Cybersecurity – the new requirement for Quality

The significance of the Information Security Management System (ISMS) to support your Quality Management System (QMS)

Knowledge Solutions

October 2023

SGS

Part number 5 10 23
not May-10-2023
Or…..
Is it 5th Oct 2023 ?

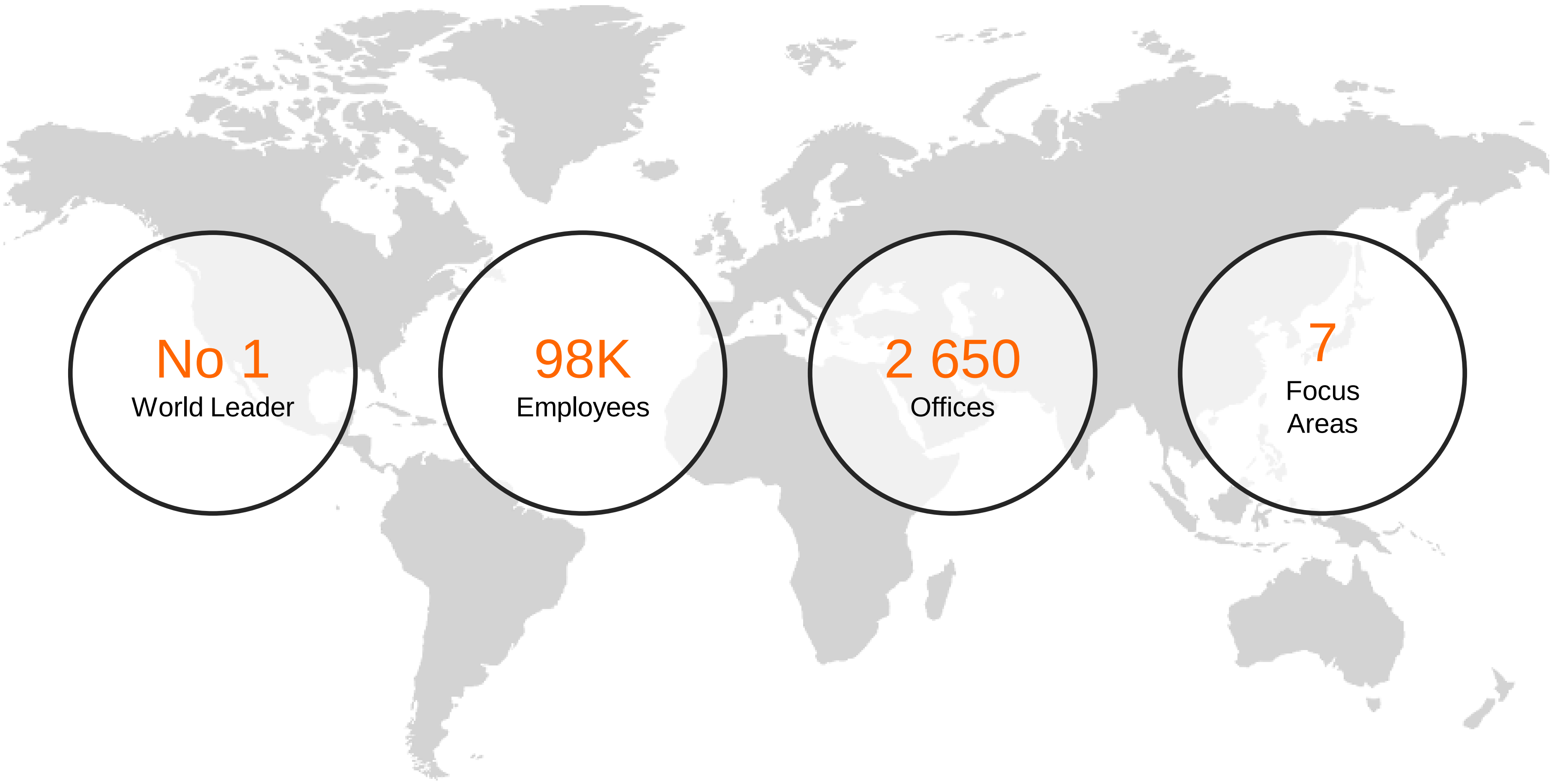
Quick Look: 3rd-Party Cyber-Risk Mitigation by Using ISO Standards	How Information Security and Business Continuity are Linked (w/ Willy Fabritius) - YouTube	
Quick Look: 3rd-Party Cyber-Risk Mitigation by Using ISO Standards	Quick Look: 3rd-Party Cyber-Risk Mitigation by Using ISO Standards - YouTube	
Minimizing Cyber-attack Impacts: Digital Supply Chain Management	Minimizing Cyber-attack Impacts: Digital Supply Chain Management (w/ Willy Fabritius) - YouTube	

Willy Fabritius,

Global Head Strategy / Business Development

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

SGS IN BRIEF



No 1
World Leader

98K
Employees

2 650
Offices

7
Focus
Areas

Our History

1878

SGS is founded

Mid 20th Century

Diversified into inspection, testing and verification services

1981

Listed on the Swiss Stock Exchange

Today

140+ years in business

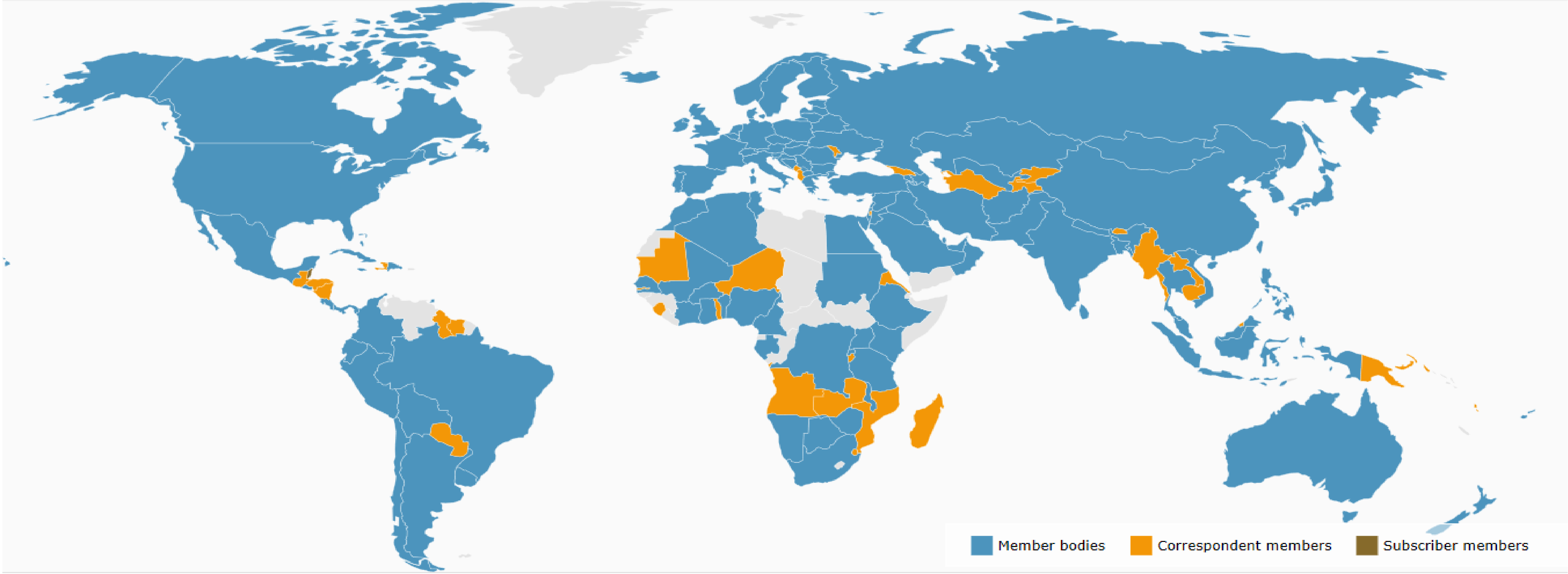
What is ISO? Who is ISO?
From the Greek word ίσος (isos): isos means equal
What are international standards?

