MSECB

Webinar Power Point

Mastering Audit Preparation for Integrated ISO/IEC 27001 and ISO 22301 Certification

Webinars by MSECB

Rinske Geerlings

MSECB

Webinar Agenda

Presentation

- How to master the audit preparation process for organizations seeking ISO/IEC 27001 and ISO 22301 certifications to achieve a smooth and successful certification journey.
- How an integrated approach strengthens the information security and business continuity management systems.

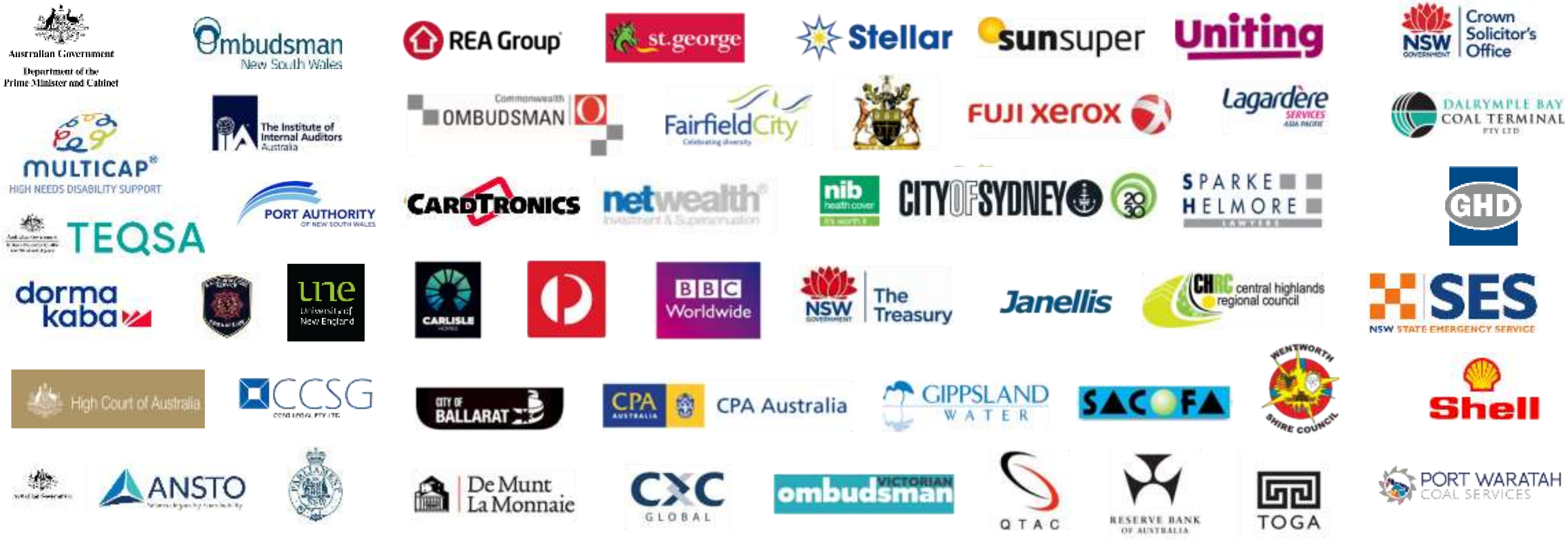
Q&A

Background of Speaker

Rinske Geerlings

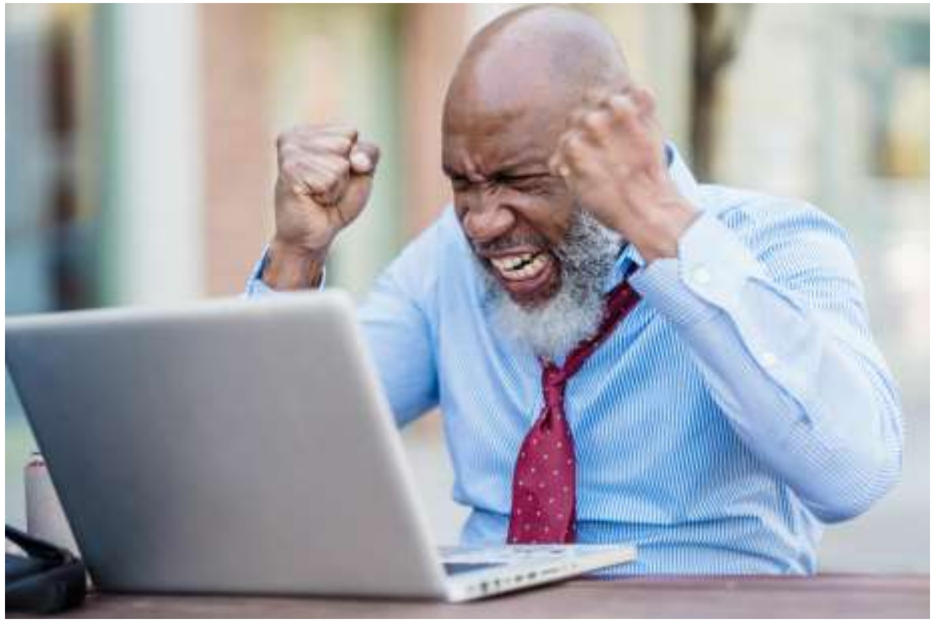
- Multi-award winning consultant, trainer and auditor in Business Continuity (BCM), IT Management, Organisational Resilience, Information Security, Crisis and Risk Management
- ISO 22301, ISO 27001, ISO 22361, ISO 22316 and ISO 31000 certified
- Consulted for 20+ years to 100s of Government entities, SMEs and larger corporates across Australasia, Africa, Europe and Latin America
- Risk Consultant of the Year 2017 by RMIA (Australasia)
- Outstanding Security Consultant of the Year 2019 Finalist in the OSPAs
- Australian Business Woman of the Year 2010-13 by BPW (global NGO)

