorities and activities for member communications
  - Member communications governance methods and approaches—What will be the methods and approaches used to communicate bi-directionally with ISAO members about matters such as membership recruitment and onboarding, ongoing policy and capabilities development, strategic planning, accomplishments, etc.?
  - Allowed ISAO communications policy—What is the defined set of allowed communications between ISAO members? Is it based on industry or government regulation? If so, what are those allowed communications?
  - ISAO member communication roles—What are the ISAO member roles that send/receive information, and what type of information should each role send/receive?
  - Communication tactical tools—What tactical tools will the ISAO use to communicate bi-directionally with members (listserv, portals, newsletters, email, news feeds, calendars, etc.)?

5.4.5 ISAO OPERATIONS AND FINANCIAL MANAGEMENT

To sustain an ISAO, defining an operations and financial management plan is paramount to ensure the ISAO's sustainability. The following factors should be considered: cost drivers, funding models, and membership models:

OPERATIONS AND FINANCIAL MANAGEMENT

- **Cost drivers**—If an assessment of the external environment is performed, the findings from that assessment are foundational requirements and key inputs into the ISAO's Operations and Financial Plan.
- **ISAO costs**—Depending upon the services, skills, and technologies needed by the ISAO to deliver its services, certain costs may prove to be a significant portion of the ISAO's operational expenditure. The following key cost drivers, expenses and capital requirements are needed to be taken into consideration for creating and sustaining an ISAO, and for day-to-day operation.
    - ▪ <u>ISAO management and operations</u>
        - o Organization formal formation—Legal services, state/federal regulatory requirements, tax/accounting services
        - o Support staff—Regardless of the size and number of members belonging to the ISAO, careful consideration should be noted as to the support staff required for ISAO management and operations day-to-day: executive management, managers, analysts, product development, member identify management, risk & compliance, membership development, etc.
        - o Professional services (consulting support, etc.)
    - ▪ <u>Infrastructure and technology</u>—Technology plays a key role in the ISAO, and technology solutions vary widely in terms of cost. The ISAO should determine the operational and infrastructure requirements to support and sustain the ISAO including, but not limited to:
        - o Software—Applications and licensing fees for core ISAO services (information capture/distribution/analysis/alerting (build vs. buy decision), tools for handling sensitive data (i.e., anonymization), applications for supporting ISAO daily operations (finance, security, IT service management, membership development, collaboration tools, etc.)
        - o Analytics—Analytics processing capabilities required and to what degree to support analysis and enrichment of data (in-house, outsourced, or hybrid model)
        - o Hardware—Onsite vs. cloud computing, system security, large storage capacity requirements, disaster recovery, etc.
        - o Data feed providers—External vendors providing feeds and products the ISAO can provide to their membership and to help support enhancing data analysis

- Promotion costs—Developing in-house marketing and outreach capabilities to generate interest in the ISAO's target market community, grow membership, and manage member relationships
- Member needs—Number of member organizations; ISAO membership target community, including the number, size, and needs of the members that will impact costs (anticipated number of threat feeds as well as onboarding and integrating members into the ISAO information sharing infrastructure community)
- Training and education—Continuous training of management and support staff (security—all hazards, both physical and cyber), ISAO policies and procedures, ISAO infrastructure information exchange/sharing platforms, information sharing policies and protocols, and any additional services offered by the ISAO.

FUNDING MODELS

ISAO revenue streams will be dependent upon the type of business model the ISAO chooses, including membership fees. Based on the type of ISAO business model, funding options and potential sources of revenue need to be considered.

- Funding model tax implications (from ISAO and member perspective)
- Public support funding model (i.e. government grants for non-profit organizations)
- Financial reporting (board of directors, members, government).

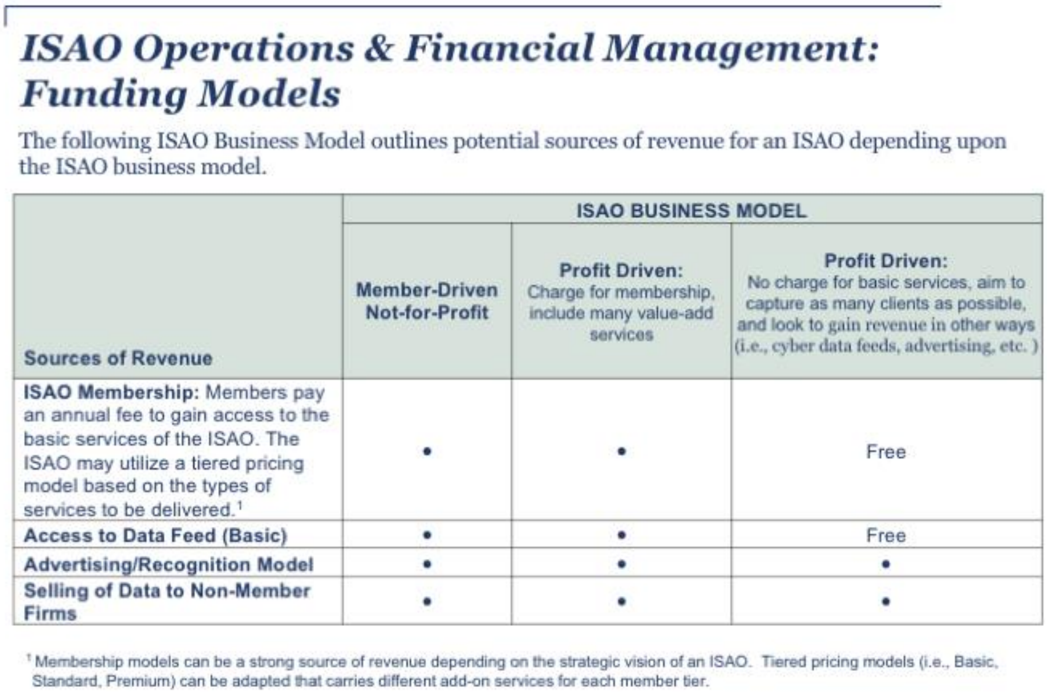
Error! Not a valid bookmark self-reference. Figure 1 identifies various types of funding models.

MEMBERSHIP MODELS

There are many different categories of membership an ISAO can offer (basic, standard, premium). Membership categories fall in line with the service offering provided as part of the strategy and membership value the ISAO is offering. The following considerations should be taken:

- What will be the different benefits associated with each membership category (i.e., analytics, data feeds, access to seminars, conferences)?
- What is the ISAO Membership Fee Structure associated with each membership category?
- Are membership fees tiered, dependent upon a member organization's size and/or business structure (i.e. for profit, nonprofit, etc.)
- Will each member have access to all services regardless of membership category?

Figure 1: ISAO Operations & Financial Management Funding Models

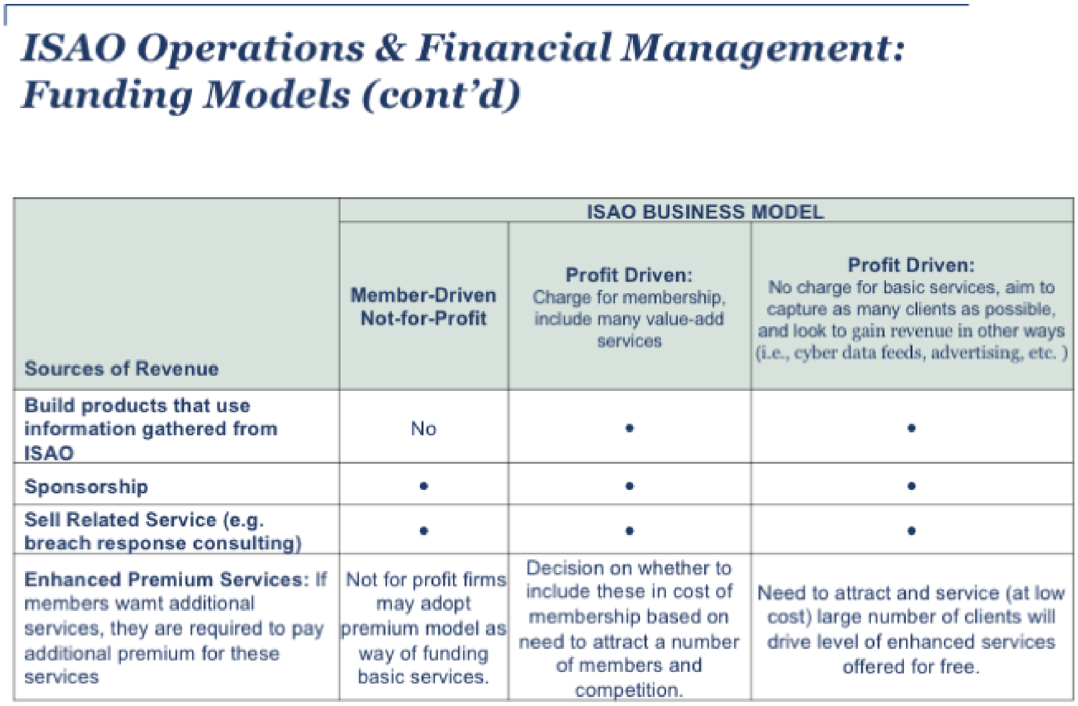


ISAO Operations & Financial Management: Funding Models

The following ISAO Business Model outlines potential sources of revenue for an ISAO depending upon the ISAO business model.

	ISAO BUSINESS MODEL		
Sources of Revenue	**Member-Driven Not-for-Profit**	**Profit Driven:** Charge for membership, include many value-add services	**Profit Driven:** No charge for basic services, aim to capture as many clients as possible, and look to gain revenue in other ways (i.e., cyber data feeds, advertising, etc.)
ISAO Membership: Members pay an annual fee to gain access to the basic services of the ISAO. The ISAO may utilize a tiered pricing model based on the types of services to be delivered.[1]	•	•	Free
Access to Data Feed (Basic)	•	•	Free
Advertising/Recognition Model	•	•	•
Selling of Data to Non-Member Firms	•	•	•

[1] Membership models can be a strong source of revenue depending on the strategic vision of an ISAO. Tiered pricing models (i.e., Basic, Standard, Premium) can be adapted that carries different add-on services for each member tier.



ISAO Operations & Financial Management: Funding Models (cont'd)

	ISAO BUSINESS MODEL		
Sources of Revenue	**Member-Driven Not-for-Profit**	**Profit Driven:** Charge for membership, include many value-add services	**Profit Driven:** No charge for basic services, aim to capture as many clients as possible, and look to gain revenue in other ways (i.e., cyber data feeds, advertising, etc.)
Build products that use information gathered from ISAO	No	•	•
Sponsorship	•	•	•
Sell Related Service (e.g. breach response consulting)	•	•	•
Enhanced Premium Services: If members wamt additional services, they are required to pay additional premium for these services	Not for profit firms may adopt premium model as way of funding basic services.	Decision on whether to include these in cost of membership based on need to attract a number of members and competition.	Need to attract and service (at low cost) large number of clients will drive level of enhanced services offered for free.

5.4.6 ISAO GOVERNANCE

A PRACTICAL APPROACH TO FORMING AN ISAO

An ISAO may elect to form in an informal or formal capacity. Although there are many legal and other considerations that may seem complicated, it is important to keep in mind that governance choices can flow easily from the founder's vision and goals for the ISAO.

It is important to recognize that the vision, goals, and membership of the ISAO may change considerably over time, which may support consideration of starting an ISAO with a smaller, less formal organization and making changes to the governance structure as the ISAO evolves and matures over time.

FORMAL VS. INFORMAL GOVERNANCE STRUCTURES

The following questions should be considered to support the decision of establishing the ISAO in an informal or formal governance structure:

- **Membership requirements**—Will the ISAO require members to agree formally to written requirements of membership? If so, one way to accomplish this is a formal legal entity to which members can agree through a membership agreement, memorandum of understanding, information sharing agreement, or similar document.

- **Membership fees/payments**—If the ISAO will receive and make payments, how will those be treated from a tax-standpoint and according to applicable law and regulatory requirements? A formal legal entity, including not-for-profit status if applicable under local and federal law, may be the best approach.

- **Third parties**—Do you expect the ISAO to engage in activities that require contracting with a third party? If not, a separate legal governance structure may not be necessary, at least until the ISAO begins to encounter such needs. The following are points to consider with respect to whether it is necessary or prudent for the ISAO to contract with third parties:

  - <u>Office space</u>—If the ISAO will be meeting in person periodically, will the ISAO need to lease space to do so, or will a particular member provide space where the ISAO management and members can meet? If the ISAO needs to rent space for meetings and operations, will an individual member step forward and sign the lease, or will the ISAO need a formal legal entity of its own to do so? Alternatively, short-term conference or meeting space rentals may be available without the need to establish the ISAO as a formal legal entity, provided the members establish a framework to share costs.

  - <u>Physical resources</u>—What physical resources will the ISAO need that may require third-party contracts? For example, will it need server space to host a cybersecurity threat intelligence information sharing platform? Will that server and the space where it resides require a third party contract? If so, establishing the ISAO as a formal legal entity may be necessary.

- Professional services—Will the ISAO engage in activities that may require the advice of outside experts, such as technical experts to assist in setting up sharing mechanisms or legal services to advise on particular activities according to local, state, or federal laws and regulations? Will the ISAO employ any full-time or part-time employees, or will it rely on consultants and contractors to facilitate the sharing and analysis of information? In either case, establishing the ISAO as a formal legal entity may be necessary.
- Financial management—Will the ISAO require its own bank account to pay for services or to receive funds? For example, if the ISAO will require members to contribute to a budget (whether by dues or otherwise) to cover the ISAO's organizational and operational costs or to hire full- or part-time staff, establishing the ISAO as a formal legal entity or establishing a separate legal entity to receive and make payments may be necessary. Similarly, if the ISAO will be funded by federal grants or private donations, its benefactors may require a separate legal entity (and, possibly, not-for-profit status) in order for the ISAO to receive funds.
- Insurance—Will members require the ISAO to obtain insurance to cover its activities? If so, establishing the ISAO as a formal legal entity may be required to enter into insurance contracts.

TYPES OF FORMAL LEGAL ENTITIES

If the ISAO has concluded based on the preceding questions that establishing the ISAO as a formal legal entity is necessary to serve the ISAO's members' needs, the ISAO and its stakeholders should consider the following information to decide on the type of formal legal structure. Ultimately, however, the ISAO may want to consult legal counsel to assist in choosing the most appropriate type of legal structure to meet the ISAO's needs.

- **For-profit or non-profit activities**—Is it the expectation of the ISAO to engage in for-profit activities or operate purely on a non-profit basis? If the latter, the ISAO may consider in consultation with legal counsel whether a non-profit status is the most advantageous form of corporate entity from a tax standpoint.
- **Formal legal structure**—What type of legal entity will best address the needs of the ISAO to conduct business while insulating the members from liability? Within the United States, a range of recognized legal entities are possible depending on applicable state law. These include corporations, limited liability companies, various forms of partnerships, and several others. Each has particular advantages and disadvantages that you should discuss with legal counsel according to applicable local and state law.

- **Legal fiduciary duties, board of directors**—Local laws may impose fiduciary duties on directors of the legal corporate entity.
    - For-profit legal fiduciary duties—Directors of for-profit corporations in the United States typically owe to shareholders the primary duties of "care" and "loyalty," requiring directors to act in the same manner as a reasonably prudent person in their position, and to act in good faith in the best interests of the corporation and its shareholders.
    - Limited liability company (LLC)—Members of a limited liability company may contractually agree to waive the fiduciary duties of directors and officers in the operating agreement governing the LLC.
    - Public benefit corporations—In the United States, many states also recognize "public benefit corporations," which may consider social or other concerns over profits. Public benefit corporations may be required to provide regular reporting of the organization's efforts to meet its public good goal, known as "public benefit assessment."
    - Non-profit legal fiduciary duties—Directors and officers of non-profit organizations are considered fiduciaries, or persons of trust, with the power and obligation to act with total trust, good faith, and honesty on behalf of the organization. Fiduciary duties include the duty of care, the duty of loyalty, and the duty of obedience.
        - Duty of care—Obligations to keep informed, remain attentive, and act in a manner that is in the best interest of the organization.
        - Duty of loyalty—Obligations to act in good faith and in a manner that the individual reasonably believes to be in the best interests of the organization (motives, purposes, and goals).
        - Duty of obedience—Obligations to adhere to carrying out the purpose and mission of the organization, as expressed in the organization's governing legal documents (bylaws, etc.).
- **Liability protection**—If liability protection is the primary consideration, a corporate form or a limited liability corporation may be most appropriate. In the United States, the concepts of "limited liability" and "separate legal personality" are actively enforced; however, it may be possible to "pierce the corporate veil" and impose an entity's "separateness" (such as by commingling assets). The ISAO should consult with legal counsel regarding liability protection, which is typically governed by state law.