ISO (International Organization for Standardization)
is a worldwide federation of national standards bodies.
ISO is a nongovernmental organization that comprises standards bodies from more than 160 countries, with one standards body representing each member country.

- American National Standards Institute (ANSI) for example, represents the United States.
- Singapore Standards Council (SSC) represents Singapore
- Department of Standards Malaysia represents Malaysia
- Bureau of Indian Standards (BIS) represents India
- Deutsches Institut für Normung (DIN) represents Germany

Member organizations collaborate in the development and promotion of international standards for technology, scientific testing processes, working conditions, societal issues and more. ISO and its members then sell documents detailing these standards.
A General Assembly, which consists of representatives from ISO members and elected leaders called principal officers, acts as the decision-making body for ISO. The organization has its headquarters in Geneva, Switzerland, where a central secretariat oversees operations.

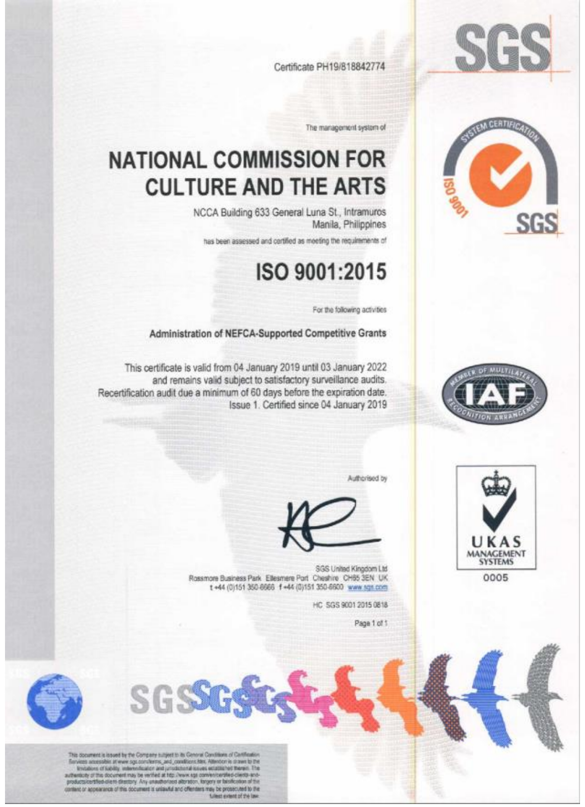
What is ISO? Who is ISO? What are international standards?



GLOBAL STANDARDS

Standard	Title
ISO/IEC 27001:2013	Information security management systems — Requirements
ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems — Requirements
ISO/IEC 27701:2019	Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
ISO 22301:2019	Security and resilience — Business continuity management systems — Requirements
CSA cloud security alliance®	Security, Trust, Assurance, and Risk (STAR) assessment and certification for both cloud provider and cloud consumers (customers) based on the Cloud Security Alliance (CSA) framework
TISAX®	TRUSTED INFORMATION SECURITY ASSESSMENT EXCHANGE Initiated by the German Car Industry

EXAMPLE OF ISO MANAGEMENT SYSTEM CERTIFICATES



Certificate PH19/818842774

The management system of

NATIONAL COMMISSION FOR CULTURE AND THE ARTS

NCCA Building 633 General Luna St., Intramuros
Manila, Philippines

has been assessed and certified as meeting the requirements of

ISO 9001:2015

For the following activities

Administration of NEFCA-Supported Competitive Grants

This certificate is valid from 04 January 2019 until 03 January 2022 and remains valid subject to satisfactory surveillance audits. Recertification audit due a minimum of 60 days before the expiration date. Issue 1. Certified since 04 January 2019

Authorised by

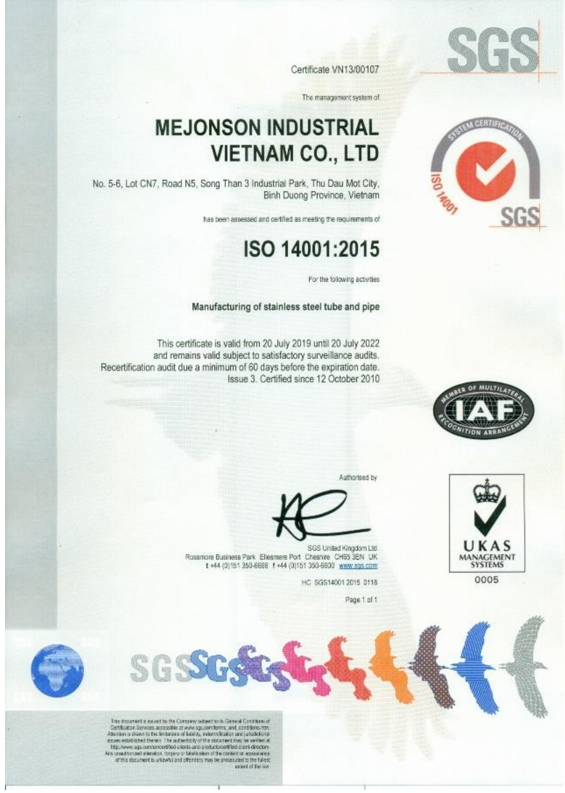
SGS United Kingdom Ltd
Rossmore Business Park Ellesmere Port Cheshire CH65 3EN UK
t +44 (0)151 350-6666 f +44 (0)151 350-6600 www.sgs.com

HC SGS 9001 2015 0818

Page 1 of 1

This document is issued by the Company subject to its General Conditions of Certification Services accessible at www.sgs.com/terms_and_conditions.htm. Attention is drawn to the limitations of liability, indemnification and jurisdictional issues established therein. The authenticity of this document may be verified at http://www.sgs.com/en/certified-clients-and-products/certified-client-directory. Any unauthorized alteration, forgery or falsification of the content or appearance of this document is unlawful and offenders may be prosecuted to the fullest extent of the law.

SGS
SYSTEM CERTIFICATION
ISO 9001
SGS
MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT
IAF
UKAS
MANAGEMENT SYSTEMS
0005
SGS



Certificate VN13/00107

The management system of

MEJONSON INDUSTRIAL VIETNAM CO., LTD

No. 5-6, Lot CN7, Road N5, Song Than 3 Industrial Park, Thu Dau Mot City,
Binh Duong Province, Vietnam

has been assessed and certified as meeting the requirements of

ISO 14001:2015

For the following activities

Manufacturing of stainless steel tube and pipe

This certificate is valid from 20 July 2019 until 20 July 2022 and remains valid subject to satisfactory surveillance audits. Recertification audit due a minimum of 60 days before the expiration date. Issue 3. Certified since 12 October 2010

Authorised by

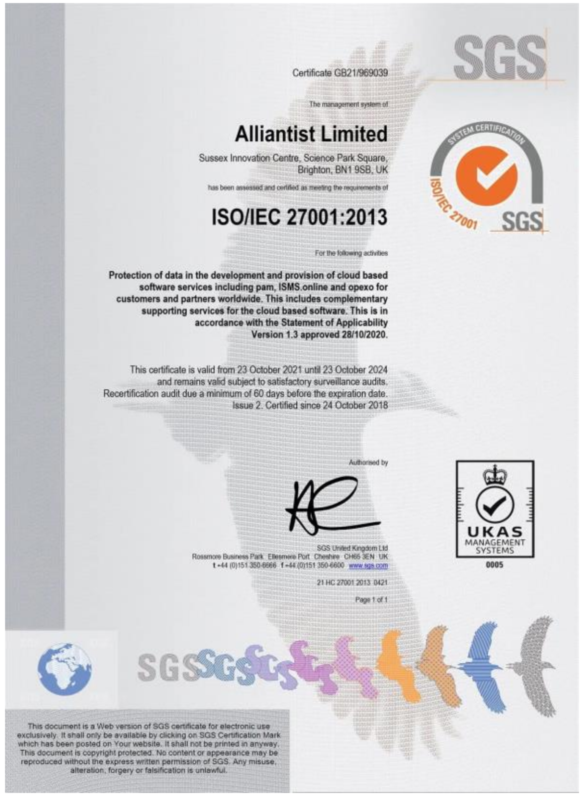
SGS United Kingdom Ltd
Rossmore Business Park Ellesmere Port Cheshire CH65 3EN UK
t +44 (0)151 350-6666 f +44 (0)151 350-6600 www.sgs.com

HC SGS14001 2015 0118

Page 1 of 1

This document is issued by the Company subject to its General Conditions of Certification Services accessible at www.sgs.com/terms_and_conditions.htm. Attention is drawn to the limitations of liability, indemnification and jurisdictional issues established therein. The authenticity of this document may be verified at http://www.sgs.com/en/certified-clients-and-products/certified-client-directory. Any unauthorized alteration, forgery or falsification of the content or appearance of this document is unlawful and offenders may be prosecuted to the fullest extent of the law.

