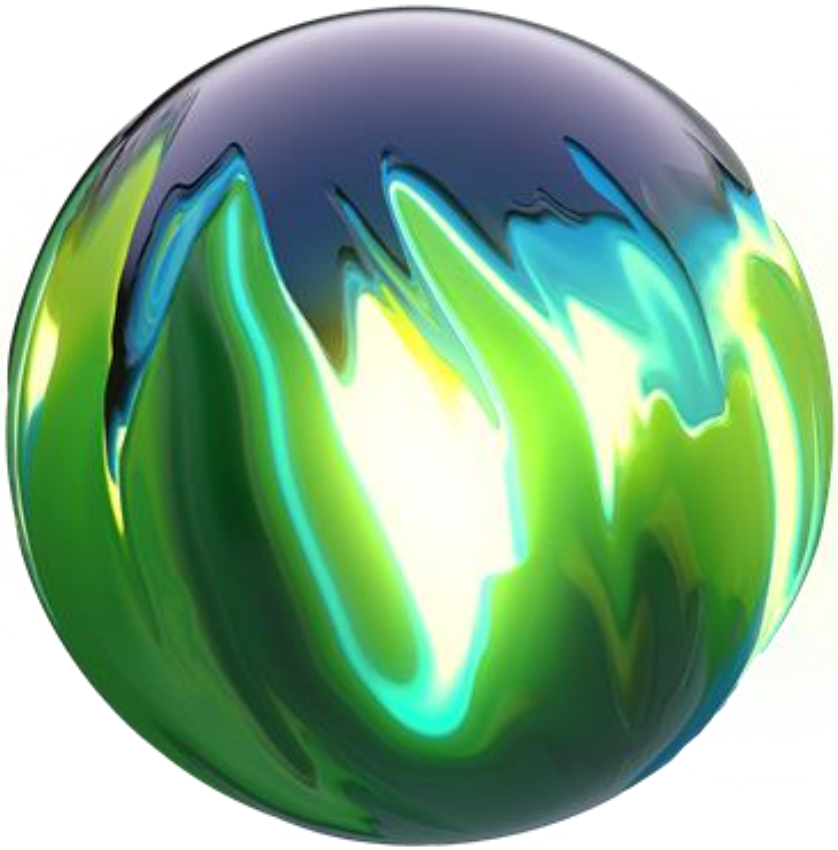
Deloitte.



Information Sharing and Analysis Centres (ISACs)

The next generation of security resilience for Australian industry

Foreword

This year is an important time for Australia as the government consults and implements the next iteration of Australia's Cyber Security Strategy. Recent events have accelerated the focus on cyber security and national resilience in boardrooms, parliaments, and households. The government's strategic decisions on AUKUS and the Defence Strategic Review will also factor significantly in discussions on how Australia protects our industrial base and critical supply chains, which include many sovereign small and medium enterprises. It has also been a very busy and demanding time for cyber security and resilience practitioners in Australia who are still hampered by workforce and skills shortages.

These challenges cannot be solved in isolation. They require a sharing of expertise and resources that can only be achieved within trusted communities. Over the past six months, our team engaged with members of information sharing communities across the Americas, Europe, and Asia-Pacific, culminating in a better understanding of circa 50 international Industry Sharing and Analysis Centres (ISACs).

We see industry ISACs as having the potential to represent the next generation in the uplift of Australia's industry cyber security resilience. We have developed this paper to improve awareness within Australia of ISACs, why they exist, how they differ from existing government-convened risk and security industry collaboration forums, the value they can offer and how they work. There is much that Australia can learn from other countries but likewise designing them for Australia requires us to factor in what is unique to us.

Australia already has a busy and active government and industry collaboration space. The key thing we have learned from our consultations is that for Australia to adopt an ISACs approach, we need to evolve from existing practices; not add new mechanisms into the mix. This will require government and industry to come together and be prepared to do things differently. As a country we're continuing to increase our investment in cyber and resilience and ISACs offers us a way to focus our resources to find ways to work together around threats and capability development.

We certainly do not have all the answers in this paper as ISACs are likely going to be different for every industry sector and will also evolve over time. However, we have been able to provide some guiding operational principles and considerations to incorporate as part of the Cyber Security Strategy consultation underway.

We'd like to thank all the international representatives who participated in our consultation and the Australian security and risk business leaders who made time to meet with us. We hope that this paper provides a compelling vision about what we could achieve by adopting ISACs and helps stimulate further conversation and co-design about how we make them fit for purpose for our country.

Ian Blatchford

National Cyber Leader
+61 2 9322 5735
iblatchford@deloitte.com.au

Rachelle Koster

Partner – Cyber
+61 421 051 630
rkoster@deloitte.com.au

Rob Parker

Partner – Cyber
+61 423 213 112
robparker@deloitte.com.au

Executive Summary

Within Australia, the previous twelve months have allowed the public to observe what cyber security professionals have been aware of for years; that Australia is not immune from large cyber security incidents. Organisations are increasingly facing threats that are systemic and interconnected and can take down multiple sectors through either operational and/or confidence failures.

These threats, on top of the effects of COVID-19, climate change, and the recent changes in the geopolitical landscape have led Australians to realise that more needs to be done to protect public safety, the environment, and our values through an increasing focus on trust and resilience in our digital and cyber systems.

Concurrently, workforce and skills shortages continue to hamper cyber security and resilience practitioners who are trying to deliver on elevated expectations as of result of this renewed focus. Organisations are realising that the threat landscape is everchanging and that it is becoming more difficult to stay on top of these threats.

Information Sharing and Analysis Centres (ISACs) are communities that help sectors work together to recognise and build resilience against these shared, systemic threats. In Australia, if setup with the right foundations, industry ISACs are going to represent the next generation in the uplift of Australia's industry cyber security resilience.

This paper has been developed to determine what components, support and strategies would be needed for this.

Deloitte has used a combination of international and local industry engagement and open-source information analysis to identify four broad capability categories that Australian industries should consider when implementing ISACs within their sectors, recognising that it won't be a "one size fits all" approach across the Australian industry landscape.

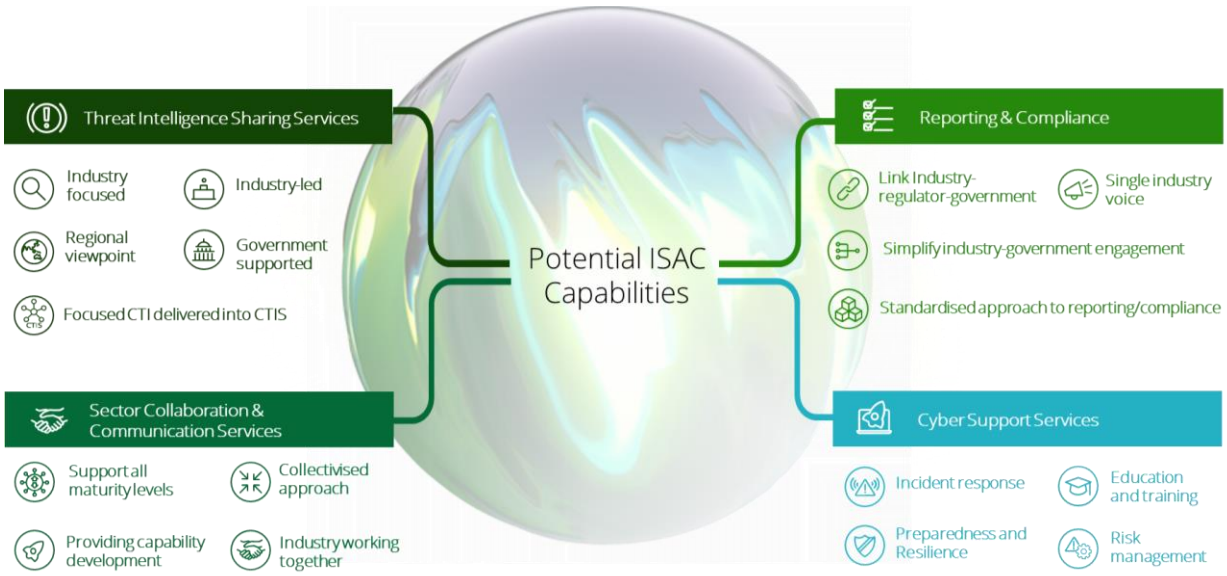
Why ISACs and why Australian specific?

In modern, well-connected economies threats do not occur within a vacuum. Organisations tend to use the same or similar capabilities to their sector peers, whether it is in the information technology (IT) or operational technology (OT) space. Consequently, vulnerabilities and risk profiles are often comparable on sector-by-sector basis.

As the ISAC concept matured internationally, it evolved to address this challenge by providing a broad suite of capabilities tailored to the unique requirements of each sector.

In Australia, ISACs can evolve from strong foundations already being provided by government – the Security of Critical Infrastructure (SOCI) Act, the Trusted Information Sharing Network (TISN) and the Australian Cyber Security Centre's (ACSC) Cyber Threat Intelligence Sharing (CTIS) community.

Potential ISAC Capabilities



ISAC Operations

Deloitte's engagement with international ISACs identified the following ISAC operational design principles:

Funding	
Recommended Model	Hybrid Funding Model (Government initiated to self-funded)
Benefits	✓ Overcomes initial investment barrier ✓ Provides industry long-term ownership
Other Models	- Strictly Industry-funded model - Government-funded model

Resourcing	
Recommended Model	Hybrid Resourcing (Teaching hospital model)
Benefits	✓ Continuity of full-time staff ✓ Capacity/trust of rotational staff ✓ Builds resource pipeline
Other Models	- Single-source fulltime resourcing - Single-source rotational resourcing

Membership	
Recommended Model	Controlled Eligibility (Multiple categories of membership)
Benefits	✓ High trust environment from vetting ✓ Visibility of participants
Other Models	- Broad Membership scope/eligibility - Controlled membership scope/ eligibility

Governance	
Recommended Model	Flexible Governance model (Ad hoc to structured over time)
Benefits	✓ Adapts to the needs of the ISAC ✓ Enables transition to formal model
Other Models	- Ad-hoc governance model - Structured governance model - Multi-level governance model
Accountability	
Benefits	✓ Reduced risk of inappropriate disclosure of shared intelligence ✓ Enshrines shared values among participants
Trust	
Benefits	✓ Increased dialogue and sharing within industry and with government ✓ Confidence to securely share intelligence

Implementation Considerations

Deloitte has reviewed the global landscape and engaged with several Australian organisations across a range of industries to uncover the most relevant capability and operational considerations. These should be used as the foundation in the development of ISACs to assist Australian industries in managing the risks associated with the constantly evolving threat landscape facing Australia.

Deloitte has developed the following seven (7) implementation considerations to assist government and industry in developing a successful uplift in Australian industry resilience:

Considerations	
1	The Australian government should allocate funding and/or refocus existing industry security advisory support services to help industries implement their own Australian based ISACs.
2	Australian industries should determine the scope of their ISACs through industry and government engagement, maintaining an Australian lens on security resilience.
3	Understand, consolidate, re-use and evolve any existing sharing capabilities or forums that may already exist.
4	Design Australian Industry ISACs with an All-Hazards approach.
5	Design inclusive Australian Industry ISACs to support all maturity levels.
6	The ACSC should make their CTIS industry co-design insights and outcomes available to industries as they undertake their journeys toward Industry ISACs.
7	Undertake co-design involving any relevant organisations within the industry, supply chain or government.

Next Steps

Deloitte has developed this paper with both government and industry in mind, and would recommend the next steps to be:

For Government – we recommend the government consider:

a) prioritising the establishment of industry ISACs into the next Australian Cyber Security Strategy (including funding measures);
b) investing in public funding and/or grant mechanisms that seed industry led ISACs; and
c) where needed, informing and facilitating the industry-led co-design and implementation of ISACs, helping to remove barriers to sharing and collaboration around capability uplift.

For Industry – we recommend engaging with government and fellow industry participants to:

a) understand what capabilities exist that could be consolidated, reused or evolved;
b) initiate and lead industry ISAC co-design, including the identification of blockers to community-based threat sharing, sectoral/supply chain risk management and collaborative cyber security activities; and
c) support sectoral and supply chain based cyber uplift such as executive and technical training activities through ISACs.

Contents

Introduction

What are ISACs?

Information Sharing and Analysis Centres (ISACs) are communities that help sectors work together to combat shared threats. ISACs were first founded in the United States by a Presidential Directive in 1998 to support collaboration and sharing between critical infrastructure operators.[1]

ISACs are now tried and tested. In the twenty-five years since that directive, US ISACs have expanded significantly and continue to be a key feature of Washington's industry-led cybersecurity strategy.[2]

This success has seen the ISAC model replicated internationally with notable initiatives emerging across the EU, Canada, Japan, and Taiwan. In addition, the individual ISACs themselves have evolved. ISACs like the Aviation ISAC (A-ISAC) and the Financial Services ISAC (FS-ISAC) have become global, while local and state government bodies have identified the need for these capabilities and developed a Multi-State ISAC (MS-ISAC).[3]

Aviation ISAC expanded to include satellite operators as a critical partner in the aviation industry

The growing adoption of the ISAC model has allowed sector groups to gain a deeper understanding of their supply chains and expanded the traditional boundaries of the organisations included in their sector.[4]

ISACs are safe spaces for industry peers to share non-commercial knowledge and resources among a network of trusted partners with the goal of increasing their collective resilience. More than just a threat intelligence feed or executive forum, ISACs are designed to bring together a range of services and capabilities that provide business value to all members of a sector, regardless of their size or maturity.

Why are ISACs important?

Threats do not occur inside a vacuum; in modern, well-connected economies a threat to one has the potential to be a threat to all. Threat actors like cybercriminals collaborate through the Dark Web to find the weakest link in this interconnected landscape, whether this be within a specific organisation or across an industry-wide vulnerability. Defending organisations internationally have embraced ISACs as a tool to fight fire with fire, collaborating to establish mutual, sector-wide defences.[5]

Organisations need to work together to mitigate cyber risk with a consistent collaborative approach. The remit of cyber security within an organisation is getting more complex and organisations cannot sufficiently expand their capabilities, knowledge or resourcing by working alone. Whether it be equipment faults, environmental hazards, or cyber-attacks, threats are most likely to be repeated when information, knowledge and solutions are siloed. ISACs were initially

developed as a tool to encourage industry to bridge these information silos and provide a secure channel for mitigating common sectoral threats.

As the ISAC concept matured internationally, it evolved to include the provision of a broader suite of important functions tailored to the unique requirements of each sector.