Client sample


Australian Government
Department of the Prime Minister and Cabinet
Ombudsman New South Wales
REA Group
st.george
Stellar
sunsuper
Uniting
NSW Government Crown Solicitor's Office
MULTICAP
HIGH NEEDS DISABILITY SUPPORT
The Institute of Internal Auditors Australia
Commonwealth OMBUDSMAN
Fairfield City
Celebrating diversity
FUJI XEROX
Lagardère SERVICES ASIA PACIFIC
DALRYMPLE BAY COAL TERMINAL PTY LTD
TEQSA
PORT AUTHORITY OF NEW SOUTH WALES
CARDTRONICS
netwealth
Investment & Superannuation
nib health cover
CITY OF SYDNEY
2030
SPARKE HELMORE LAWYERS
GHD
dorma kaba
une University of New England
CARLISLE HOMES
BBC Worldwide
NSW Government The Treasury
Janellis
CHRC central highlands regional council
SES
NSW STATE EMERGENCY SERVICE
High Court of Australia
CCSG
CCSG LEGAL PTY LTD
CITY OF BALLARAT
CPA AUSTRALIA
CPA Australia
GIPPSLAND WATER
SACOFA
WENTWORTH SHIRE COUNCIL
Shell
ANSTO
PARLIAMENT
De Munt La Monnaie
CXC GLOBAL
VICTORIAN ombudsman
QTAC
RESERVE BANK OF AUSTRALIA
TOGA
PORT WARATAH COAL SERVICES

Let's chat

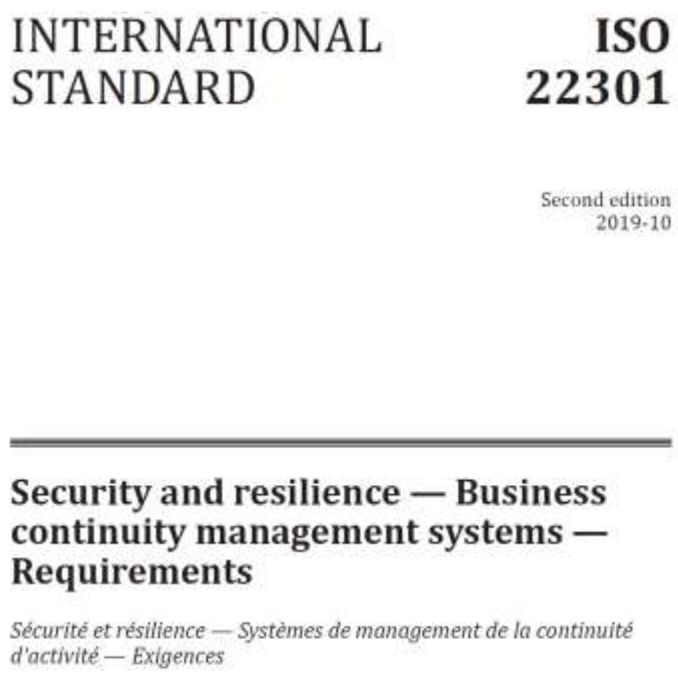
Your biggest frustration when being audited



