Building an ISAO Guidebook

The primary purpose of an information sharing and analysis organization (ISAO) is to establish a mechanism to enable public and/or private entities to collaborate to prevent, protect, mitigate, respond, and recover from cyber threats or attacks. Cyber events have the potential to devastate organizations in seconds which makes information sharing paramount to timely response. (Sjelin & White, 2017)

Building an ISAO requires thorough planning and coordination with stakeholders and members. While creating an ISAO is a complex process, the various components and processes can be synthesized into the following six steps:

- ☐ Step 1 - Define the organization
- ☐ Step 2 - Building trust, security, and privacy
- ☐ Step 3 - Establishing core offerings
- ☐ Step 4 - Implementing services and capabilities
- ☐ Step 5 - Establish partnerships
- ☐ Step 6 - Continuous improvement

Step 1 - Define the Organization

Determine the ISAO's Purpose

The purpose of defining scope is to identify the geographic area or domain the ISAO intends to cover.

- ☐ Define the type of ISAO being formed
  - Geographic
  - Sector Based
  - Special Interest
- ☐ What are the drivers for building the ISAO?
  - Community
  - Innovation
  - Directive/Legislation
- ☐ Who are the key players?
  - Stakeholders
  - Members based on location, sector, event, etc. What is the vetting process?
- ☐ Build the ISAO plan
  - Mission statement (Who are we, why do we exist, what do we value?)
  - Vision statement (What do we want to become)
  - Strategy (How do we achieve our vision?)
  - Goals (What do we want to achieve and how do we gauge our success?)
  - Objectives (How do we achieve our goals?)
  - Milestones (What major events or activities will show our progress?)

Overcoming the Gnarly Nine

The Gnarly Nine identifies strategic challenges every ISAO must overcome to be successful. Each of the Gnarly Nine challenges are addressed in this guidebook.

- ☐ Identify the ISAO's short, mid, and long-term goals. Short-term might be sharing cyber threat indicators and defensive measures. Mid-term - collaborative research and development. Long-term - engage in regional economic development.
- ☐ Implement milestones. Develop a high-level plan congruent with the ISAO mission including specific milestones.
- ☐ Determine what and how members will share information. Determine what information will be shared by whom and for what purposes.
- ☐ Establish a value proposition. Establish a value proposition that sets the ISAO apart to encourage potential members to commit resources, time, and effort. Determine what services the ISAO will provide for its members.
- ☐ Establish membership criteria and composition. Decide if membership will be based on location, sector, event, or type of threat. Will it be capped or unlimited? Is there a vetting process for membership?
- ☐ Create an ISAO members can trust to safeguard their sensitive information. Determine the appropriate controls or look for a trusted, independent, third party to manage operations. Create platforms and mechanisms for building trust among members, such as institutional and individual nondisclosure agreements.
- ☐ How does the ISAO fit into the local, regional, and global cyber ecosystem? Determine who has access, under what circumstances information can be shared or used outside the ISAO, and define the consequential obligations.
- ☐ Determine leadership and governance. Identify key stakeholders and their roles. Consider the benefits of organizing as a non-profit. Develop a plan for selecting a board of directors, creating committees, and for staffing.
- ☐ Establish a financial plan. How you address the other eight strategies will drive your financial plan. Explore seed funding and grants to get started. Determine fee structure for founding members and other membership categories to include sponsors.

Establishing a Membership Structure

The elements of an ISAO membership structure include criteria, agreements, recruitment, and model. Each of these elements are essential to growing a successful organization. Define and establish each of the following:

- ☐ Membership criteria are the rules and requirements organizations and/or individuals must fulfill to become members of the ISAO.
- ☐ What are the foundational requirements and how will they be monitored and enforced?
- ☐ Are there participation and engagement requirements?
- ☐ Does membership include organizations, individuals, or both?
- ☐ Membership agreements are the contracts between the ISAO and the users which outline expectations for all parties.
- ☐ Membership recruitment plans that communicate the value proposition and return on investment (ROI) received by joining the ISAO.
- ☐ Membership model refers to the tiers or levels of membership offered by the ISAO.

Selecting the Organizational Structure

The ISAO organizational structure determines how it will be managed and defines the core obligations to its members. Answer the following questions when selecting the structure:

- ☐ Will the ISAO be informal, formal, or an integrated entity?
- ☐ Will the ISAO be for-profit or nonprofit?
  - For-profit - Which business structure best suites your mission, vision, and goals?
  - Nonprofit - 501(c)(3) or 501(c)(6).
- ☐ How will the ISAO be funded? Grants, membership dues, organizational resources, etc.
- ☐ Which governance structure works best?