SGS
SYSTEM CERTIFICATION
ISO 14001
SGS
MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT
IAF
UKAS
MANAGEMENT SYSTEMS
0005
SGS



Certificate GB21/969039

The management system of

Alliantist Limited

Sussex Innovation Centre, Science Park Square,
Brighton, BN1 9SB, UK

has been assessed and certified as meeting the requirements of

ISO/IEC 27001:2013

For the following activities

Protection of data in the development and provision of cloud based software services including pam, ISMS.online and opexo for customers and partners worldwide. This includes complementary supporting services for the cloud based software. This is in accordance with the Statement of Applicability Version 1.3 approved 28/10/2020.

This certificate is valid from 23 October 2021 until 23 October 2024 and remains valid subject to satisfactory surveillance audits. Recertification audit due a minimum of 60 days before the expiration date. Issue 2. Certified since 24 October 2018

Authorised by

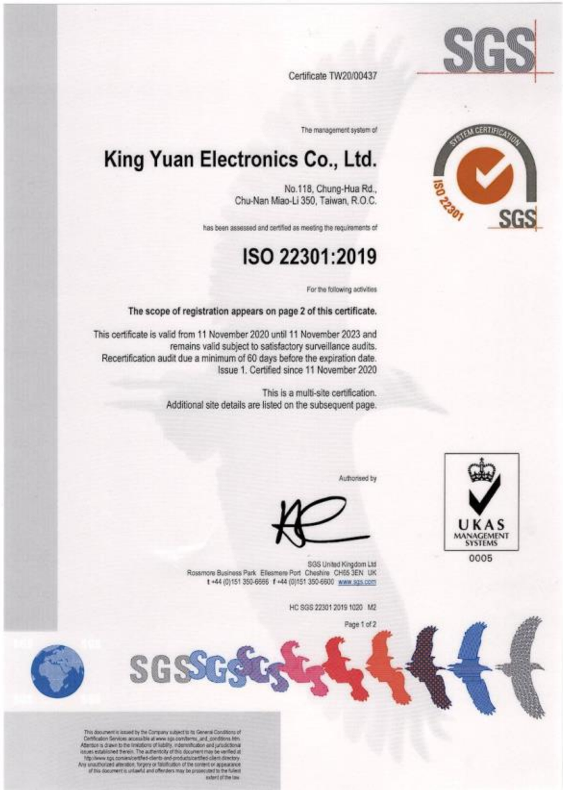
SGS United Kingdom Ltd
Rossmore Business Park Ellesmere Port Cheshire CH65 3EN UK
t +44 (0)151 350-6666 f +44 (0)151 350-6600 www.sgs.com

21 HC 27001 2013 0421

Page 1 of 1

This document is a Web version of SGS certificate for electronic use exclusively. It shall only be available by clicking on SGS Certification Mark which has been posted on Your website. It shall not be printed in anyway. This document is copyright protected. No content or appearance may be reproduced without the express written permission of SGS. Any misuse, alteration, forgery or falsification is unlawful.

SGS
SYSTEM CERTIFICATION
ISO/IEC 27001
SGS
UKAS
MANAGEMENT SYSTEMS
0005
SGS



Certificate TW20/00437

The management system of

King Yuan Electronics Co., Ltd.

No.118, Chung-Hua Rd.,
Chu-Nan Miao-Li 350, Taiwan, R.O.C.

has been assessed and certified as meeting the requirements of

ISO 22301:2019

For the following activities

The scope of registration appears on page 2 of this certificate.

This certificate is valid from 11 November 2020 until 11 November 2023 and remains valid subject to satisfactory surveillance audits. Recertification audit due a minimum of 60 days before the expiration date. Issue 1. Certified since 11 November 2020

This is a multi-site certification.
Additional site details are listed on the subsequent page.

Authorised by

SGS United Kingdom Ltd
Rossmore Business Park Ellesmere Port Cheshire CH65 3EN UK
t +44 (0)151 350-6666 f +44 (0)151 350-6600 www.sgs.com

HC SGS 22301 2019 1020 M2

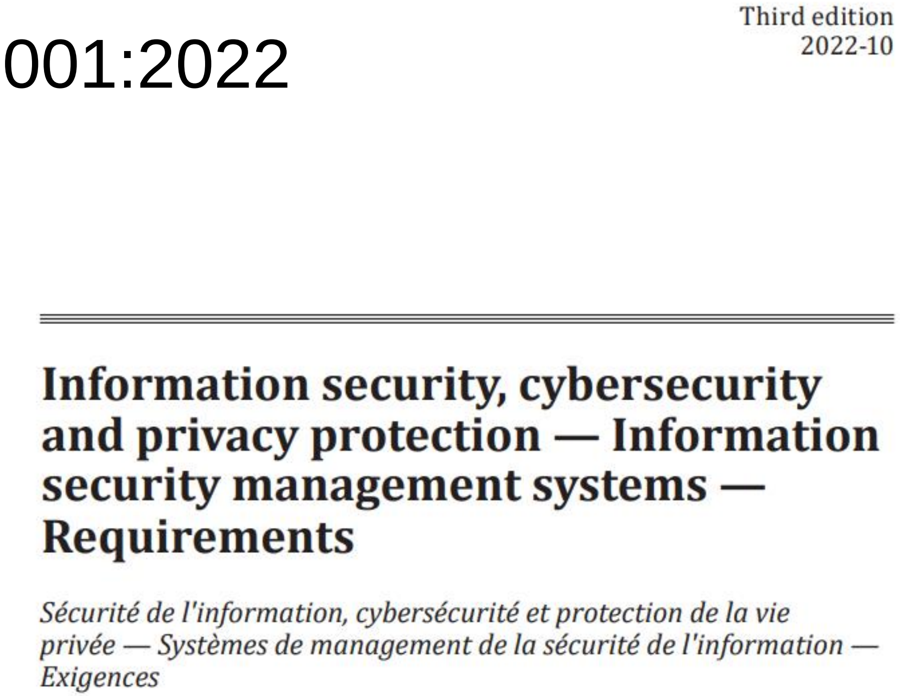
Page 1 of 2

This document is issued by the Company subject to its General Conditions of Certification Services accessible at www.sgs.com/terms_and_conditions.htm. Attention is drawn to the limitations of liability, indemnification and jurisdictional issues established therein. The authenticity of this document may be verified at http://www.sgs.com/en/certified-clients-and-products/certified-client-directory. Any unauthorized alteration, forgery or falsification of the content or appearance of this document is unlawful and offenders may be prosecuted to the fullest extent of the law.

INTRODUCTION TO ISO/IEC 27001:2022

What is an ISMS

Benefits and purpose of ISO/IEC 27001



Third edition
2022-10

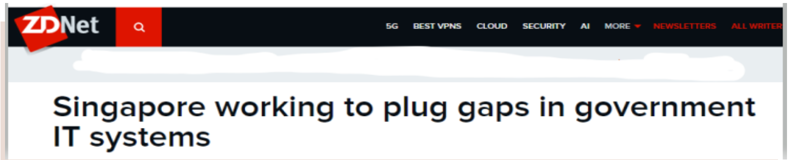
Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

What are some of the worrying trends in Information Security

As a quality manager I am worried more about supply chain availability, why should I worry about Information Security?