  Foreign jurisdictions also generally recognize various forms of limited liability entities, though the specific contours vary. This guidance document does not attempt to catalogue non-U.S. law. If the ISAO desires to establish a foreign legal entity, local legal counsel should be consulted.

- **Tax liabilities**—How much of a concern is the ability to avoid separate tax liabilities for the ISAO itself? Some entities, such as limited liability companies and partnerships in the United States, have the advantage of "pass-through" tax liability, meaning that tax liability passes through to the individual member-owners or partners of the entity, who report the profits (or losses) on the individual tax returns.

  Foreign jurisdictions also generally recognize various forms of "pass-through" taxation, though the specific contours vary. This guidance document does not attempt to catalogue non-U.S. law. If the ISAO desires to establish a foreign legal entity, local legal counsel should be consulted.

- **Formal governance structure**—What type of legal entity will best address the needs and requirements of the ISAO? For example, a very large ISAO with significant resources may consider incorporating under local or state law, providing the most formal governance structure and clearest protection from liability; in contrast, a smaller ISAO that simply needs the ability to conduct business as a separately recognized legal entity may require a less formal structure, or one with greater governance flexibility, such as an LLC.

  The ISAO should also consider whether benefactors, regulators, and other third parties with whom the ISAO may desire to interact and contract may have greater comfort with corporations, as compared to LLCs, as a result of the larger and more developed body of statutory and case law relating to corporations.

FORMING A LEGAL ENTITY

When forming a legal entity, certain high-level topics should be considered. This guidance document focuses on corporations and limited liability companies, which are two of the most common legal entities in the United States. The ISAO should consult with local legal counsel for more detailed information regarding the appropriate legal structure, to assist in entity formation, and to draft the necessary documentation.

- **Filing to establish a legal entity**—To formally create a legal entity, it is necessary to file a certificate, charter, articles of incorporation, or other similar documentation (the contours of which are generally governed by local or state law) in the state where you choose to incorporate (in the case of a corporation) or organize (in the case of an LLC). In the United States, these are commonly called the certificate of incorporation or articles of incorporation (for a corporation) or certificate of formation or articles of organization (for an LLC).

  Formation documentation typically contains only basic information, such as the ISAO's name and registered address. Corporations must also provide their articles of incorporation (name, registered address, purpose, board of directors). For-profit corporations authorize the total number of shares that the corporation may issue. Not-for-profit or non-profit corporation formation requirements vary by the state in which the corporation is established.

- **Operating agreement**—The operating agreement (for LLCs) or bylaws (for corporations) are the primary documents establishing how the entity will be managed. This includes defining the rights and obligations of members or shareholders—and the managers or board of directors (if any)—creating officer positions, and delegating management responsibilities as appropriate. Whereas an operating agreement is a very flexible contract among members of an LLC, the bylaws of a corporation may be more limited in scope by local law, making it necessary to enter into additional “member” or “shareholders” agreements” in certain circumstances.

FOR A FOR-PROFIT CORPORATION

- **Shareholders vs. members**—The owners of the corporation are its shareholders, whereas the owners of a limited liability company are referred to as its members. The following are items an ISAO should consider with regard to shareholders or members:
  - Who may be a shareholder of member? Should this be limited to domestic private companies and individuals, or may it also include public interest entities and foreign companies and individuals?
  - How do shareholders of members join? Are there initial or continuing capital contribution requirements?
  - What are the ongoing rights and obligations of shareholders and members (including management of the organization, capital contributions, and information sharing, among others)?
  - When and where will shareholders or members meet? May actions by shareholders or members be decided only at a meeting, or also by written consents, and how will voting (and veto) rights be defined?
- **Board of directors**—Corporations are typically managed by a board of directors elected by the shareholders, while LLCs are often member-managed. However, LLCs may also establish a board of directors, as the members see fit. The operating agreement or bylaws should establish the board of directors, if any. The following are key considerations when establishing the board of directors:
  - Structure—What will be the size of the board, and who will be the initial founding directors? How will directors be chosen in the future, and when will elections take place? Will there be term limits or other requirements or qualifications of directors?
  - Delegations of duties—What management rights will be within the purview of the directors? What actions will require additional approval by the shareholders or members?
  - Meetings and voting—When and where will directors meet? May official actions be decided only at a meeting, or also by written consent and in meeting minutes? How will voting (and veto) rights be defined?

- **Officers**—Corporations and LLCs may also appoint officers to manage the day-to-day operations of the entity. In certain circumstances, it may also be necessary to appoint officers to take certain actions on behalf of a corporation, such as executing leases or financing agreements.
    - Officer titles—Corporations will typically have a president, secretary, and treasurer, and may also have vice-presidents.
    - Delegation of responsibilities—When establishing the board of directors, the operating agreement or bylaws should define and delegate those responsibilities to the officers or shareholders or members, as deemed appropriate. Term limits, the manner of election or appointment and any other rights, duties, or qualifications should also be considered.
- **Committees**—In certain circumstances, it may also be beneficial to establish committees of the board of directors (the members of which are typically directors), to which particular duties may be delegated. Areas uniquely suited to oversight by experts (such as audit or other financial matters) or smaller more nimble groups (such as certain special projects or transactions) may benefit from this governance structure.
- **Delegation of responsibilities**—When establishing the board of directors, the operating agreement or bylaws should define and delegate those responsibilities to the committees or shareholders or members as deemed appropriate. Committees will typically also be governed by their own charter establishing committee purpose, membership, term limits, elections, meetings, voting rights, deliverables, etc.

5.5 DESCRIBING ISAO CAPABILITIES

ISAO capabilities are chosen by the organization and support the needs of its members. The capabilities generally fall into three types: foundational, additional, and unique. Most ISAOs will have capabilities chosen from some distinctive combination of these three types. As an example, a small group wanting to establish an ISAO may choose primarily foundational capabilities, in order to meet projected membership requirements.

- **Foundational** capabilities are generally considered fundamental in nature for most ISAOs, depending on the needs of its members. Foundational capabilities are those from which most ISAOs might find a larger number of applicable capabilities to consider for serving their members. They might include using a standard method to send and receive cyber threat indicators, vetting members (a trust capability), and storing threat indicator information, to name a few.
- **Additional** capabilities typically might encompass those which further differentiate the ISAO or meet the needs and constraints of its particular operational or business environment, driven by its own member needs. Additional capabilities tend to represent enhanced capabilities beyond those afforded by

foundational capabilities, in the case of most ISAOs, as they construct a portfolio of capabilities designed to address the needs of their members. An example might include analysis of incoming cyber information in order to assess its relevance to membership needs.

- **Unique** capabilities are special functions or activities developed or adopted by the organization itself to meet its own particular needs or opportunities. Unique capabilities are those that are not otherwise identified as foundational or additional. This construct deliberately refrains from specifying particular unique capabilities, because these are the specific capabilities that ISAOs design and apply for their members. In other words, a unique capability is electively created and applied by any individual ISAO, but has a common lexicon term to describe its type (unique) that is understood by all ISAOs. The existence of the term “unique” within the lexicon of this construct enables all members of the ISAO sharing community to understand immediately the type of capability being discussed, applied, or considered so that best practices, research, event programming, and development of active defense and resilience doctrine is better enabled. They might include understanding effective firewall settings, growing mentor-protégé opportunities, or instituting listserv mechanisms.

Capabilities an ISAO decides to choose depend on the service it wishes to provide to its members. There is no requirement to “package” or select any specific capability or groups of capabilities—it is a pick-and-choose environment. Experience may well reveal certain capabilities that all or most organizations consider essential in actual practice for an effective and secure information sharing partnership.

The ISAO SO will develop a common lexicon to describe the capabilities so there will be an understanding of each capability in order to accelerate adoption and improve the ability for collaboration. Additionally, a common lexicon supports operational techniques, as well as procedural and doctrinal development, while fueling innovation. The better everyone understands ISAO capabilities in advance, the more we can accelerate and support an overall ecology of trusted sharing. This is because ISAOs—which include Information Sharing and Analysis Centers (ISACs)—that see a known indicator of recognized trusted sharing and analytic capabilities (a “Basic Voluntary Capability,” as explained below) will instantly recognize it and can form collaborative partnerships and trusted relationships more readily and quickly than they otherwise might. This approach leverages the proven experience that well-crafted and minimal standardization can actually improve diversity and trusted collaboration. It acts as an accelerant and catalyst to prospective partners who will share data and knowledge for benefit of the entire ISAO community.

For this reason, we will develop a one-page *standard descriptive form* that states an ISAO’s name, mission, purpose, and particular capability using a common lexicon built on the scheme of foundational, additional, and unique capabilities offered in this document. One portion of that form could contain a standard and recognizable icon representing the Basic Voluntary Capability. That symbol would reassure potential partners about the organization's understanding of the capability level, thereby increasing the probability that trusted collaborative relationships will form which are mutually productive for not only the partner organizations but also the ISAO community as a whole. This is the intent of the ISAO voluntary standards development effort.

The *standard descriptive form* would avoid:

- Statements of any particular requirements for any ISAO, because all standards and guidelines are voluntary.
- Issues involving complexity or excessively detailed information.

This approach would feature:

- A comprehensive roadmap, informed by subject matter expertise, to consider for ISAO development that invites formation and informs sustainment.
- A standard lexicon and model to accelerate collaborative innovation within the growing community of ISAOs.
- A common lexicon that addresses, specifically names, and invites—but does not constrain or restrain—ISAO-specific and member-driven innovation and customization.
- A way ahead to standardize and simplify an essential ISAO Basic Voluntary Capability in order to accelerate ISAO partnering for trusted collaboration, a key resilience benefit, by using a universally understood approach to make it more efficient.
- An achievable, elective, and aspirational component to encourage a basic capability. New and evolving ISAOs might aspire to attain the Basic Voluntary Capability, but they would not be required to select its use because it is voluntary. ISAOs that do develop the Basic Voluntary Capability may find benefits that accrue for their members from more efficient ISAO collaborative partnerships and that may accelerate trusted relationships.

The following are among the foundational capabilities that a Basic Voluntary Capability should indicate:

- Administering day-to-day operations and providing sufficient support to members.
- Vetting new members. This is one aspect of demonstrating trustworthiness and credibility to current and potential members, as well as to partners.

- Enabling members to collaborate and share information among themselves and with ISAO administrators or analysts. This may include the capability to send and receive suspicious activity reports (SARs) and incident reports.
- Analyzing incoming information to assess its relevance to members and implications for them.
- Managing and sharing restricted or otherwise sensitive information in a way that respects originators' preferences. This might include binding members to an information sharing policy.
- Disseminating information to members. Possible mechanisms include, but are not limited to, face-to-face meetings, secure portals, mailing lists and other email distribution platforms, online discussions, message boards, webinars and chat applications.

The capabilities represented by the above Basic Voluntary Capability are among the foundational capabilities that new and evolving ISAOs might choose to select, along with other additional and unique capabilities, in any mix they deem appropriate to the needs of their members, the threat and vulnerability environment they face, and the resources and constraints of their particular organization.

This model means that every ISAO can be described in a standard manner that consists of:

- A discrete core capabilities statement summarizing the organization's distinctive blend of descriptive foundational, additional, and unique capabilities, which could be numbered or digitized for reference.
- Basic Voluntary Capability (if chosen by the ISAO) expressed through a recognizable, accepted icon, to promote sharing and inter-ISAO collaboration; and a standard, one-page Basic Voluntary Capability template summary for reference and doctrinal development for operationalized resilience (unity of effort and message).
- Compatibility with measures of effectiveness. All ISAOs can be described in a standard lexicon and format that specifically identifies each capability by type and number. That being the case, research products and resilience plans can benefit from the fact that capabilities application may be further enhanced by digital processing and automated sharing for the benefit of the ISAO community and the nation. The result is a standard lexicon construct that supports continuous improvement in operationalized resilience for the ISAO community as a whole.

5.6 CATEGORIES OF ISAOs

Four strategic drivers—information sharing, analytics, member value delivery, and business and IT operations—support the various core capability areas. Additionally, there are three types of capabilities: foundational, additional, and unique. All have been tied together within a comprehensive structure of *voluntary* standards and guidelines that use a common lexicon and a way for prospective trusted collaboration partner organizations to identify a set of capabilities. This section discusses the types of ISAOs that may emerge; the intent is to *describe, not prescribe,* what ISAOs might look like as they develop over time.

Although there will be many variations of ISAOs, all will fall into one of the four categories described below, each with different characteristics, attracting different participants, and having different capabilities. A second factor considers degrees of trust, which may be gauged in many ways. Examples may include possession of security clearances, vetting of members, non-disclosure agreements, and other contractual arrangements. When an ISAO is operating within the framework of a larger response organization, the ISAO's host or sponsoring organization might ask for its operation to be aligned with higher level guidance, which promotes unity of effort and message.

Examples include the methods for response used by established ISACs, methodologies and procedures used by the DHS National Cybersecurity and Communications Integration Center (NCCIC), and other proven processes. In these instances, an ISAO will be in a category such as "industry or technology" and have capabilities that support its operation.

To restate, this section provides a high-level description of the different categories of ISAOs going forward. The list is non-exhaustive and illustrative only. Our proposed model, which contains numerous capabilities, could identify any specific requirements there as unique that are not already identified within the proposed foundational or additional capabilities. In these instances, an ISAO may be in any of the below categories. It is important to remember that some ISAOs, in the individual and/or informal group-based category, may wish to have minimal capabilities and choose to receive cyber threat information by means of email or other less complex means. In the end, what matters is improving the U.S. cybersecurity posture.

5.6.1 EXAMPLE 1: INDIVIDUALS OR INFORMAL GROUP-BASED

Characteristics: A single entity, event-driven (such as a new virus or malware requiring a group formed ad hoc to respond); or an informal collection of organizations or individuals with limited sharing in scope or duration and analysis objectives, infrequent sharing of information, information obtained from public sources or other similar ISAOs or between members; generally little or no tailored information analysis or incident response.

Examples: A self-employed security consultant; a localized group of professionals; a rapidly convened or issue-driven ISAO.

5.6.2 EXAMPLE 2: INDUSTRY- OR SECTOR-BASED

Characteristics: Groups of organizations (public, private, or blended) or a private company sharing a common interest, goal, or purpose. Some members may be capable of sharing information with federal and law enforcement entities at classified levels. The industry or sector size may vary greatly. Examples might be a small town, an unaffiliated bank, a software consulting firm, or a government contractor. Information received may be from public sources or members. The organization might perform ISAC or other ISAO incident response coordination, perhaps as part of government response frameworks (such as DHS NCCIC) that consist of both public- and private-sector partners. It may analyze shared information as it pertains to the ISAO and its members and other collaborative security partners in coordination efforts.

Examples: Southern U.S. mega churches; U.S. electronic game developers industry; existing ISACs.

5.6.3 EXAMPLE 3: GEOGRAPHICALLY-BASED

Characteristics: Members come from a geographic region and cross multiple businesses or sectors. Some members may be able to share information with federal and law enforcement entities at a classified level. Incident response coordination is generally a significant goal of the members. Members regularly analyze government and member-shared information. Entities may provide for a member-supported security operations center or similar shared resources or contracted support.

Examples: The State of Texas; the City of San Antonio; Bowie County.

5.6.4 EXAMPLE 4: OTHER

Characteristics: Groups of technical individuals who have an active interest in cyber threat indicators due to their engagement of cyber defenses, or other computer technology in their business. These members or groups desire to share information and, in some cases, perform analysis of threat vectors and software. It may be that this group shares directly with the U.S. government in order to collect the most current cyber threat indicator information.

Examples: Computer security firms, cyber defense service providers.