Energy ISAC includes an OT security lens

ISACs are not one size fits all. They are self-organising bodies that adjust to the needs of the sectors they serve. ISACs often identify and fill significant sector-specific gaps in security and resilience beyond their core operational-information sharing offerings. The Space-ISAC, for example, has developed a task force for addressing the recent U.S. Presidential directive on Cybersecurity Principles for Space Systems (SPD-5).[6] The ISAC in this case is acting as a single voice for the industry it represents, engaging external stakeholders on the industry's behalf while collectivising resources to develop best practices and learnings for participants internally.[7]

ISACs are ultimately "value-seeking" originations. To remain relevant, they must seek out industry pain-points and threats that can be best resolved by applying industry-expertise and collective efforts. This ongoing process of value-identification and relevancy results in ISACs playing an important role in filling sector-specific gaps that may otherwise go unnoticed by peak bodies or governments.

The case for Australian ISACs

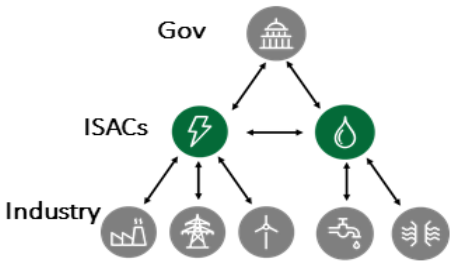
ISACs represent the next generation in the uplift of Australia's industry resilience. Strong foundations have been established by government initiatives like the Cyber Threat Intelligence Sharing (CTIS) program and the protection of systems of national significance (SONS) through the Security of Critical Infrastructure (SOCI) Act. There has, however, been limited progress in Australia to date to cultivate industry-led initiatives.

Building on the foundations of these government initiatives, and the global ISACs, Australian ISACs present the opportunity for organisations to collaboratively provide a regional and industry focused approach to managing security risks across their industry. This will allow organisations to manage the risks across their threat landscape and uplift the cyber security resilience of their region and industry, whilst also utilising the SOCI legislation as a basis to implement an all-hazards view of security.

Today, Australia is well placed to implement an all-hazards approach to industry ISACs that can provide real benefits to the Australian economy.

Information Sharing

ISACs represent a key opportunity to expand on the information sharing capabilities of the nation. Programs like CTIS can be enhanced by the implementation of sector specific bodies in their information sharing pool.



ISACs can help to reduce the "noise" of general information feeds by using their sector-specific knowledge to refine and enrich intelligence with relevant sectoral context.

The integration of ISACs into the Australian information sharing ecosystem also provides new opportunities for information between sectors.

At present, if an energy sector organisation identifies a critical vulnerability in a SCADA system that is also employed by organisations in the water sector, there are no clear direct channels for passing along this information. Standing up ISACs would provide clear, dedicated bodies for disseminating information between interlinked sectors with shared risks.

Financial, Telecom and Energy sectors maintain tri-sector ISAC playbooks

All-Hazards Approach

An increased focus on national resilience has compelled Australian organisations in all sectors to think more comprehensively about threats and risk. For some critical infrastructure operators, the shift to an "all-hazards" view of risk is more acute, having become enshrined in law through the SOCI legislation. ISACs present an opportunity to help organisations collectively understand the broad suite of threats and risks that impact their sector.

ISACs are not just cyber intelligence bodies. They often support the tracking and mitigation of threats and risks in other domains that might manifest differently within each sector.

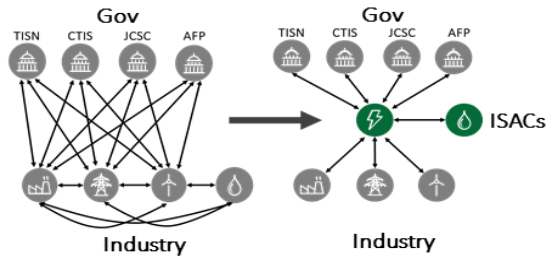
Energy ISACs both in the U.S. and Europe emphasise physical threats like service outages, climate risks and natural disasters in their ISAC offerings.[8] Other ISACs emphasise personnel threats like workplace safety, sabotage/insider threats and public health.[9] ISACs in Australia could serve to inform organisations about threats and provide collective solutions to help mitigate these threats on a sector-wide level.

Water ISAC shares water contaminant data

Simplification and Consolidation

Australian organisations are expected to navigate an increasingly complex web of obligations and reporting as they respond to threats.

The management of cyber threats in particular has become a confusing process for some organisations that must interact with several government agencies and regulators as threats are realised.



ISACs represent an opportunity to simplify this complex industry-government engagement landscape. Representing a single voice of industry into government, ISACs can sit at the middle of this complex web facilitating faster, more consistent engagement between relevant stakeholders.

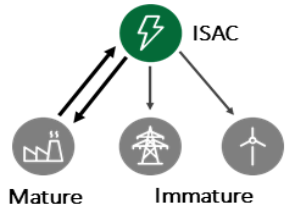
This simplification of engagement can extend to government-led and convened programs like CTIS and Trusted Information Sharing Network (TISN) with ISACs acting as a sector specific broker. Over time programs like TISN have the potential to evolve from government-convened to industry-led if certain resource-intensive functions are operationally integrated into appropriate industry-ISACs.

In the spirit of simplification, ISAC-implementors should also consider capabilities that already exist within an Australian industry sector and look to consolidate and/or re-use these collaboration capabilities, rather than simply adding to them.

Our local industry engagement specifically noted that some of the existing ad-hoc industry engagement forums could be consolidated into an ISAC. Existing bodies, like the Australian Banking Association (ABA) or the Water Services Association of Australia (WASA), already provide some of the key capabilities that an ISAC would be attempting to deliver. Reuse and expansion of these established mechanisms could consolidate ISAC-functions within existing trusted bodies where appropriate.

ABA and **WASA** could form strong ISAC foundations for their industries

"Rising Tides Lift all Boats" Approach



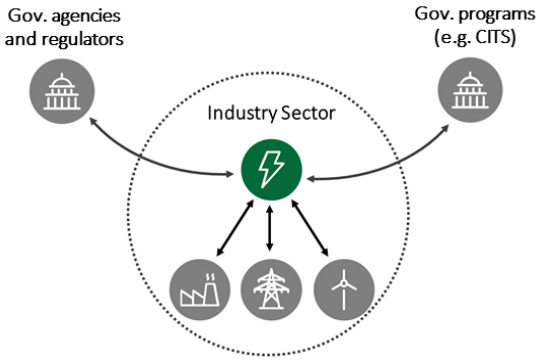
ISACs are built on the philosophy that organisations are stronger on matters of security when they work together. In smaller economies, like Australia, this philosophy is particularly important as organisations that are left behind potentially pose a disproportionate risk to the wider whole. An 'All-Maturity, All-Party' culture, in which organisations are enriched by an ISAC regardless of their size or maturity is therefore central to any potential Australian model.

Large, established organisations often have a leading role to play in an ISAC. They are more likely to possess the most up-to-date threat information that can be missed by their smaller, less mature peers. They might also have the additional resources to share approaches and best practices at ISAC working groups and committees. These contributions provide lessons-learned for the benefit of the whole sector and once acted upon, create a more secure environment for all parties to do business in.

ISACs are not just 'all-give and no take' for larger organisations. International ISAC models have been designed to provide explicit business benefits to large, contributing organisations. These benefits include technical perks like additional accounts for accessing portals, reputational advantages like guaranteed board membership or speaker slots at major ISAC-run events, and people benefits like access to discounted training or analyst-level networking events.[10]

IT-ISAC provides value to large & small organisations

Industry Leadership and Ownership



ISACs succeed when participating organisations feel a sense of ownership and accountability towards the model. This 'buy-in' relies on ISACs having an industry-first lens that facilitates honest and free engagement between participants without the fear of reprisal from government agencies or regulators. While anonymisation of shared information is standard practice in ISACs, the optic of government ownership is sometimes enough to dissuade organisations from sharing openly.

Engagement with local industry revealed that Australian organisations have a significant preference for industry owned and led ISACs. In contrast to existing programs like TISN, ISACs represent an opportunity for industry to self-organise and manage their own challenges — engaging with government on their own terms.

Space ISAC – industry-owned and industry-run model

ISAC Capabilities

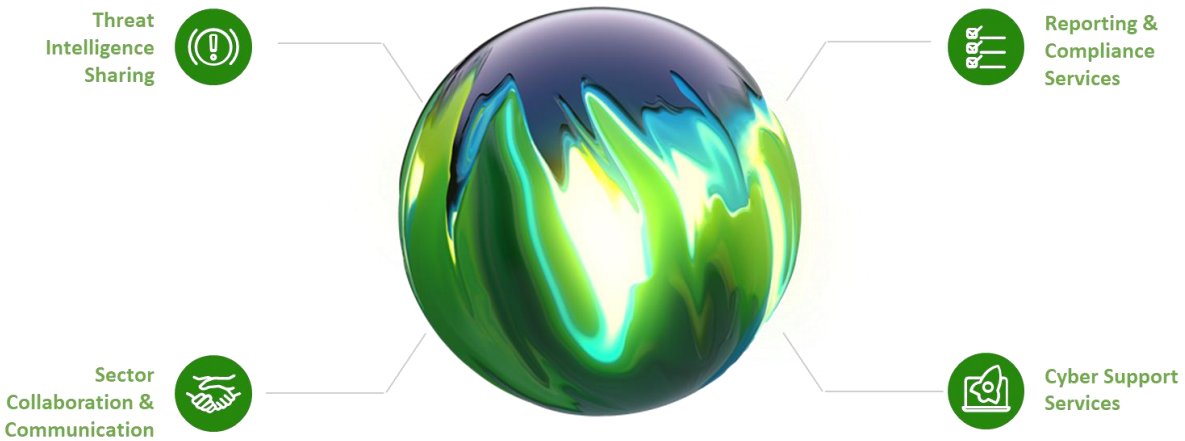
Established international ISAC capabilities that are likely to be applied to the Australian context

ISAC Capabilities

ISACs are independent, value-seeking organisations that adapt to the needs of the sectors they serve. Our investigation of international examples reveals that while successful ISAC models are defined based on the needs of the industry sector, ISAC services generally conform to four broad capability categories: threat intelligence sharing, sector collaboration and communication, reporting and compliance and cyber support services.

Industries choose capabilities
"One size **does not** fit all"

These capability categories represent the foundational building blocks on top of which ISACs deliver their services and grow their participant base.



Each ISAC will place a different weight or emphasis on these capabilities depending on the needs of their sector. The global Financial Service ISAC (FS-ISAC) for example typically provides consistent resources across the four capabilities. The U.S. Public Transportation ISAC (PT-ISAC) by contrast generally places more emphasis on its threat intelligence sharing capability and relies on more passive services like communication channels and newsletters to deliver the other capabilities.

FS-ISAC – balanced capabilities
PT-ISAC – CTI dominance

Prospective Australian ISACs need to consider which services are most critical to the sectors they serve and build these considerations into their capability mix.

Threat Intelligence Sharing Capability

Key Elements	
All-hazards Intelligence	Threat Intelligence Sharing is a core capability offered by ISACs and should include the distribution of all-hazard intelligence, not just cyber security.
Bi-directional Sharing	ISACs should incorporate bi-directional sharing, to ensure appropriate intelligence is being shared across the community.
'Hub-and-Spoke' Intelligence Sharing Ecosystem	Gradually ISACs can play a role as sector hubs in a broader national threat intelligence sharing ecosystem.

Cyber and All-Hazards Intelligence Sharing

Threat intelligence sharing is the common denominator across all ISACs identified in Deloitte's international investigation. This capability includes services that provide greater situational awareness of trends in an organisation's threat landscape and aid in their deployment of countermeasures before they are impacted. Threat intelligence sharing generally involves the gathering and distribution of security data, including Indicators of Compromise (IoC) and actionable alerts relevant to each sector.

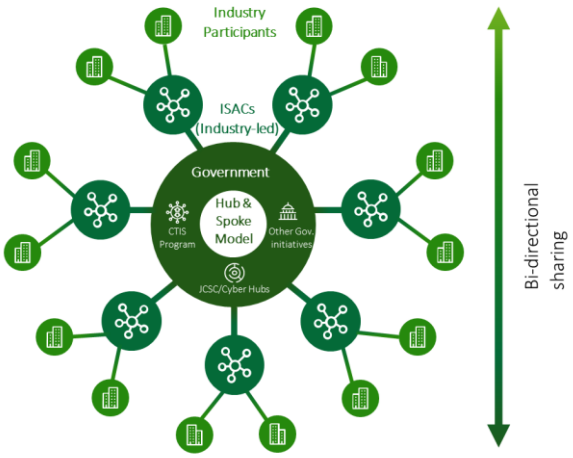
Some ISACs implement an "all hazards" intelligence approach to help organisations manage risks beyond the cyber domain including national security, environmental and economic risk.

Bi-directional Intelligence Sharing

In most cases, ISACs aim to implement threat intelligence sharing capabilities on a bi-directional basis. Industry participants are encouraged to proactively push intelligence on threats sighted in their environments to an ISAC to be analysed and distributed for the benefit of the wider community.

Sourcing these insights directly from the community not only builds trust among participants, but also helps ensure the data is relevant and timely. The ISAC is then able to aggregate and normalise these community-sourced insights into actionable intelligence.

'Hub-and-Spoke' Model



'Hub-and-Spoke' Intelligence Sharing Ecosystem

Japanese National 'hub-and-spoke' model

This bi-directional dynamic can also be expanded to an ecosystem-wide level. A national hub-and-spoke model between industry participants, ISACs and government can help establish a trusted sharing network to collaborate, collect threat intelligence and anonymously exchange threat indicators across the Australian economy.

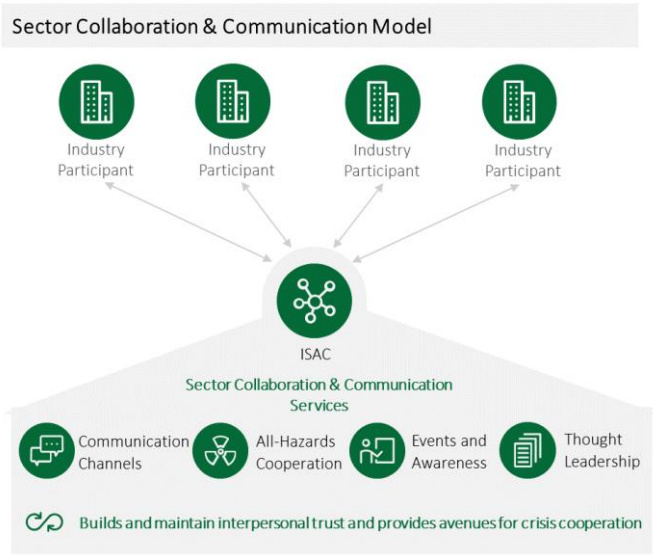
This model has precedent in other jurisdictions like Japan, where ISACs have begun to integrate with government programs.[11] These efforts support the identification of shared cross-sector vulnerabilities and minimise the potential negative consequences of major systemic cyber threats. A bi-directional 'hub-and-spoke' dynamic enables intelligence to be distributed with greater efficiency between government and industry, with ISACs as a critical broker performing the analysis and context setting for the industries they serve.