What is the connection between Quality and InfoSec



Singapore working to plug gaps in government IT systems

https://www.zdnet.com/article/singapore-working-to-plug-gaps-in-government-it-systems/

Central Bank of Ireland : “Governance and risk in a time of uncertainty and change” - Deputy Governor Ed Sibley

02/17/2021 | 07:36am EST

https://www.marketscreener.com/news/latest/Central-Bank-of-Ireland-ldquo-Governance-and-risk-in-a-time-of-uncertainty-and-change-rdquo-De--32461268/

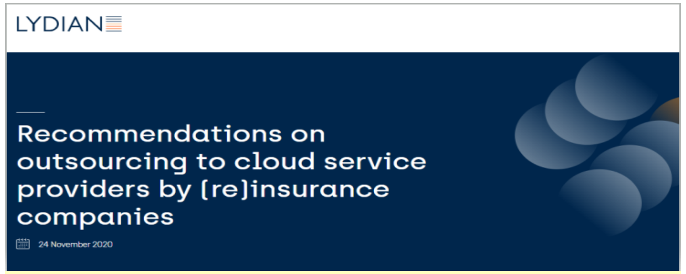
January 25, 2021

ESMA publishes final cloud outsourcing guidelines what do firms need to do to prepare?

https://www.jdsupra.com/legalnews/esma-publishes-final-cloudhttps://www.jdsupra.com/legalnews/esma-publishes-final-cloud-outsourcing-7381911/-outsourcing-7381911/

Auditability of AI vital for financial services

https://www.pinsentmasons.com/out-law/analysis/auditability-of-ai-financial-services



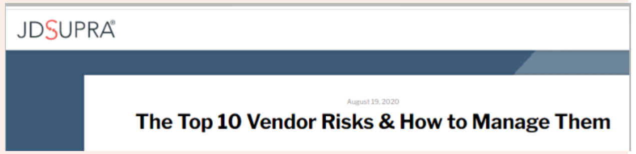
Recommendations on outsourcing to cloud service providers by (re)insurance companies

24 November 2020

https://www.lydian.be/en/news/recommendations-outsourcing-cloud-service-providers-reinsurance-companies

What financial services should learn from the SolarWinds cyber attack

https://www.consultancy.uk/news/26997/what-financial-services-should-learn-from-the-solarwinds-cyber-attack



August 19, 2020

The Top 10 Vendor Risks & How to Manage Them

https://www.jdsupra.com/legalnews/the-top-10-vendor-risks-how-to-manage-40256/

What is in it for me? Why should I, the quality manager / director spearhead the InfoSec or Cyber-security initiative in my company?

Fulfilling expressed and non-expressed expectations of the customer

What is a management system?

A management system is the way in which an organization manages the interrelated parts of its business in order to achieve its objectives.

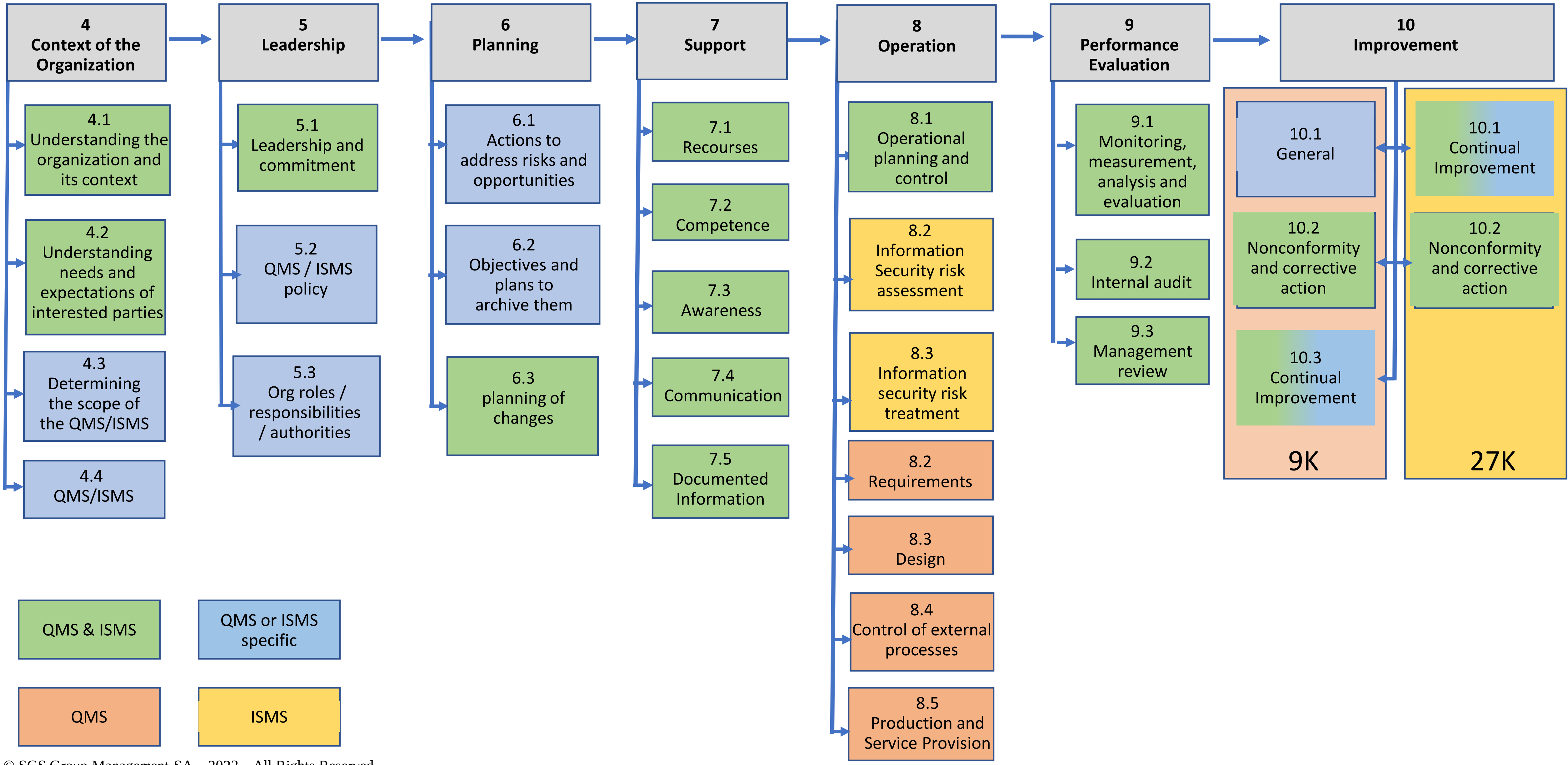
These objectives can relate to a number of different topics, including

- product or service quality,
- environmental performance,
- health and safety in the workplace or
- Information security, cybersecurity and privacy protection

The level of complexity of the system will depend on each organization's specific context.

Source: https://www.iso.org/management-system-standards.html

Integration of QMS (ISO 9001) and an ISMS (ISO/IEC 27001)



4 Context of the Organization
- 4.1 Understanding the organization and its context
- 4.2 Understanding needs and expectations of interested parties
- 4.3 Determining the scope of the QMS/ISMS
- 4.4 QMS/ISMS

5 Leadership
- 5.1 Leadership and commitment
- 5.2 QMS / ISMS policy
- 5.3 Org roles / responsibilities / authorities

6 Planning
- 6.1 Actions to address risks and opportunities
- 6.2 Objectives and plans to archive them
- 6.3 planning of changes

7 Support
- 7.1 Recourses
- 7.2 Competence
- 7.3 Awareness
- 7.4 Communication
- 7.5 Documented Information

8 Operation
- 8.1 Operational planning and control
- 8.2 Information Security risk assessment
- 8.3 Information security risk treatment
- 8.2 Requirements
- 8.3 Design
- 8.4 Control of external processes
- 8.5 Production and Service Provision

9 Performance Evaluation
- 9.1 Monitoring, measurement, analysis and evaluation
- 9.2 Internal audit
- 9.3 Management review

10 Improvement

9K
- 10.1 General
- 10.2 Nonconformity and corrective action
- 10.3 Continual Improvement

27K
- 10.1 Continual Improvement
- 10.2 Nonconformity and corrective action

QMS & ISMS	QMS or ISMS specific
QMS	ISMS

SOME FACTS ABOUT ISO/IEC 27001 & ISO/IEC 27002

1 ISO/IEC 27001

- Requirements
- **Certifiable**
- Annex A controls are directly derived from and aligned with those listed in ISO/IEC 27002

- ISO/IEC 27001:2022 released in October 2022.