Your biggest frustration as an auditor

Content comparison ISO 27001:2022 vs. ISO 22301:2019

MSECB



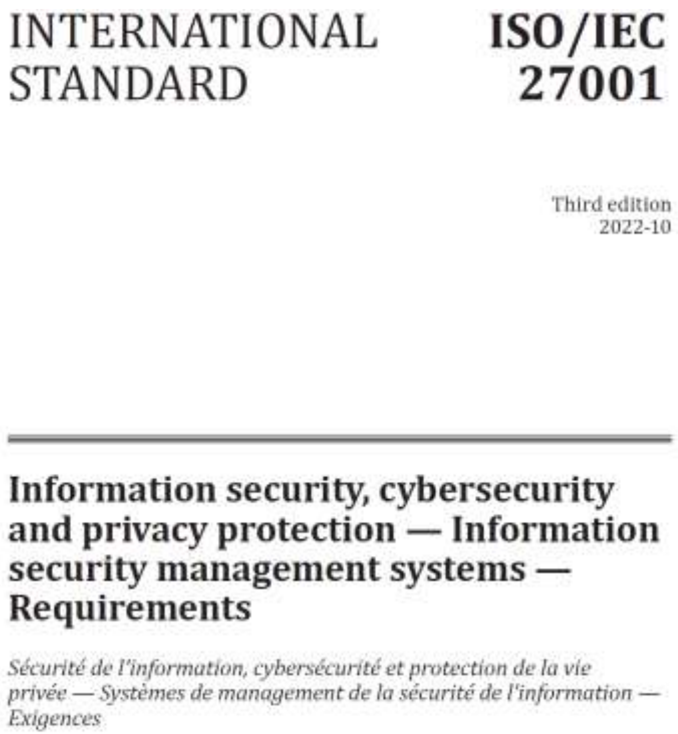
INTERNATIONAL STANDARD

ISO 22301

Second edition
2019-10

Security and resilience — Business continuity management systems — Requirements

Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences



INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

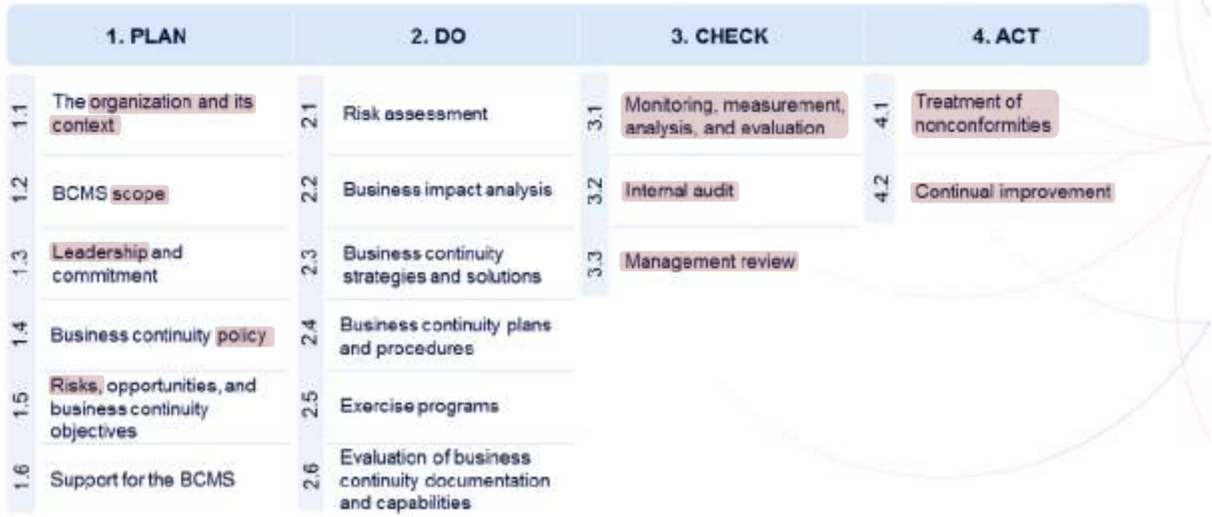
Information security, cybersecurity and privacy protection — Information security management systems — Requirements

