RSA Conference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID:

3rd-Party Cyber-Risk Mitigation by Using ISO Standards

What is ISO? Who is ISO? What are International Standards?

What is ISO? Who is ISO? What are International Standards?

ISO (International Organization for Standardization) is a worldwide federation of national standards bodies and is nongovernmental organization that comprises standards bodies from more than 160 countries

- American National Standards Institute → United States
- Singapore Standards Council → Singapore
- Bureau of Indian Standards → India
- British Standard Institution → UK

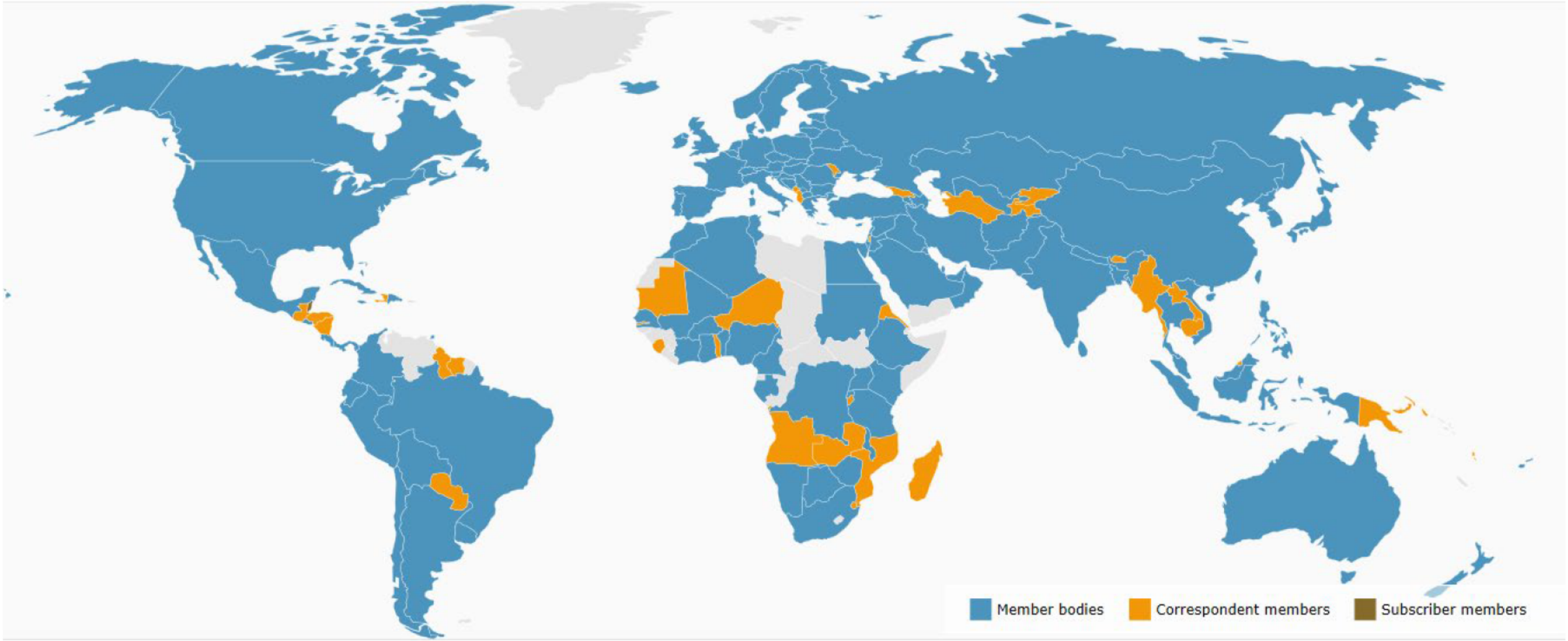
What is ISO? Who is ISO? What are International Standards?

ISO is not an abbreviation. It is a word, derived from the Greek *isos*, meaning "equal," which is the root for the prefix *iso-* that occurs in a host of terms, such as

- ***Isometric***
- ***Isonomy***
- ***Isobar***
- ***Isogenic***

“ISO” is used globally to denote the organization, avoiding varies abbreviations that would result from the translation of "International Organization for Standardization" into the different.

What is ISO? Who is ISO? What are International Standards?