Governance and Legal Obligations

Building governance defines how the ISAO will be directed and overseen. Governance refers to the process of making decisions which define expectations, systems, and management. Consider the following when building governance:

- ☐ Select governing bodies. Choose one or more of the following: Board of Directors, Steering Committee, Collective Board, Policy Board, Board of Advisors, etc.
- ☐ Define the governance model including but not limited to structure, oversight responsibilities, culture, and infrastructure.
- ☐ Account for the eight major characteristics of good governance:
  - Rule of law
  - Transparency
  - Responsiveness
  - Consensus oriented
  - Equity and inclusiveness
  - Effectiveness and efficiency
  - Accountability
  - Participation

ISAOs have an obligation to uphold and abide by the laws of their governing jurisdictions. Legal obligations include the laws, rules, regulations, and practices guiding the ISAO. In consultation with appropriate legal counsel, review at least the following:

- ☐ GDPR
- ☐ PCI DSS
- ☐ ISO 27010
- ☐ CISA
- ☐ FISMA
- ☐ HIPAA

Business Model

The ISAO business model is a set of plans defining how the ISAO will operate. At a minimum, the plans should include:

- ☐ Marketing plan capturing marketing objectives, responsibilities, and activities designed to inform constituents and grow membership.

- ☐ Communications strategy is the "selection of appropriate communication objectives and the identification of specific ISAO awareness goals." (ISAO 100-2, 2016) The communication strategy should contain:
  - Clarity of purpose
  - Audience definition
  - Staff and stakeholder alignment
  - Effective use of resources
  - Measure success
- ☐ Financial plan defining and evaluating the assets, expenditures, and revenue to ensure the continued sustainability of the organization.
- ☐ Cost drivers are the services, skills, and technologies utilized by the ISAO that generate fixed or variable expenditures. Consider costs associated with:
  - Management and operations
  - Infrastructure and technology
  - Promotion
  - Member needs
  - Training and education
  - Office space
  - Financial management
  - Insurance

Step 2 - Building Trust, Security, and Privacy

Trust, privacy, and security are at the center of all ISAO services and capabilities. Without any of these three elements, an ISAO will likely fail. This step covers many of the best practices and recommendations on building trust, security, and privacy.

Building Trust

Trust is defined as a willingness to take risks in a relationship. The trust relationships are between members, the members and the ISAO, and the ISAO and its partners or customers.

- ☐ For all constituents, create and cultivate the ABCDs of trust.
  - Able - Demonstration of competence
  - Believable - Act with integrity
  - Connected - Genuinely care about others
  - Dependable - Maintain reliability, be accountable and organized
- ☐ Build the ISAO trust model
- ☐ Establish rules of engagement and participation in contracts and/or agreements
- ☐ Set ground rules for sharing
- ☐ Set expectations for how members will act
- ☐ Create a transparent dispute resolution process
- ☐ Promote trust building activities and participation through in-person meetings, encouraging specific members to share, member provided presentations, etc.

Creating a Security Policy

A security policy is essential to building trust and protecting the ISAOs assets and members. The security and privacy policy contain some overlapping requirements, each ISAO should:

- Consult relevant legal counsel and subject matter experts when building the security and privacy policies for your ISAO.
- Review relevant privacy and security laws for your region and/or sector.
- Build processes to audit compliance with policies and procedures.

A security policy should be annually reviewed by all employees and members and include:

- Security awareness training
- Password policies and rules
- Backup and recovery mechanism
- Data classification and handling rules
- Access control
- Secure communication
- Use of encryption
- Data breach notification rules

Create a Privacy Policy and Procedures

Establishing a privacy policy and procedures are essential to an ISAO. The following are some recommendations when establishing a privacy policy:

- Consult the appropriate legal counsel and subject matter experts when crafting a privacy policy and procedures.
- Remove personally identifiable information (PII) and other types of sensitive information from the information being shared.
- Build processes and procedures for escalation and notification of violations of the privacy policy.
- Consider all parties involved in the exchange including source, victim, and attacker.
- Review the Cybersecurity Information Sharing Act's requirements for receiving legal protections by sharing with relevant federal agencies. Determine if the ISAO will share with the Federal Government.

Step 3 - Establishing Core Offerings

The core offerings of an ISAO are built around the Information Sharing and Analysis Framework (ISAF). The Framework provides all ISAOs a structure for building and organizing the core offerings through six phases including planning, collection, analysis, dissemination, application, and disposition. This step highlights the essential items that should be included when ISAOs are building their core offerings.