5.7 CONSIDERING CAPABILITIES

An ISAO may choose capabilities that will determine its category or, inversely, the category by which an ISAO defines itself may suggest the capabilities it may choose to consider. Either way, ISAO capabilities and categories potentially help inform each other, depending on the approach an ISAO chooses to best serve the needs of its members. The voluntary standards describe possible capabilities for new and developing ISAOs to consider that may help them serve their members, while organizing those capabilities within a comprehensive construct. The construct further accelerates and enables future resilience efforts by offering a standard digital-ready lexicon and a Basic Voluntary Capability, which any ISAO can aspire to and elect to apply, and which may help accelerate the development of trusted security collaboration for the ISAO that employs it and at ISAO community levels writ large.

We have described above three types of ISAO capabilities: foundational, additional, and unique. Although most ISAOs will likely choose to commence operations with primarily foundational capabilities, their evolution over time will probably include relatively greater use of additional and unique capabilities that may potentially broaden and enhance the effectiveness of information sharing and analysis offerings for their members.

6 CYBERSECURITY-RELATED INFORMATION SHARING

The ISAO SO recognizes that not all new ISAOs may be capable initially of or desire to fully achieve these objectives. This information sharing guideline is structured to provide a new or existing ISAO with a context identifying outcomes to be considered when selecting and implementing information sharing and collaboration efforts for the ISAO. In addition to a context framework and information uses, we also present a functional decomposition of possible ISAO information sharing activities. This guideline also offers a path to consider for evolving an ISAO’s information sharing capabilities. Note that the framework is conceptual as opposed to prescriptive, and inclusion is meant to illustrate options rather than mandate. Information sharing may also be supported by other future relevant documents (statements of principle, policy documents, processes, procedures, data standards, etc.).

6.1 SUPPORTING CYBERSECURITY RISK AND INCIDENT MANAGEMENT

Companies, enterprises, and organizations manage strategic and tactical cyber-related risks, as a result of the technology they employ or their interaction with others. Managing these risks entails understanding the environment in which they are operating (situational awareness), determining directions to pursue (decision-making), and detailing efforts (actions) to undertake. These are activities an organization executes daily.

With respect to cybersecurity-related information, an organization has a need for various types of information, which we place for discussion purposes into a *context for information sharing* with two major categories.

6.1.1 TYPE OF ACTIVITY SUPPORT

The first category of information relates to the purpose for which the information is used. While the overall purpose of information sharing is to enable effective risk management, this can be distilled into three groups of information. These different groups build up to a full spectrum of risk management.

- *Situational awareness* information provides awareness of the broader threat landscape.
- *Decision making* information is customized to a particular organization's needs and enables more effective security management.
- *Action* information directly supports the implementation of a particular measure that improves security.

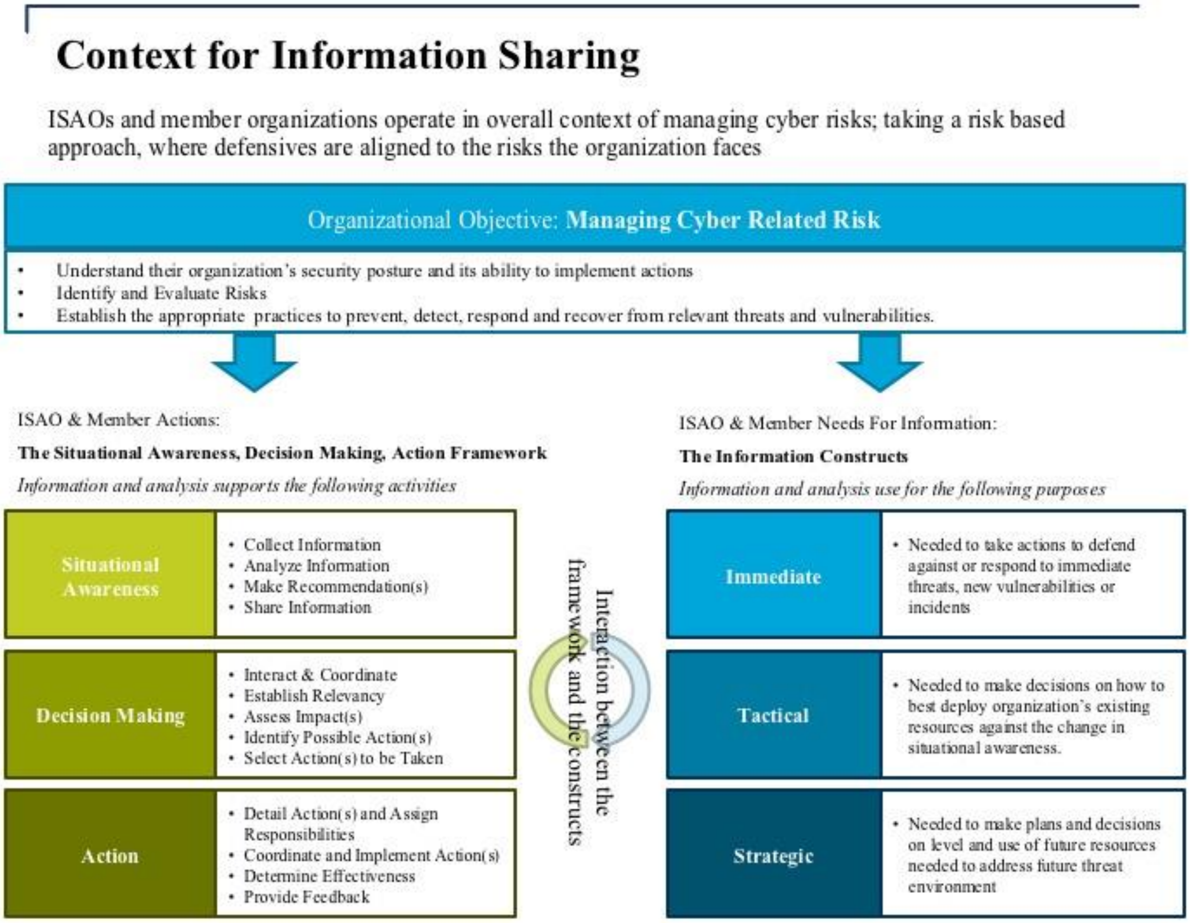
6.1.2 TYPE OF INFORMATION USE

The second category of information revolves around time and the application of resources. This type of information seeks to capture the complementary efforts that need to occur for effective cybersecurity. It begins with information most operationally relevant to security and builds upon it.

- *Immediate* information relates to actions to defend against or respond to new threats, vulnerabilities, or incidents.
- *Tactical* information relates to decisions on how to best deploy organization's existing resources against the change in situational awareness.
- *Strategic* information relates to making plans and decisions on efforts and resources needed to address emerging or future threat environments.

The situational awareness, decision-making, and action framework and the information construct levels are depicted in Figure 2. Conceptually, a mature ISAO will have a close and interactive relationship between the framework an organization is executing and the information sharing construct levels an ISAO is performing.

Figure 2. Context for Information Sharing



Context for Information Sharing

ISAOs and member organizations operate in overall context of managing cyber risks; taking a risk based approach, where defensives are aligned to the risks the organization faces

Organizational Objective: **Managing Cyber Related Risk**

- Understand their organization's security posture and its ability to implement actions
- Identify and Evaluate Risks
- Establish the appropriate practices to prevent, detect, respond and recover from relevant threats and vulnerabilities.

ISAO & Member Actions:

The Situational Awareness, Decision Making, Action Framework

Information and analysis supports the following activities

Situational Awareness
- Collect Information
- Analyze Information
- Make Recommendation(s)
- Share Information

Decision Making
- Interact & Coordinate
- Establish Relevancy
- Assess Impact(s)
- Identify Possible Action(s)
- Select Action(s) to be Taken

Action
- Detail Action(s) and Assign Responsibilities
- Coordinate and Implement Action(s)
- Determine Effectiveness
- Provide Feedback

Interaction between the framework and the constructs

ISAO & Member Needs For Information:

The Information Constructs

Information and analysis use for the following purposes

Immediate
- Needed to take actions to defend against or respond to immediate threats, new vulnerabilities or incidents

Tactical
- Needed to make decisions on how to best deploy organization's existing resources against the change in situational awareness.

Strategic
- Needed to make plans and decisions on level and use of future resources needed to address future threat environment

6.2 ISAO INFORMATION SHARING VALUE PROPOSITION

Fundamental to the establishment of an ISAO will be the "value proposition" to be offered its participants, partners, and collaborators and the specific categories of information to be collected, disseminated, and shared. The following guidance can assist ISAOs as they develop their information sharing policy considerations.

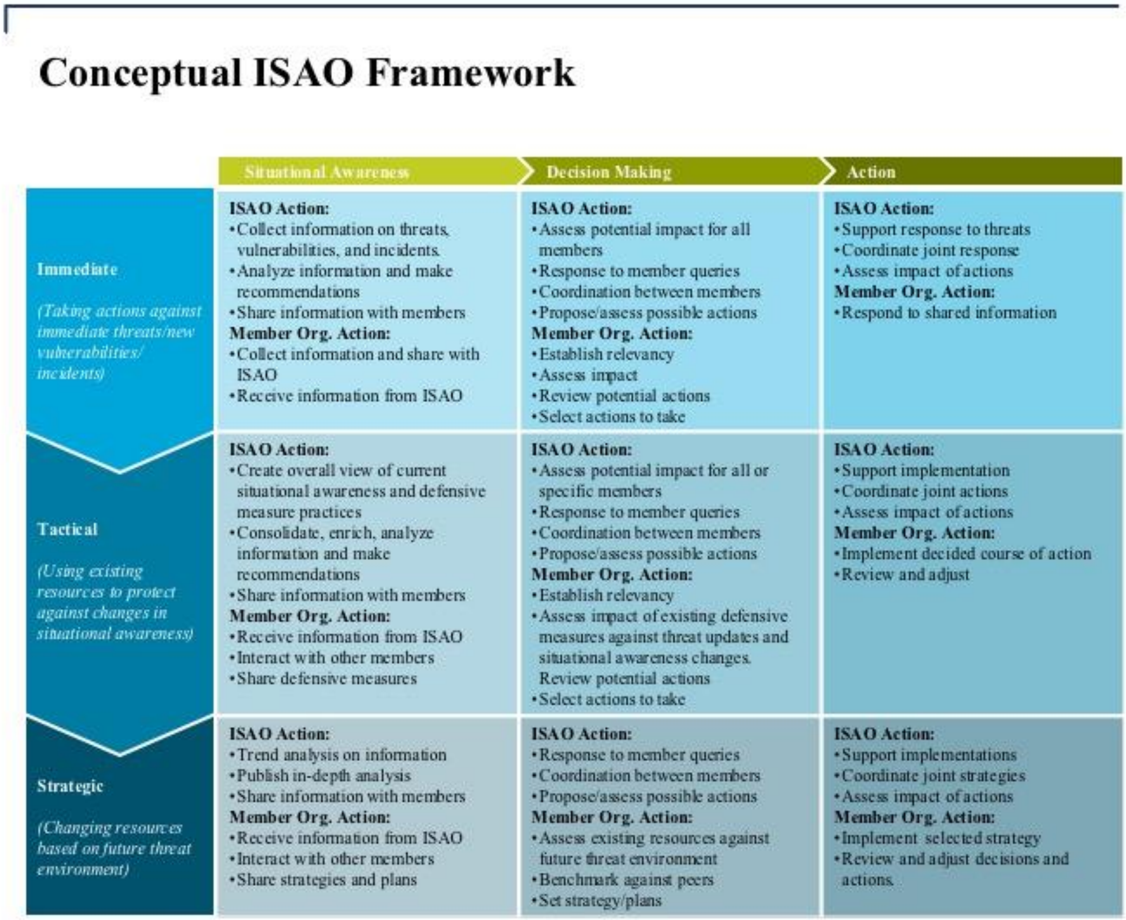
Using the activities and categories of information discussed previously, an ISAO can consider and respond to the questions below to begin establishing an information sharing policy.

- Which categories of information does the ISAO want to provide members to give them *situational awareness* relevant to their affinity group?
- Will the ISAO provide raw data, analysis, or both to assist members in their *tactical decision-making* efforts?
- Will members expect information related to *action* recommendations, including defensive measures, best practices, and/or procedures for incident coordination?

- Will the ISAO provide analysis of a *strategic* nature related to trending analysis and threat actor targeting and motivation?

In the context of the framework and information construct levels, Figure 3 presents various interactions to consider as an ISAO develops its information sharing objectives and policies.

Figure 3. Levels of Information Related to Activity Framework



Conceptual ISAO Framework

	Situational Awareness	Decision Making	Action
Immediate *(Taking actions against immediate threats/new vulnerabilities/ incidents)*	**ISAO Action:** •Collect information on threats, vulnerabilities, and incidents. •Analyze information and make recommendations •Share information with members **Member Org. Action:** •Collect information and share with ISAO •Receive information from ISAO	**ISAO Action:** •Assess potential impact for all members •Response to member queries •Coordination between members •Propose/assess possible actions **Member Org. Action:** •Establish relevancy •Assess impact •Review potential actions •Select actions to take	**ISAO Action:** •Support response to threats •Coordinate joint response •Assess impact of actions **Member Org. Action:** •Respond to shared information
Tactical *(Using existing resources to protect against changes in situational awareness)*	**ISAO Action:** •Create overall view of current situational awareness and defensive measure practices •Consolidate, enrich, analyze information and make recommendations •Share information with members **Member Org. Action:** •Receive information from ISAO •Interact with other members •Share defensive measures	**ISAO Action:** •Assess potential impact for all or specific members •Response to member queries •Coordination between members •Propose/assess possible actions **Member Org. Action:** •Establish relevancy •Assess impact of existing defensive measures against threat updates and situational awareness changes. Review potential actions •Select actions to take	**ISAO Action:** •Support implementation •Coordinate joint actions •Assess impact of actions **Member Org. Action:** •Implement decided course of action •Review and adjust
Strategic *(Changing resources based on future threat environment)*	**ISAO Action:** •Trend analysis on information •Publish in-depth analysis •Share information with members **Member Org. Action:** •Receive information from ISAO •Interact with other members •Share strategies and plans	**ISAO Action:** •Response to member queries •Coordination between members •Propose/assess possible actions **Member Org. Action:** •Assess existing resources against future threat environment •Benchmark against peers •Set strategy/plans	**ISAO Action:** •Support implementations •Coordinate joint strategies •Assess impact of actions **Member Org. Action:** •Implement selected strategy •Review and adjust decisions and actions.

6.3 CATEGORIES OF INFORMATION AN ISAO MAY WANT TO SHARE

There are several key factors to consider when evaluating the categories of cyber threat information an ISAO may want to share. In addition, there are various ways to share that information, including machine to machine, human to human, or human to machine. Machine-to-machine sharing requires structured information and should utilize standardized data formats and protocols to enable interoperability. Human-to-human sharing should utilize a common framework for describing cyber threat information to facilitate shared understanding among members, but the information may naturally be less structured than what is required for machine-to-machine sharing.

ISAOs and their members may wish to share information across ISAOs, with other ISAO members, and with the various government entities. Consistent standardized frameworks and data formats should be used when possible to facilitate these diverse cross organization information exchanges. Additionally, leveraging a consistent framework will enable integration and analysis of threat information from disparate sources that may have different focuses, like integrating indicator information with threat actor or incident information.

The Structured Threat Information eXpression (STIX) language is one of a few commonly used languages for capturing and sharing cyber threat information. STIX defines a broad framework for expressing and sharing cyber threat information in a consistent manner. This framework consists of a set of core concepts (threat actors, campaigns, TTPs, incidents, indicators, course of actions, observables, and exploit targets) and the set of relationships among those core concepts. The STIX framework is broad to support the full scope of cyber threat intelligence use cases and flexible to allow users or communities to define the subset of the STIX language that they need for their use cases. Trusted Automated eXchange of Indicator Information (TAXII) defines a standardized set of services to enable the exchange of cyber threat information. STIX and TAXII were developed through active collaboration with dozens of organizations, including threat intelligence teams from government and industry, security product and service vendors, ISACs, and major Computer Emergency Response Teams (CERTs). ISAOs should consider utilizing STIX and TAXII for automated exchanges of cyber threat information.

The STIX language enables users to define profiles for specific cyber threat sharing needs. These profiles simply document which subset of the STIX language will be used. When using STIX, it is helpful for ISAOs to develop or leverage well known STIX profiles to document the specific data elements to be exchanged in a given scenario.