2 ISO/IEC 27002

- Guidelines
- **Not certifiable**
- Contains implementation guidance of the controls

- ISO/IEC 27002:2013 is **withdrawn**
- **No transition** to the 2022 edition as ISO/IEC 27002
- **Not** the audit criteria for ISO/IEC 27001 certification

RISK ASSESSMENT, RISK TREATMENT AND STATEMENT OF APPLICABILITY (SOA)

1. Risk Matrix
1. Risk Assessment
3. Risk Treatment
4. Statement of Applicability (SoA)

RISK MATRIX

ISO/IEC 27005:2022 describes two approaches

Qualitative approach

Likelihood	Severity / Consequences	Minor	Significant	Serious	Critical	Catastrophic
		1	2	3	4	5
Unlikely	1	1	2	3	4	5
Rather unlikely	2	2	4	6	8	10
Likely	3	3	6	9	12	15
Very likely	4	4	8	12	16	20
Almost certain	5	5	10	15	20	25

Quantitative approach

Likelihood	Severity / Consequences (a loss of)	Less than £100	£100	£1 000	£10 000	£100 000	£1 000 000
		1	2	3	4	5	6
Once a year	1	1	2	3	4	5	6
Once a month	2	2	4	6	8	10	12
Twice a week	3	3	6	9	12	15	18
Every 8 hours	4	4	8	12	16	20	24
Every hour	5	5	10	15	20	25	30

RISK ASSESSMENT

ISO/IEC 27005:2022 describes the risk assessment process as:

Risk assessment consists of the following activities:

a) risk identification, which is a process to find, recognize and describe risks (further details on risk identification are provided in 7.2);

b) risk analysis, which is a process to comprehend the types of risk and to determine the level of risk. Risk analysis involves consideration of the causes and sources of risk, the likelihood that a specific event occurs, the likelihood that this event has consequences and the severity of those consequences (further details on risk analysis are provided in 7.3);

c) risk evaluation, which is a process to compare the results of risk analysis with risk criteria to determine whether the risk and/or its significance is acceptable and to prioritize the analysed risks for risk treatment. Based on this comparison, the need for treatment can be considered (further details on risk evaluation are provided in 7.4)

SGS

RISK ASSESSMENT

Example of an Assessment using the Qualitative Approach

RISK ASSESSMENT

Area	Threat	Vulnerability	C	I	A	Likelihood	Severity / Consequences	Total level of risk	Risk owner
Physical Access	*Unauthorised Acess to server room*	*Servers accidentally or otherwise compromised*	*x*	*x*	*x*	*3*	*5*	15	Security
	Loss of electricty from external provider for Datacenter	*Datacenter not availabale*			*x*	*4*	*5*	20	Facilities
	UPS and Standby generators not working	*Datacenter not available*			*x*	*3*	*5*	15	Facilities
	Employee Laptop stolen	*Data extract and accessable by unauthozed person*	*x*			*4*	*5*	20	IT
								0	
People	Hiring & Employing people with questionable background	untrust worthy individuals having access to sensitive information	x			3	4	12	HR
	Hiring people not qualified for the job	unqualifed people working on systems and inadvertingly changing information		x		3	4	12	HR
	Employee leaves laptop on plane / subway	*Data extract and accessable by unauthozed person*	*x*			*4*	*5*	20	HR
Assets	Laptops / servers / etc infected by malware	Lost of data (extracted)	x			3	**5**	15	IT
		Lost of data (encrypted by Ransomware)			x	3	**5**	15	IT
	Network / Laptops / IT slow, no responsive	Too many users, too much data, not enough bandwidth, capacity			x	2	**3**	6	IT
	no legaly binding agreement with suppliers with regard to information security	in case of issues no way to ensure co-operation with external parties	x	x	x	3	**4**	12	Legal & Supply chain management
	Externally purchased hardware and/or software has information security vulnerability	Security incidence affects ability to deliver service	x	x	x	3	**4**	12	Procurement / Supplychain management & IT

RISK TREATMENT

ISO/IEC 27005:2022 describes the risk treatment process as:

The input of the information security risk treatment is based on the risk assessment process outcomes in the form of a prioritized set of risks to be treated, based on risk criteria.

The output of this process is a set of necessary information security controls [see ISO/IEC 27001:2022, 6.1.3 b)] that are to be deployed or enhanced in relation to one another, in accordance with the risk treatment plan [see ISO/IEC 27001:2022, 6.1.3 e)]. Deployed in this way, the effectiveness of the risk treatment plan is to modify the information security risk facing the organization so that it meets the organization's criteria for acceptance.

SGS

RISK TREATMENT

Example of a Risk Treatment plan, based on the previous example

RISK TREATMENT

											after implementation of Control Measure		
Area	**Threat**	**Vulnerability**	C	I	A	**Likelihood**	**Severity / Consequences**	**Total level of risk**	**Risk owner**	**Control Measure**	**Likelihood**	**Severity / Consequences**	**Total level of risk**
Physical Access	*Unauthorised Acess to server room*	*Servers accidentally or otherwise compromised*	*x*	*x*	*x*	*3*	*5*	15	Security	Physical entry 7.2 Premises shall be continuously monitored for unauthorized physical access 7.4	*1*	*5*	5
	Loss of electricty from external provider for Datacenter	*Datacenter not availabale*			*x*	*4*	*5*	20	Facilities	Protecting against physical and environmental threats 7.5	*1*	*5*	5
	UPS and Standby generators not working	*Datacenter not availabale*			*x*	*3*	*5*	15	Facilities	Equipment maintenance 7.13	*2*	*5*	10
	Employee Laptop stolen	*Data extract and accessable by unauthozed person*	*x*			*4*	*5*	20	IT	Security of assets off-premises 7.9 Encrytion	*4*	*1*	4
								0					0
People	Hiring & Employing people with questionable background	untrust worthy individuals having access to sensitive information	x			3	4	12	HR	Screening 6.1	1	4	4
	Hiring people not qualified for the job	unqualifed people working on systems and inadvertingly changing information		x		3	4	12	HR	Screening 6.1	1	4	4
	Employee leaves laptop on plane / subway	*Data extract and accessable by unauthozed person*	*x*			*4*	*5*	20	HR	Information security awareness, education and training 6.3	*4*	*1*	4
								0					
Assets	Laptops / servers / etc infected by malware	Lost of data (extracted)	x			3	**5**	15	IT	Protection against malware 8.7	2	**5**	10
		Lost of data (encrypted by Ransomware)			x	3	**5**	15	IT	Information backup 8.13	2	**5**	10
	Network / Laptops / IT slow, no responsive	Too many users, too much data, not enough bandwidth, capacity			x	2	**3**	6	IT	Capacity management 8.6	2	**3**	6
	no legaly binding agreement with suppliers with regard to information security	in case of issues no way to ensure co-operation with external parties	x	x	x	3	**4**	12	Legal & Supply chain management	Addressing information security within supplier agreements 5.20	2	**4**	8
	Externally purchased hardware and/or software has information security vulnerability	Security incidence affects ability to deliver service	x	x	x	3	**4**	12	Procurement / Supplychain management & IT	Managing information security in the information and commu nication technology (ICT) supply chain 5.21	3	**2**	6

