INTRODUCTION TO ISO 27001:2022

OVERVIEW

Business is full of risk, and to ensure continuity, organisations need to identify, evaluate, and respond accordingly to all relevant risks. This process is called risk management. Methodologies range from active decisions to subconscious and responsive choices made based on data from a wide variety of fields, including information security. Risk management may be a complex task but does not need to be one that is unnecessarily mystified.

ISO 27001:2022 exists to address information security risks through an effective Information Security Management System (ISMS). Achieving ISO 27001 certification does not guarantee that information breaches will never occur, but instead creates a robust system to reduce risks and disruptions, thereby keeping costs to a minimum.

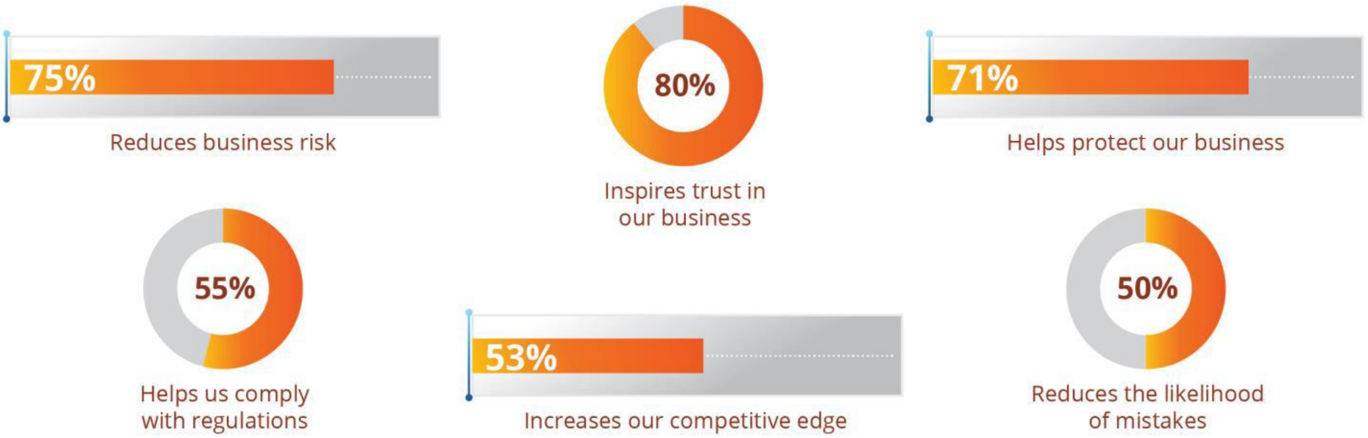
An ISO 27001 accredited Information Security Management System may help organisations:

- Identify risks
- Assess the implications of risks
- Implement systemised controls to limit damage to the organisation