STIX data model documentation is available here:
https://stixproject.github.io/data-model/

STIX profile documentation is available here:
https://stixproject.github.io/documentation/profiles/

To ensure that members are sharing and receive information valuable to them and others, ISAOs and their members should consider systematically determining what information to share and how to share it. ISAOs should consider establishing periodic reevaluations of this to ensure that member needs are being met.

CORA[3]—Cyber Operations Rapid Assessment—is a method developed to rapidly assess an organization's cyber operations and provide actionable recommendations for the collection, utilization, and sharing of threat information. A CORA assessment can help both the organization being assessed and a cyber threat information provider or ISAO by helping the provider understand the assessed organization's capabilities and needs. BLAISE[4]—Bilateral Analysis of Information Sharing Efforts—was developed to analyze information sharing efforts and determine their expected effectiveness. ISAOs should use methodologies like CORA and BLAISE to ensure that the information sharing aligns with member needs and capabilities.

The following sections describe commonly shared cyber threat information that an ISAO may wish to share. When applicable, these sections have been aligned with the terminology and definitions used in STIX.

6.3.1 CAMPAIGNS

Campaign information can relate information about intended effects of an adversary or group with the tools they employ, the threat actors that are believed to participate, incidents that have been associated with the group, and other related campaigns.

The following fields are commonly shared:

- Names—Short names or alias used for the campaign
- Description
- Intended effects—Military, economic, or political advantage, theft, destruction, disruption, etc.
- Related TTPs
- Related incidents
- Associated campaigns
- Attribution (related threat actors).

Tracking and sharing campaign information is critical for cyber threat intelligence analysis. This information allows organizations to develop an understating of the threats they face as well as the specific objectives and capabilities that an adversary or group is believed to have employed. Sharing campaign information among organizations can help all participants develop a much more comprehensive understanding of these threats.

[3] https://www.mitre.org/publications/technical-papers/cyber-operations-rapid-assessment-cora-examining-the-state-of

[4] http://dl.acm.org/citation.cfm?id=2663880

Organizations may be reluctant to include attribution information when sharing campaign information due to its sensitive nature. Sharing campaign attribution information is not always necessary to facilitate a broader understanding of a given campaign.

Campaign information often comes from government or industry cyber threat intelligence sources. More established sharing organizations including ISACs may operate their own cyber threat analysis teams and track campaigns that are relevant to managing their cyber security risk or risk to their members.

Campaign information is frequently more strategic in nature and used to inform situational awareness and decision making.

6.3.2 THREAT ACTORS

Threat actor information describes malicious actors that may represent a cyber threat or have been historically observed or related to known incidents.

The following fields are commonly shared:

- Names—Short names or alias used for the threat actor
- Description—A textual description of the threat actor
- Identity—Information that may identify the actor
- Type—Hacker, hacktivist, state actor, electronic crime actor, insider threat, etc.
- Motivation—Political, economic or financial, ideological, military, etc.
- Sophistication—Novice, practitioner, expert, innovator, etc.
- Intended effects—Military, economic, or political advantage, theft, destruction, disruption, etc.
- Observed TTPs—TTPs that an actor has been observed to use
- Related campaigns—Campaigns that have been attributed to the actor.

Tracking and sharing threat actor information is critical for cyber threat intelligence analysis. This information allows organizations to develop an understating of the threats they face as well as the specific objectives and capabilities that an adversary or group is believed to have employed. Sharing threat actor information among organizations can help all participants develop a much more comprehensive understanding of these threats.

Threat actor information often comes from government or industry cyber threat intelligence sources. More established sharing organizations including ISACs may operate their own cyber threat analysis teams and track threat actors relevant to managing their cyber security risk or risk to their members.

Threat actor information is frequently more strategic in nature and used to inform situational awareness and decision making.

6.3.3 TACTICS, TECHNIQUES, AND PROCEDURES (TTPs)

TTPs represent a fairly broad set of information that can be used to describe the behavior or capabilities of a threat actor of campaign. TTPs characterize what adversaries do and how they do it. As such, TTPs encompass specific adversary behaviors, resources leveraged, target victim information, and vulnerabilities or weaknesses being targeted.

The following fields are commonly shared:

- Title
- Description
- Intended effect
- Behavior—Specific attack patterns, malware, or exploits
- Resources—Tools, infrastructure, or personas
- Victim targeting—People, organizations, information or access being targeted
- Kill chain phase
- Related TTPs.

Malware samples represent one commonly shared type of TTP. Sharing malware samples can enable broad distributed analysis of the sample as well as higher level trending of both malware and the types of organizations being targeted.

TTPs are a critical component to cyber threat intelligence analysis and they are frequently related or shared in the context of incidents to describe the TTPs detected during an incident investigation. Cyber threat indicators relate low-level observables to TTPs to give context to what defenders should look for. Campaigns and threat actors are often related to TTPs to characterize either previously observed or expected adversary capabilities.

Aggregated TTP information can enable cyber threat analysts to develop a more holistic understanding of the threat or more narrowly advance the understanding of a specific adversaries. This information may inform strategic, tactical, and immediate situational awareness, decision making, and actions.

6.3.4 INCIDENTS

Incident information is specific information related to or discovered while investigating or responding to a cybersecurity incident. The amount and level of detail included in shared incident information varies widely depending upon the intended use of the shared information and sensitivities related to financial, reputational or other negative impacts of incident disclosure.

The following fields are commonly shared:

- Title
- Description
- Category—Improper usage, scanning or probing, denial of service, etc.
- Reporter—The reporting source of the incident description
- Victim—Details about the victim of the incident
- Affected assets—Describes the assets that were affected during the incident
- Impact assessment—Describes the impact of the incident
- Related indicators—IP addresses, file hashes, domains, etc.
- Leveraged TTPs—Attack techniques, malware, tools, etc.
- Attributed threat actors
- Intended effect—Theft, disruption, account take over, fraud, etc.
- Related incidents
- Courses of action.

The U.S. government publishes several well-known guides for reporting incident information and incident handling.

US-CERT has established the following guidelines for incident notification: https://www.us-cert.gov/incident-notification-guidelines

The National Institute of Standards and Technology (NIST) has a special publication on incident handling: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

These are excellent references for the type of information that is commonly shared to support incident response and analysis.

Sharing incident information can enable or support a wide variety of use cases and different use cases will naturally have different incident information requirements. Incident information sharing can enable large scale analysis to uncover adversary trending across the cybersecurity ecosystem. Detailed incident information sharing may enable advanced cyber threat intelligence analysis related to specific threat actors and campaigns. Incident information sharing can also help uncover key indicators of malicious activity to inform partner cyber defenses.

One well-known example of large scale incident analysis enabled by the sharing of detailed incident information is Verizon’s Data Breach Investigations Report.[5]

[5] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

This report is the result of analyzing a large collection of incident information contributed by a variety of organizations. This report is oriented toward providing strategic and tactical value to inform situational awareness and decision making.

6.3.5 INDICATORS

Indicators convey specific patterns combined with contextual information intended to represent artifacts and/or behaviors of interest within a cyber security context and are used for detecting activity of interest. Indicators are widely shared today, with examples ranging from malicious file hashes to command and control IP addresses, phishing emails, and other types.

Effective indicator sharing includes contextual information to allow downstream consumers to determine whether an indicator is relevant to their organization, how to handle the indicator, what TTP is indicated, the valid time window of the indicator, and related incidents, threat actors, and campaigns.

The following fields are commonly shared:

- Title
- Description
- Pattern—The machine readable pattern
- Confidence—The level of confidence in the indicator
- Indicated TTP
- Valid time position—The time window for which the indicator is valid.

Indicator sharing tends to focus on machine-to-machine information exchanges. One example of automated indicator sharing is the DHS-operated Automated Indicator Sharing (AIS) initiative to enable cyber threat sharing among the federal government departments and agencies and the private sector. This initiative utilizes STIX and TAXII for the automated exchange of cyber threat information and has defined a profile of the STIX language for indicator exchange. The AIS STIX profile documents the specific data elements of the STIX language that will be used for AIS cyber threat sharing. This provides a good starting point for basic cyber threat indicator sharing and can be easily leveraged to establish a consistent approach to sharing indicators within and among ISAOs.

Indicators are often generated through malware analysis, incident response, and endpoint and network monitoring. As such, indicator information frequently comes from a variety of sources including ISACs, CERTs, security product and service vendors, organization-specific security teams, and open source reporting. This variety of sources of indicator information adds emphasis to the need to convey contextual information with shared indicators. A common challenge to indicator sharing today is simply determining which indicators are relevant.

When sharing indicators there is an opportunity to capture basic indicator sighting information. That is simply a report that a given indicator matched or was seen within some sector or even specific organization. In aggregate this sighting information can assist in understanding the prevalence, targeting information, and more. This aggregate sighting information widely seen as a low-cost and low-risk method of supporting more sophisticated cyber threat intelligence analysis.

6.3.6 VULNERABILITY INFORMATION

Vulnerability information may include details about the vulnerabilities in specific systems or infrastructure, specific application vulnerabilities, or general classes of vulnerabilities.

The following fields are commonly shared:

- Title
- Description
- Vulnerability ID—A reference to a Common Vulnerabilities and Exposures threat or other well-known identifier
- Score—A Common Vulnerability Scoring System rating or similar score for the referenced vulnerability
- Affected software.

Mature software vendors routinely publish vulnerability information related to their products and services. Many governments issue vulnerability reports or security advisories to raise awareness as well. The US-CERT alerts[6] are one example of these government advisories.

Shared vulnerability information frequently informs immediate response actions, especially when the information is related to recently discovered high-severity vulnerabilities in exposed systems. Vulnerability trends and more general classes of vulnerability information regularly inform tactical and strategic situational awareness and decision making.

6.3.7 COURSES OF ACTION

Courses of action are specific measures to mitigate a threat or respond to an incident. They may be relatively low level like blocking a specific IP address or higher level like using application whitelisting. As such, sharing courses of action can span the full range of immediate, tactical, and strategic information to impact decision making and actions.

[6] https://www.us-cert.gov/ncas/alerts

The following fields are commonly shared:

- Title
- Description
- Type—Training, monitoring, patching, blocking, etc.
- Objective
- Impact
- Cost
- Efficacy
- Course of action—Firewall or intrusion detection system rule, specific configuration change, etc.

Sharing courses of action can enable automated actions to mitigate threats as well as enable organizations to collaborate and arrive at the overall best course of action given a variety of options.

6.3.8 THREAT INTELLIGENCE REPORTS

Threat intelligence reports are a broad category of cyber threat information that may range from high-level trending reports to detailed analysis of specific campaigns.

One well-known example of an industry-developed cyber threat intelligence report is Mandiant's APT1 report[7] This report includes the full range of cyber threat intelligence providing strategic, tactical, and immediate response value. The report includes campaign, threat actor, TTP, and indicator information. This report is the result of several years of analysis and tracking of cyber threats.

In addition to this report and other well-known industry examples, there are numerous government and open source threat intelligence reports.

6.3.9 ANALYSIS

Potentially important services an ISAO can choose to provide its participants are analytical services. Many organizations focus on information sharing, but analysis can also provide value to ISAO stakeholders. As noted in the framework and information constructs described in earlier sections of this document, ISAOs can choose from a range of analysis options to provide its participants. Participants who engage in analysis find benefits in their immediate, tactical and strategic decision-making. This section discusses analysis considerations to support immediate and tactical actions.

ISAOs provide some level of continuous information flow to or among its participants. When an ISAO interprets cybersecurity information, participants receive

[7] http://intelreport.mandiant.com

relevant and coherent intelligence that assists members in making decisions on how to deploy operational resources. An ISAO may elect to apply its own knowledge and expertise along with the needs of its participants to develop written assessments.

An ISAO can provide a trusted environment for its participants to encourage analysts to collaborate and share relevant information. ISAOs providing, facilitating and leading these analysis activities can significantly increase the value of their efforts

The following are examples of informational analysis:

- **Risk awareness and mitigation communications**—One of the most valued analytical contributions an ISAO makes involves the collaboration among ISAO participants, its analysts, and others to raise awareness and educate participants on cybersecurity risks and approaches to be considered for mitigating those risks. The sharing of collective knowledge and collaboration among expert personnel and could involve only a small number of the ISAO participants—should result in broader communication to the ISAO participants. These "*tactical*" or operations-focused communications can provide guidance to prevent successful attacks, identify methods or procedures to mitigate specific risks, identify effective practices being applied by others, and report details from participants on their experiences and effectiveness of actions they have taken.

  Such communications can be tailored for various audiences within the ISAO constituency (executives, managers, and operational personnel) and delivered as required and/or as a periodic communication. Communication can take the form of emails, reports, briefings (webinars), conference calls, and other networking/collaboration events among participants and others. These communications will assist those responsible for making informed decisions for their organization.

- **Alert notifications**—By examining the flow of information through an ISAO the ISAO has the opportunity to identify new, changing, or escalating cybersecurity risks or incidents of particular interests to its participants and others. This analysis can alert members and partners to urgent, crisis, or other levels of notification and help ISAOs provide information and recommendations to their members and partners on immediate action they can take to mitigate the risk. Providing subsequent updated alerts and additional analysis can further assist an ISAO, its partners, and others to understand the evolving nature of an incident, threat, or risk.

- **Incident response coordination**—Some ISAOs may envision a role of understanding and sometimes becoming actively involved in responding to cybersecurity-related incidents. ISAOs may be asked by some members to assist in incident response. In such cases, an ISAO can provide an opportunity for collaboration among analysts of member organizations to determine necessary operational coordination and the effectiveness of response actions taken as a situation progresses and is resolved. After-action and root cause reports can be prepared and provide valuable information that can be shared among ISAO participants and others. If an ISAO is to assume a role in coordinating incident response, it may want to consider identifying the specific value of the ISAO's incident response function, its role in incident response, and triggers for activating it.

ISAOs at some level will all perform some form of analysis, even if it is only a decision to share relevant information. In addition to the items discussed above, an ISAO may produce other operationally oriented analysis products. Further, beyond these operational products, ISAOs are in a position to provide trending analysis reporting and also strategic analysis to help those who make decisions affecting their organization's future planning and resource requirements.

6.3.10 SECURITY ADVISORIES AND ALERTS

Security advisories and alerts are published by a variety of sources, including international CERTs, governments, software and security tool vendors, ISACs, not-for-profit organizations, and security researchers. These publications vary from rebroadcasting of important software vendor's security advisories to tailored products aimed to raise awareness of important new vulnerabilities and security issues.

Many of the major international CERTs provide security advisories and alerts. For example, US-CERT publishes alerts about current security issues, vulnerabilities, and exploits. These alerts attempt to describe the issue, explain the impact of the issue, and offer a solution to address the issue. These alerts are available at https://www.us-cert.gov/ncas/alerts.

Similarly Aus-CERT, an organization based at the University of Queensland in Australia, publishes two different types of security bulletins for its members. These security bulletins are available at https://www.auscert.org.au/render.html?cid=1.

MS-ISAC is an example of an ISAC that publishes security advisories. These advisories are available at https://msisac.cisecurity.org/advisories/.

Sharing security advisories and alerts can provide the full range of immediate, tactical, and strategic information to impact decision making and actions.

6.3.11 BEST PRACTICES

Sharing cybersecurity best practices among ISAO members is an important way for organizations to collaborate and build trust, learn from each other, and collect feedback as they mature their cybersecurity practices.

ISAOs can support the interactions shown above in Figure 3 by providing their members information needing immediate action, information of a tactical nature, and/or information of a strategic nature. There are various types of information an ISAO and its members may want to share. This following is not an exhaustive list of types of information and ISAO may choose to share, and there is no expectation that an ISAO share all or any of the following information. An ISAO and its members or customers can choose to share or not share information based on what meets the mission of the ISAO and the needs of the ISAO members. Not all information sets are appropriate for all ISAOs or ISAO members and customers.