STATEMENT OF APPLICABILITY

ISO/IEC 27001:2022 requires:

produce a Statement of Applicability that contains:

- the necessary controls
- justification for their inclusion;
- whether the necessary controls are implemented or not; and
- the justification for excluding any of the Annex A controls

STATEMENT OF APPLICABILITY

Example of a Statement of Applicability – based on the previous example

Annex A Control	Control	control requirement	Control Implemented (Y / N)	Control Applicable (Y / N)	justification of exclusion & inclusion reason / control requirement	Control Owner
5.1	**Policies for information security**	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Y	Y	Corporate requirement	Departmen t heads
…..	…..	…..				
6.1	**Screening**	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Y	Y	risk assessment and risk treatment	HR
6.2	**Terms and conditions of em ployment**	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	N	Y	no need, we love each other	
6.3	**Information security awareness, education and training**	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	Y	Y	risk assessment and risk treatment	HR
7.1	**Physical security perimeters**	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Y	Y	risk assessment and risk treatment	Security
7.2	**Physical entry**	Secure areas shall be protected by appropriate entry controls and access points.	Y	Y	risk assessment and risk treatment	Security
7.3	**Securing offices, rooms and facilities**	Physical security for offices, rooms and facilities shall be designed and implemented.	Y	Y	risk assessment and risk treatment	Security
7.4	**Physical security monitoring**	Premises shall be continuously monitored for unauthorized physical access.	Y	Y	risk assessment and risk treatment	Security
7.5	**Protecting against physical and environmental threats**	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Y	Y	risk assessment and risk treatment	Security

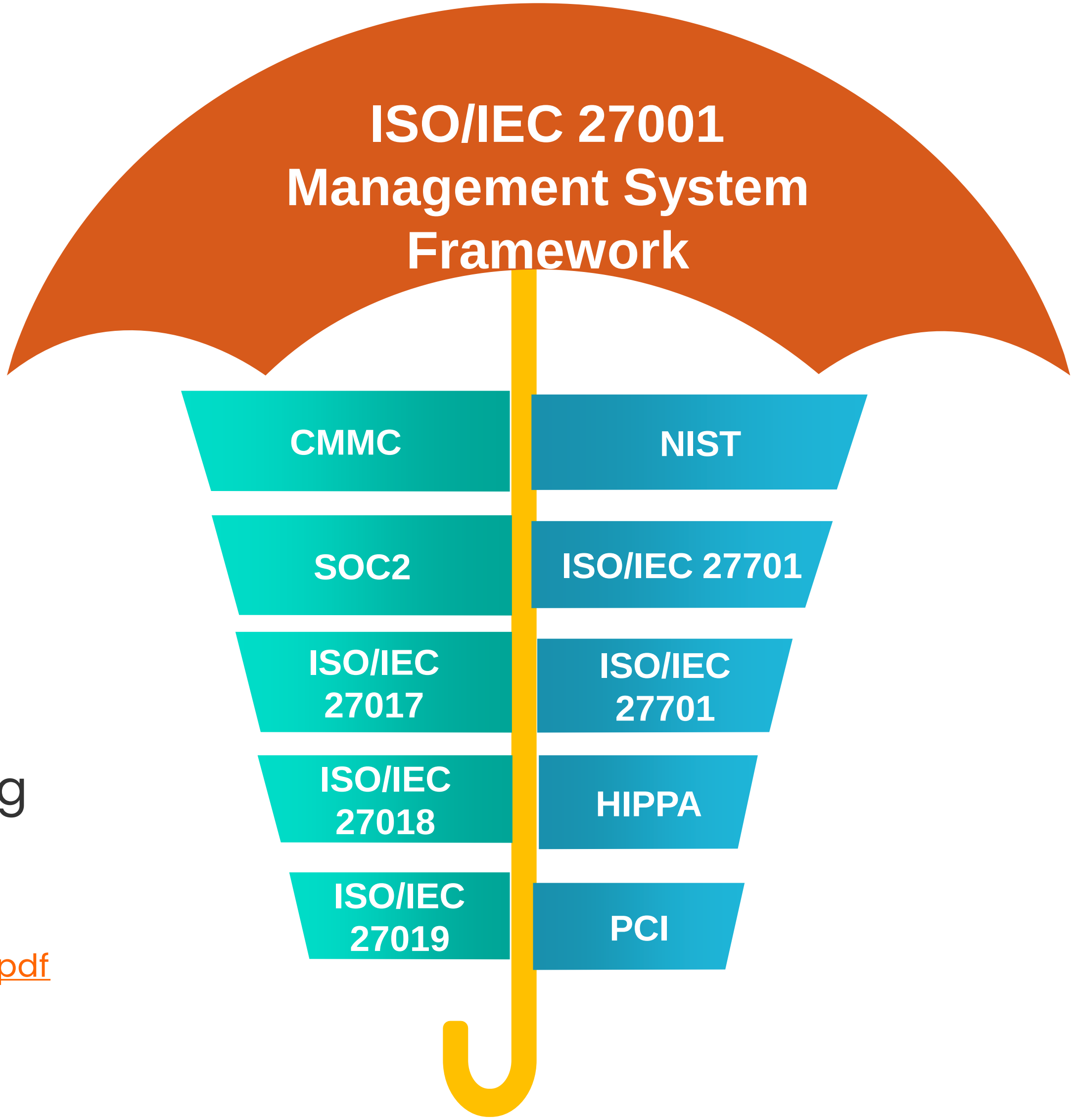
	ISO/IEC 27001:2022	NIST 800-171rev2	CMMC 2.0
Regional Applicability	International	US focused	US focused
Owner	ISO/IEC	NIST	DoD
Certification ?	Available, well established and globally recognized approach for many years	NO “should” versus “shall”	Scheme requirements are still being developed, a few C3PAOs have been approved
Compliance Requirements	Driven by individual participants in certain markets	Any federal agency who engages with 3rd parties, any nonfederal system or organization used by a federal agencies.	Anyone in the defense contract supply chain and Certain DoD contractors that handle sensitive unclassified DoD information pending on Maturity Level
Information Protected	All forms of Information Assets	CUI in Nonfederal Systems and Organizations	FCI and CUI shared with contractors and subcontractors of the DoD through acquisition programs
Conformance	3rd party assessment & Certification • Initial Certification (Stage 1 & Stage 2) • Annual surveillance audits • Recertification audits – 3 years	Voluntary compliance and self-certification with no formal compliance certification.	ML 1 – annual self-assessments ML 2 – C3PAO assessments ML 3 - government-led assessments

BENEFITS OF CERTIFICATION BY ACCREDITED CB

Using an accredited certification body can:

- de-risk your procurement
- win new business
- gain access to overseas markets
- help to identify best practice
- offer market differentiation and leadership
- help to identify best practice
- demonstrate due diligence
- reduce paperwork and increase efficiency by reducing the need to re-audit your business.

Source:
https://iaf.nu/iaf_system/uploads/documents/IAF_Why_use_accredited_CB_0112.pdf



INFORMATION SECURITY SEEMS SO TECHNICAL

I AM NOT AN IT PERSON. DO YOU NEED TO BE A CYBER SECURITY EXPERT TO IMPLEMENT ISO 27001?

AND WHAT KIND OF RESOURCES ARE NEEDED TO DO SO?

Typical Questions

We have already our IT department taking care of this ---- why should I get involved?

Will ISO 27001 support our efforts at compliance with government regulations?

What about Client / OEM requirements?

Does every company need ISO 27001, or is it for specific industries?

What other standards are there that fit to my specific use case or that I should be aware of ?

Does ISO 27001 also make me compliant with data privacy regulations?

What is ISO/IEC 27701?

- Published August 2019
- ISO/IEC 27701 provides specific requirements and guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) as an extension of ISO/IEC 27001 Information Security Management and ISO/IEC 27002 Security Controls.
- Note: the new ISO/IEC 27001:2022 has a new/revised title:

  Information security, cybersecurity and privacy protection — Information security management systems — Requirements

- An international management system standard, it provides guidance and requirements on the protection of privacy, including how organizations should manage personal information, and assists in demonstrating compliance with privacy regulations around the world.