Sector Collaboration and Communication Capabilities

Key Elements	
More than just CTI Sharing	Collaboration activities beyond the CTI information sharing level represent a significant part of an ISAC's value proposition.
Solving Sectoral Challenges	Sector collaboration initiatives leverage the sector-specific expertise of ISAC participants to solve cyber and all-hazard challenges.
Building Interpersonal Trust	Collaboration initiatives like working groups serve as the basis for much of the participant-to-participant trust in ISACs.

More than just CTI Sharing

ISACs are more than just providers of threat feeds to be passively consumed. They are sector-based communities with trust at the core of their operations. The collaboration and cooperation services that facilitate non-CTI information sharing and build these trust connections represent a significant part of an ISAC's value proposition.



Solving Sectoral Challenges

One of the strengths of ISACs is their reach into and across sectors. Because each ISAC is a participant-driven organisation, they well understand their sector's interdependent and interrelated risks and are typically the most effective mechanism for communicating with the organisations that are subject to these shared risks. Sector collaboration and communication initiatives like industry working groups, secure collaboration channels and thought leadership all leverage the sector-specific expertise of ISAC participants to solve collective cyber and all-hazard challenges. The European-Rail ISAC (ER-ISAC), for example, provides its participants with access to working groups to influence railway standards and industry best practices in response to emerging threats.

ER-ISAC influences through working groups

Building Interpersonal Trust

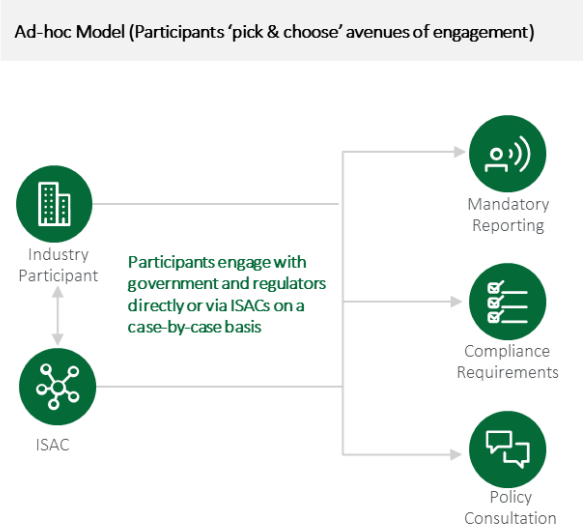
A by-product of these sector collaboration efforts is a positive impact on the long-term effectiveness and sustainment of an ISAC. Participating organisations are often unwilling to engage in meaningful sharing initiatives if they cannot trust the community they are sharing into. Collaboration initiatives like working groups serve as the basis for much of the participant-to-participant trust within these bodies and help build a long-term culture of ISAC contribution and engagement.

Reporting and Compliance

Key Elements	
Single Industry Voice	ISACs hold sector-specific knowledge and expertise on compliance commitments and can act as a single voice 'lobbying' for the sectors they represent.
Link between Industry, Regulator and Government	ISACs can become formal or informal intermediaries that link industry, regulators, and government in a reporting capacity.
Standardised approach to reporting/ compliance	ISACs can develop tools and policies that enable participants to adapt to regulatory changes via templates and automation.

Single Industry Voice

The importance of reporting and compliance, particularly in cyberspace, cannot be understated. It is a critical process for ensuring regulatory visibility into security programs and validating that community expectations across key sectors are being met.



Globally, some ISACs have sought to simplify this increasingly complex regulatory landscape by acting as a single industry touchpoint and voice on reporting and compliance matters.

These ISACs hold sector-specific knowledge and expertise on compliance commitments, while acting in a 'lobbying' capacity on proposed policy and legislation that may impact the sectors they represent. The National Council of ISACs preforms this function at the Federal level in the U.S., routinely advocating for regulatory decisions that improve sectoral information sharing and testifying before Senate committees and congressional briefings.

Link between Industry, Regulator and Government

ISACs are a potentially useful tool to support organisations through their compliance and reporting obligations as a formal or informal intermediary. In practice, the decision for ISACs to act in either a formal or informal reporting capacity is dictated by the regulatory demands the sectors they represent.

The FS-ISAC, for example, has established working groups as an avenue for discussing industry regulatory compliance in an informal capacity. This provides participants from the highly regulated

financial services sector with the flexibility to engage with the ISAC or their regulator in a separate, ad hoc, and case-by-case basis.

ND-ISAC formal compliance assistance

The US Defence Industrial Base ISAC (ND-ISAC) by contrast provides its members formal with assistance meeting their Defence Federal Acquisition Regulation Supplement (DFARS) compliance requirements, including options to assist in the reporting of incidents to the Department of Defence.

This represents more of a 'bow-tie' model, with the ISAC sitting as a formal intermediary liaising with government and regulators on its participants' behalf.

Standardised approach to reporting/compliance

On a more technical and operational level, ISACs are positioned to develop tools and policies that enable participants to adapt to their ever-changing regulatory obligations in a standardised manner. The sector-specific mandates of ISACs can incentivise the production of templates to help participants respond to sector-wide reporting and compliance items with greater efficiency, consistency, and accuracy. This service could assist Australian organisations as sector-specific requirements are continually developed and updated as part of the ongoing enhanced obligations for SONS.

As Australian ISACs develop deeper expertise in providing a standardised approach to reporting and compliance, opportunities may emerge for ISAC-driven compliance automation. By acting as the intermediary between industry and regulators, ISAC could establish consistent data models and facilitate compliance automation. In the future, this would provide participants with options for their ISAC to use the data collected to develop relevant reports on the participants' behalf.

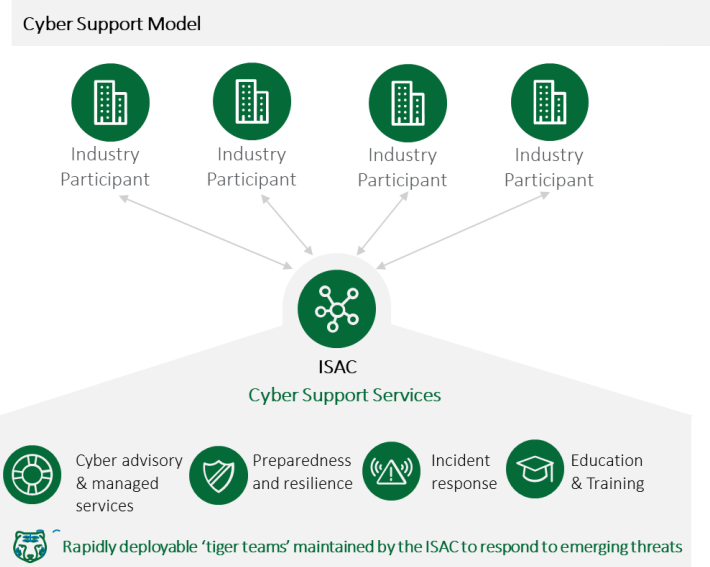
Cyber Support Services

Key Elements	
Pooling Resources	ISACs leverage the strength of a community to provide more equitable access to cyber support services for all-parties.
Facilitation of Access to Support	ISACs facilitate access to cyber support services either by directly providing the service themselves or negotiating with third parties on an organisation's behalf.
Improving Cyber Posture	The sector expertise of ISACs can inform the cyber support services provided to partners, delivering better outcomes.

Pooling Resources to Support All

ISACs are intended to support organisations of all sizes and maturity levels. This includes organisations that may not have the resources, budgets, or in-house skills to establish large internal security teams and capabilities.

Services like threat detection and hunting, vulnerability management, cyber education and incident response can be inaccessible for individual organisations that are in the process of building their cyber maturity. ISACs provide an opportunity to leverage the strength of a community, pooling resources to provide more equitable access to cyber support services in each sector.



Facilitating Access to Support Services

Accessing these ISAC-provided cyber support services can vary significantly based on how an ISAC is funded and the cyber security 'baselines' in each sector.

MS-ISAC – provides support services

In some instances, ISACs are funded to administer these services directly to participants, as is the case for the MS-ISAC.

IT-ISAC – negotiates discounted rates

In cases where a sector may have a higher collective maturity, ISACs like the IT-ISAC do not administer the services themselves and instead negotiate discounted rates with third party service providers and maintain up-to-date service catalogues on behalf of participants.

In both instances the goal of the ISAC is to use the collective resources of the community to make cyber support services more accessible than they otherwise would be on an organisation-by-organisation basis.

Improving Cyber Posture with Sector-Specific Support

This capability enables ISAC participants to get more out of their cyber budgets and to fast-track their cyber security posture uplift with sector-specific advice. The Health ISAC (H-ISAC), for example, provides its members access to cyber benchmarking, legal and regulatory surveillance, and independent risk assessment services. A participating organisation can therefore employ the same ISAC membership fee to both remain vigilant about emerging threats and work with an ISAC to implement, monitor and manage the compensating security controls that matter most to their sector.

H-ISAC sector-informed support services

ISAC Operations

Key operational decisions to be made before developing an ISAC

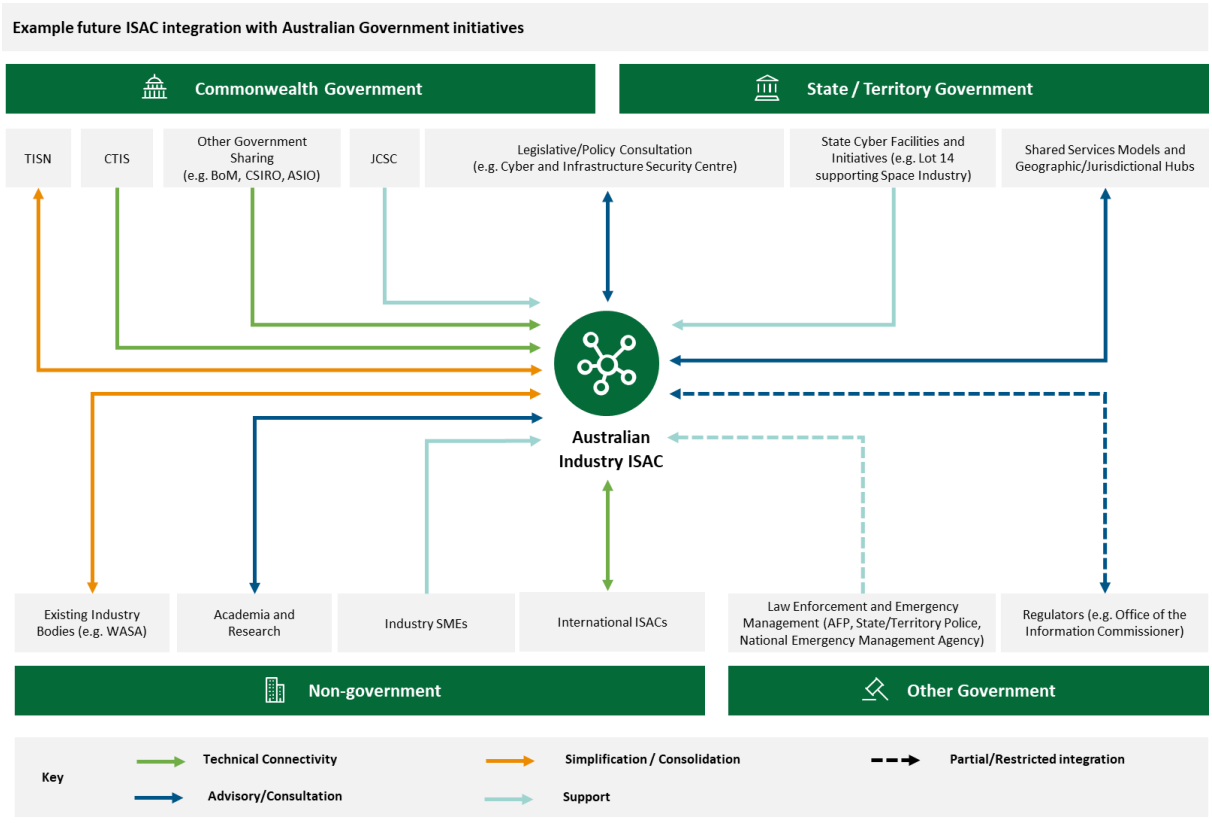
Operating an ISAC

Australia is well positioned to benefit from the various operational decisions that have been tried and tested in successful European, North American and Asian ISAC deployments. Deloitte's research into these international ISACs identified six recurring operational considerations that were critical to each ISAC's establishment and ongoing success. These considerations include governance, funding, resourcing, membership eligibility, accountability, and trust.

In support of these operational considerations, Australia should consider the existing government provided services and how they can be supported and improved by greater integration with Australian Industry ISACs.

Possible Future of Government Programs like TISN

Australian government programs like the Trusted Information Sharing Network (TISN) have the potential to evolve from government-convened to industry-led if certain functions are operationally integrated into appropriate industry-ISACs. This would provide a vehicle for government to 'tap-in' to industry where required, while handing over resource intensive 'business-as-usual' engagement and outreach tasks to the ISAC itself. ISACs in this model could be positioned as an industry-led capability of TISN — enabling government to focus on its efforts on specialised advisory, formal consultation and helping critical infrastructure operators manage unforeseen risks.



Other programs, such as those delivered by the ACSC, Department of Home Affairs and the Australian Federal Police, can also be made more effective by establishing clear, dedicated integration points with Australian industry ISACs. Areas like the Cyber and Infrastructure Security Centre and the Defence Science and Technology Group share similar objectives to industry ISACs and thus have a natural synergy that can be expanded upon through the establishment of formal advisory and support channels.

International Viewpoint: Operational Considerations

ISACs from each sector and jurisdiction have sought to manage the six identified operational considerations differently, resulting in various models. These models provide a conceptual starting point for Australian ISACs and outline the kinds of operational decisions that each sector will need to explore. It is possible, for example, that an Australian financial services sector ISAC will embrace a different funding model to an ISAC for the education sector.

A consolidated view of these operational considerations and models have been included in this section, each with an accompanying analysis of their respective benefits, limitations and international examples.