ADAPTIVE CERTIFICATIONS

CERTIFIED ISO 27001 ADAPTIVE

BENEFITS

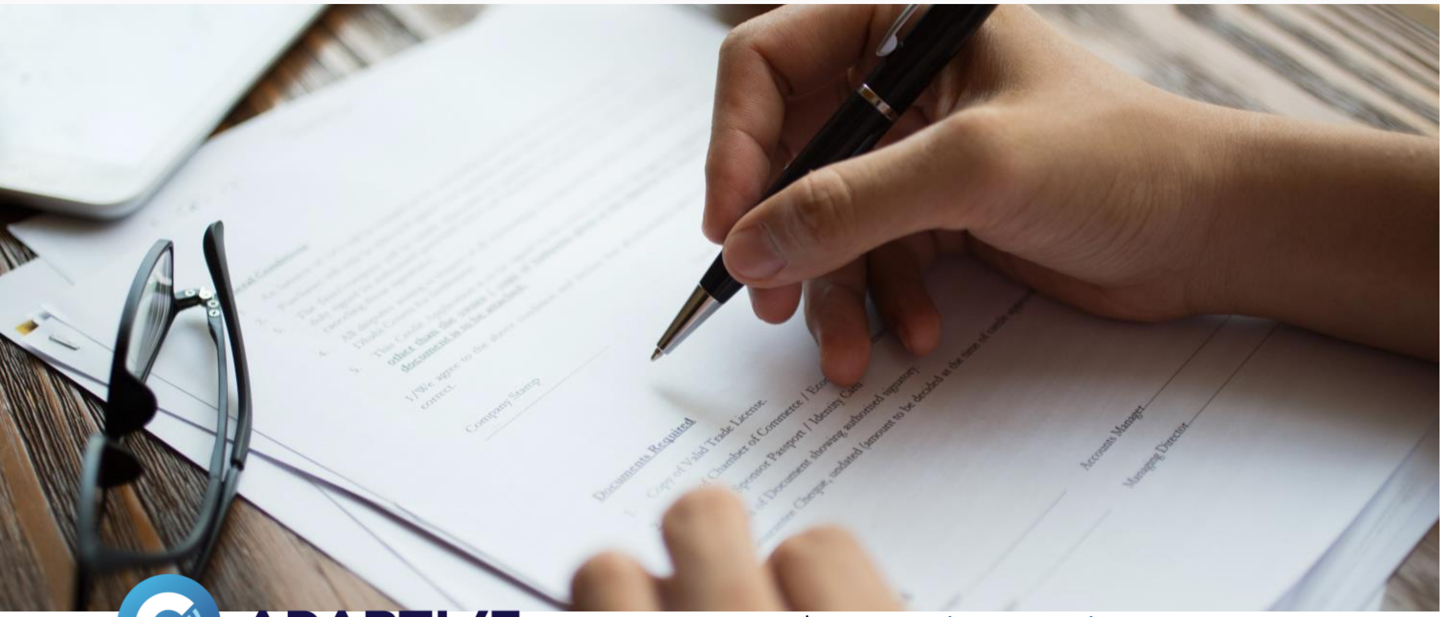


EXTERNAL

- Procedures that will promptly detect security breaches improves your reputation with stakeholders
- Aligns with customer requirements.
- Communicates your regulatory requirements to all interested and invested parties
- Shows a commitment to ensuring continued improvements and responding to potential threats accordingly

INTERNAL

- Improves the reliability and security of systems and information
- Improved management processes
- Integrates with corporate risk strategies
- Increases business resilience.
- Builds employee confidence



HOW TO MEET THE ISO ISO 27001 REQUIREMENTS

Terms and Definitions

ISO 27001:2022 is an international standard outlining the management framework for Information Security Management Systems (ISMS). It covers a range of activities and processes pertaining to the management of information risks. The international standard for Information Security Management Systems (ISMS), a suite of activities concerning the management of information risks (referred to as 'information security risks' in the standard). The standard indicates appropriate controls within the ISMS that organisations can select and implement based on the relevancy to their processes.

All terms and definitions related to ISO 27001:2022 are in the standard. However, the standard does not provide any explanations for the words used. It is necessary to understand the terms before starting to implement the requirements of the standard.

Here are some of the most important terms and definitions

ACCESS CONTROL

Access control refers to ensuring that access to assets is authorised and restricted determined by the business and security requirements.

ANNEXURE A

Annexure A is 'normative', meaning that certified organisations are expected to use it, but may deviate from it or supplement it based on their specific requirements.

AVAILABILITY

Information that is accessible and usable upon demand by an authorised entity.

CONFIDENTIALITY

Confidentiality implies that information is not made available or disclosed to unauthorised individuals, entities or processes.

DOCUMENTED INFORMATION

Documented information refers to information that needs to be controlled by the organisation. It may be contained in a medium from any source and can relate to; the management system, including related processes.

EXTERNAL CONTEXT

Information is an asset that is essential to a business and consequently needs to be suitably protected.

INFORMATION SECURITY

Information security refers to the procedures that are in place to ensure the confidentiality, availability, and integrity of information.