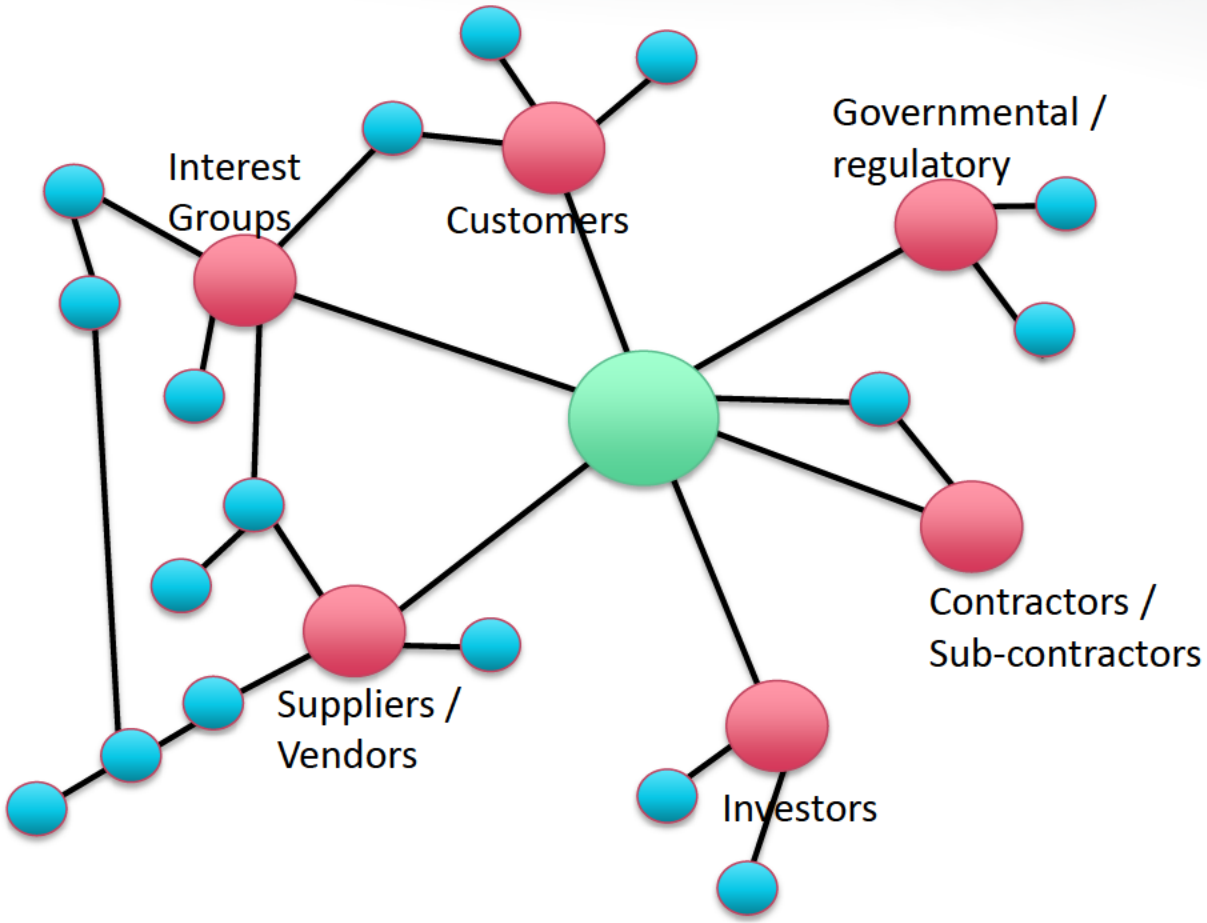


RSAConference2020 APJ

A Virtual Learning Experience

3rd parties

3rd parties



- The relationships of 3rd parties has become increasingly complex and interconnected
- IT systems are interconnected with a variety of 3rd parties
- Connections are not limited to 1 level
- Any of this external parties are subject to Cyber-Risk

RSAConference2020 APJ

A Virtual Learning Experience

ISO 31000:2018
Risk Management

ISO 31000:2018

- Risk Management
- For organizations of all types and sizes
- Managing risk is iterative
- The standard and assists organizations in setting strategy, achieving objectives and making informed decisions
- Guidance document, not certifiable

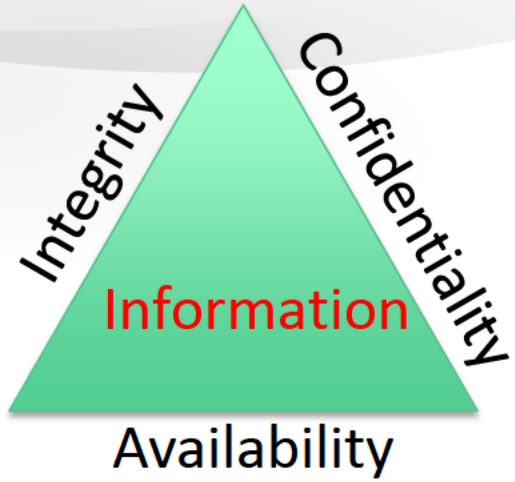
RSAConference2020 APJ

A Virtual Learning Experience

ISO 27001:2017
Information Security

ISO 27001

Risks address confidentiality, integrity and availability



Describes requirements for an information security management system (ISMS).

The establishment and implementation of the ISMS is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization.

The ISMS gives confidence to interested parties that risks are adequately managed.