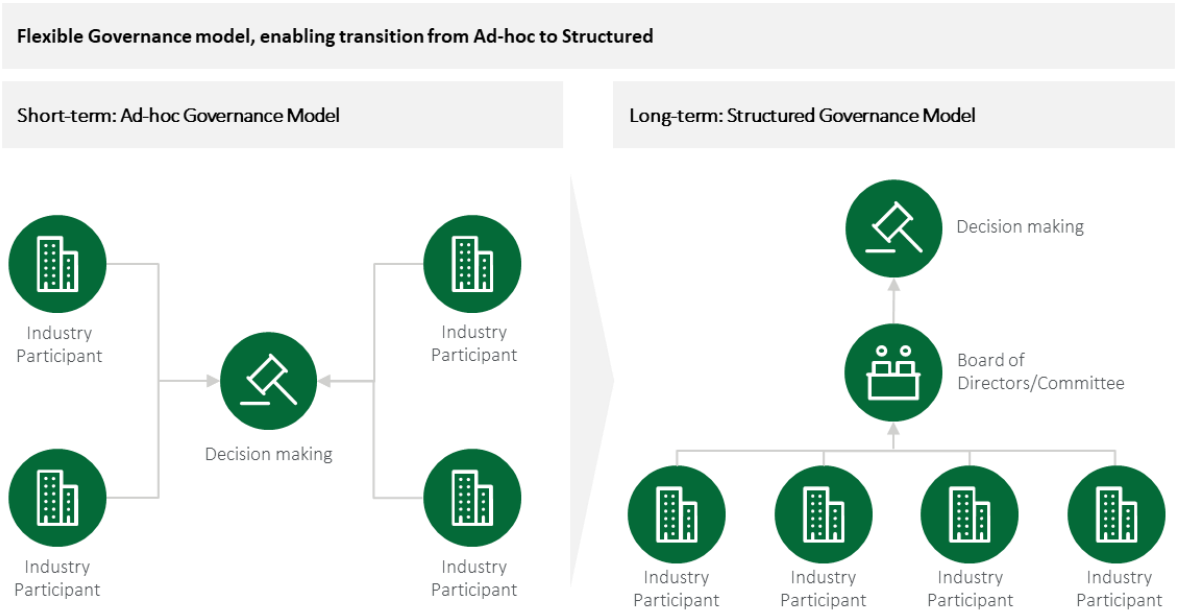
Governance Models

As ISACs are participant-driven initiatives there are opportunities to align how they are governed to the preferences of the industries they serve. Governance within the ISAC context defines the administrative structure and decision-making mechanisms, outlines the obligations of each participant, and establishes the overall offerings of the ISAC.

Models	Benefits	Limitations
Flexible Governance Model*	- Adapts to the needs of the ISAC - Enables transition to formal model	- Potential disruption to decision-making/operations as transition occurs - Need to identify the point at which a transition should occur
Ad Hoc Governance Model	- Suited to small ISACs - Flexible decision making – can adapt to change quickly - Builds on existing trust between members	- Lack of formality impacts accountability and engagement - Requires an existing level of trust between members
Structured Governance Model	- Suited to established ISACs - Clear structure, well defined roles/practices - Supports other initiatives e.g. committees	- Requires either a significant cost or time investment from participants - Less flexible than other models
Multi-level governance Model	- Suited to industries with significant government/public service integration - Facilitates communication with government	- Government integration may undermine trust and inhibit sharing - Adds complexity/ bureaucracy to governance structure

**Deloitte recommended model*

Flexible Governance Model

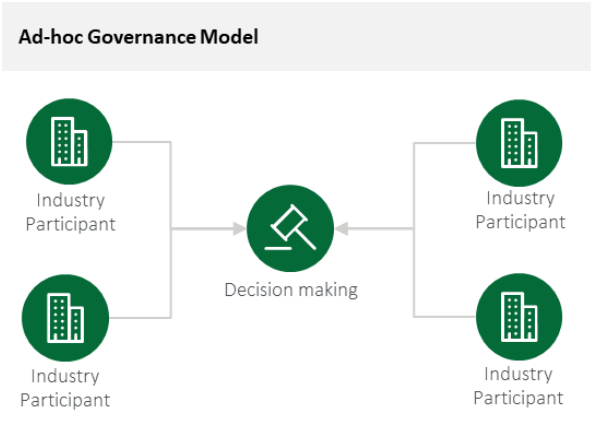


A flexible governance model is designed to adapt to the needs of the ISAC over time. When the ISAC is in its start-up phase, an ad-hoc governance model is implemented which enables all members to contribute to decision making on a case-by-case basis. As the ISAC grows, this governance model transitions into a structured model in which a formal board of directors or committee receives delegated decision-making power on behalf of all participants.

The distinct advantage of this flexible model is its ability to adapt to the needs of the ISAC overtime. Notably, when ISACs are in their 'start-up' phase this model ensures that effort and resources can remain nimble and focus on standing up core ISAC functions without being constrained by rigid governance procedures that may prove too cumbersome for early-stage ISAC teams. This empowers participants to make decisions about when it is appropriate to transition to a more formal governance approach.

Auto-ISAC: flexible governance model

Ad-hoc Governance Model



An ad-hoc or 'light-weight' governance model pulls together ISAC participants to make joint decisions on a case-by-case basis.

It is especially suited to smaller ISACs where one or few entities help drive this structure.

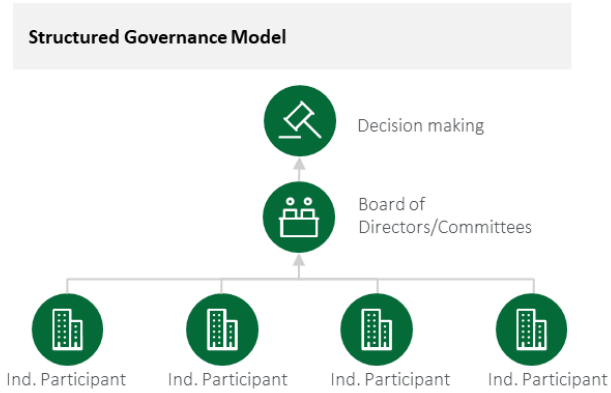
It facilitates flexible decision making and is characterised by its ability to adapt quickly to change. It relies on the ability to draw together

all relevant participants at short notice to make decisions and approve administrative processes as challenges and opportunities arise.

This model is particularly well suited to small, close-knit ISACs with established levels of sectoral cooperation and trust. Without this existing level of trust between participants, however, it may be challenging to establish the necessary levels of accountability and engagement.

Real Estate ISAC: Smaller, close-knit

Structured Governance Model



The most common ISAC governance model is a traditional structured approach, often employed by non-government organisations and industry bodies. It usually involves the formation of a Board of Directors or a group of key members that are in decision-making positions in the ISAC and have formally established engagement cadences and escalation processes.

A fixed, structured governance model can present significant benefits to industry participants. It replicates a tried and tested structure that provides well defined roles and practises that are wildly understood. This strong governance foundation can then support the development of other auxiliary initiatives like working groups and committees.

Instituting this approach from an ISAC's conception requires time and cost investments from participants that may be unrealistic for a newly formed body.

As such, this approach may be more suitable for sectors seeking to consolidate their ISAC offering into an established industry body that has existing "buy-in" and support for a formal governance structure.

REN-ISAC: structured governance model

Multi-level Governance Model

There are scenarios in which a supporting body may be required to contribute to the coordination and governance of an ISAC. This can result in a shared management model or a structure where there is both a management and a secretarial body where the secretariat can act as a facilitator.

A multi-level governance model is best suited to industries with significant government/public service integration.

Internationally, this model has proven successful in sectors like Transporation and Energy where the ISAC benefits from in-built mechanisms for communication with government stakeholders that own or operate key infrastructure assets.

ER-ISAC: multi-level governance model

This approach does, however, introduce additional complexity and bureaucracy to a governance structure and may not be appropriate for sectors with more automony from governments.

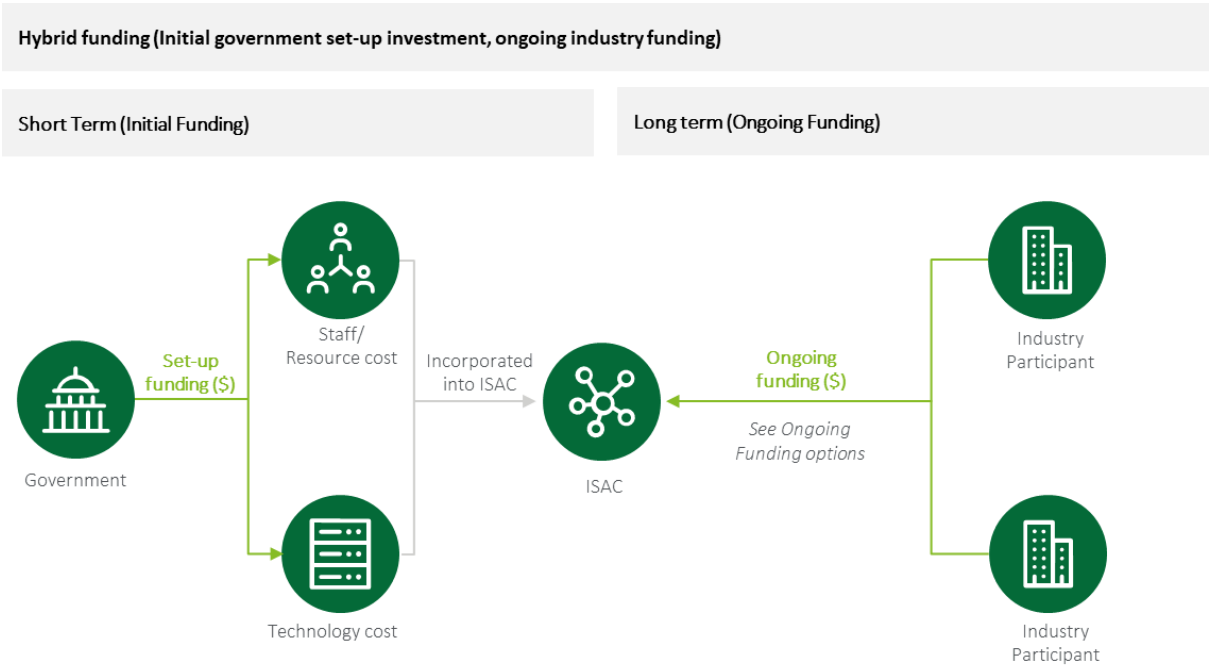
Financial Models

As independent industry-led initiatives, one of the primary questions ISACs need to answer is how they will be funded. These funding considerations should include both models for funding the initial cost of setting-up an ISAC and well as options for their ongoing financial sustainment.

Models	Benefits	Limitations
Hybrid Funding Model*	- Overcomes barrier of industry raising set-up investment - Industry ownership of ISAC via ongoing funding	- Transition plan required to avoid disruptions in operations as ISAC moves from a government funded to an industry funded
Standard Annual Fees Model	- Simple, predictable estimates of ISAC contributions - Imposes consistent contribution across all members	- May not reflect the relative contributions of organisation - If the fee is set too high, it could be prohibitive to smaller players
Revenue-based Tiered Fees Model	- Strong 'All-Party' culture, supports smaller party participation - Larger parties play a proportionate role in uplifting the sector	- Larger parties may feel they are carrying the financial brunt of the ISAC - Lower fees for some could result in the ISAC being treated as a threat feed to be consumed
Service-based Tiered Fees Model	- Participants pay for the services most appropriate to them - Enables ISACs to market exclusive or 'premium' offerings	- Risks creating a 'pay-to-play' environment, where critical services are set behind inaccessible cost barriers for smaller parties
Government funded, operated through an intermediary	- Reliable, ongoing government funding source - Low barrier to entry encourages a culture of 'All-Party' participation	- Significant cost placed on government. - Low barrier to entry may result in the ISAC being treated as a threat feed to be consumed
Operated and funded as part of existing government body	- Reliable, ongoing government funding source - Legitimacy and confidence as a government-led initiative	- Significant cost placed on government - Direct sharing with government may breed apprehensiveness among industry participants.

**Deloitte recommended model*

Hybrid Funding Model: Initial government set-up investment, ongoing industry funding



Industry has developed a range of options for long-term, ongoing funding options for ISACs; however privately mustering the initial funding to establish the technological and resource base of these ISACs has proven challenging. Examples of ISAC development internationally suggests that government, by contrast, may be better suited in some instances to provide this upfront investment rather than covering the ongoing cost of operations.

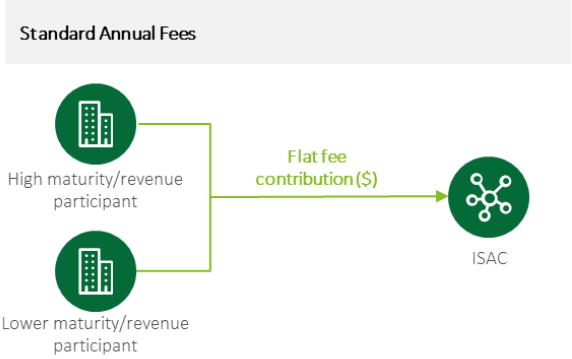
A viable model for the establishment of an ISAC may therefore comprise of initial seed funding provided by government, while the cost of ongoing operations becomes the responsibility of industry participants. This model helps overcome one of the most significant obstacles to ISAC development (the initial setup cost), while also ensuring that industry can retain a sense of ownership and responsibility.

EE-ISAC transitioned from government to industry funded

It is noteworthy, however, that a strong transition plan is required to facilitate the transition from government to private funding.

Standard Annual Fees

One approach for sourcing funding for the ongoing operations of an ISAC is the establishment of a standard annual flat fee for participants to access the services offered by the ISAC. This standard fee model provides a simple, predictable approach to funding that enables ISAC administrators to forecast financial contributions more accurately over time.

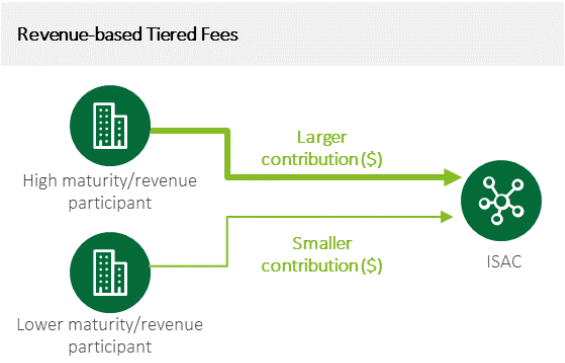


Consistent contributions from all participants enforces a philosophy that all participants are treated equally. This approach may not, however, reflect the relative size and resources of each participant, and thus to succeed must ensure fees are not prohibitively large for smaller players.