Potential information sets an ISAO and its members could choose to share include:

- Malicious IP addresses
- Malware analysis
- Automated sharing of raw threat indicators
- Effective cybersecurity practices for a specific community or incident
- Generic effective cybersecurity practices
- Big data analytics
- Attack trending and analysis
- Assessments on specific threat actors or campaigns
- Attacks specific companies have seen on their networks
- Aggregated attack information from multiple customers/members
- Those shared by for-profit company ISAOs through managed security services
- Single vendor vulnerability information
- Cross-platform or multi-vendor vulnerability information
- Vulnerability remediation tactics
- Information on a specific, ongoing, or current cyber threat or attack
- Threat intelligence reports developed by other parties
- Open-source news reporting
- Presentations and discussions from subject matter experts
- Government alerts
- Vendor alerts
- Indicators of compromise
- Threats
- Vulnerabilities

- Targets
- Impacts
- Analysis
- Indicators of compromise
- Tactics, techniques, and procedures
- Incident information
- Campaigns
- Defensive measures and courses of action
- Best practices
- Trending and strategic analysis
- Threat actor targeting and motivations
- Existing industry practices.

6.4 COLLECTION, DISSEMINATION AND ANALYSIS—FUNCTIONAL DECOMPOSITION

At this point the information sharing functional components described below are not intended to be a one-to-one mapping to the context depicted above, as the high-level functional categories are generic and support various aspects of the framework. The high-level categories are decomposed into sub-categories to identify the more specific information capabilities needed to support those categories.

This section describes in more detail the functional components of information sharing an ISAO may want to consider.

Participation in information sharing efforts is mainly driven by interests—either personal, organizational, or both. Those responsible for managing cybersecurity risks and taking actions to deal with them will participate in an ad hoc, defined, or institutionalized information sharing activity to better understand the environment in which they are operating and/or to contribute to collective interests.

Personal or organizational interests generally value the following:

- New knowledge for a better understanding of the threat and vulnerability environment in which they are operating
- Recommendations for dealing with specific threats and vulnerabilities
- Receipt of situational alerts that may affect their security posture
- Validation of their understanding of a current situation or incident

- Additional information that may improve their current understanding of threats, vulnerabilities, and/or incidents
- Knowledge of the actions being taken by others
- Coordination of collective actions
- Feedback on the effectiveness of actions being taken by others individually or collectively.

These personal or organizational interests can be used to describe four functional component categories that together make up the broad tactical and strategic efforts that an ISAO can perform:

- Threat landscape awareness
- Response measures
- Coordination
- Trend and pattern analysis.

These broad categories, as shown below, can be further decomposed to more specific functional elements and information sharing capabilities to support the personal or organizational interests of those participating in or working with an ISAO.

Table 1 describes these categories and sub-categories and identifies information sharing capabilities that support them.

Table 1. Functional Categories and Information Sharing Capabilities

Functional Category or Sub-category	Description	Information Sharing Capability
Threat landscape awareness	Know what’s going on related to cybersecurity or other issues of interest to the ISAO.	
◆ Collect information: — General.	◆ Obtain threat, vulnerability, and incident information from ISAO participants and other sources for information of interest.	◆ Anonymous and attributable submissions ◆ Email and listservs ◆ Calls ◆ Meetings ◆ Secure portal submissions ◆ Automation feeds ◆ Direct cybersecurity partner feeds ◆ Traffic Light Protocol (TLP) labelling implementation
◆ Focus on community of interest.	◆ As necessary, encourage community of interest participation to build deeper trust relationships.	◆ Similar capabilities as above that can be segregated and tailored for community of interest participants
— Make appropriate information available.	◆ Distribute or make information available in accordance with TLP procedures and labelling.	◆ Distribution through appropriate communication channels (portal access, email, automation platforms, etc.)

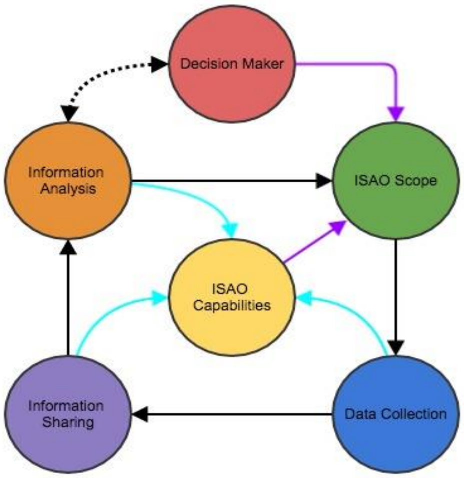
Functional Category or Sub-category	Description	Information Sharing Capability
— Analyze collected information.	◆ Review, de-conflict, validate, sanitize, and analyze collected information. ◆ Conduct research or intelligence to alert the members of evolving or existing threats, incidents, and vulnerabilities.	◆ Analysts and analysts' tools
— Develop alerts.	◆ Identify changes in situational awareness that may be of interest to ISAO participants and others.	◆ Communication mechanisms for levels of alert criticality ◆ Multiple mechanisms for highest level of alerts
Response measures	Establish operational or procedural measures to mitigate the utility or deny the effectiveness of vulnerabilities or exploits to infrastructure, operations, or systems.	
◆ Distribute alerts and rapid notification..	◆ Provide developed alerts and notifications to appropriate participants or partners.	◆ Communication mechanisms for levels of alert criticality ◆ Multiple and diverse mechanisms for highest level of alerts
◆ Develop countermeasures: — Immediate — Long-term.	◆ Develop in collaboration with participants and partners, countermeasures to mitigate risks of new threats or vulnerabilities. ◆ Focus on immediate and then longer term measures.	◆ Conferencing and networking collaboration mechanisms for both technical experts and participants ◆ Access to capabilities that provide searchable topic analysis for participants
◆ Identify "best" and "good" practice recommendations.	◆ Based on interests of participants, make recommendations for "best" and "good" practices to mitigate and respond to cybersecurity and other relevant risks and incidents.	◆ Conferencing, networking, and forums for collaboration among technical experts and participants ◆ Surveying capabilities ◆ Publishing and providing references and a repository for availability of recommendations to participants ◆ Access to capabilities that provide searchable topic analysis for participants
◆ Determine effectiveness.	◆ Develop metrics and perform surveys to continually measure the effectiveness and satisfaction of participants with the services being provided.	◆ Participant survey capabilities
Coordination	Synchronize and integrate activities to ensure the pursuit of the shared objectives established by the ISAO.	
◆ Establish coordination processes and capabilities	◆ Policy and procedures established for assessing the need for coordination among members with shared interests to discuss and coordinated	◆ Communication/network mechanism for a leadership group (identified sub-group) to make a decision to activate coordination.
◆ Activate coordination	◆ Issue notification for an "emergency" call for coordination.	◆ Established diverse communication capability to initiate an "Emergency Call"

Functional Category or Sub-category	Description	Information Sharing Capability
◆ Establish coordination actions/efforts	◆ Establish “playbooks” for various situations where coordination among participants is required.	◆ For ongoing incidents of specified severity implement conferencing capabilities to determine the status, countermeasures, and response information related to an ongoing situation.
◆ Assess coordination efforts	◆ During and following coordination events continually assess decisions and actions taken.	◆ Survey capabilities. ◆ Conferencing capabilities
Trend and Pattern Analysis	Collect information and attempt to spot a pattern or trend derived from the information of interest to the ISAO participants.	
◆ Retain historical information.	◆ Maintain history of submissions, analysis and decisions in a secure database.	◆ Secure operational database and software with appropriate access controls to segregate and deal with various sensitivity of information
◆ Perform strategic analysis: — Identify trends, discontinuities, or patterns of activity. — Determine threat actors and motivations.	◆ Analyze the ISAO historical information along with other information to provide value-added insights on trends and new activity of significant to the interest of participants.	◆ Analysts and analysts’ tools ◆ External collaboration mechanisms for analysts to engage other experts
◆ Publish analysis and recommendations.	◆ Regularly communicate with ISAO participants and others based on ISAO policy and procedures.	◆ Communication channels and networking events for members to receive analysis ◆ Access to capabilities that provide searchable topic analysis for participants

6.4.1 INFORMATION ANALYSIS

Successful information sharing and analysis depends on the production of actionable intelligence and the likelihood that threat information will be in one place and accessible to participating analysts. The purpose of information analysis is to learn and understand data, use its context with other data to produce information that encourages action to improve systems, people and corporations. Information sharing and information analysis interdependence combined with data collection and an ISAO’s scope and capabilities creates the framework for delivering intelligence to decision makers as shown in the figure below.

Figure 4 Framework for delivering intelligence



The act of information analysis involves reviewing data for signs or indications of malicious activity. The findings from the review can identify artifacts or evidence that analysts use to link with similar threat data to define threat groups or campaigns. Information Sharing and Analysis Organizations work to bring together data from multiple sources to engage the expertise of its participants for producing actionable intelligence. This section describes information analysis and the application of information analysis.

Information analysis involves operational learning and this section deconstructs into this into two stages. The first stage is the initial review of shared data. For example, an ISAO may offer their expert analysts to assess shared data to identify related threats. In the second stage, analysts interpret relevant threat data to produce threat group, campaign summaries, or business risk assessments. The ISAO could include a service to use their knowledge and experience to improve the coherence and relevance of the threat data to produce reports for decision makers to improve network security or adjust IT security roadmaps.

Information analysis has inherent challenges. First among them is identifying relevant data amongst streams of data feeds and data lakes. ISAO members may need assistance with data comprehension, its relevance to other data, and its coherence to similar data. The application of information analysis with the use interpretation models may address these challenges. A list of interpretation models and examples is shown below. The list is separated into two sections: first and second stage. The first stage applies to finding relevant threat data and the second stage shares examples of how to improve data context.

- First Stage
    - Order Estimation is the estimate of a variable whose precise value is unknown. For example, a malware reverse engineer may develop calculations (the estimate) to triage a large binary data set to identify a subset of binaries with possible malicious code (the unknown).
    - False positives and false negatives are concepts in statistical testing. False positives and false negatives in information analysis often relates to host and network based signatures and the quality of detection. A false positive indicates threat detection when actually there was no threat. A false negative may occur when a threat scan failed while it was successful.

- Second Stage
    - Second-order and higher-order logic—This logic reasons that a set of relevant threat data can be identified with properties that also define each data point. For example, analysts could take indicators of compromise and develop parameters to create sets of indicators of compromise to describe a campaign, threat activity, or threat groups.
    - Confidence Interval—Analyst may use estimations based on their observations to describe confidence within unknown data sets. Level of confidence is subjective and set by the analyst. The analyst's assessment should be complimented with the data significance. Significance may be based on the parameters defined by second-order logic.
    - Bayes' Theorem—"Describes the probability of an event, based on conditions that might be related to the event. For example, suppose a threat researcher is interested in whether a threat actor uses a specific command and control binary, and knows the threat actor's spear phishing tactic. If the binary is related to the spear phishing tactic, then, using Bayes' theorem, information about the spear phishing tactic can be used to more accurately assess the probability that the threat actor used the command and control binary."

The above models aid analysts in their effort to explain their assessment of threat information. For example, a threat group may refer to actors who work together to target and penetrate networks of interest. These individuals may share the same set of tasks, coordinate targets, and share tools. They work together to gain access to their targets and steal data. A group is defined by its actors and not solely by methodology. Distinguishing one threat group from another is possible with enough information and analytical experience.

Analysts ultimately communicate their assessments to decision makers. Common communication report types are alerts, notifications or assessments. ISAOs may need to survey their members to determine the content format that works best for its decision makers. The following list suggests content for information analysis reporting:

- Impact of threats to core corporate functions
- Describe threat activity relative to an attack life cycle
- Pro-active (assessments) and reactive reporting (post-mortem to an incident)

An ISAO offering information analysis services should be capable of storing data from varied data sources (both privileged and public) and experienced in data review, threat interpretation, and development of intelligence assessments.

6.4.2 TREND AND PATTERN ANALYSIS

After determining the collected data points, how data will be accessed and securely stored the ISAO can consider their analytic approach and the types of reports available to their members. ISAO members may have different appetites for intelligence consumption. For example, an ISAO focused on security or network operations may desire information that filters relevant data from network noise. Another ISAO may choose to engage on comparable threat activity. An ISAO should consider a survey of their members to understand what type of reporting is most useful and what each member is willing to contribute to the aggregate collection.

Analysis involves interpretation and learning based on all available data sources. The analytical options for an ISAO includes detection of first-seen or anomalous activity, identification of an exploit to a software or network vulnerability, collecting of related threat activity, or attribution to an individual, criminal enterprise, or nation-state. ISAOs considering analytical services could consider data stores to enable trend and pattern analysis and facilitate member communication about threats. For example, a threat knowledge base consisting of indicators for detection, threat information for response, and attribution for risk management. This threat knowledge base enables the ISAO and its participants to use analytic methods and share their knowledge and assessments.

Analyst assessment help to better understand relevant threat information however the analyst’s environment or visibility may introduce bias when categorizing threat or attributing threat activity to an actor. A threat intelligence sharing community creates a culture that reduces analyst bias and provides continuous feedback through detection, peer communication, and external confirmation.

Prior to doing analysis, ISAOs may want to begin by helping their members take data quality measurements. The validity of trend and pattern analysis relies on accurate and relevant inputs.

While all members must agree on what to share, a number of common reports have been useful in the past, which they might want to create:

- Pivot reports—Observed IP addresses that show connecting hop points. Members can utilize these reports to identify areas of common concern.
- Malware—An ISAO could collect the hash values of malware that the members see on their networks each month.
- Campaigns—ISAO members may want to share information on a given campaign, such as ransomware or business email compromise. They can share observed TTPs used by the actors.

Anonymous member surveys may be a reporting method ISAOs may want to utilize to do trends. A collaborative tool can be used to collect aggregated metrics from companies on a monthly basis that cover observables such as number of phishing attempts, intrusion attempts, successful intrusions, intrusions with data theft, accounts compromised, distributed denial of service attacks, etc. The ISAO can then create a trend report for its members which can use attributes about members without specifying the member name. For example, the ISAO weekly or monthly report could identify attack types by size of the business, the sector, time of day the activity occurred during, the IP and the country of origin of the attacker (if known), vector used, etc.

If member companies agree, an ISAO may want to utilize sensors on member networks that look at IDS logs and report attributes back to a secure shared database managed by the ISAOs, to which all members have access for generating reports and alerts.

ISAOs should also consider using a common vocabulary for reporting cyber activity, which can be aggregated across ISAOs and, if they choose, with government agencies. STIX is an example of a commonly used structured expression for tracking cyber activity. A number of companies and information sharing analytic centers utilize STIX and TAXII servers for information exchange and reporting. The Industrial Control Systems ISAC (ICS-ISAC) is one such example. Examples of reporting using STIX can be found on Github.

As ISAOs mature and aggregate data, they can look at creating baselines of normal behavior and doing predictive analytics that will identify anomalies and indicators of future actions.

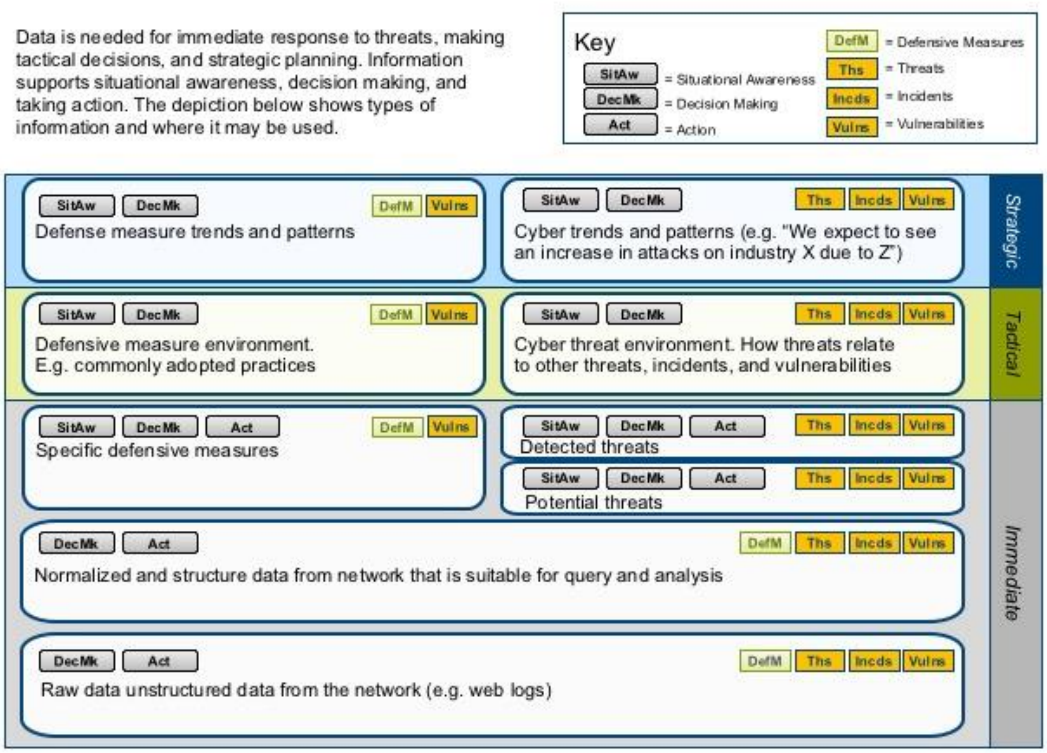
6.4.3 APPLYING SHARED INFORMATION

Specific types of information—namely, regarding threats, vulnerabilities, and incidents—can support the framework and an organization’s efforts to manage and mitigate its cybersecurity-related risks.