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

MSECB

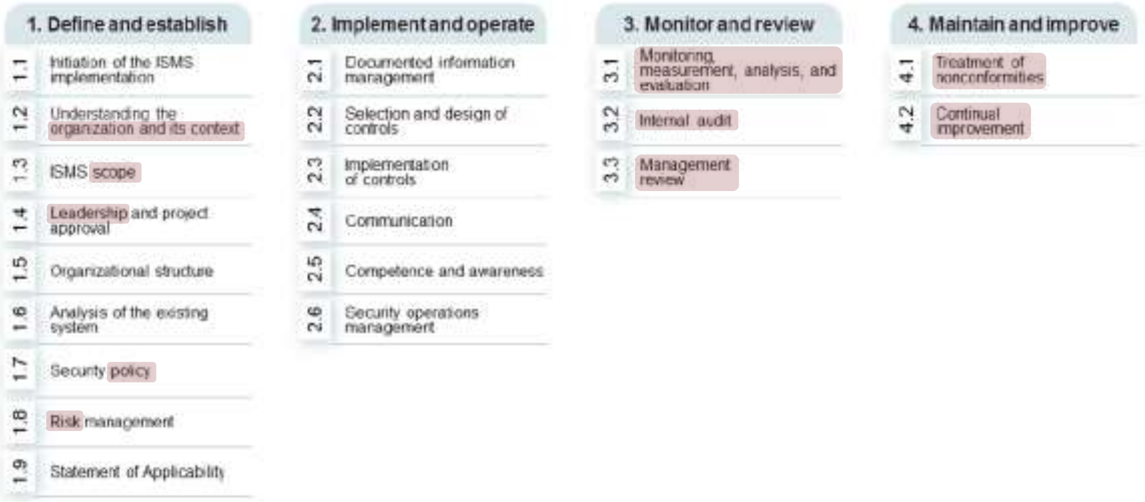
Methodological implementation framework

BCMS



1. PLAN		2. DO		3. CHECK		4. ACT	
1.1	The organization and its context	2.1	Risk assessment	3.1	Monitoring, measurement, analysis, and evaluation	4.1	Treatment of nonconformities
1.2	BCMS scope	2.2	Business impact analysis	3.2	Internal audit	4.2	Continual improvement
1.3	Leadership and commitment	2.3	Business continuity strategies and solutions	3.3	Management review		
1.4	Business continuity policy	2.4	Business continuity plans and procedures				
1.5	Risks, opportunities, and business continuity objectives	2.5	Exercise programs				
1.6	Support for the BCMS	2.6	Evaluation of business continuity documentation and capabilities				

ISMS

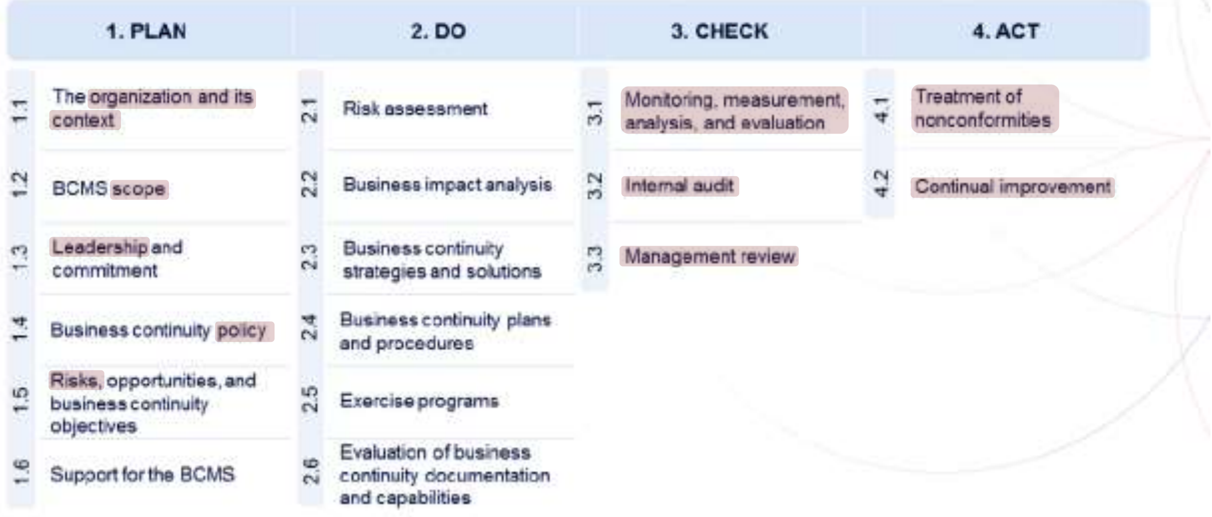


1. Define and establish		2. Implement and operate		3. Monitor and review		4. Maintain and improve	
1.1	Initiation of the ISMS implementation	2.1	Documented information management	3.1	Monitoring, measurement, analysis, and evaluation	4.1	Treatment of nonconformities
1.2	Understanding the organization and its context	2.2	Selection and design of controls	3.2	Internal audit	4.2	Continual improvement
1.3	ISMS scope	2.3	Implementation of controls	3.3	Management review		
1.4	Leadership and project approval	2.4	Communication				
1.5	Organizational structure	2.5	Competence and awareness				
1.6	Analysis of the existing system	2.6	Security operations management				
1.7	Security policy						
1.8	Risk management						
1.9	Statement of Applicability						

MSECB

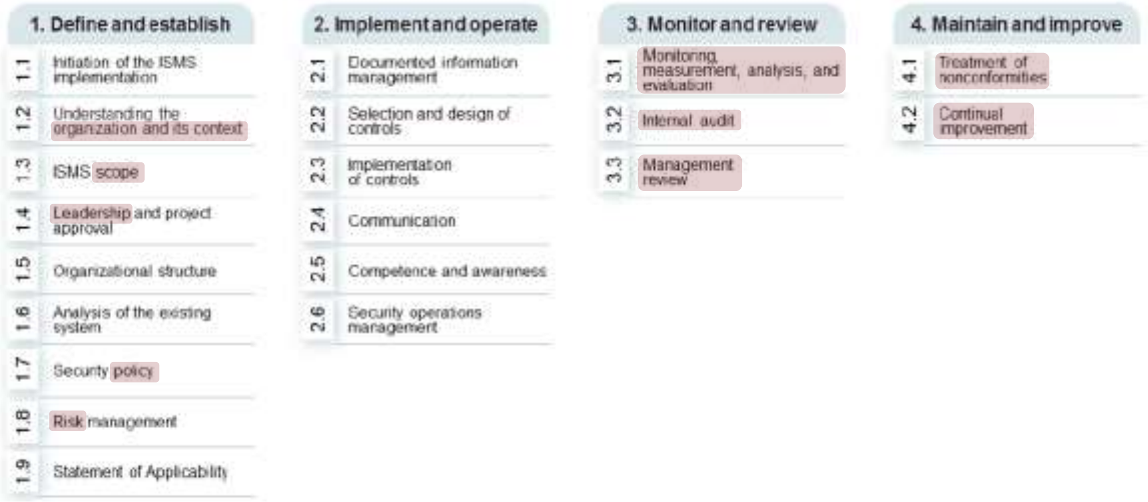
Opportunities for efficiency/alignment Involvement of stakeholders