What is ISO/IEC 27701?

- Published August 2019
- ISO/IEC 27701 provides specific requirements and guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) as **an extension** of ISO/IEC 27001 Information Security Management and ISO/IEC 27002 Security Controls.
- An international management system standard, it provides guidance and requirements on the protection of privacy, including how organizations should manage personal information, and assists in demonstrating compliance with privacy regulations around the world.

What is ISO/IEC 27701?

The ISO/IEC addresses both controllers (as well as joint controllers) and processors (including sub-processors) of PII, regardless of the jurisdictions and sectors in which they operate. **The standard includes mappings to the GDPR, ISO/IEC 29100, ISO/IEC 27018 and ISO/IEC 29151.**

Benefits of ISO/IEC 27701

compliance with the requirements of ISO/IEC 27001 is pre-requisite for Compliance with ISO/IEC 27701. The standards are intended to complement each other. Fulfilling the requirements of ISO/IEC 27701 will create evidence of how an organization is handling the processing of PII, and that can be used to facilitate agreements with business partners where the processing of PII is relevant and to clarify the organization’s processing of PII with other stakeholders.

Structure of ISO/IEC 27701

3 Terms, definitions and abbreviations

4 General

5 PIMS-specific requirements related to ISO/IEC 27001

6 PIMS-specific guidance related to ISO/IEC 27002

7 Additional ISO/IEC 27002 guidance for PII controllers

8 Additional ISO/IEC 27002 guidance for PII processors

normative Annex
Annex A   PIMS-specific reference control objectives and controls (PII Controllers)
Annex B PIMS-specific reference control objectives and controls (PII Processors)

informative
Annex C Mapping to ISO/IEC 29100
Annex D Mapping to the General Data Protection Regulation
Annex E Mapping to ISO/IEC 27018 and ISO/IEC 29151
Annex F How to apply ISO/IEC 27701 to ISO/IEC 27001 and ISO/IEC 27002

Summary ISO/IEC 27701

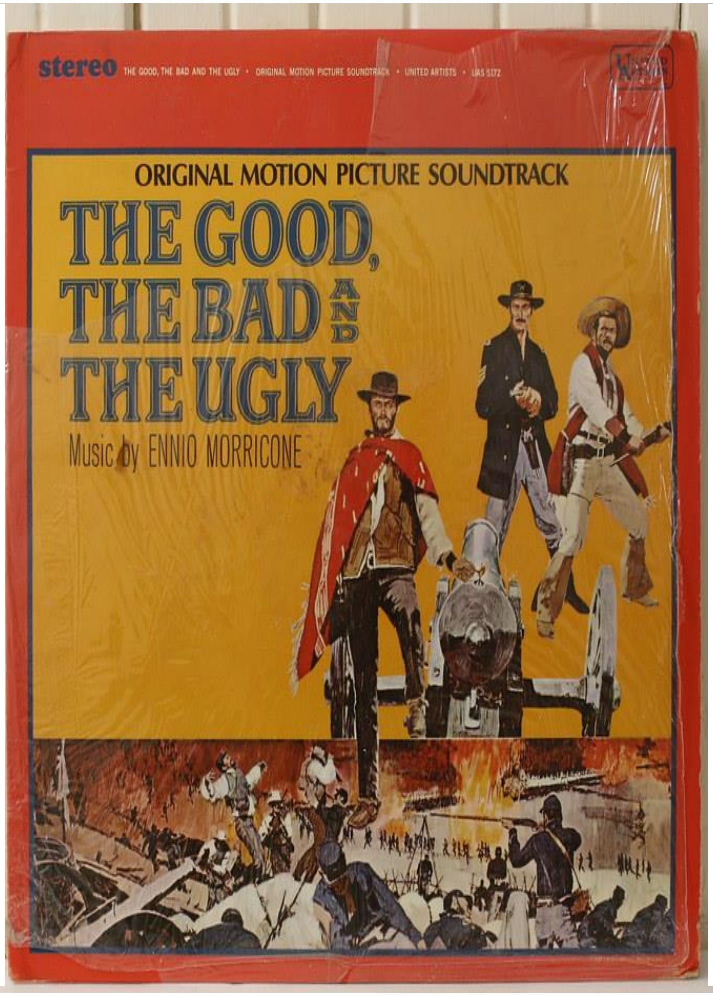
ISO/IEC 27701 is an extension to ISO/IEC 27001 for the management of a Privacy Management System.

ISO/IEC 27701 contains both requirements and guidance.

ISO/IEC 27701 can be used by organizations that are PII controllers and/or PII processors.

ISO/IEC 27701 contains an Annex mapping the standard to the GDPR.

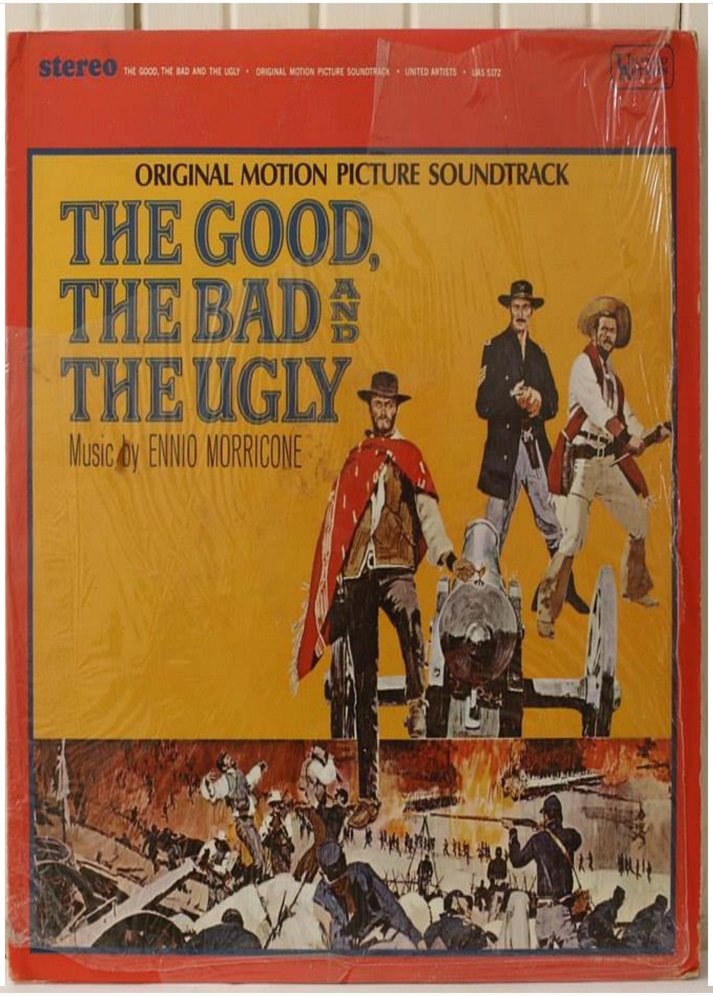
THE UGLY


stereo
THE GOOD, THE BAD AND THE UGLY • ORIGINAL MOTION PICTURE SOUNDTRACK • UNITED ARTISTS
ORIGINAL MOTION PICTURE SOUNDTRACK
THE GOOD, THE BAD AND THE UGLY
Music by ENNIO MORRICONE

- Box solutions
- Consultants and assessors not worth their money
- Sheer incompetence
- Getting certified as one method to get points in government bidding projects
- Certification is seen as the ultimate goal, not really interested in an effective management system ---

  yes, I had calls like: “Are you selling ISO certification, and how much is it” and this leads to extremely un-disable behavior