Figure 5 depicts at a high level where specific types of information can be used. The depiction seeks to show the hierarchy of information and how progressive levels of analysis can turn raw, unstructured data into valuable knowledge of the environment. Armed with this knowledge, organizations can then prioritize efforts to defend against the most prevalent threats. As discussed previously, the categories of information are:

- **Immediate**—Information needs that concern actions to defend against or respond to new threats, vulnerabilities, or incidents.
- **Tactical**—Information needs that concern decisions on how to best deploy an organization’s existing resources against the change in situational awareness.
- **Strategic—**Information needs that concern making plans and decisions on the efforts and resources needed to address emerging or future threat environments.

Figure 5. Applying Information to Cybersecurity Risks


Data is needed for immediate response to threats, making tactical decisions, and strategic planning. Information supports situational awareness, decision making, and taking action. The depiction below shows types of information and where it may be used.
Key
SitAw = Situational Awareness
DecMk = Decision Making
Act = Action
DefM = Defensive Measures
Ths = Threats
Incds = Incidents
Vulns = Vulnerabilities
SitAw DecMk DefM Vulns
Defense measure trends and patterns
SitAw DecMk Ths Incds Vulns
Cyber trends and patterns (e.g. "We expect to see an increase in attacks on industry X due to Z")
Strategic
SitAw DecMk DefM Vulns
Defensive measure environment. E.g. commonly adopted practices
SitAw DecMk Ths Incds Vulns
Cyber threat environment. How threats relate to other threats, incidents, and vulnerabilities
Tactical
SitAw DecMk Act DefM Vulns
Specific defensive measures
SitAw DecMk Act Ths Incds Vulns
Detected threats
SitAw DecMk Act Ths Incds Vulns
Potential threats
DecMk Act DefM Ths Incds Vulns
Normalized and structure data from network that is suitable for query and analysis
DecMk Act DefM Ths Incds Vulns
Raw data unstructured data from the network (e.g. web logs)
Immediate

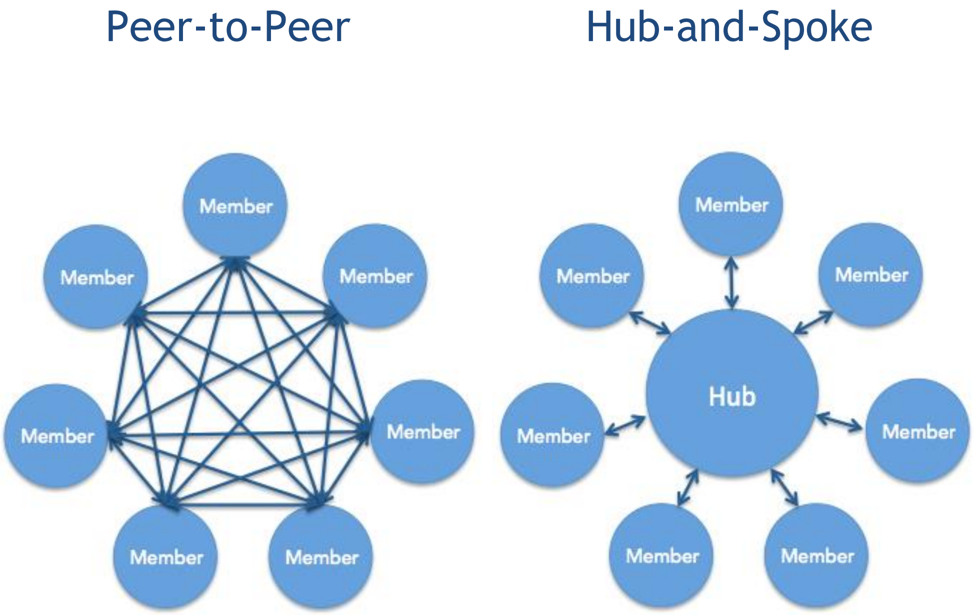
7 ARCHITECTURAL CONSIDERATIONS

People share information in many ways, but there is a tendency toward a few basic models commonly used among ISAOs. This section details two common sharing models that ISAOs may consider adopting. They are driven primarily by the role of an information "authority" and can be blended into hybrid approaches. This section also details several methods that can be applied to either of the models. Sharing methods are largely directed by community requirements and concepts of operations, and are also tied to how the tools and technology adopted by an ISAO enable certain kinds of sharing. Finally, this section introduces some popular sharing mechanisms that can be considered for adoption when establishing or further developing an ISAO.

These are nothing more than concepts and practices that have been used successfully by ISAOs, and that may serve as guidance for a community interested in forming a new ISAO. Ultimately, how models, methods, and mechanisms are implemented will vary widely based upon ISAO member needs, administrator capabilities, community goals, available technology, and the centers and dynamics of trust in a community. ISAOs are encouraged to consider what models and mechanisms could be a good fit for the context in which each operates, but they are equally encouraged to refine, adapt, and expand them to best meet the ISAO's needs.

7.1 GENERALIZED ARCHITECTURES

Peer-to-peer and hub-and-spoke sharing models may be the most useful basic arrangements that new ISAOs may consider when getting established.



7.1.1 PEER-TO-PEER

The peer-to-peer sharing model is defined generally by the ability of any member of a community to interact and share with any other member. Peer-to-peer networks can be especially beneficial for smaller communities or when members only interact with a part of a community. They may also be especially beneficial for those whose members have asymmetrical trust relationships or share under highly dynamic conditions that often change based upon content, current threat, etc. Members generally have a high degree of choice when determining with whom they share in the community. In this model, there is no “gatekeeper” governing event-by-event sharing, and how and what sharing occurs. That is not to say that an authority (ISAO administration, for example) does not create or enforce a sharing policy, or perform other authoritative duties. Instead, members of the community generally share when, what, and with whom they see fit, based upon established ISAO policy and procedures and within the confines of the tools used.

A challenge with this model is the potential difficulty managing many trust relationships when community membership grows. In addition, redundant sharing of the same information may be more likely in this model, and may lead to inefficient “churn” depending upon ISAO technology and other conditions.

7.1.2 HUB AND SPOKE

Generally, the hub-and-spoke sharing model incorporates a “gatekeeper” at the center, or hub, of the community. Members share through the hub while some combination of people, process, and technology drive redistribution out to the rest of the community. This sharing model provides opportunities to centralize, formalize, or otherwise influence information exchange for the benefit of the community. This may take the form of ISAO administration funneling and vetting widely disparate member and vendor threat intelligence, offloading threat analysis services from the membership to achieve economies of scale, enforcing policy, or simply playing a more central and visible role in the day-to-day activities of the ISAO. In addition, the hub is a logical place for a single “ground truth” to exist for the community, whether that has to do with policies and procedure, a current or official take on recent incidents or campaigns, or other areas relevant to the ISAO.

There are a few challenges to consider with this model. Dependency on the hub could lead to problems if the hub is not performing as strongly as it should. A high degree of trust should exist in the people, process, and technology at the hub in order for this sharing model to succeed. And regardless of the level of trust in the hub, members will always have varying degrees of trust relationships elsewhere among ISAO membership. Always funneling threat data or cyber (common) threat Indicators (CTIs) through the hub could inhibit the growth of personal relationships among ISAO members. Relationship building will lead to trust among the membership, and trust is arguably the primary key performance indicator for successful threat intelligence sharing.

7.1.3 HYBRID APPROACH

An ISAO can address some of the challenges of the peer-to-peer and hub-and-spoke models by forming a hybrid approach that combines elements of both. This could take virtually limitless forms, but the following are some possibilities:

- Channel some kinds of threat intelligence through the hub for redistribution, based upon hub strengths and core competencies. Budget, people, technology, or geography, and how these factors articulate with member requirements and objectives could all help determine what obligations and tasks are a good fit for the hub.
- Leverage peer-to-peer sharing for certain kinds of intelligence, such as strategic intelligence. Peers working together to build a threat actor profile, for example, is a great way to leverage community resources, build relationships and trust among ISAO membership, and make a positive contribution back to the ISAO community. And the work product could be re-distributed through the ISAO hub, combining aspects of both peer-to-peer and hub-and-spoke models.

These sharing models are high-level conceptualizations of how an ISAO can share information. When a newly forming ISAO has a good sense of what it wants to do, the kinds of sharing methods and mechanisms that it employs will be paramount to getting things done.

7.2 SHARING METHODS

7.2.1 PUBLISH–SUBSCRIBE

A publish-subscribe method for sharing threat intelligence consists of a producer who publishes information on a regular or irregular basis, and whose publications are individually subscribed to by one or more community members. This approach can be applied in either the peer-to-peer or the hub-and-spoke sharing models. In the case of a peer-to-peer network, a producer could, for example, automate CTI sharing into a repository from which other members pull feeds, or a producer can post to a message board/forum and subscribers can receive alerts. In the case of the hub-and-spoke model, the publisher may be the ISAO hub and the producers (members) could submit to the hub for processing—usually to verify, refine, de-dupe, or correlate with other known threat intelligence—before publishing it out to the ISAO subscriber base. The precise role of the hub can vary widely, depending upon ISAO CONOPS and other conditions. One of the benefits of the publish-subscribe method in a hub-and-spoke model is the ability for the ISAO to communicate a “ground truth” on an issue, incident, or actor—something very useful when many passionate voices are saying slightly different things in a rapidly evolving environment, which may create misunderstanding or confusion.

7.2.2 CROWDSOURCING

Crowdsourcing for threat intelligence says as much about the generation of CTI as how it is shared. ISAO members collectively contribute to a discussion thread, an automated threat sharing repository, or other system to organically transform granular threat data into more coherent threat intelligence. By virtue of participating in crowdsourcing the intelligence picture, the information is also shared with members. Like the publish-subscribe method above, crowdsourcing can take place in both peer-to-peer and hub-and-spoke networks—the key distinction being the presence of a central party directing the crowdsourcing through the hub, versus true organic freewheeling among the community. Both, of course, can be very effective. One of the benefits of crowdsourcing is that the virtual social interactions among ISAO members help to build trust and community.

These are two common sharing methods that are closely tied to the tools and technology an ISAO uses to support its CONOPS. New ISAOs can seek certain tools to enable sharing methods that it already believes will be effective. Alternatively, the tools it already uses may determine what sharing methods are at its disposal.

7.3 SHARING MECHANISMS

A variety of mechanisms and practices can be used to share information among an ISAO's members and partners. The table presented in this section can provide guidance for new or existing ISAOs considering initial or additional mechanisms and practices. The mechanisms and practices selected will need to be tailored to the scope, timeliness, and sensitivity of the information to be shared.

Information sharing can occur one-to-one, one-to-many, many-to-many, and many-to-one. As a result, practices an ISAO selects for communication and sharing information must reflect the overall objectives an ISAO is seeking to achieve for its members.

Due to the sensitivity of some information, methods and mechanisms use to share information must be capable, in accordance with an ISAO's policies or other authoritative restrictions, to protect and provide information to authorized members. ISAO that use a Traffic Light Protocol (TLP) to handle and distribute sensitive information will need to use mechanisms that have capabilities to comply with their TLP policy.

If anonymity of sources of information is required, additional information sharing processes, procedures, and features will be required. For that reason, the practices selected by an ISAO and its operational procedures will need to provide the operational, security, and management features necessary to meet the ISAO members' objectives.

Information sharing mechanisms should also be selected with consideration for the importance, timeliness, and criticality of receipt of information by ISAO participants. Members should be able to authenticate and trust that the information comes from expected sources. In some cases, positive confirmation of receipt of information may be required to ensure delivery of time-sensitive information.

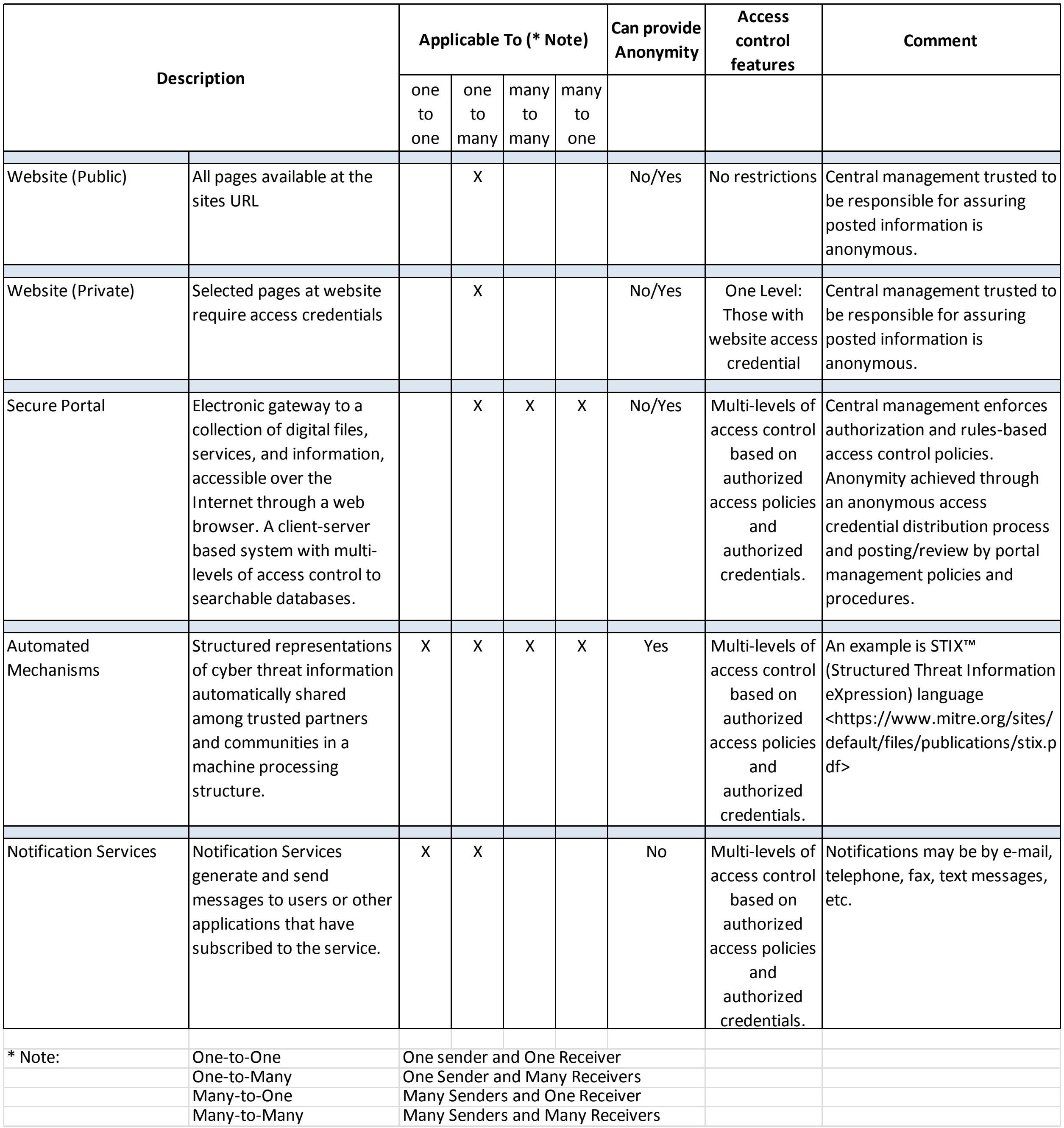
Effective ways of sharing information among ISAOs can include, based on member and customer needs, the following:

- Automated (primary indicator and defensive measures, then follow-on information)
- Direct feeds from threat intelligence firms
- Automated information sharing platforms
- Chat and social media platforms.