BCMS



1. PLAN	2. DO	3. CHECK	4. ACT
1.1 The organization and its context	2.1 Risk assessment	3.1 Monitoring, measurement, analysis, and evaluation	4.1 Treatment of nonconformities
1.2 BCMS scope	2.2 Business impact analysis	3.2 Internal audit	4.2 Continual improvement
1.3 Leadership and commitment	2.3 Business continuity strategies and solutions	3.3 Management review	
1.4 Business continuity policy	2.4 Business continuity plans and procedures		
1.5 Risks, opportunities, and business continuity objectives	2.5 Exercise programs		
1.6 Support for the BCMS	2.6 Evaluation of business continuity documentation and capabilities		

ISMS

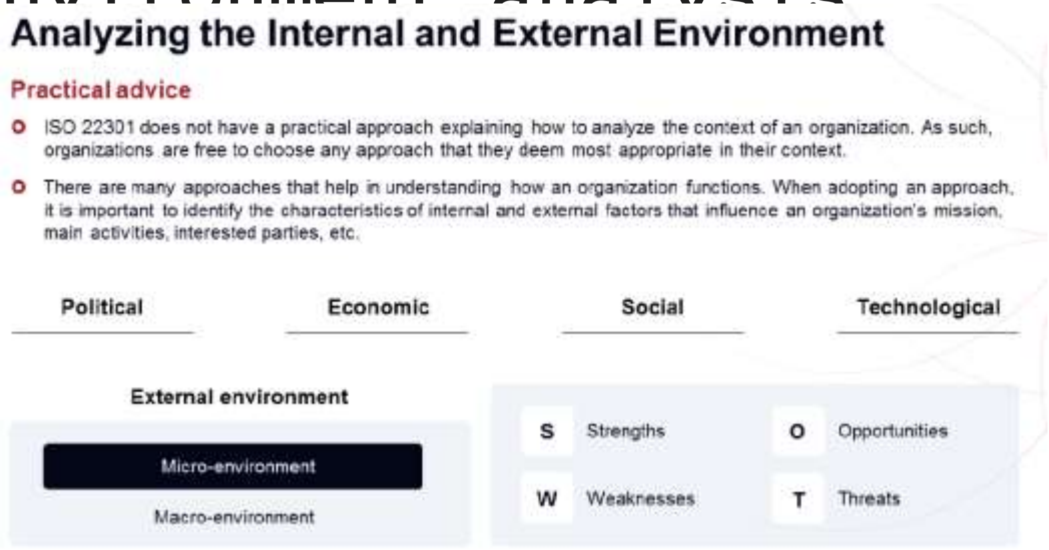


1. Define and establish	2. Implement and operate	3. Monitor and review	4. Maintain and improve
1.1 Initiation of the ISMS implementation	2.1 Documented information management	3.1 Monitoring, measurement, analysis, and evaluation	4.1 Treatment of nonconformities
1.2 Understanding the organization and its context	2.2 Selection and design of controls	3.2 Internal audit	4.2 Continual improvement
1.3 ISMS scope	2.3 Implementation of controls	3.3 Management review	
1.4 Leadership and project approval	2.4 Communication		
1.5 Organizational structure	2.5 Competence and awareness		
1.6 Analysis of the existing system	2.6 Security operations management		
1.7 Security policy			
1.8 Risk management			
1.9 Statement of Applicability			

MSECB

Opportunities for efficiency/alignment Example – Environment analysis

ISO 22301



Analyzing the Internal and External Environment

Practical advice

- ISO 22301 does not have a practical approach explaining how to analyze the context of an organization. As such, organizations are free to choose any approach that they deem most appropriate in their context.
- There are many approaches that help in understanding how an organization functions. When adopting an approach, it is important to identify the characteristics of internal and external factors that influence an organization's mission, main activities, interested parties, etc.