Transportation ISAC of Japan: standard annual fee model

Revenue-based Tiered Fees

The most common model internationally for securing ongoing ISAC funding is the revenue-based model. This model consists of the implementation of a tiered fee structure that reflects the annual revenue of each participant — e.g. an organisation that has an annual revenue less than <$100 million might be in Tier 1 which has a lower fee than Tier 2 that accommodates organisations with revenues between $100 million and $1 billion.



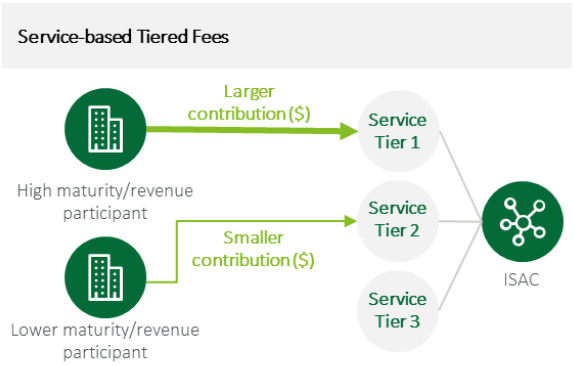
The advantage of this model is that is compatible with an 'All-Party' ISAC philosophy. This means that smaller participants are not excluded by prohibitively high fees that are designed to cater to organisation with larger cyber budgets. Instead, smaller participants that are more susceptible to cyber-attacks are incentivised to participate while larger parties play a proportionate role in uplifting the sector.

This 'All-Party' culture is an important factor that needs to be carefully managed. Without the appropriate strategic messaging, larger participants may feel they are carrying a disproportionate financial burden.

ONG-ISAC: revenue-based fee structure

Service-based Tiered Fees

Service-based funding is an emerging ISAC model that involves participants financially contributing to ISACs based on the services they consume. This is typically achieved through creation of service tiers (e.g. Gold, Silver, Bronze) in which services are packaged together and offered to ISAC participants on top of a number of core services that all participants are entitled to (e.g. CTI services).



This model enables participants to develop a tailored ISAC experience by only paying for the services they need.

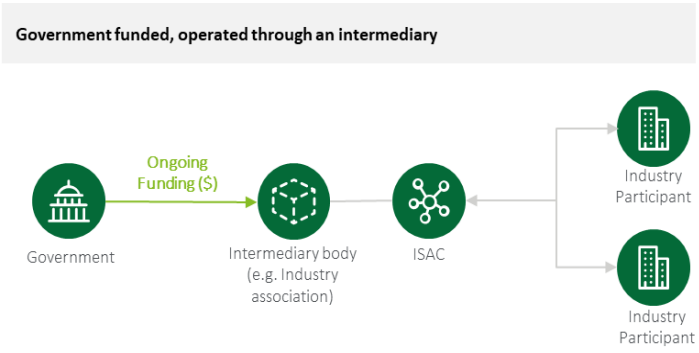
Space ISAC: service-based fee model

Smaller participants benefit from this model by accessing basic ISAC services at a more competitive price, while the ISACs continue to market exclusive or 'premium' offerings to larger participants.

This approach, however, needs to be tempered by offering core services like CTI sharing to all participants, to avoiding creating a 'pay-to-play' environment that sets critical services behind cost barriers.

Government funded, operated through an intermediary

In some contexts, it may be appropriate to consider an entirely government funded ISAC initiative like the U.S. Elections Infrastructure ISAC (EI-ISAC). One way this can be achieved is by funding an intermediary body to manage the setup and operations of an ISAC on behalf of the government. This option is commonly adopted by industries with pre-existing non-profit or advocacy bodies that facilitate public-private interaction.



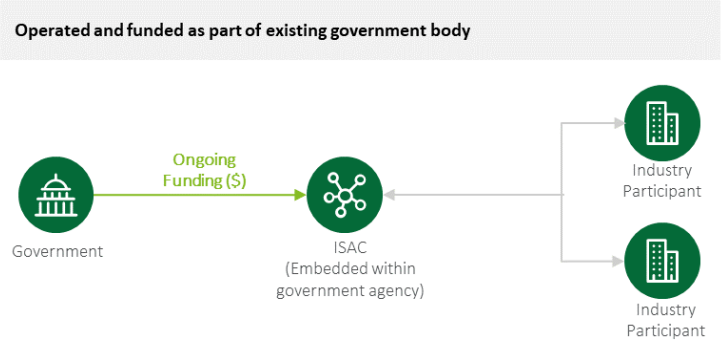
This model provides the advantage of a reliable government funding source that ensures an ISAC can maintain operations while simultaneously avoiding potential apprehensiveness that may come from industry sharing directly with government. This fosters a low barrier to entry that encourages an 'All-Party' culture among participants.

This approach does, however, place a significant cost on government; a cost that may be subject to the priorities of the government of the day.

Additionally, adopters of this model need to ensure that the low barrier to entry does not result in the ISAC being treated as "just another threat feed" to be passively consumed.

EI-ISAC: government funded

Operated and funded as part of existing government body



An alternative approach to establishing government funded ISAC models can be achieved by incorporating the ISAC function into an existing government body.

This approach combines the reliable government funding source with the legitimacy of a government-led initiative. In doing so, however, this approach potentially sacrifices the trust and open-collaboration that is traditionally more prevalent in industry-led initiatives.

For this reason, an entirely government funded and operated ISAC may only be appropriate for sectors with a high level of existing government integration.

ISACs in **Finland, Belgium & Taiwan** are government run and funded

Resourcing Models

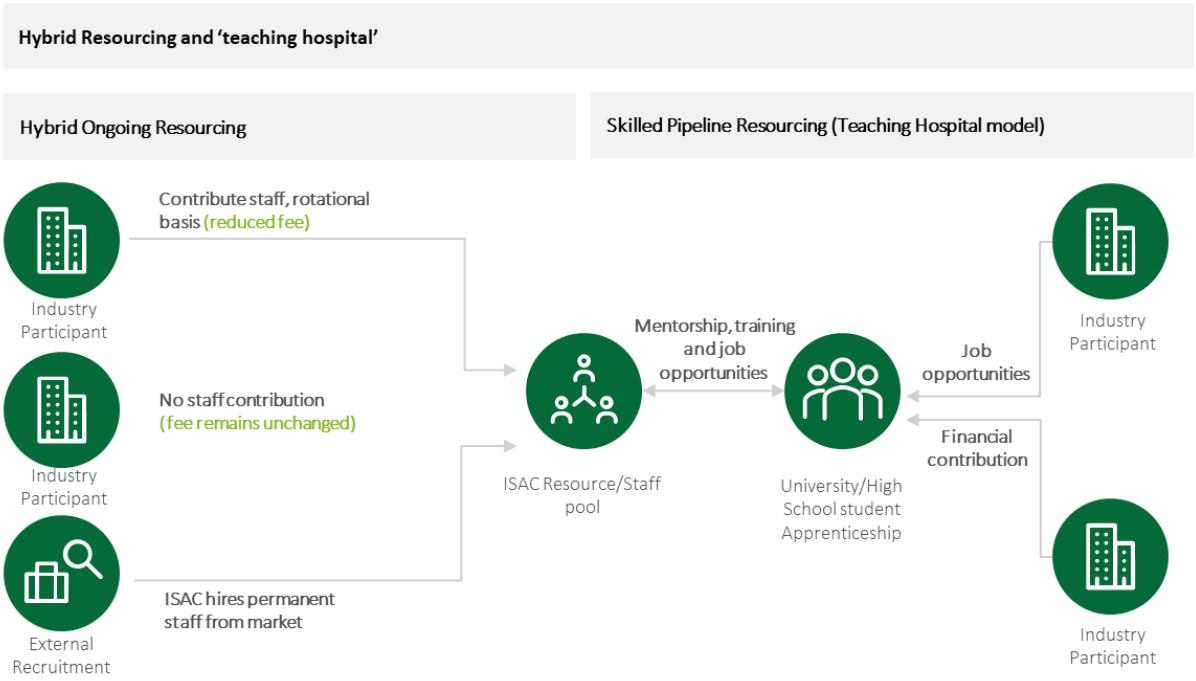
ISACs require a combination of highly technical CTI skilled personnel and business stakeholders to operate, manage participant relationships and market their benefits to prospective members. To meet these resourcing needs ISACs usually source staff either via voluntary contributions (e.g. secondments) from participation organisations or hire full-time permanent staff.

Given the cyber skills shortage, ISACs may also seek to incorporate the development of a skilled pipeline into their resourcing model.

Models	Benefits	Limitations
Hybrid Resourcing and 'Teaching Hospital model*	- Provides the benefits of both full-time and rotational staff - Provides additional funding options - Develops a more sustainable resource pipeline	- Potential disruptions to services as staff are rotated - Full-time employees and pipeline initiatives at an additional expense to the ISAC
Rotational/Voluntary Staff Contributions	- Reduces the ongoing costs of the ISAC - Enables the ISAC to build and maintain high levels of trust between participants	- Staff pool restricted to those personnel appointed/volunteered by participants which may lack required skills - Loss of continuity as resources are rotated between participants
Full-time Permanent Staff	- Full-time staff provide continuity and avoids the disruptions of a rotational approach - ISAC identify and access resources with specific required skills	- Stronger 'All-Party' culture, supporting smaller party participation - Larger parties play a proportionate role in uplifting the sector

**Deloitte recommended model*

Hybrid Resourcing and 'Teaching Hospital' Model



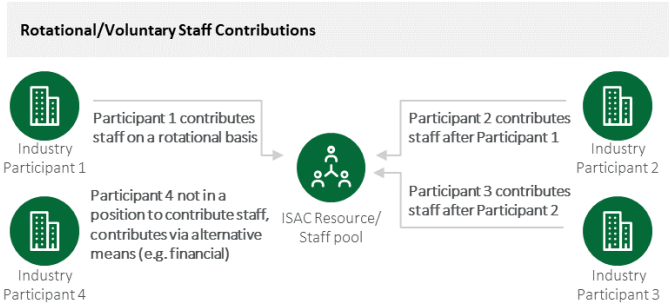
A hybrid ISAC resourcing model seeks to benefit from the advantages of both permanent and rotational resources within an ISAC. It is typically achieved by implementing several core roles resourced by permanent ISAC employees to ensure ongoing continuity while also leveraging voluntary staff in subject matter expert, analyst, and operational roles on a rotational basis.

This hybrid approach can be accompanied by a 'teaching hospital' skilled pipeline development model in which university and high school students are provided with mentorship, training and a potential job offer from the ISAC itself or an Industry participant.

MS-ISAC: 'teaching hospital' resourcing model

A funding model could be adjusted to support this model, potentially reducing the required fees for those who provide opportunities, work placements for trainees or contribute staff to the ISAC on a rotational basis.

Rotational/Voluntary Staff Contributions



One approach to resourcing an ISAC is to exclusively source personnel on a rotational or voluntary basis from participating industry members. This approach is commonly adopted by smaller industry groups will high levels of existing trust between participants.

This approach synergizes well with the needs of smaller industry groups as it has a more manageable ongoing cost compared to full-time staffing and provides a low barrier to entry for smaller participants.

The model is limited, however, in its ability to maintain knowledge and continuity across the ISAC as resources change. Additionally, it may be challenging to find resources with specific skills, as the staff pool is restricted to those personnel that are appointed/volunteered by their organisations.

Sharing initiatives between **Dutch banks** use a rotational resourcing model

Full-time Permanent Staff

ISAC resourcing can alternatively be achieved through hiring permanent staff from the market. This resourcing model is generally best suited for larger ISACs and requires ISAC administrators to independently identify required skills and personnel to achieve an ISAC's goals.

PT-ISAC: full-time resources

Full-time staffing models provide ISACs with greater continuity and avoids the disruptions associated with rotating staff between roles.

This approach also enables ISACs to plan and adapt their offerings and capabilities based on the needs of its partners rather than the skills of its volunteers. This of course comes at a great financial cost to ISAC operations.

Membership Eligibility

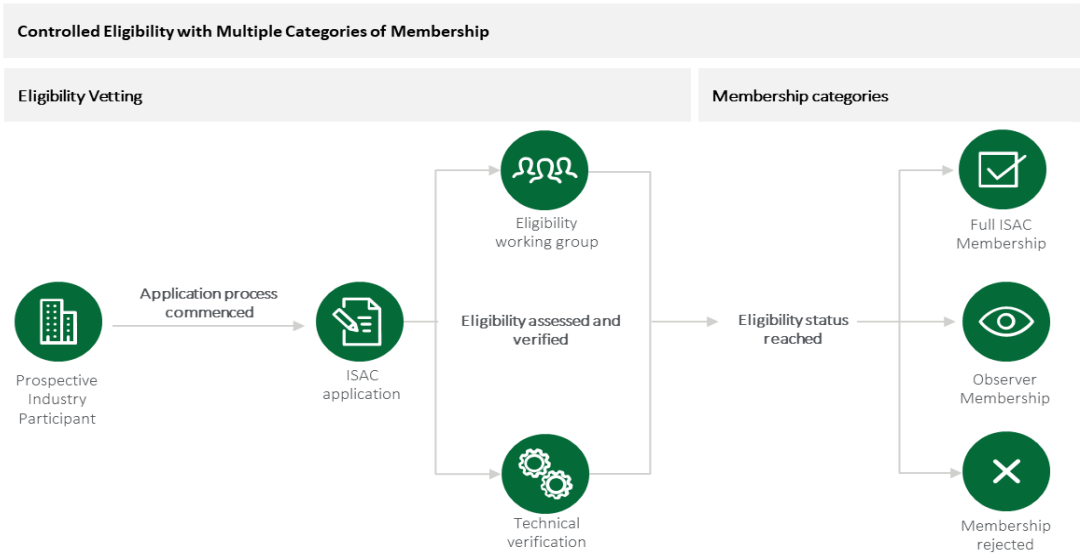
To foster and maintain a trusted community, ISACs often develop processes for determining participants eligibility. The vetting of prospective ISAC participants ensures organisations are joining a relevant ISAC and mitigates the risk of malicious actors from gaining access.

There is a large disparity between how different ISACs set and manage these membership eligibility requirements. Some ISACs have very broad, open categories for membership whereas others can be narrow, or even invite only.