INFORMATION SECURITY EVENT

An information security event is an identified occurrence of a system, service or network state that indicates a possible breach of information or failure of controls.

INFORMATION SECURITY CONTINUITY

Details the processes and procedures for ensuring continued information security operations.

INFORMATION SECURITY INCIDENT

A single or series of unwanted information security events that present a significant risk of compromising business operations and threatening information security.

INTEGRITY

Integrity refers to the accuracy and completeness of information.

INTERESTED PARTY

A person or organisation that can affect, be affected by or perceive themselves to be affected by a decision or activity.

INTERNAL CONTEXT

The environment in which the organisation seeks to achieve its objectives.

RISK ASSESSMENT

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

RISK OWNERS

The entity or person that is responsible and has the authority to manage risk.

STATEMENT OF APPLICABILITY

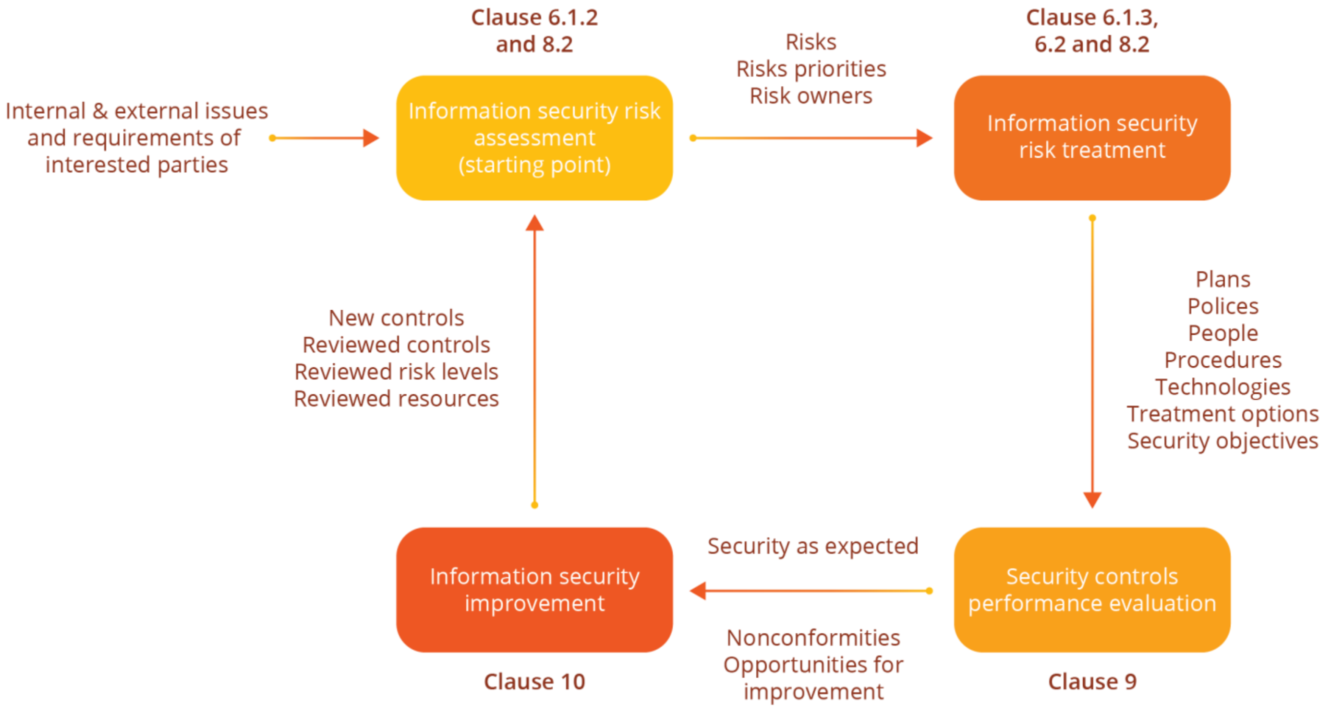
This refers to the output from the information risk assessments, particularly the decisions around treating those risks.