Political | Economic | Social | Technological

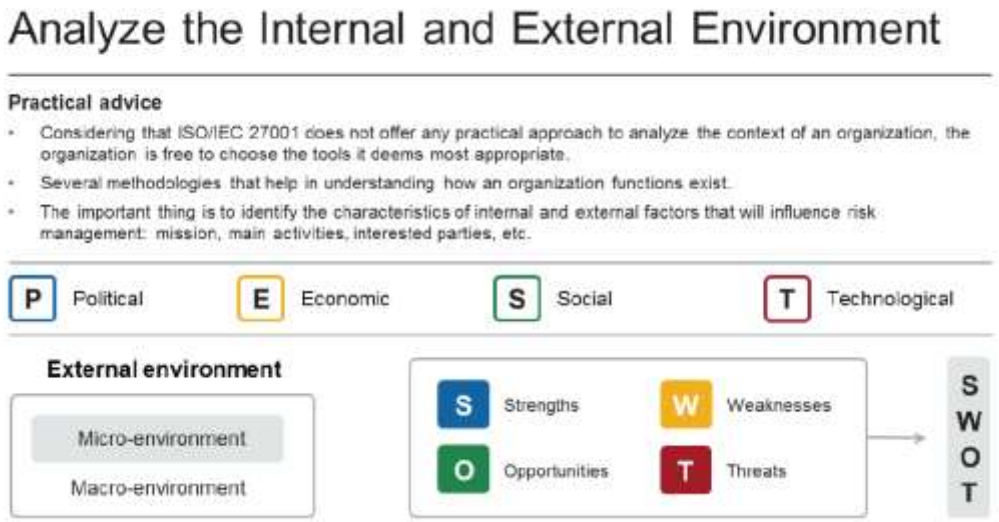
External environment

Micro-environment

Macro-environment

S	Strengths	O	Opportunities
W	Weaknesses	T	Threats

ISO 27001



Analyze the Internal and External Environment

Practical advice

- Considering that ISO/IEC 27001 does not offer any practical approach to analyze the context of an organization, the organization is free to choose the tools it deems most appropriate.
- Several methodologies that help in understanding how an organization functions exist.
- The important thing is to identify the characteristics of internal and external factors that will influence risk management: mission, main activities, interested parties, etc.

P Political | E Economic | S Social | T Technological

External environment

Micro-environment

Macro-environment

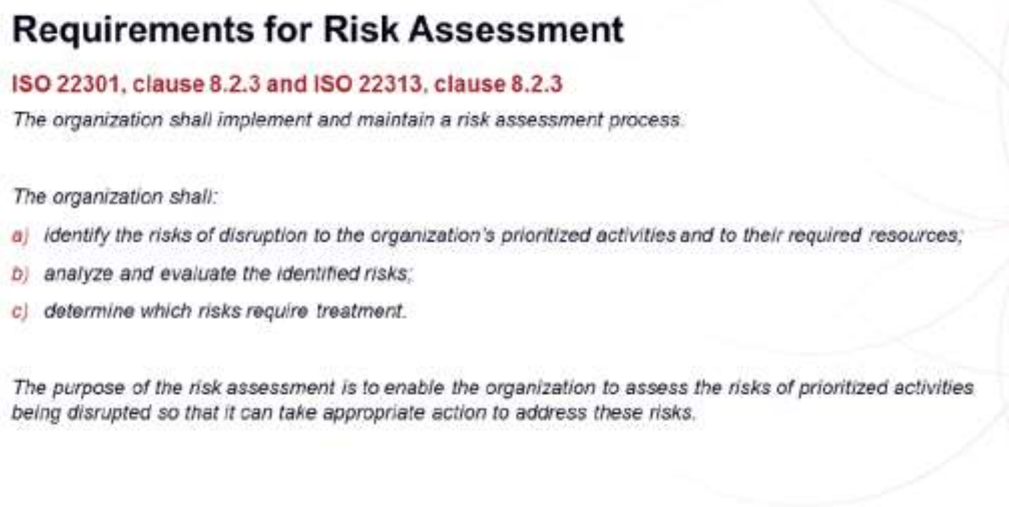
S	Strengths	W	Weaknesses
O	Opportunities	T	Threats

→ SWOT

Both BCMS and ISMS aim to protect the Crown Jewels

Opportunities for efficiency/alignment Example: Risk-based approach

ISO 22301



Requirements for Risk Assessment

ISO 22301, clause 8.2.3 and ISO 22313, clause 8.2.3

The organization shall implement and maintain a risk assessment process.

The organization shall:

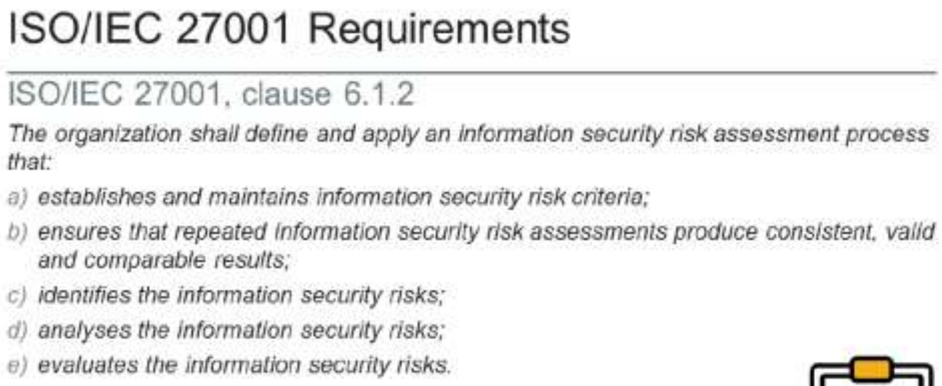
a) identify the risks of disruption to the organization's prioritized activities and to their required resources;

b) analyze and evaluate the identified risks;

c) determine which risks require treatment.