Planning

The planning phase provides the policies, scope, direction, requirements, and procedures to guide ISAOs in building a comprehensive program. There are four major components in this process, and they include:

- ☐ Defining the type of information to share, whether structured and/or unstructured. Select one or more of the following:
  - Indicators
  - Vulnerability information
  - Courses of action
  - Incidents
  - Threat actors
  - Tactics, techniques, and procedures (TTPs)
  - Campaigns
  - Analytical records
  - Threat intelligence reports
  - Security advisories and alerts
  - Operational Practices
- ☐ Building a classification and handling policy.
  - Create a data classification policy such as private, restricted, and public.
  - Consider using Traffic Light Protocol (TLP)
    - Red - Not for disclosure, restricted to participants only
    - Amber - Limited Disclosure, restricted to participants' organizations
    - Green - Limited disclosure, restricted to the community
    - White - Disclosure not limited
- ☐ Selecting sharing models, methods, and mechanisms.
  - Select a sharing model:
    - Source-subscriber - Central source sends information to subscribers
    - Hub-spoke - Central hub receives information from member spokes, operates on it, and distributes it to members
    - Peer-to-peer - Share directly with each other in a mesh pattern
    - Hybrid - Contain characteristics of the other models
  - Select sharing mechanisms (how the information is shared). The mechanisms can be one-to-one, one-to-many, many-to-many, or many-to-one. These mechanisms may include automated platforms. Consider using:
    - Structured Threat Information Expression (STIX) is a language used to exchange cyber threat intelligence (CTI) in a constant and machine-readable manner.
    - Trusted Automated eXchange of Intelligence Information (TAXII) defining how CTI is shared over HTTPs. It supports common sharing models including hub-spoke, source-subscriber, and peer-to-peer.
  - Select sharing methods (organizational structure and governance for sharing information):
    - Formal exchanges are based on agreement such as a Non-Disclosure Agreement (NDA), contract, or member agreement.
    - Clearance-based mechanisms are a subset of the formal and requires information to be shared only through protected channels and in accordance with established rules.
    - Trust-based exchanges are often closed groups who inform one another on security issues of a common concern. They may or may not have formal agreements and may utilize TLP.

        - Ad-hoc sharing typically occurs in informal groups, in response to an event, and often for a limited duration.
- Establishing policies and procedures including but not limited to:
    - Data retention
    - Data classification and handling
    - Expressing, applying, and properly handling sharing designations, such as TLP.
    - Unauthorized or inadvertent disclosure
    - Escalation to law enforcement
    - Collection and preservation of evidence
    - Forensic techniques, processes, and procedures

Collection

ISAOs collect information to enable their members to identify, assess, monitor, and respond to cyber threats. The information can come from diverse sources, tools, sensors, and/or repositories. When building the collection capability consider:

- Sources
    - What information is important?
    - What information is legally allowed to be shared?
    - What information do members what to share?
    - Select systems or sources based on these considerations
- Formats
    - Unstructured and/or structured
    - Structured Threat Information Expression (STIX)
    - Trusted Automated eXchange of Intelligence Information (TAXII)
    - Cyber Observable eXpression (CybOX)
- How to collect
    - External sources
    - Emails
    - Scripts
    - Parsing text
- Vetting and validation should include
    - Relevance to membership
    - Credibility of source
    - Ability to verify the source
- Post-collection steps
    - Data transformation
    - Data storage

Analysis

Analysis provides decision makers with the necessary context and intelligence required to act. The analysis phase includes defining who is examining information and which techniques will be used to make the information actionable. Analysis involves the following staffing models, techniques, and processes:

- Staffing may include directly hiring employees, contractors, or reliance on partners.
- Prioritization provides focus and ensures better, more actionable outcomes.
- De-attribution including sanitizing the data to prevent revealing protected sources and reduce the likelihood of sharing private and sensitive data.
- Enrichment provides multiple points of reference to aid in revealing previously hidden data and correlation includes reviewing previous cases of similar data points.
- Documenting processes and outcomes of research including negative results.
- Weaving a narrative should include a well written report around targets, severity, impact, scope, and correlation.

Dissemination

The goal of dissemination is to ensure the right information is going to the right people. Information needs to be distributed as quickly and widely as is relevant. Dissemination guidelines govern formats and techniques used to distribute information to members. Consider:

- Mechanisms
  - Telephone
  - Email
  - In person meetings
  - Websites
  - Bulletins
  - TAXII
- Content
  - Alerts
  - Publications
  - Education, training, and awareness
- Format
  - Briefing
  - Reports
  - STIX
- Policy considerations
  - Encryption
  - Storage and retention periods
  - Frequency
  - TLP

Application

The application of disseminated information helps members manage cyber-related risks. Information is logically group into purpose-based and time-application categories. Consider the application of information when evaluating the usefulness of the information being provided:

- Purpose-based information
  - Situational awareness
  - Decision making
  - Action information
- Time and Application of resources information

- Immediate
- Tactical
- Strategic

Disposition

Disposition includes the classification, handling, and retention of data. Earlier in this guidebook, participants should have developed these policies and procedures. This phase is where the execution of those decisions happens in the Information Sharing and Analysis Framework. Data and information distributed to members should be processed in accordance with (IAW):

- ☐ Classification policies and procedures
- ☐ Handling guidelines
- ☐ Archived or purged IAW retention policies.