THE UGLY part 2

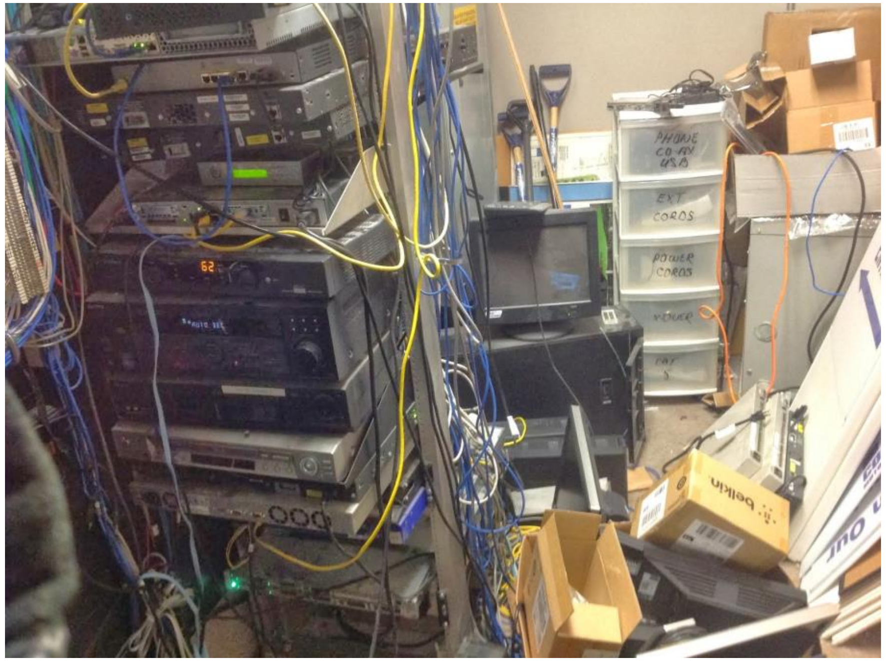

stereo
ORIGINAL MOTION PICTURE SOUNDTRACK
THE GOOD, THE BAD AND THE UGLY
Music by ENNIO MORRICONE

Seen “datacenters” in a closet with consumer grade UPS.

Furnaces for industrial plant next to two server racks.

Switches that are still “on” with a dozens cut CAT cables.

Home Air-condition systems literally hanging on top of a server rack with the discharge hose hanging on the rack.

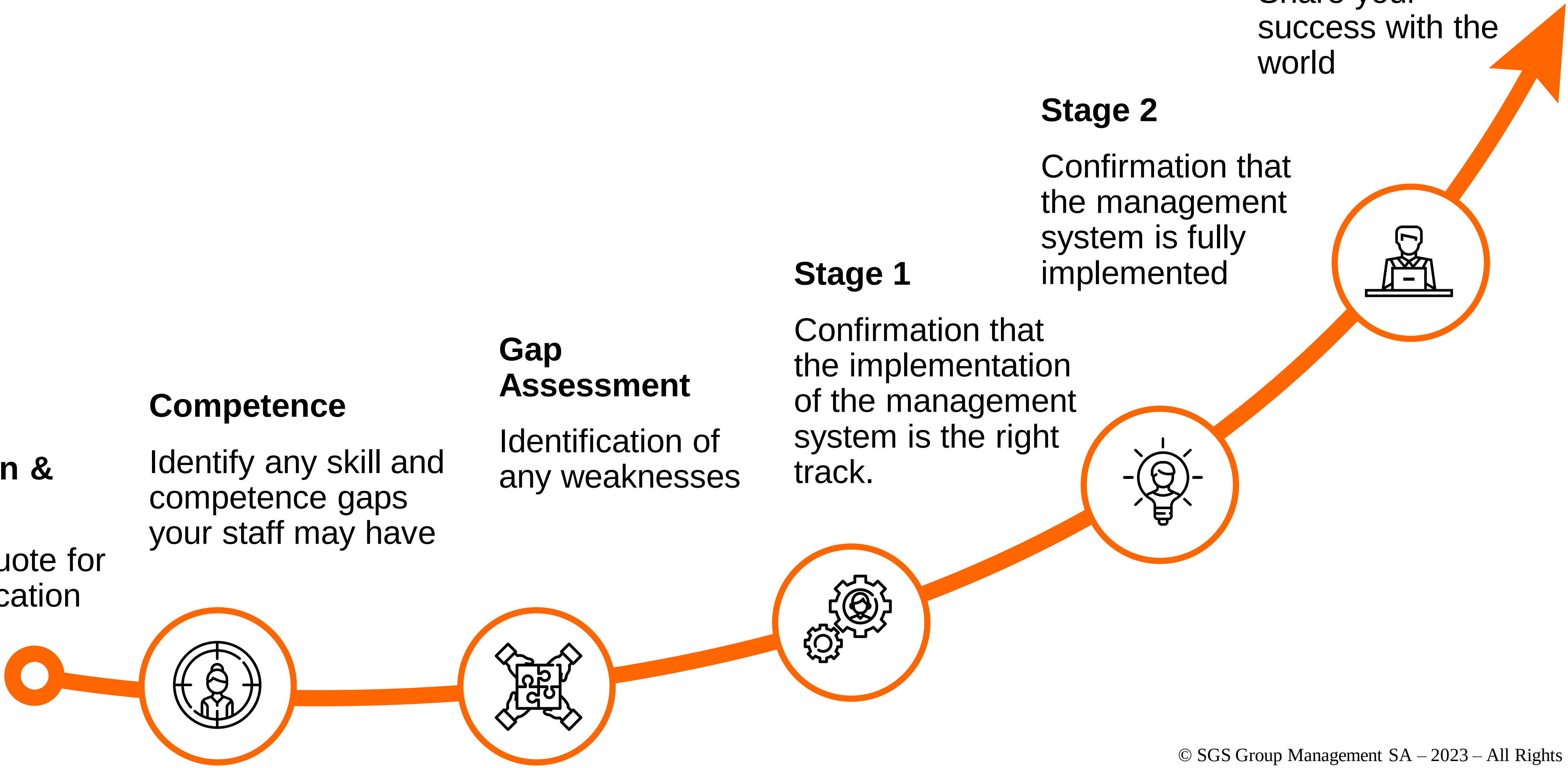


Datacenter with servers of presidential servers

CERTIFICATION

What does a typical 27001 (27701) certification process look like, if you are already 9001 certified? How long does it take?

CERTIFICATION PROCESS



Application & Quote

Obtain a quote for your certification project

Competence

Identify any skill and competence gaps your staff may have

Gap Assessment

Identification of any weaknesses

Stage 1

Confirmation that the implementation of the management system is the right track.

Stage 2

Confirmation that the management system is fully implemented

Certification

Share your success with the world

Ongoing improvement

Regular surveillance visits will ensure your management system

Where do we go from here

With the 2022 edition ISO/IEC 27001 is now in the 3rd edition is one of the fasted growing management system certification standards in the world. It would be not surprising to see the standard reaching the same level of adaptation as ISO 9001, just simply because of the wider understanding of the need to securing Information.

We see more national and industry specific frameworks

We will see progression towards “continuous or continual assessments” with computer systems continuously monitoring (and altering if necessary) processes for compliance

We see AI solutions helping with both the maintenance as well as the assessment of Management systems (in particular ISMS)

27001 applicable to small and large organization and this is not different than other management system standards

While certainly some organizations are struggling, the overwhelming majority of organization have no real problems implementing and maintaining their ISMS

Certification by a reputable, well known and accredited certification body will provide the assurance clients are looking for.

APPLY WHAT YOU HAVE LEARNED TODAY

- Next week you should:
  - Review ISO/IEC 27001 -- published October 2022
  - Review the content of ISO/IEC 27002:2022 -- published 2022
  - Research training classes

- Within three months of this presentation, you should:
  - Attend an online ISO/IEC 27001 auditor class
  - Book your pre-assessment and stage 1 assessments

- Within six months you should:
  - Book your stage 2 assessments

THANK YOU !

THANK YOU!

Do you have any questions?

Reach out to our team:

Willy.Fabritius@sgs.com

Visit our website, to learn more about our certification and training services

https://www.sgs.com/en/campaigns/transforming-cyber-integrity-and-availability-with-sgs-solutions