Table 2 below lists a number of mechanisms to consider.

Table 2. Sharing Mechanisms To Consider

The mechanisms listed below provide general guidance on various options and their applicability:								
Description		**Applicable To (* Note)**				**Can provide Anonymity**	**Access control features**	**Comment**
		one to one	one to many	many to many	many to one			
In persons meetings	Individuals physically meet with participation restricted to authorized individuals.		X	X		No	One Level: All authorized receive the information.	Access control to information can be restricted to a selected participating community through procedures.
Tele-conferencing/WebEx, etc.	Commercial conferencing and collaboration services		X	X		No/Yes	One Level: All authorized receive the information.	A central management function required to achieve anonymity but in general not anonymous. Access control to information can be restricted to a selected participating community through procedures.
Email (general)	Internet-based email	X	X	X	X	No/Yes	Distribution can be restricted	A central management function required to achieve anonymity but in general not anonymous. Distribution restrictions possible but difficult to manage for a large number of participants.
Email (wirh encrypted message)	Encrypted file or message	X	X			No/Yes	Access to information based on	Use of end-to-end encryption mechanisms, e.g. SMIME, PGP, etc.
Email - Listservers	Services for managing email lists		X	X		No/Yes	Distribution can be restricted	A central management function required to achieve anonymity but in general not anonymous.
Messaging Services (Short, Enhanced and Multi-media)	Carrier and vendor based services	X	X			No	Distribution can be restricted	Examples, Slack, HipChat, etc. Challenge-reply authentication can prevent spoofing.
Peer-to-Peer Networks	Characterized as a server-less network.			X		No	Distribution can be restricted	Security policies should be implemented to define what types of P2P software is acceptable and what information can be shared through them due to various risks.



Description		Applicable To (* Note)				Can provide Anonymity	Access control features	Comment
		one to one	one to many	many to many	many to one			
Website (Public)	All pages available at the sites URL		X			No/Yes	No restrictions	Central management trusted to be responsible for assuring posted information is anonymous.
Website (Private)	Selected pages at website require access credentials		X			No/Yes	One Level: Those with website access credential	Central management trusted to be responsible for assuring posted information is anonymous.
Secure Portal	Electronic gateway to a collection of digital files, services, and information, accessible over the Internet through a web browser. A client-server based system with multi-levels of access control to searchable databases.		X	X	X	No/Yes	Multi-levels of access control based on authorized access policies and authorized credentials.	Central management enforces authorization and rules-based access control policies. Anonymity achieved through an anonymous access credential distribution process and posting/review by portal management policies and procedures.
Automated Mechanisms	Structured representations of cyber threat information automatically shared among trusted partners and communities in a machine processing structure.	X	X	X	X	Yes	Multi-levels of access control based on authorized access policies and authorized credentials.	An example is STIX™ (Structured Threat Information eXpression) language <https://www.mitre.org/sites/default/files/publications/stix.pdf>
Notification Services	Notification Services generate and send messages to users or other applications that have subscribed to the service.	X	X			No	Multi-levels of access control based on authorized access policies and authorized credentials.	Notifications may be by e-mail, telephone, fax, text messages, etc.
* Note:	One-to-One	One sender and One Receiver						
	One-to-Many	One Sender and Many Receivers						
	Many-to-One	Many Senders and One Receiver						
	Many-to-Many	Many Senders and Many Receivers						

8 OPERATIONAL SECURITY CONSIDERATIONS

The trusted relationships essential to an effective ISAO must embrace a culture of operational security among its members, partners, and those with whom they share information. This culture is enabled through well designed ISAO operational policies, procedures, awareness, and good practices.

An ISAO's operational security efforts should include the following considerations:

- Establishing the criteria and vetting process for those eligible to participate in the ISAO.
- Examining the full range of the sensitive information an ISAO will be handling and communicating, and then using a risk-based assessment to develop the ISAO's operating rules,[8] information policies, and controls to be implemented across the ISAO and for members when interacting with the ISAO.
- Defining policies that address any identification of membership, the ownership of the information shared with the ISAO, the use of the information shared, the sharing of information among members and with others, along with any analytic product developed by the ISAO. To implement these policies, the agreed upon controls and practices to be exercised by members shall be documented and be a condition for participation in the ISAO.
- Specifying how information is to be provided the ISAO and members along with any review processes that may be implemented to protect the confidentiality and privacy of the content.
- Since information often has value when it is shared in a timely manner, establishing procedures for expediting and prioritizing information to be shared.
- Defining the labelling and handling procedures for the range of sensitive information to be handled within the ISAO and among members. Implementing the Traffic Light Protocol[9] approach used by ISACs and others for these purposes should be considered.
- Specifying procedures and practices where anonymity of information sources will enhance the sharing and trust among members and maintaining them in the operations of the ISAO. In practice there will be times when the owner of the information can decide that anonymity is not necessary or practical, and procedures should accommodate an information owner's prerogative.
- The responsible leadership/management of an ISAO shall ensure there is an active and periodic awareness effort to keep members informed of the expected code of conduct and their responsibilities in accordance with the ISAO's policies, procedures, and practices for the sharing and interactions

[8] As an example, the "Operating Rules" of the FS-ISAC are available at https://www.fsisac.com/sites/default/files/FS-ISAC_OperatingRules_2015.pdf

[9] https://www.us-cert.gov/tlp

among and with members. Any changes made should be fully vetted with and promulgated to participants.

- Developing specific operating rules for automation capabilities for real-time or near-real time information sharing, if used by the ISAO, because of the critical impacts (both positive and negative) such capabilities can have on an ISAO or those participating in the automated sharing of information.
- Establishing procedures and criteria for removing members who violate the trust and agreements of the ISAO; ensuring that organizations which assign personnel to be a member of an ISAO notify the ISAO of any changes in their assigned personnel status; ensuring that access authorizations are periodically reviewed and procedures are in place for removing access authorizations that are no longer valid.
- For ISAOs directly employing active measures against those attempting to compromise or exploit systems, establishing and thoroughly examining their operations security measures to avoid tipping off exploiters.

These operational considerations only highlight general aspects that ISAOs should establish, and their specific operational security policies and procedures must address their specific operations and the sensitivity of information being handled. ISAO operations will change over time, and periodic review of operational security procedures and policies may require updates. Annual reviews can be an effective check to ensure that they are up to date.

9 INFORMATION PRIVACY

It is important for ISAOs that receive, analyze, retain, use, or disseminate cyber threat indicators or other information through a voluntary cybersecurity information sharing process to be sensitive to and protective of privacy considerations. This includes the privacy of the individual members of an organization, any individuals concerning whom data may be available or provided, and a full range of other constituencies, customers, and individuals. To protect privacy while accomplishing the goals of an ISAO, it is important for the ISAO to provide guidance to members, participants, and ISAO staff on how to balance the goals of sharing information with protecting privacy. The purpose of this section is to help ISAOs attain that balance.

Before sharing cyber threat indicators, the privacy implications of what is being shared must be considered, including:

- whether information not directly related to cybersecurity threats or the purposes for which the information may be shared is included;
- whether information is included that the ISAO knows to be personal information about a specific individual or that identifies a specific individual; and
- whether the ISAO staff or members have made efforts to identify and assess any such information.

Given the nature of a cyber threat indicator, oftentimes an individual whose personal information is directly related to a cybersecurity threat does not have the opportunity to consent to involvement in the process used to collect that information, or access or correct that information. ISAOs must limit the impact of the data they collect on individual privacy.

Sensitive information such as personally identifiable information (PII), intellectual property, and trade secrets may be encountered when handling cyber threat information. The improper disclosure of such information could cause harm. Accordingly, organizations should implement the necessary security and privacy controls and handling procedures to protect this information from unauthorized disclosure or modification.

Often data requires protection, either by law, regulation, or contractual obligation. This includes PII and other sensitive information afforded protection under the Sarbanes-Oxley Act, the Payment Card Industry Data Security Standard, the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Modernization Act of 2014, the Gramm-Leach-Bliley Act, and Health Information Technology for Economic and Clinical Health (HITECH) Act, among others. It is important for ISAOs to identify and appropriately protect such information. ISAOs should consult legal, privacy, and data experts familiar with the various regulatory frameworks when developing procedures for identifying and protecting sensitive information to ensure compliance with all existing privacy regulatory and legal requirements at the federal, state, local, and international level.

As noted above, ISAOs should limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information about specific individuals or information that identifies specific individuals.

9.1 CORE PRINCIPLES

- ISAO members are encouraged to identify and contribute indicators that are critical to identifying threats, make efforts to minimize the PII shared with the ISAO or other members, and ensure compliance with all existing privacy regulatory and legal requirements at the federal, state, local, and international level.
- If a member inadvertently submits PII to an ISAO, the member should understand how to notify the ISAO.
- ISAOs may want to develop policies and procedures that provide for the timely destruction or return of cyber threat indicators containing personal information about specific individuals or information that identifies specific individuals.
- ISAOs are encouraged to consider providing information to members regarding with whom they intend to share or may share information, such has whether they may share with the government, and notice of any material changes in policy or practice. An ISAO should also seriously consider, after obtaining any legal advice

it may need, disclosing to its members whether it seeks to operate within the confines of the Cybersecurity Information Sharing Act of 2015 (CISA) in order to obtain liability protection and how it may do so, including the potential risks and implications of that choice for privacy and other matters.

9.2 SUPPORTING PRINCIPLES

For example, DHS has issued guidance related to privacy issues when sharing within industry. That guidance is important for attaining liability protections under U.S. law and is referenced here and in Appendix A.[10] It is important that ISAOs and their participants and member organizations are familiar with applicable privacy law and policy and incorporate appropriate commitments and policy provisions into member rules, foundational documents, and user agreements.

ISAOs may want to consider designating responsibility and authority to a staff member, board member, or outside party (such as a contractor or attorney) for ensuring compliance with applicable state and other privacy laws privacy laws and taking action if such issues arise,

Segmentation, a process for identifying certain data fields that may require special handling of sensitive personal information, is important to ISAOs when developing cyber threat indicators. Segmentation may include a process for identifying certain data fields that could require some review, either always or by sampling (and the sampling could be by field, by item, a combination, or otherwise); a procedure for returning, deleting, or otherwise minimizing PII; and a way to counsel or advise members, if any, who frequently handle PII with less than the necessary care. If information to be shared is not always subjected to a privacy review by the ISAO, it may want to consult with legal experts to identify whether there are any implications for liability or the availability of liability protection.

When sharing automated indicators with DHS, ISAOs may be required to adhere to various practices and agreements, including the DHS Automated Information Sharing (AIS) Terms.[11]

Certain DHS requirements of note are included in the Terms of Use:

- Section 3.2 states that “An AIS Producer shall use reasonable efforts to ensure that any Indicator or Defensive measure shared is accurate at the time that it is supplied. Further, the AIS Producer will associate any Indicators or Defensive Measures it produces with the appropriate Information Handling Level as defined by the NCCIC [National Cybersecurity and Communications Integration Center].”
- Section 3.3 states that “Each AIS Producer will use reasonable efforts to remove from any Indicators or Defensive Measures provided to the NCCIC any information not directly related to a cybersecurity threat that the AIS Producer

[10] https://www.us-cert.gov/ais

[11] https://www.us-cert.gov/sites/default/files/ais_files/AIS_Terms_of_Use.pdf

knows at the time of sharing to be personal information that identifies a specific individual."

- Section 3.4 states that "Each AIS Producer agrees that, in the event it discloses Indicators or Defensive Measures by mistake, in error, or without their appropriate Information Handling Level (through mismarking or a failure to mark), it shall promptly notify the NCCIC and take all reasonable steps to mitigate, including sending a versioning update, as soon as it is able."

When engaging with international partners or sharing information across national borders, ISAOs and their members should be aware that international privacy laws may differ from U.S. federal, state, or local laws. For example, depending on membership and circumstances, ISAOs should seek to understand what information, if shared, might need to be compliant with U.S.-European Union (EU) agreements like Privacy Shield, the EU General Data Protection Regulation (GDPR), and the Network and Information Security Directive.

If an ISAO decides to share threat indicators or defensive measures with the NCCIC or other government partners—particularly if it intends to secure the legal protections available under CISA—it must become familiar (with the help of legal counsel, if needed) with the privacy guidance available from the DHS, the Department of Justice, and other agencies regarding information sharing and the requirements of CISA for securing liability protection. Depending on the sharing in which it may engage, it should implement that guidance in connection with its processes and procedures. It must do so if it is sharing with the federal government and seeking the full scope of protections available under CISA, and may consider doing so for sharing that is only within industry. That guidance is intended to help protect privacy and to provide a path to secure such legal protection for sharing as may be available under CISA, whether sharing with the federal government through the NCCIC or sharing only in the private sector. Liability protection under CISA may require the sharing party to conduct some privacy scrub in accordance with the statute.

See, for example, Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015, including at p. 14 and Annex 1: Sharing of Cyber Threat Indicator and Defensive Measure Sharing between Non-Governmental Entities under CISA, June 15, 2016.[12]

The guidance also provides examples of certain personally identifiable information that can be part of a threat indicator and be shared, including particular IP addresses in certain circumstances and also gives examples of personal or other information that should not be shared and of impermissible uses of shared information.

[12] https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf

The following are additional examples of actions an ISAO may wish to consider and address in processes and procedures developed to guide its functions:

- Socialize the processes, procedures, plans, and exercises to make sure ISAO managers know what to do and respond appropriately if the ISAO receives PII that it possibly should not have received.
- Review various guidance on privacy considerations, such as the privacy section in the NIST Framework for Improving Critical Infrastructure Cybersecurity and determine which of those recommended actions are relevant to their operations.
- Identify the safeguards necessary at all stages of the PII lifecycle within the organization and proportionate to the sensitivity of the PII to protect against loss, theft, unauthorized access or acquisition, disclosure, copying, use, or modification.
- Identify the processes and procedures necessary to securely dispose of, de-identify, or anonymize PII that is no longer needed.
- Identify the processes to ensure that access to databases containing PII is audited. Log PII as part of an independent audit function, and determine how such PII could be minimized while still implementing the cybersecurity activity effectively.
- Evaluate the DHS profile for the AIS portal, including any privacy requirements.
- Determine whether a minimum information exchange process is needed to minimize information shared to only the data necessary to address the threats the ISAO is intending to cover.
- Consider developing a preventive plan for data protection, including both systems and human elements, and an equally clear remedial plan in the event of a breach.
- Develop an encryption policy that meets the needs and expectations of employees, customers, and counterparts.
- Determine their core membership and audience, and build in security and privacy requirements that match the maturity levels commensurate with their membership, recognizing that not all entities or participants receiving information have equal capabilities or equal privacy concerns.
- Adopt privacy and security controls that match the capabilities of their members and the criticality of the information shared. This means, for example, that sharing threats via email or a phone call to specifically identified recipients may have less impact than disseminating information to members broadly through a portal. Therefore, depending upon the tools an ISAO is implementing, the security and privacy requirements will vary.

- Establishing clear policy and procedures for data retention and disposition.

10 INFORMATION SECURITY

ISAOs will vary in size, sophistication, and abilities. ISAOs will also vary in the types of information they share. However, all ISAOs, no matter how established or new, face common security challenges. By considering these security issues as the ISAO is formed and baking security considerations into an ISAOs business process at the beginning, ISAOs and their members will be more effective in building trust among the members, between the members and the ISAO. Further, ensuring security issues are addressed provides assurances to members that their information is secure and, therefore, increases the likelihood of them sharing information.

Security policies can reflect the various types of information being shared, the different degree of sensitivity of that information, and how the information is shared. For example, a security policy related to sharing automated indicators likely will be different from a security policy related to sharing PDF documents. Similarly, the policy for storing open-source news might differ from the policy for storing sensitive member submissions.

An ISAO's membership may also drive the levels of security needed. ISAOs whose members have robust security capabilities themselves will likely have more robust security procedures than ISAOs whose members have less advanced capabilities. Regardless, however, whether the organization is for-profit or non-profit, large or small, security is an important component of an ISAO's success.