Models	Benefits	Limitations
Controlled Eligibility with Multiple Categories of Membership*	- Vetting a smaller 'known group' aiding in the development of interpersonal trust - Support entities through additional membership categories	- Restrictive eligibility requirements may inadvertently exclude some organisations - Additional upfront burden on prospective participants
Controlled membership scope and eligibility	- Facilities a high trust environment, small group facilities interpersonal trust - Ongoing commitments to ISAC facilitate accountability	- Potentially excludes some organisations - Large commitment required from participants, initial and ongoing
Broad Membership Scope and Eligibility	- Large pool of participants generating a large quantity of CTI from diverse sources. - Inclusive, uplifts a large cross section of the industry	- Potentially easier for a malicious actor to gain access to ISAC membership/information - Manual vetting process, labour intensive

**Deloitte recommended model*

Controlled Eligibility with Multiple Categories of Membership

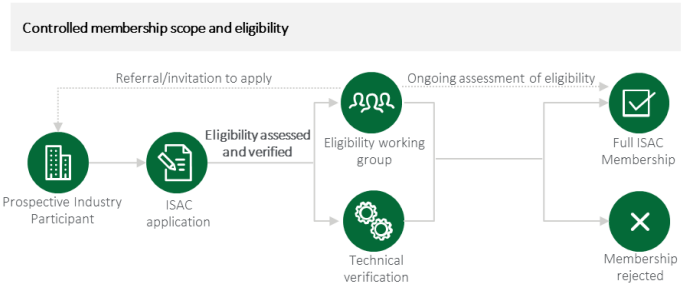


Within this model the eligibility of a prospective industry participant is vetted via both a controlled eligibility definition (e.g. assessed by a dedicated working group) and technical means (e.g. verification of the legitimacy of the email addresses used in the application).

Successful applicants are sorted into membership categories with varying levels of access and trust. This may include full membership for those participants directly involved in the industry and observer status for secondary or supporting entities. The advantage of this model is that an ISAC can develop a high trust environment, with a smaller 'known group' aiding in the development of interpersonal trust without excluding supporting entities in the secondary supply chain.

Transportation ISAC of Japan: membership category model

Controlled membership scope and eligibility



ISACs may seek to maintain trust and safeguard sensitive information by applying significant restrictions and controls to their eligibility and scope. This can be applied at the application level by restricting membership to invite-only or at the vetting level by implementing more rigorous verification assessments.

ER-ISAC: controlled eligibility model

This model facilitates a high trust environment for sharing and cooperation based on a small group of trusted and vetted participants.

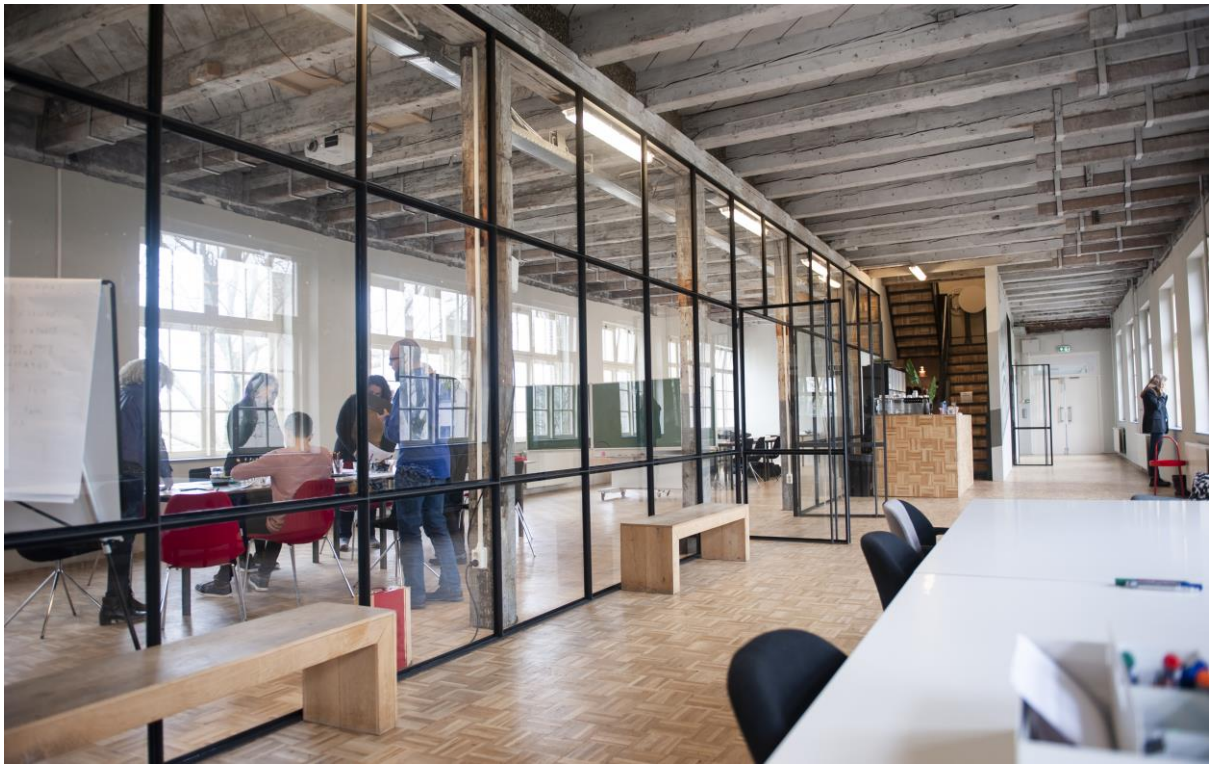
The approach may, however, exclude organisations with a legitimate claim to ISAC participation and therefore should be governed by clear eligibility guidelines.

Broad Membership Scope and Eligibility

One option is for ISAC membership eligibility requirements to be relatively broad, being open to a large section of entities in their industry. Some ISACs which have adopted this broad eligibility approach appear to use a lower effort intensive, human vetting process for assessing membership.

This approach tends to be more common among Industries with a broad range of stakeholders (Retail, Food and Grocery, Wholesale Trading). ISACs that implement this approach benefit from an inclusive and well-rounded participant pool that represents a greater cross-section of their supply chain. Additional measures and controls are often needed alongside this approach to ensure that malicious actors are unable to inappropriately gain ISAC membership.

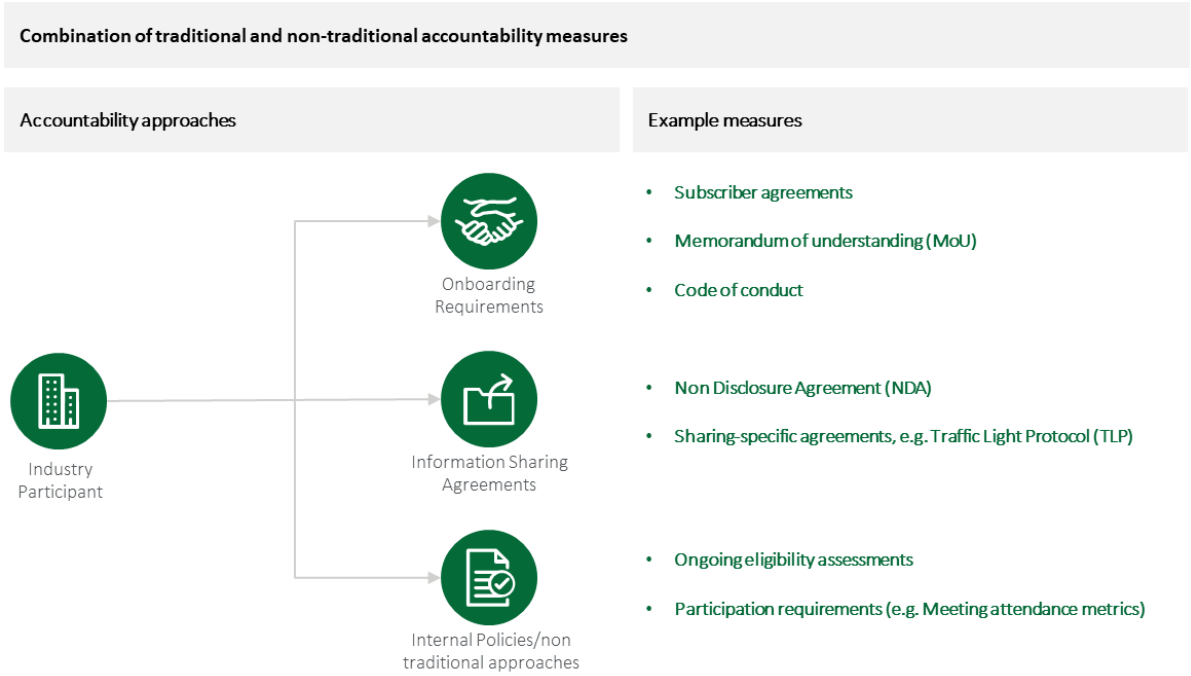
Retail and Hospitality ISAC:
broad membership scope



Accountability Models

Accountability measures, in the context of ISACs, are the activities that drive common approaches, behaviours and obligations among participants and create an environment of trust and integrity. Accountability measures should also ideally contribute to a culture of shared responsibility, in which industry participants feel a sense of obligation to act in the best interest of the ISAC.

Traditional and Non-Traditional Accountability Measures



ISACs are increasingly implementing broad accountability models that adopt multiple measures to maintain accountability at various stages of a participant's interaction with the ISAC. This includes formal agreements at the onboarding phase (e.g. subscriber agreements, MoU) and information sharing phase (e.g. NDA, TLP). This model also seeks to maintain accountability on an ongoing basis through internal policies (e.g. ongoing assessment).

The adoption of in-built accountability mechanisms ensures that participants can engage with an ISAC with reduced risk of inappropriate disclosure of sensitive information. This enshrines shared values and priorities among participants that is fostered over the life of the ISAC through ongoing measures.

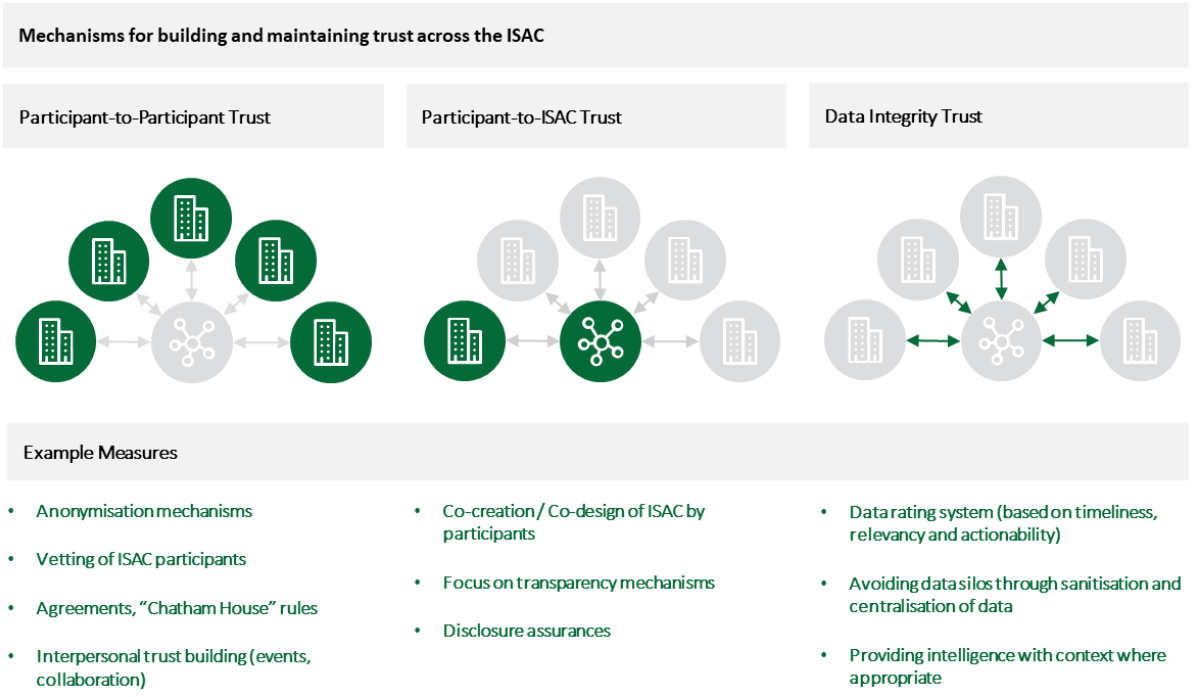
Auto-ISAC uses multiple accountability measures

Trust Models

Trust is a critical factor in the success of an ISAC. Without the appropriate levels of trust, participants may be unwilling to fully engage with ISAC, potentially inhibiting an ISAC's ability to perform its core intelligence sharing and cooperation functions.

ISAC operators internationally have sought to develop mechanisms to both establish the necessary levels of trust, and ensure this trust is maintained as the ISAC grows.

Mechanisms for Building and Maintaining Trust



A strong trust model views trust from multiple perspectives: participant to participant trust, participants to ISAC trust, and trust in the integrity of ISAC data. In recognition of these multiple layers of trust, a range of mechanisms are often required to ensure trust is built and maintained within an ISAC.

This includes integrating trust measures into an ISAC's development, vetting and onboarding processes, policies and legal agreements, and technical decisions regarding intelligence sharing and anonymisation.

SecureNed employs computational anonymisation (MPC)

Implementation Considerations

Recommendations for establishing an Australian ISAC approach

Recommendations

The cyber threat landscape is constantly evolving, and with the convergence of IT systems with operational technology (OT) systems, managing risk is becoming more complex for organisations. This complexity and limited resourcing make it almost impossible for organisations to maintain privacy, integrity and security of their environments.

Industries and governments alike are trying to find ways to collaborate to uplift the Australian cyber security resilience. Industry organisations are reaching out to their global counterparts to share information and are developing collaboration bodies as they try to find ways to work together to tackle this challenge.

Government has built a strong foundation through initiatives in the Security of Critical Infrastructure Act (SOCI), Australian Cyber Security Centre's (ACSC) Cyber Threat Intelligence Sharing (CTIS) ecosystem and other government engagement models.

Deloitte has reviewed the global landscape and engaged with several Australian organisations to uncover the capabilities and operational capabilities that Australian organisations can use to manage this dilemma.

Industry ISACs represent the next generation in the uplift of Australia's industry cyber resilience, and Australia is well placed to implement an all-hazards approach to industry ISACs

These industry ISACs will provide real world benefits to industry and government in Australia. To support this uplift in cyber resilience through the deployment of industry ISACs, Deloitte has provided the following recommendations:

Seed Funding

Deloitte identified that the most successful implementation model from our research started with a level of government seed funding. Noting that the research also found that the seed funding needed to be supported by a transition model to be supported by an operational funding model, whether that is self-funded, as most of the US ISAC models are, or continued government models, for those government operated ISACs.