THE PROCESS FLOWCHART

A process is a set of interrelated or interacting activities that transforms inputs into outputs. These activities require allocation of resources such as people and materials. The process approach is a way of applying processes as a system. The process flowchart is a graphical overview of all processes within an organisation. Flow charts aid in the management of operations and provide the framework to track process performance.

The following diagram represents an example of e risk management process, forming the basis of an ISO 27001 ISMS, demonstrating how a process approach is an excellent way to organise and manage information security processes to create value for the organisation.

PROCESS APPOROACH APPLIED TO INFORMATION SECURITY RISK MANAGEMENT



Internal & external issues and requirements of interested parties

Clause 6.1.2 and 8.2

Information security risk assessment (starting point)

Risks
Risks priorities
Risk owners

Clause 6.1.3, 6.2 and 8.2

Information security risk treatment

Plans
Polices
People
Procedures
Technologies
Treatment options
Security objectives

Security controls performance evaluation

Clause 9

Security as expected

Nonconformities
Opportunities for improvement

Information security improvement

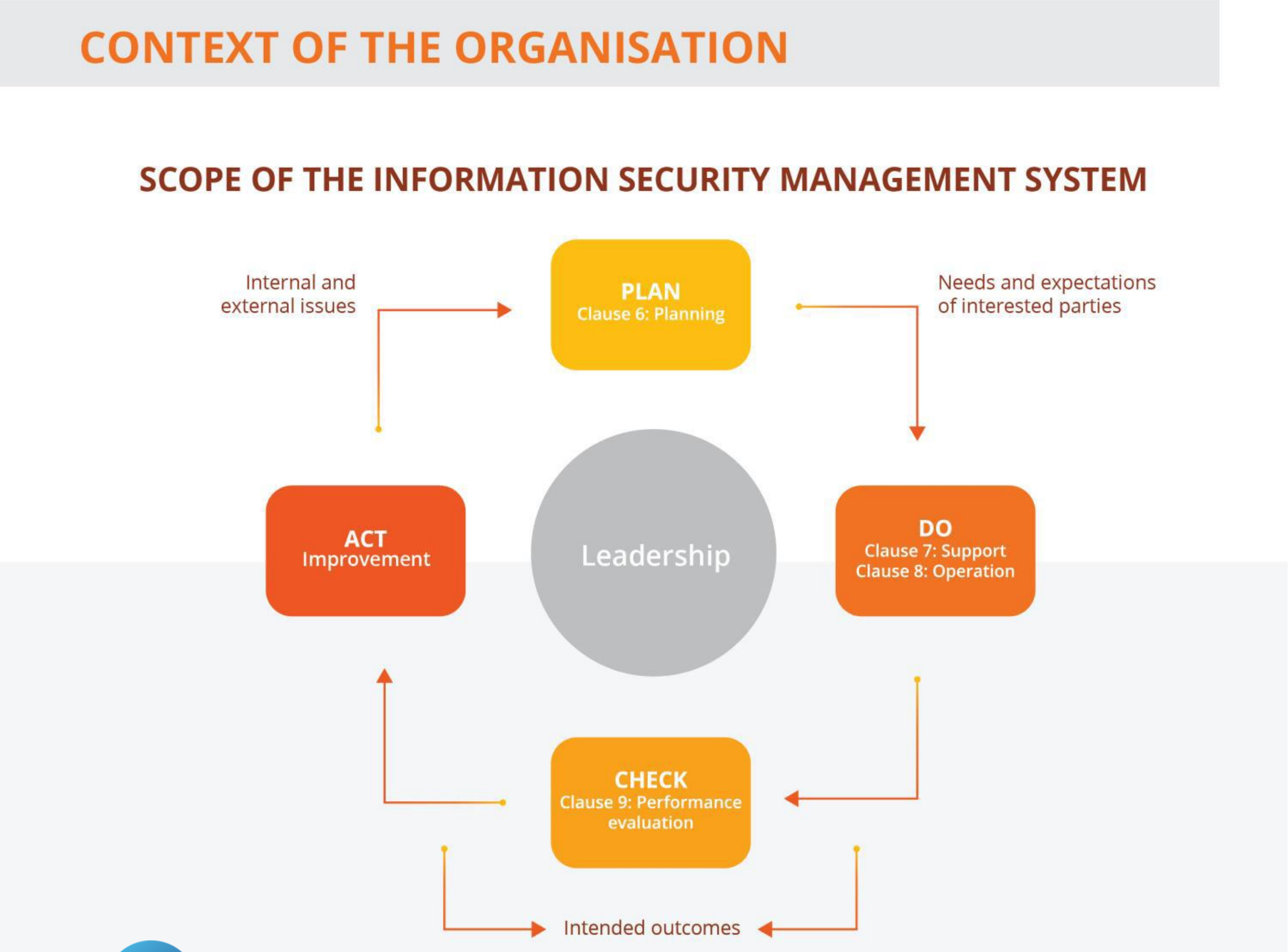
Clause 10

New controls