The purpose of the risk assessment is to enable the organization to assess the risks of prioritized activities being disrupted so that it can take appropriate action to address these risks.

ISO 27001



ISO/IEC 27001 Requirements

ISO/IEC 27001, clause 6.1.2

The organization shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria;

b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;

c) identifies the information security risks;

d) analyses the information security risks;

e) evaluates the information security risks.

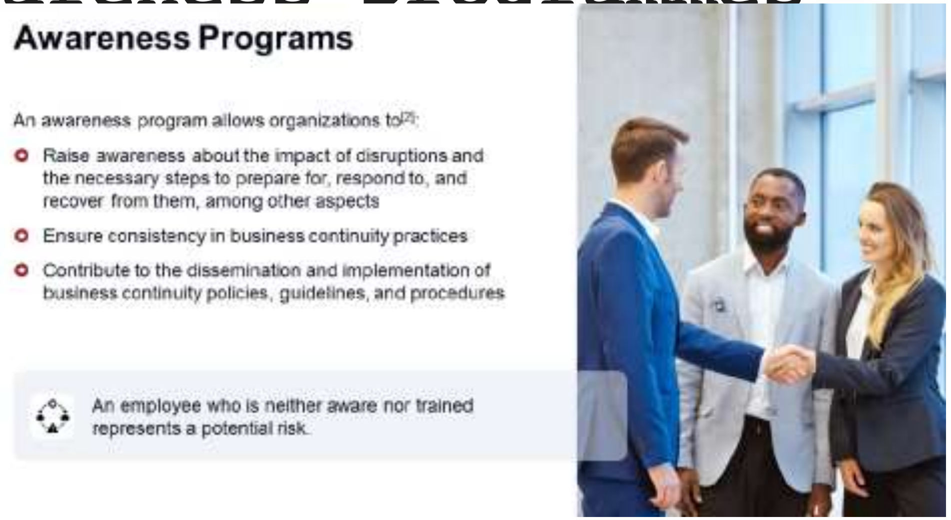
MSECB

Benefits of supporting a technical expert on the audit team

MSECB

Opportunities for efficiency/alignment Example: Awareness programmes

ISO 22301



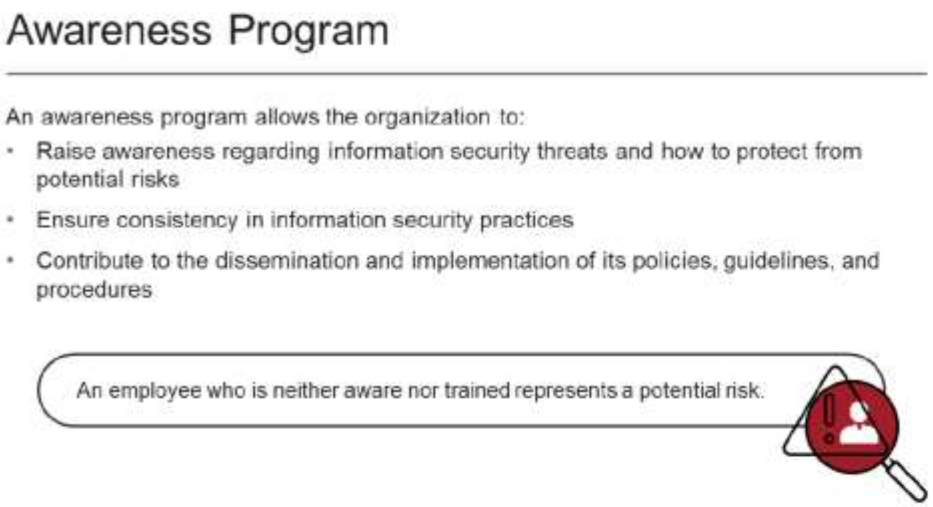
Awareness Programs

An awareness program allows organizations to[2]:

- Raise awareness about the impact of disruptions and the necessary steps to prepare for, respond to, and recover from them, among other aspects
- Ensure consistency in business continuity practices
- Contribute to the dissemination and implementation of business continuity policies, guidelines, and procedures

An employee who is neither aware nor trained represents a potential risk.