Our belief is that for Industry ISACs within Australia to be truly successful, they should be industry owned and industry run, but they will need some level of kick-start funding from the government to ensure they successfully become the next generation in the uplift of Australia's industry cyber resilience.

Recommendation 1	Australian Government allocate funding to support industries in the implementation of their own Australian based ISACs

Australian focus

Deloitte's assessment provided coverage of the global landscape and a viewpoint of Australian industry, and from this we determined that for Australian industry ISACs to provide the benefits to the Australian economy that is expected, these bodies needed to be industry owned and industry run.

This doesn't mean that these Industry ISACs:

a) Won't engage with government. In fact, our assessment identified that one of the key drivers for these Industry ISACs is to support a simplified engagement with government.

b) Don't need seed funding from government. As previously mentioned, the success of the implementation of these bodies in a timely manner will be greatly improved should government provide this assistance.

c) Won't engage Internationally. In fact, Deloitte expects that the true value of these bodies will be based on providing an Australian industry viewpoint both into government and into the international industry landscape.

Recommendation 2	Australian industries should determine the scope of their Industry ISAC through industry and government engagement, maintaining an Australian lens on security resilience

Consolidation and re-use

Deloitte's assessment identified that there are some capabilities that exist today that an Industry ISAC may formalise. As such, Deloitte recommends that the approach to an ISAC doesn't have to be a "one-size-fits-all" model for all industries. Industries should identify what services they need, what existing capabilities can be re-used, and what capabilities need to be consolidated to ensure that their Industry ISAC is having the biggest impact to all industry organisations.

Recommendation 3	Consolidate, focus and re-use any existing sharing capabilities or forums that may already exist, possibly with a re-evaluation of their impact

All-Hazards

Australian industries, especially those in the critical infrastructure sectors, have new legislative requirements under the SOCI Act. Deloitte recommends that with the timing of that Act and the release of these new Australian Industry ISACs, the benefits of these ISACs will be wider spread, if they are designed with an All-Hazards approach.

Recommendation 4	Design Australian Industry ISACs with an All-Hazards approach

Rising tide lifts all boats

One of the greatest analogies to come out of Deloitte's partnership with ACSC in the delivery of CTIS is that ACSC wanted CTIS to support all maturity levels when it comes to CTI sharing, in other words, ACSC wanted CTIS to be the "rising tide that lifts all boats" through ensuring that any ACSC partner could participate within the CTIS community.

Deloitte recommends that Australian Industries take this approach when designing their specific sector's ISAC, and they should design the industry community to support all maturity levels within their sector. This way, the community can work together to build the resiliency of that industry.

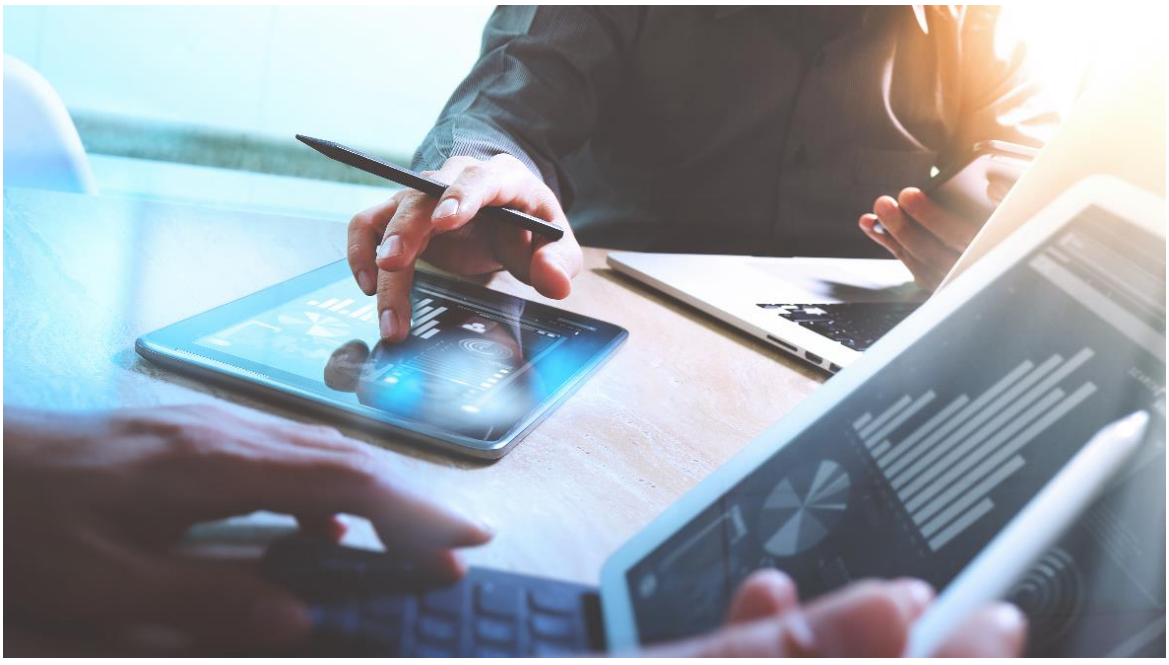
Recommendation 5	Design Australian Industry ISACs to support all maturity levels

Re-use lessons learnt

The ACSC CTIS program today is a strong example of a collaborative community that provides a subset of those services proposed to support Industry ISACs. This program has achieved this through great engagement throughout the implementation and operational phases. This has allowed the ACSC to develop great insights in co-design processes, lessons learnt and technology support, which could be invaluable in the initial implementation of Industry ISACs.

Deloitte recommends that ACSC consider packaging up these insights and making them available to industries that are wanting to undertake the journey towards Industry ISACs.

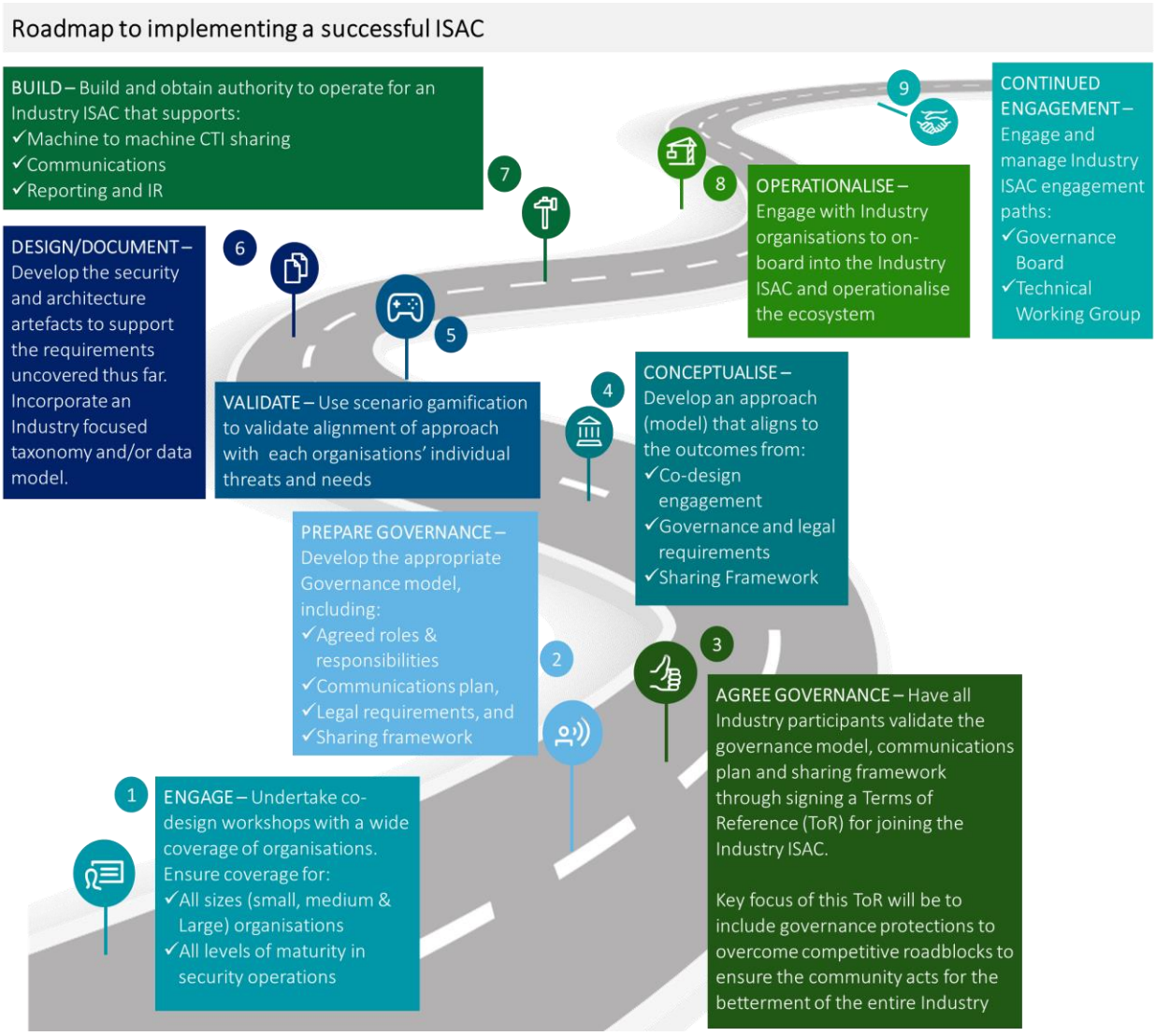
Recommendation 6	ACSC consider packaging up their CTIS insights and making them available to industries as they undertake the journey towards Industry ISACs



Co-design is key

The Australian Government's CTIS community has grown significantly in a relatively short timeframe, due in part to the fact that the government engaged industry with a co-design approach. Similar co-design approaches have been seen to succeed within national security and federal government programs both in Australia and Internationally. Accordingly, Deloitte recommends that as each industry initiates their development of an Industry ISAC, that they engage in a co-design approach and undertake several key steps along the journey towards implementing an Industry ISAC community.

Recommendation 7	Undertake co-design involving any relevant organisations within the industry, supply chain or government



Appendix

Case Studies and Lessons Learnt from International ISACs

Approach & Case Studies

Deloitte analysed and engaged with international ISACs to inform the findings of this research. This comprised of direct engagement and open-source analysis of over 50 international ISACs and equivalent information sharing communities across the United States, UK, EU, Canada, Japan, and Taiwan:

North America ISACs			
FS-ISAC – Financial Services	MT-ISAC – Maritime Transportation	E-ISAC – Electricity Industry	Water-ISAC – Water and Sanitation
S-ISAC – Space	ME-ISAC – Media and Entertainment	EASE – Energy Analytic Security Exchange	MFG-ISAC – Manufacturing
MS-ISAC – Multi-State (Local/State Government)	NEI – Nuclear	EI-ISAC – Elections Infrastructure	CyberShare – Broadband Internet
Auto-ISAC – Automotive	ONG-ISAC – Oil and Gas	Healthcare Ready	DNG-ISAC – Natural Gas
A-ISAC – Aviation	PT-ISAC – Public Transit	H-ISAC – Health	ChemISAC – Chemicals
NCC – Communications	RE-ISAC – Real Estate	IT-ISAC – Information Technology	MM-ISAC – Mining and Metals
ND-ISAC – Defence Industry	REN-ISAC – Research and Education	M-ISAC – Maritime	
EMR-ISAC – Emergency Services	RH-ISAC – Retail and Hospitality	SC-ISAC – Supply Chain	

Asia Pacific ISACs		Europe, the Middle East, and Africa ISACs	
ICT-ISAC – ITC Providers in Japan	OT-ISAC – Operational Technology Singapore	EE-ISAC – European Electricity	ITAIR- ISAC – Italian Airport ISAC
Financial ISAC Japan – Financial Services Japan	J-Auto-ISAC – Japan Automotive	ER-ISAC – European Rail	T-ISAC – Telecommunications
JE-ISAC – Electric Power Japan	Transport ISAC of Japan	EM-ISAC – European Maritime	UBF-ISAC/TASHARUKA – UAE Banks
F-ISAC Taiwan – Financial Services Taiwan	Software ISAC of Japan	14C+ – Cities ISAC	Africa-wide ISAC – Senegal
Japan Foreign Trade Council ISAC	Medical ISAC of Japan	EA-ISAC – European Aviation	SecureNed – Dutch Information sharing initiative

While all the identified ISACs contributed to the conclusions in this research, a select few provided particularly valuable lessons learnt and models. These have been captured as high-level case studies in the following section.

Public Transportation ISAC (PT-ISAC)

PT-ISAC forms part of a wider transport sector ISAC umbrella, including the Over the Road Bus (OTRB) and the Surface Transportation (ST) ISACs. This ISAC grouping functions as a clearinghouse for security-related information, providing transport-industry specific knowledge and dedicated analytical capabilities to participants. PT-ISAC maintains a high degree of integration with the US government as a financial patron, intelligence provider and facilitator. This has led to PT-ISAC being treated more as a useful threat feed than a sharing community.

Industry Alignment	US-based, aligned to 'Transportation Systems' critical infrastructure sector.
Membership Eligibility	Open eligibility model – extended globally. Participants manually verified.
Funding Structure	Funded by US government – American Public Transportation Association (APTA).
Resourcing	Fulltime staff employed – including analysts with top secret clearances and FBI/DoD experience.
Governance	Limited public information available. Indication that federal government are significant decision-makers.
Accountability	Lightweight model. Emphasis on unidirectional sharing means less focus on accountable participation.
Lessons Learnt	• Timely, actionable all-hazards intelligence: PT-ISAC is regarded as one of the best threat feeds as it provides timely, industry specific, all-hazards intelligence. It was praised for providing data faster than government agencies during a recent live shooting. • Unidirectional intelligence sharing: PT-ISAC shares by a "push" unidirectional approach. This method lacks timely input from participants but can collate open-source intelligence and share relevant data quickly. • Managing participant trust via "black box": PT-ISAC implements a "black box" model where trust is established between ISAC and participant only. Participants have no visibility of each other which means there is no "Sector Collaboration/Cooperation" or any kind of active participation services but adds a layer of confidence for sharing.

Multi-State ISAC (MS-ISAC)

MS-ISAC is a cybersecurity partner for over 13,000+ organisations in the US, with the goal to improve the overall cybersecurity posture of U.S. State, Local, Tribal, and Territorial (SLTT) government organisations through coordination, collaboration, cooperation, and increased communication. MS-ISAC's relationship with government is unlike any other ISAC in the US, where the involvement of DHS is a driver for success by establishing a high level of trust for sharing and active collaboration between government participants and non-government SME's. Participants can share directly with the MS-ISAC or omnidirectionally with each other via collaboration channels.