Step 4 - Implementing Services and Capabilities

This section highlights the additional services and capabilities one should consider in order to enhance the value proposition of joining your ISAO. Below are a list of foundational, additional, and unique services and capabilities offered by ISAOs. Foundational services and capabilities should be implemented, then consider creating a plan to augment those basic services with additional ones to differentiate from other ISAOs. Consider some of the following:

- ☐ Foundational services and capabilities are the basic functions an ISAO performs and are covered in Step 3 of this guidebook. They include planning, collection, analysis, dissemination, application, and disposition.
- ☐ Additional services differentiate the ISAO and/or meet other needs or constraints and may include:
  - Secure online discussion forum
  - Establishing relationships with government entities
  - Conducting exercises
- ☐ Unique services are specialized functions or activities developed or adopted by the organization to meet specific member needs. Some examples include:
  - Providing threat intelligence
  - Facilitate mutual aid
  - Testbed for malware analysis
  - Establishing a library of TTPs
- ☐ Surveys enable organizations to identify member opinions and needs. Surveys can be:
  - Web-based
  - In-person
  - Over the phone
- ☐ Use enhanced services and capabilities that help establish trust, including:
  - Training
  - Face-to-face meetings
  - Webinars
  - Conferences
  - Workshops

- ☐ Review *ISAO 100-2 Guidelines for Establishing an ISAO* for more information about other services and capabilities.

Step 5 - Establish Partnerships

Partnerships assist ISAOs in strengthening the offerings they provide members. ISAOs should rely on a systematic approach for partnerships, because unstructured approaches are destined to fail. A successful approach to partnerships should leverage strategy, planning, and operational phases.

- ☐ Strategy should include determining if partnering is the right choice for the solution the organization wants to implement. Activities include:
  - Alliance specific strategy
  - Evaluation and selection
- ☐ Planning involves negotiating agreements or contracts. Activities include:
  - Building trust and value
  - Operational planning
  - Alliance structuring and governance
- ☐ Operation flows from initiation, execution, and exit. Activities include:
  - Launching and management
  - Transform, innovate, evaluate, and exit

Once a process for building and managing partnerships is established, organizations should consider the following guiding questions, taken from *ISAO 100-2 Guidelines for Establishing and Information Sharing and Analysis Organization.* When evaluating prospective partnerships and collaborations:

- ☐ What does the ISAO have to offer the community of sharing partners to enhance the protection of critical infrastructure, industry, business, or government?
- ☐ Has the ISAO defined strategic information sharing partners? Have the mutually beneficial objectives of partner strategic alliances been defined?
- ☐ What are similar ISAOs currently providing and how can you coordinate, collaborate, and work together?
- ☐ Are there other ISAOs that could be partnered with? Consider other ISAOs for mentoring and support to assist with the early defining phases and the transition to operations. Consider other ISAOs for ongoing collaboration.
- ☐ Will the ISAO work with other partners to enhance the value of the information received? Will the ISAO openly share with other ISAOs?
- ☐ Is internal and external collaboration part of the ISAO's natural workflow?

Step 6 - Continuous Improvement

All successful organizations must measure their progress and strive for continuous improvement to be competitive and/or compelling in the information sharing and analysis space. ISAOs should periodically assess services, capabilities, business plan, mission and vision through SWOT, risk analysis, quantitative pros and cons, cost/benefit analysis, force field analysis, and/or cash flow forecasts. The plan-do-check-act (PDCA) cycle is a simple and common approach to continuous improvement which is widely adopted as a reference framework in the information security space. (Sutton, 2014) The PDCA cycle includes:

- Plan - identify your problems
- Do - test potential solutions
- Check - study the results
- Act - implement the best solution

ISAOs have several potential areas they can leverage the PDCA cycle to assess their performance and establish a culture of continuous improvement. Some of these areas include but are not limited to:

- Revamp the strategic goals of the ISAO
- Survey the membership for services and capability changes/upgrades
- Refresh of critical hardware
- Re-evaluation of threat feeds and data sources
- Refine marking and communications plan
- Update market analysis and competitive analysis
- Review of NDAs, contracts, and other legal documents