ISO 27001



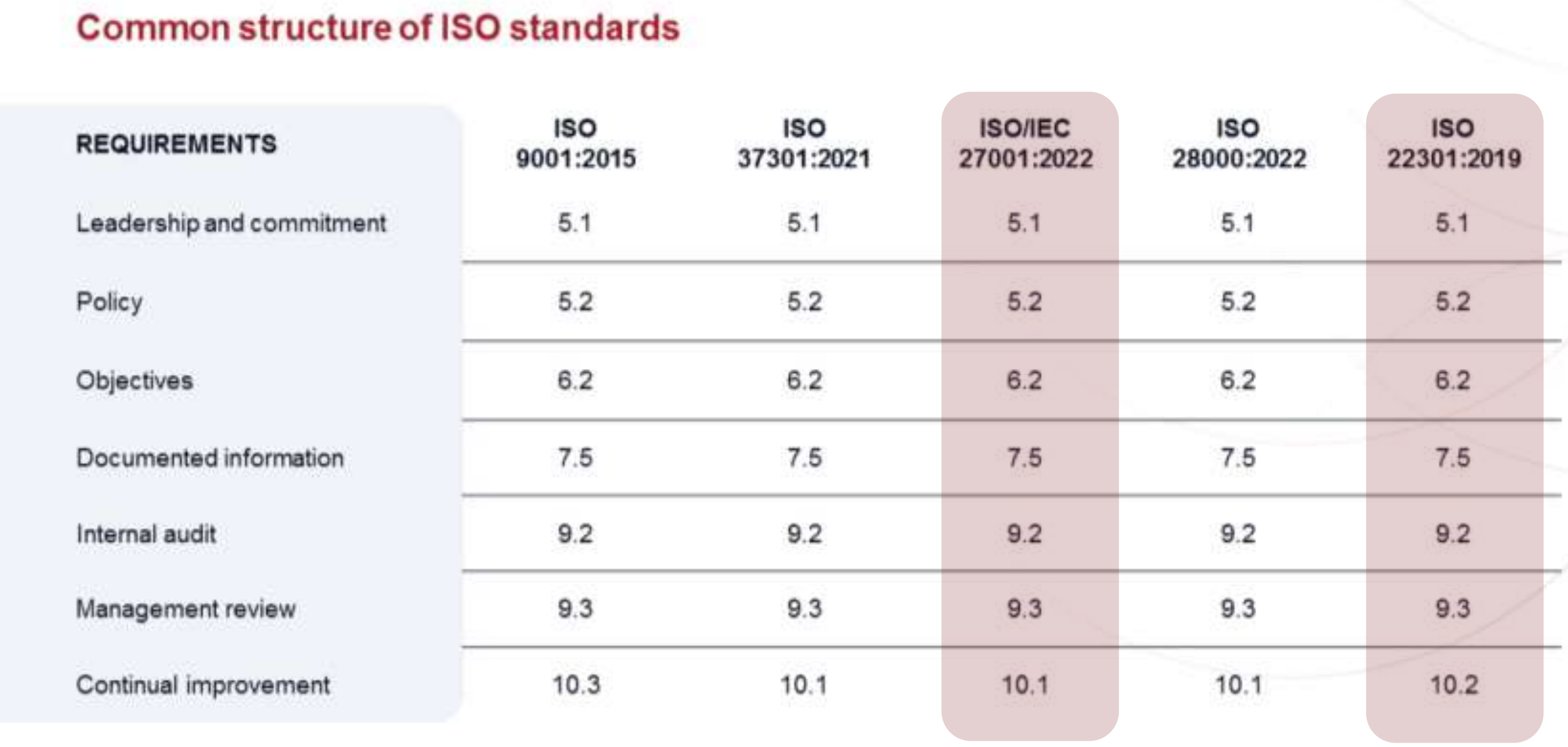
Awareness Program

An awareness program allows the organization to:

- Raise awareness regarding information security threats and how to protect from potential risks
- Ensure consistency in information security practices
- Contribute to the dissemination and implementation of its policies, guidelines, and procedures

An employee who is neither aware nor trained represents a potential risk.

Opportunities for efficiency
Example: Documentation



Common structure of ISO standards

REQUIREMENTS	ISO 9001:2015	ISO 37301:2021	ISO/IEC 27001:2022	ISO 28000:2022	ISO 22301:2019
Leadership and commitment	5.1	5.1	5.1	5.1	5.1
Policy	5.2	5.2	5.2	5.2	5.2
Objectives	6.2	6.2	6.2	6.2	6.2
Documented information	7.5	7.5	7.5	7.5	7.5
Internal audit	9.2	9.2	9.2	9.2	9.2
Management review	9.3	9.3	9.3	9.3	9.3
Continual improvement	10.3	10.1	10.1	10.1	10.2

Questions...

- Are your documents easily findable?
- What if a new version of a standard comes out?
- Quantity vs. Quality?

MSECB

Benefits of a pre-audit

before being thrown into the Lions’ Den

MSECB

Q&A

✉ rinskeg@businessasusual.com.au

in Rinske Geerlings

Thank you for your attention!

Stay updated!

+1 (450) 328-1227

info@msecb.com

www.msecb.com