The ISMS is integrated with the organization's processes and overall management structure.

It is expected that an information security management system implementation will be scaled in accordance with the needs of the organization.

What is ISO/IEC 27001?

Business Issue	How ISO/IEC 27001 helps	Benefits to your organization
 Reputation	Risk identification Establishment of procedures Continual Improvement	Improved reputation Stakeholder confidence Trust building
 Engagement	Knowing stakeholders Communicate policy Top Management	Improved InfoSec awareness Demonstrate Management Commitment
 Compliance	Framework for requirements Review / communicate requirements	Reduced likelihood of legal issues
 Risk management	Assess risks continuously Mitigating controls	Cost saving due to minimized risk Improved CIA posture

What is ISO/IEC 27001? How does it work ?

- ISO/IEC 27001 published in 2017
- Based on the high level structure (Annex SL), common framework for all ISO management system standards
- Annex SL encourages incorporating Information Security Management System (ISMS) into business processes and therefore involvement from senior management.
- ISO 27001 addresses explicitly information security (cyber risks) in Supplier relationships

ISO/IEC 27001 – Supplier Relationship

- Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.
- Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.
- Organizations shall regularly monitor, review and audit supplier service delivery.

RSAConference2020 APJ

A Virtual Learning Experience

ISO 22301
Business Continuity

ISO 22301

- Risks addressed in 22301: very generic: “disruption”
- This standard specifies the structure and requirements a business continuity management system (BCMS)
- The outcomes of maintaining a BCMS are shaped by the organization’s legal, regulatory, organizational and industry requirements, products and services provided, processes employed, size and structure of the organization, and the requirements of its interested parties.

ISO 22301 --- Business impact analysis (BIA) and Risk Assessment

- The organization shall use the process for analyzing business impacts to determine business continuity priorities and requirements. The process shall …. determine the dependencies, including partners and suppliers, and interdependencies of prioritized activities.
- The organization shall implement and maintain a risk assessment process and the organization shall:
  - identify the risks of disruption to the organization's prioritized activities and to their required resources;
  - analyze and evaluate the identified risks;
  - determine which risks require treatment.

ISO 22301

With the Business Continuity Management standard, ISO 22301, you will have the framework for assessing critical suppliers and their associated risks, assessing current business practices, and planning contingency measures.

Do not let your business suffer from the unexpected. In today's fast-moving world where supply chains are often complex, the management of business risk is vital for the success of your business; therefore, it is vital that you understand and prioritize threats to your business.

DEFINITION ORGANIZATIONAL RESILIENCE

- **Organizational Resilience** is the ability and capacity of a corporation to withstand potential significant economic / systemic risk or systematic discontinuities or business interruption, by adapting or recovering or resisting being affected and resuming its (core) operations to continue to provide an acceptable level of functioning and structure.
- A resilient organization is able to adapt and align its strategy, operations, management systems, governance structure, supply chain, etc, quickly to significantly changing environments.

Every organization is connected with their suppliers IT systems --- how to you send EDI (Electronic Data Interchange) to your suppliers? – How do you receive ASNs (advance shipping notifications) from your suppliers?

Moving towards resilience / increasing resiliency

Major industries (Automotive / Aerospace) require their suppliers to address continuity of service / delivery even in case serious incidents or events.

Upcoming new additional requirements are even more stringent and require a formal assessment of the supplier's information security / information resilience program.

Refer to ISO 22316, *Organizational resilience – Principles and attributes*, provides a framework to help organizations future-proof their business, detailing key principles, attributes and activities that have been agreed on by experts from all around the world.

RSAConference2020 APJ

A Virtual Learning Experience

Conclusion

Conclusion and Summary

Standard	Title	Comment
31000:2018	**Risk management**	**Guidelines**
27001:2017	**Information security management system**	**Certification** possible
22301:2019	**Business continuity management systems**	**Certification** possible
22316:2017	**Organizational resilience**	**Guidelines**

Both, 22301 and 27001 are certifiable standards, using **a risk based approach** and include the requirements to review and manage **3rd party risks**.

Next steps

Apply What You Have Learned Today

- Next week you should:
  - Identify the top 10 critical 3rd parties your organization is dealing with
  - Review the content of ISO 31000, ISO 27001, ISO 22301 and ISO 22316
- In the first three months following this presentation you should:
  - Understand what these 3rd parties interaction with your organization is and how their vulnerabilities may affect you
  - Identify the risk associated with these 3rd parties
  - Define suitable controls dealing with these 3rd party risks
- Within six months you should:
  - Define and implement a process which allows for a proactive review of all 3rd parties
  - Determine a timeline for the risk based assessment of your 3rd parties

Speaker Information

Willy Fabritius
Global Head InfoSec & Business Continuity
Willibert.Fabritius@bsigroup.com

https://www.linkedin.com/in/fabritius