Reviewed controls
Reviewed risk levels
Reviewed resources

PLAN-DO-CHECK-ACT (PDCA) CYCLE

Businesses are continually evolving as a result of internal and external influences. This makes it necessary for the ISMS also to develop (adjusting objectives and procedures, for example). ISO 27001:2022 ensures that the constant evolution is accounted for by adopting a “Plan-Do-Check-Act” cycle as part of its framework.

Below is an example of such an approach:



CONTEXT OF THE ORGANISATION

SCOPE OF THE INFORMATION SECURITY MANAGEMENT SYSTEM

Internal and external issues

PLAN
Clause 6: Planning

Needs and expectations of interested parties

ACT
Improvement

Leadership

DO
Clause 7: Support
Clause 8: Operation

CHECK
Clause 9: Performance evaluation

Intended outcomes

ISO 27001 REQUIREMENTS

The structure of the ISO 27001:2022 standard splits into 10 sections (clauses):

- 1 to 3 are introductory, and
- 4 to 10 contain the requirements for the Information Security Management Systems

PRINCIPAL CLAUSES OF ISO 27001

Clause 4: Context of the organisation – Understand your organisation to implement an ISMS.

- This section covers requirements for:
- Identifying internal and external concerns
- Identifying interested parties and their expectations, including regulatory requirements

Defining the scope of the ISMS.