CISA outlines procedures for private-sector entities to follow when sharing cyber threat indicators and defensive measures with the federal government. It also includes basic structures and security requirements that companies must meet to participate in the process with DHS. It defines strong privacy protections, which are also addressed in a companion document. Not all ISAOs will participate in the program, for a variety of reasons, but it is important to include reference to statutory requirements in this document for ISAOs that choose to participate in that program. ISAOs that choose to not participate might still benefit from an understanding of the security requirements of that program. DHS and the Department of Justice have issued CISA implementation guidance for the private sector.[13]

(NOTE: The following list of issues is a draft for discussion. It is not intended to be comprehensive but to provide a foundation throughout the ISAO public commenting process. Specific issues–including core privacy issues, the type of in-formation that could be shared, categories of information, and others–would be handled in companion groups in the Standards Organization process.)

[13] https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf.

10.1 CORE SECURITY SUGGESTIONS FOR ISAOs

10.1.1 BASIC SECURITY COMPONENTS FOR AN ISAO

SECURE WEB PORTAL FOR COMMUNICATIONS

When establishing an ISAO, and at periodic intervals thereafter, ISAO members may want to consider and discuss the minimum levels of security they require to perform the basic functions expected of their ISAO.

When establishing and ISAO, and at periodic intervals thereafter, ISAOs their members may want to discuss and decide on appropriate requirements for securing communications. Once the requirements are established, the ISAO can deploy the appropriate tools to meet those requirements.

When establishing an ISAO, members may want to understand the security levels and maturity of individual members. This will help ensure that policies are developed in a manner that is effective and appropriate for all members. Once an ISAO is formed and established, the ISAO may want to conduct a periodic review to ensure that its capabilities and policies are appropriate to member capabilities and requirements.

DHS has information sharing programs that have defined security requirements for how shared information needs to stored and handled. For example, the Cyber Information Sharing and Collaboration Program states specific requirements for how an organization must store information as part of that program. If ISAOs intend to participate in such programs, they should ensure that they establish security policies that meet these requirements.

PUBLIC KEY INFRASTRUCTURE (PKI) AND “SECURITY BY DESIGN”

Before building or buying a platform for information sharing, it is first worth understanding the basic security requirements that will be needed to facilitate information sharing among members. It is much easier and less expensive to build the security requirements into the system up front, than it is to add them on later.

This includes considering whether encryption is required and, if so, what level of encryption is appropriate.

As an example, policies could detail whether all members will use certificates for signing and authenticating emails in a PKI exchange mechanism, whether the ISAO will deploy two-factor authentication, and whether documents being shared would be encrypted separately from the PKI process.

ACCESS CONTROLS

Generally, a key component of security is access controls, which govern the fact that not everyone in an organization needs access to all of its documents. Therefore, it is appropriate that controls are in place so that people can only access documents they are authorized to access. It also is appropriate that the ISAOs and their members discuss and decide on appropriate access controls for individuals within member entities and ISAO staff.

Another component of access control is to revoke credentials for people if they change jobs within an organization or leave an organization completely. Thus it is appropriate for ISAOs and its members to agree on a common policy on how to ensure that credentials are revoked when a member or employee is no longer permitted access to information.

Another general security principle is that data should be federated based upon their criticality, and access controls may vary for different types of data. For example, it might be appropriate to allow the head of marketing access to an organization’s collection of open source news reports, but that person may not need access to sensitive indicators shared by members or partners.

CYBERSECURITY ATTACK AND DATA BREACH NOTIFICATION

To maintain a level of trust and dependability between and among members, ISAOs may want to consider establishing internal reporting plans and communication lines with companies in the event that they are a victim of a cybersecurity attack that impacts the ISAO and its members. It should be noted that ISAOs are subject to state and local data breach notification laws should the ISAOs be victims of a cyberattack that impacts PII an ISAO holds for ISAO employees, contractors, members, or partners.

10.1.2 DATA CLASSIFICATION, DISTRIBUTION, AND LABELING

Another general security principle is to appropriately mark and label information. This could include noting specific handling instructions for a particular document or marking it with a general classification. Such marking helps consumers understand how the information can be used and stored. ISAOs and their members can develop a classification scheme that fits their individual security policies. Further, generally a common practice is to enable the entity that owns the document to control how that information is shared. This concept is commonly known as “originator control.” The following are some examples of potential components to consider in a security policy:

- Using the Traffic Light Protocol (TLP) Red/Amber/Green or other classification schemes, which can help members understand how to share information according to data classification standards.
- Policies that detail how members can use indicators that are shared. For example, can they use those indicators to protect their customers or to only protect their specific network?
- Internal structures and policies that limit the risk of members sharing non security proprietary information.

- Determining whether the ISAO should establish multiple sharing groups or forums based that reflect the ability of its members to receive or store various levels of sensitive information.
- Issues for anonymizing member submissions, as well as establishing parameters for sharing when they want to use anonymization.
- Clear data retention and disposition policy and procedures.
  (NOTE: The current DHS AIS program has established data retention policies that are more specific.)
- Options for sharing information that may include automated intake and dissemination, email, and other methods.
- Policies that deal with verbal submissions by members.
- As an example, it would be helpful to consider distribution policies to set up rules for sharing data via email. Policies could cover matters such as:
  - When to utilize the blind copy email feature.
  - What information should be sent via encrypted email.
- Criteria for who has access to mailing lists and who can be on the mainlining list.
- When to use “reply all” structures.

10.1.3 ISAO MEMBER SECURITY

While security of the ISAO itself is important, trust is enhanced when members understand how other members will handle and store information that is being shared through and within the ISAO. Therefore, when creating and ISAO, members may want to consider and develop policies related to the security responsibilities of members companies. Some potential considerations include:

- Detailing, in a common member agreement or other document common to all members, what the responsibilities are of each member in securing information shared through the ISAO.
- Detailing what tools will be used for sharing information and the policies for granting members access to those tools.
- Establishing methods to communicate and/or train members on what their responsibilities are under the ISAO security policy.

It is important to note that these ISAO security policies are not a replacement for appropriate enterprise-wide cybersecurity practices of an ISAO member company. They also are not a replacement for any regulatory requirements or obligations ISAO member companies might be required to follow. ISAO members should take all appropriate steps to secure their enterprises. There are a myriad of guides to help ISAO members manage cyber risk, including the NIST Cybersecurity Framework. Instead, the point of an ISAO security policy is to detail member responsibilities specific to securing information they receive from or share with the ISAO.

10.1.4 GLOBAL SECURITY ISSUES

If ISAOs include global corporations, it is important for the ISAO to be aware of and discuss other existing requirements for companies involving information security, cybersecurity, privacy, and overall information sharing.

- If there are cross-border data transfers for information sharing, ISAOs should become familiar with any governing international requirements. For example, the United States is in the process of working with the EU on Privacy Shield, which includes information security, privacy, and other requirements. Other EU requirements that are important to be aware of include the EU GDPR and the EU Network and Information Security Directive.
- ISAOs should be aware of and integrate other regulatory requirements as needed for other countries around the world. In some instances these requirements extend to vendors and third parties, so ISAOs will need to be aware of and comply with these requirements.

11 ISAO STANDARDS ORGANIZATION SUPPORT

11.1 ASSISTING EMERGING ISAOs

The purpose of the Standards Organization’s support function is to assist emerging ISAOs as they implement and adopt processes that enhance their value toward and their coordination with one another.

Organizations have been seeking information and assistance for defining the value of and becoming ISAOs long before the ISAO SO was formed. The ISAO SO is assuming a broad responsibility for processes that began long before its existence, and that will not wait for it to develop and mature.

ISAO support can look at emerging organizations and existing ISAOs to identify processes and capabilities that are required to identify and establish meaningful relationships of support between them and the ISAO SO, and to help the ISAO SO translate their support requirements into efficient and sustainable organizational processes that the ISAO SO can review and adopt to meet the needs of its larger and growing constituency.

The following discussion outlines five key processes that ISAO support has identified and is researching and developing to support ISAO SO intake and sustained engagement with organizations and ISAOs relevant to its support mission. These process areas include intake, ISAO checklists, alignment, mentorship, and feedback. The deliverables and outcomes of ISAO support will provide an investment in the infrastructure that will hopefully support potential, emerging, or developing ISAOs for many years to come.

11.2 SUPPORT FUNCTIONS

ISAO support seeks to define and enhance the flow of the ISAO SO's post-outreach support efforts to organizations seeking its assistance. In doing so, support is initially focused on five basic functions associated with ISAO SO coordination: intake, ISAO checklists, alignment, mentorship, and feedback.

These functions are briefly defined as follows:

- **Intake**—The workflows and processes for the ISAO SO connecting with organizations seeking information about or assistance in forming an ISAO.
- **ISAO checklists**—The content and processes for identifying the data necessary to inform ISAO SO products, services, relevant standards, and relationships of value to a particular organization or ISAO in its intake process.
- **Alignment**—The activities and functions by which the ISAO SO and/or the organization seeking ISAO SO assistance may identify and connect with products, services, relevant standards, and relationships of value to their organizational development and maturity.
- **Mentorship**—The ISAO SO capability that allows organizations seeking ISAO SO assistance to identify, connect with, obtain support from, and to evaluate the effectiveness of organizations that have identified themselves as mentors for particular aspects of organizational development and maturity, and that have offered to make themselves available to support or assist the development of other organizations.
- **Feedback**—The content and processes for soliciting, capturing, and leveraging organizational input on ISAO SO products, services, relevant standards, and relationships as provided by organizations seeking ISAO SO assistance in order to assess their value to the ISAO user community and to enable organizations to continually refine them.

12 APPENDIX A REFERENCES

[Placeholder—reserved for primary reference sources]

13 APPENDIX B GLOSSARY

Selected terms used in the publication are defined below.

Alert: Timely information about current security issues, vulnerabilities, and exploits. [Source: US-CERT]

Analysis: A detailed examination of the elements or structure of cybersecurity information, in order to identify the applicability to increasing the security of an information system in some way.

Automated Cybersecurity Information Sharing: The exchange of data-related risks and practices relevant to increasing the security of an information system utilizing primarily machine programmed methods for receipt, analysis, dissemination, and integration.

Campaigns: In the context of cybersecurity, a campaign or attack via cyberspace that targets an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, destroying the integrity of the data, or stealing controlled information. [Source: NIST Glossary of Key Information Security Terms, NISTIR 7298 Revision 2]

Computer Security Incident: See “Incident.”

Computer Security Incident Response Team (CSIRT): A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).

Cyber Threat Information: Information (such as indications, tactics, techniques, procedures, behaviors, motives, adversaries, targets, vulnerabilities, courses of action, or warnings) regarding an adversary, its intentions, or actions against information technology or operational technology systems.

Cybersecurity Information: Data-related risks and practices relevant to increasing the security of an information system.

Cybersecurity Information Sharing: The exchange of data-related risks and practices relevant to increasing the security of an information system.

Cybersecurity Purpose: The purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

Cybersecurity Threat: An action on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. The term does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Cyber Threat Indicator: Information that is necessary to describe or identify—

- malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
- a method of defeating a security control or exploitation of a security vulnerability;
- a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
- a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
- malicious cyber command and control;
- the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; or
- any combination thereof.

Defensive Measure: An action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

Enriched Cybersecurity Information: Cybersecurity information that is combined with multiple different data sets/streams to produce a more comprehensive set of data.

Enhanced Cybersecurity Information: Cybersecurity information that is analyzed to identify trends, insights, or other understanding.

Event: Any observable occurrence in a network or system.

False Negative: An instance in which a security tool intended to detect a particular threat fails to do so.

False Positive: An instance in which a security tool incorrectly classifies benign content as malicious.

Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Incident Handling: The mitigation of violations of security policies and recommended practices.

Incident Report: A written summary of an incident that describes the steps in the investigation of the event, the findings, and the resolution.

Incident Response: See “Incident Handling.”

Indicator: An artifact or observable evidence that suggests that an adversary is preparing to attack, that an attack is currently underway, or that a compromise may have already occurred.

Information Life Cycle: The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition. [Source: Office of Management and Budget, Circular A-130]

Malware: A program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim’s data, applications, or operating system. [Source: NIST SP 800-83, Revision 1]

Malicious Cyber Command and Control: A method for unauthorized remote identification of, access to, or use of an information system or information that is stored on, processed by, or transiting an information system.

Malicious Reconnaissance: A method for actively probing or passively monitoring an information system for the purpose of discerning its security vulnerabilities, if such method is associated with a known or suspected cybersecurity threat.

Monitor: To acquire, identify, scan, or possess information that is stored on, processed by, or transiting an information system.

Operational Analysis: Examination of any combination of threats, vulnerabilities, incidents, or practices that results in methods to protect specific data, infrastructure, or functions (for example, incident analysis, identification of specific tactics, techniques, procedures, or threat actors, etc.)

Precursor: A sign that an attacker may be preparing to cause an incident.

Profiling: Measuring the characteristics of expected activity so that changes to it can be more easily identified.

Privacy Framework Catalog:

NIST Special Publication 800-53, Revision 4

Appendix J, *Privacy Control Catalog*, is a new addition to NIST Special Publication 800-53. It addresses the privacy needs of federal agencies. The Privacy Appendix outlines a structured set of privacy controls, based on best practices, that comply with applicable federal laws, Executive Orders, directives, instructions, regulations, policies, standards, and guidance. Additionally, it establishes a linkage and relationship between privacy and security controls for purposes of enforcing privacy and security requirements that may overlap in concept and in implementation within federal information systems, programs, and organizations.

HITRUST CSF (Healthcare)

The Health Information Trust Alliance, or HITRUST, formed in 2014 to integrate privacy requirements into the healthcare industry's Common Security Framework (CSF) security control standard, initially to support the SECURETexas covered entity privacy and security certification program, but with the intent to support the healthcare privacy community more broadly. Primarily based on the language in the HIPAA Privacy Act, the Working Group also integrated the privacy requirements specified in NIST SP 800-53 r4 Appendix J to support both civilian and federal government healthcare entities. HITRUST is also working with the Texas Health Services Authority and the Texas Medical Association to create a simplified information privacy and security program for smaller organizations, such as physician practices, that would adequately address HIPAA's standards and implementation specifications while providing the flexibility necessary for successful implementation and broad adoption across the industry.

American Institute of CPAs (AICPA)

The AICPA and the Canadian Institute of Chartered Accountants (CICA) have formed the AICPA/CICA Privacy Task Force, which has developed Generally Accepted Privacy Principles (GAPP). This document supersedes the AICPA and CICA Privacy Framework. Using GAPP, CPAs can help organizations design and implement sound privacy practices and policies. These principles and criteria were developed and updated by volunteers who considered both current international privacy regulatory requirements and best practices. These principles and criteria were issued following the due process procedures of both institutes, which included exposure for public comment. The adoption of these principles and criteria is voluntary.

Real-time information sharing: See "Automated Cybersecurity Information Sharing."

Secure Portal: A web-enabled resource that provides controlled secure access to and interactions with relevant information assets (information content, applications, and business processes) to selected audiences using web-based technologies in a personalized manner.

Security Control: The management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

Security Vulnerability: Any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

Signature: A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.

Situational Awareness: Comprehension of information about the current and developing security posture and risks, based on information gathered, observation, analysis, and knowledge or experience.

Social Engineering: An attempt to trick someone into revealing information (such as a password) that can be used to attack systems or networks.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. [Source: NIST SP 800-30, Revision 1]

Threat Actor: An individual or group involved in malicious cyber activity. [Source: MITRE, STIX]

Threat Source: The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability. [Source: NIST SP 800-30, Revision 1 and CNSSI No. 4009]

Trend Analysis: Examination of data to identify any combination of broad, non-obvious, or emerging actions (for example, threat actor campaigns and intent, common vulnerabilities and configurations exploited, merging operational analytics with non-like data streams such as assessments, etc.).

Vulnerability: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [Source: NIST SP 800-30, Revision 1]

14 APPENDIX C ACRONYMS

AIS	Automated Indicator Sharing
CERT	Computer Emergency Response Team
CISA	Cybersecurity Information Sharing Act
CONOPS	Concept of Operations
CTI	Cyber (Common) Threat Indicator
DHS	Department of Homeland Security
EO	Executive Order
EU	European Union
GDPR	General Data Protection Regulation (Directive 95/46/EC)
HIPAA	Health Information Privacy and Portability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
IT	Information Technology
LLC	Limited Liability Company
NCCIC	National Cybersecurity & Communications Integration Center
NIST	National Institute of Standards and Technology
PII	Personable Identifiable Information
SO	Standards Organization
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information
TLP	Traffic Light Protocol
TTP	Tactics, Techniques & Procedures