Industry Alignment	US-based, aligned to 'Government Facilities' critical infrastructure sector. Several public sectors represented – education, utilities, transport.
Membership Eligibility	All US SLTT government entities and private entities that are outsourced by government are eligible to join (including Fusion Centres and non-for-profits).
Funding Structure	No service fee to join. Funded by CISA and a division of Centre for Internet Security (CIS). Also generates revenue from paid services.
Resourcing	Predominantly resourced by permanent staff and contractors and supports working groups made up of volunteers. Invests in "teaching hospital" that works to improve cyber talent pipeline.
Governance	Structure includes Chair, Executive Committee and Executive Secretariat – all elected from ISAC participant entities. Also working groups and subcommittees to support specific activities.
Accountability	Formal agreements based on principles of Coordination, Collaboration, Communication and Cooperation.
Lessons Learnt	• Effective partnership with government: Part of the CIS (coordinate the use of the self-assessment tool - CIS CSAT) and has strong relationships with CISA and DHS. Limited constraints around competitiveness and allows all government levels to access information and have input into industry – such as identifying which schools could be targets for cyber-attacks. • 'Teaching hospital' training and cyber student initiatives: Students can join the SOC apprenticeship program where they can work and develop cyber security experience. MS-ISAC also participates in the US Cyber Challenge which includes Cyber Quests and Cyber Camps that allow students to work on activities, network and potentially receive employment.

Automotive ISAC (AUTO-ISAC)

Auto-ISAC is an industry-driven community to share and analyse intelligence about emerging cybersecurity risks to the vehicle industry. It includes light and heavy-duty vehicle OEMs, suppliers, and the commercial vehicle sector. The automotive industry is traditionally highly competitive; however, the Auto-ISAC has been described by Automotive Executives as "foundational" to collaboration and uplifting the cyber preparedness of the industry (Jeff Massimilla, General Motors, 2019). The success is largely due to the strong sense of accountability among participants to encourage trusted sharing.

Industry Alignment	US-based, aligned to 'Critical Manufacturing Sector' critical infrastructure sector.
Membership Eligibility	Global representation from participants across US, Europe, and Asia. Participants are manually verified using email addresses.
Funding Structure	Pricing varies depending on revenue of participant. Strategic Partnership Program for solution providers, associations, academia, and researchers
Resourcing	Light resourcing model with small number of fulltime CTI analysts and a director.
Governance	Board of Directors established initial framework and governance structure. Key participants elevated to governance positions overtime as ISAC grew.
Accountability	Ensuring fee structure encourages active participation. Formal documentation (NDA, internal policies) and enforcing meeting attendance and participation.
Lessons Learnt	• Fostering accountability among participants: Auto-ISAC uses legal policies and agreements paired with technical practices to ensure participants manage shared information consistently across the ISAC. There are also non-traditional polices to drive behavioural accountability – such as mandatory meeting attendance with penalties for lack of participation. • Building active participation through fee structure: Auto-ISAC implemented a tiered membership fee structure that participants would view as substantial and proportionate. This fostered a culture where participants felt accountable and encouraged actively sharing data. • Transitioning governance model: ISAC began using a flexible and ad hoc governance model where there was an inherent level of trust among a small participant pool. As the ISAC grew, the Auto-ISAC transitioned to a structured governance model where key industry participants were elevated into coordination positions.

Space ISAC (SPACE-ISAC)

Space-ISAC serves to facilitate collaboration across the global space industry to enhance sector ability to prepare for and respond to vulnerabilities, incidents, and threats. It also aims to disseminate timely and actionable information among participants; and to serve as the primary communications channel for the sector. The ISAC includes large and small-scale organisations involved with space sector or supply chain.

Industry Alignment	US-based, aligned to the global space sector.
Membership Eligibility	Largely open global eligibility model. Prospective participants manually verified.
Funding Structure	Tiered membership structure depending on organisation revenue.
Resourcing	15 founding participants allocate staff to manage Project Management Office that work together to resource the activities of the ISAC.
Governance	Board of Directors that include the founding participants and other ISAC participants can join on a rotational basis. Work with 18+ US Government agencies to determine future direction.
Accountability	Participants and US Government agencies hold each other and the Board of Directors accountable for decision making and quality of outputs.
Lessons Learnt	• Sectoral group leadership model: The Space-ISAC facilitates collaboration across the global space industry and aims to be the primary communications channel for the space sector. Due to the diverse supply chain and lack of space security professionals, information security can be a burden on some space organisations. The Space-ISAC has implemented a model that seeks to be the single source for data and analysis on space security and is able to reach all organisations, including those with tight resource channels. • Setting minimum security standards: The Space-ISAC focuses on using regulatory and financial tools to ensure basic cyber hygiene for all participants. The Space-ISAC works with government to establish minimum cybersecurity standards for space-critical infrastructure service providers – such as GPS or satellite technologies.

Japan Model (J-CISP and ISACs)

The Japanese government has developed a national information sharing ecosystem that comprises of both government and industry managed components. The Japan-Cyber Security Information Sharing Partnership (J-CSIP) is a government managed component that acts as an exchange hub for cyber incident information between participating organisations and 13 Special Interest Groups (SIGs) servicing specific critical industries. These government components are mirrored by Industry managed ISACs which also facilitate industry-specific intelligence sharing with varying degrees of integration with their SIG equivalents.

Industry Alignment	SIGs align to Japan's 13 defined critical infrastructure sectors and ISACs cover 8 industries (FS, ICT, Power, Transport, Auto, Software, Trade & Health).
Membership Eligibility	SIG membership is extended to Japanese organisations on an opt-in basis. ISAC eligibility varies between organisation, but generally involves manual verification.
Funding Structure	J-CSIP government run and funded. While some ISACs that interface with the J-CSIP ecosystem, are industry funded, largely through fee-based structures.
Resourcing	J-CSIP is government operated and staffed primarily by IPA employees. ISAC manage their own resourcing independently, often with full-time employed staff.
Governance	Japanese national intelligence sharing model sits within a multi-layered governance structure, including oversight from the IPA and the inter-agency Cybersecurity Strategic Headquarters.
Accountability	J-CSIP accountability is managed through non-disclosure agreements. While each ISAC manages accountability independently.
Lessons Learnt	• An integrated public-private ecosystem: The government managed J-CSIP program created 13 SIGs to directly consult and share with industry. Some of these SIGs provided opportunities for industry managed ISACs to integrate and consult with government run initiatives. This led to more effective dissemination of intelligence between the ecosystems and more direct lines of communication. • Avoiding confusion and maintaining clear points of contact: The Japanese ecosystem lacks a consistent one-to-one, government to industry mapping that may impede the timely dissemination of critical threat intelligence. Industries that do not have the SIG-ISAC integration lack a clear path for information sharing between J-CSIP to ISAC. It may be unclear due to the duplication in the ecosystem where a company should report an early indicator of compromise. The Japanese government has identified the key to avoiding confusion is establishing clearly defined information sharing flows.

Netherlands Financial Services Industry (ISACs and CERTs)

The Netherlands was one of the first adopters of the ISAC model outside of North America. As one of the most digitally mature nations in Europe, the Netherlands pioneered the implementation of industry-led intelligence sharing initiatives in the region. In particular, the Dutch financial services industry has a high concentration of intelligence sharing bodies, including both ISACs and CERTs. This case study will consider the approach to ISACs, and other ISAC-like initiatives adopted by the Dutch financial services industry.

Industry Alignment	ISACs and CERTs support organisations that provide banking services, electronic transfers between banks and the public.
Membership Eligibility	Eligibility requirements vary across the industry, however some ISACs and CERTs require a Dutch banking licence to verify eligibility.
Funding Structure	Some intelligence sharing initiatives are facilitated by government (e.g. NCSC) and are free to participate, however most are fee-based initiatives (e.g. FI-ISAC).
Resourcing	Resourcing models vary across the industry, including hybrid models which involved both permanent hires and participant resource contributions.
Governance	Governance models vary across the industry, however most ISACs and CERTs were governed by participants on a rotational basis.
Accountability	While there is no one approach to accountability across the industry, many of the examined ISACs and CERTs identified trust through interpersonal relationships as key to engagement and good will.
Lessons Learnt	• Applying a domestic lens to build relevancy: ISACs and CERTs developed intelligence sharing initiatives that were specific to the digital maturity of the Netherlands cyber landscape. This meant intelligence was directly relevant to the Dutch market and built a sense of community among the financial industry that encouraged active sharing. • Interpersonal relationships as foundational to ISAC trust: An intelligence sharing initiative was operated by the CTI teams of 3 major banks that had strong personal relationships with each other. The sharing was strong at first, but it was very 'people-dependent' which meant as the people changed and transitioned, so too did the appetite for sharing. • Representation from the correct staff and stakeholders: ISAC participants were overrepresented by business and managerial level staff as opposed to 'on the ground' cyber practitioners. This led to an ISAC that was primarily concerned with compliance and struggled to disseminate intelligence to the right stakeholders during an incident.

Reference List

[1] Bill Clinton, *Presidential Decision Directive 63 (PDD-63): Protecting America's Critical Infrastructures §*. Washington D.C.: Office of the Press Secretary, 1998.

Elaine M Sedenberg and James X Dempsey. "Cybersecurity Information Sharing Governance Structures: An Ecosystem of Diversity, Trust, and Tradeoffs." In *Rewired: Cybersecurity Governance*, edited by Ryan Ellis and Vivek K Mohan. Hoboken, NJ: John Wiley & Sons, Inc., 2019.

[2] Department of Homeland Security. *Critical Infrastructure Threat Information Sharing Framework A Reference Guide for the Critical Infrastructure Community*. Washington, D.C.: Department of Homeland Security, 2016.

Department of Homeland Security. *U.S. Department of Homeland Security Cybersecurity Strategy*. Washington D.C.: Department of Homeland Security, 2018.

Gary C Peters. Bill, *Strengthening American Cybersecurity Act of 2022 §. S.3600.* Washington D.C.: Congress of the United States of America, (2022).

[3] Committee on Financial Services and Consumer Credit. "Protecting Critical Infrastructure: How the Financial Sector Addresses Cyber Threats" Hearing before the *Subcommittee on Financial Institutions and Consumer Credit*. Washington D.C. U.S. House of Representatives, 2015.

Faye Francy. "The Aviation Information Sharing and Analysis Center (A-ISAC)" Conference Paper in *2015 Integrated Communication, Navigation, and Surveillance Conference (ICNS)*. Herndon, Virginia, 2015.

National Cyber Security Centre (The Netherlands). *Starting an ISAC: Sectoral Collaboration*. The Hague: Ministry of Justice and Security, 2018.

National Institute of Standards and Technology. *Success Story: Multi-State - Information Sharing and Analysis Center*. Gaithersburg, MD: NIST, 2021.

Robert Dacey. "Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors" Statement before *Subcommittees on Cybersecurity, Science, and Research & Development and Infrastructure and Border Security, and Select Committee on Homeland Security*. Washington D.C.: United States General Accounting Office, 2004.

Stefan Soesanto. *Cyber Defence Report: Japan's National Cybersecurity and Defense Posture.* Cyber Defense Project (CDP) Center for Security Studies (CSS) ETH Zürich, 2020.

Tarek Gaber, Yassine El Jazouli, Esraa Eldesouky, and Ahmed Ali. "Autonomous Haulage Systems in the Mining Industry: Cybersecurity, Communication and Safety Issues and Challenges" *Electronics* 10, no. 11: 1357, 2021.

[4] Financial Services Information Sharing and Analysis Center (FS-ISAC). *Whitepaper: Appropriate Software Security Control Types for Third Party Service and Product Providers*. FS-ISAC, Third-Party Software Security Working Group. Undated.

Kathleen M. Moriarty. *ISACs' Possible Role in Software Supply Chain Assurance*. East Greenbush, New York: Center for Internet Security, 2022.

[5] Mishra, Alok, Yehia Ibrahim Alzoubi, Memoona Javeria Anwar, and Asif Qumer Gill. "Attributes Impacting Cybersecurity Policy Development: An Evidence from Seven Nations." *Computers & Security* 120, 2022.

[6] Donald Trump. *Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems*. Washington D.C.: Office of the Press Secretary, 2020.

Erin Miller. *Space ISAC Releases Statement on SPD-5: Comprehensive Space Cybersecurity Principles Released by White House*. Colorado Springs, Colorado: Space-ISAC, 2020.

[7] Gregory Falco. "Cybersecurity Principles for Space Systems." *Journal of Aerospace Information Systems* 16, no. 2, 2019.

[8] Electricity Information Sharing and Analysis Center (E-ISAC). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Washington D.C.: E-ISAC, 2016.

Electricity Information Sharing and Analysis Center. "Join the E-ISAC." E-ISAC *Website*, 2022. https://www.eisac.com/s/join-the-eisac

Tania Wallis and Rafał Leszczyna. "EE-ISAC—Practical Cybersecurity Solution for the Energy Sector" *Energies* 15, no. 6: 2170, 2022.

[9] Department of Homeland Security. *Chemical Security Analysis Center Brief*. Washington D.C.: Department of Homeland Security: Science and Technology Directorate, 2022.

[10] ENISA. *Information Sharing and Analysis Centres (ISACs) Cooperative models*. Athens: European Union Agency For Network and Information Security, 2018.

Denise Anderson. "Testimony of Denise Anderson On Behalf of The National Health Information Sharing & Analysis Center and the National Council of Information Sharing and Analysis Centers" Before the *Committee on Energy and Commerce Subcommittee on Oversight and Investigations*. Washington D.C.: United States House of Representatives, 2017.

Mathew, Ashwin J, and Coye Cheshire. *A Fragmented Whole: Cooperation and Learning in the Practice of Information Security*. Berkeley: Packet Clearing House (PCH), 2018.

[11] Stefan Soesanto. *Cyber Defence Report*, 2020.

Deloitte.

Authors

Trevor Hancock
Specialist Director – Cyber
Deloitte Canberra

Amani Ibrahim
Senior Manager – Cyber
Deloitte Melbourne

Harrison Rule
Manager – Cyber
Deloitte Canberra

Joachim (Jo) Copeland
Senior Analyst – Cyber
Deloitte Canberra

About Deloitte

Deloitte was ranked #1 globally in Security Consulting by Gartner, for multiple years. We have helped some of the largest and highly regulated companies in the world be Secure, Vigilant and Resilient in the face of ever-changing threat landscape.

We have 5,500+ cyber risk professionals worldwide who specialize in various cyber risk domains. We bring the best athletes to the game by combining our cyber risk subject matter knowledge along with our government experience.

Deloitte.

About this publication