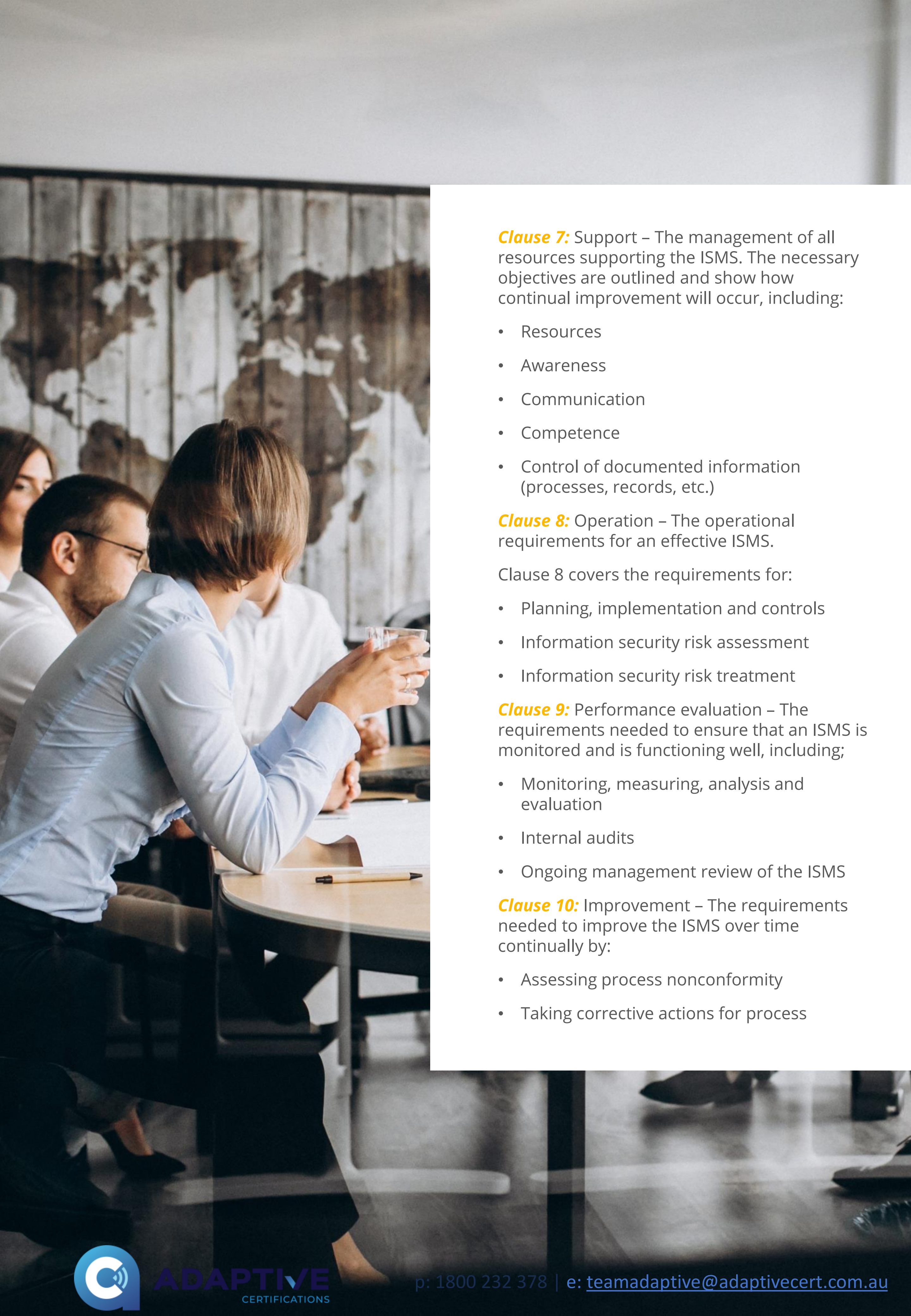
Clause 5: Leadership – Top management is instrumental in the implementation of the ISMS.

- Top management needs to demonstrate a commitment to the ISMS by:
- Ensuring policies and procedures align with each other and the direction of the business
- Defining and maintaining well-documented procedures throughout the organisation

Assigning roles and responsibilities throughout the organisation.

Clause 6: Planning – Top management must plan for and address risk and opportunities.

- The organisation must plan to handle risks and opportunities where relevant
- Information security risk assessment and risk treatment
- Outline objectives for the organisation and a plan to achieve them



Clause 7: Support – The management of all resources supporting the ISMS. The necessary objectives are outlined and show how continual improvement will occur, including:

- Resources
- Awareness
- Communication
- Competence
- Control of documented information (processes, records, etc.)

Clause 8: Operation – The operational requirements for an effective ISMS.

Clause 8 covers the requirements for:

- Planning, implementation and controls
- Information security risk assessment
- Information security risk treatment

Clause 9: Performance evaluation – The requirements needed to ensure that an ISMS is monitored and is functioning well, including;

- Monitoring, measuring, analysis and evaluation
- Internal audits
- Ongoing management review of the ISMS

Clause 10: Improvement – The requirements needed to improve the ISMS over time continually by:

- Assessing process nonconformity
- Taking corrective actions for process

HOW TO PLAN YOUR CERTIFICATION PROJECT

PROJECT PLAN

A management system be?

- Fit for Purpose
- Simple, easily understood, and accessible
- Effective
- Able to integrate with other management systems.

TASK	ACTIONS	NOTES
1. Gap Analysis	Undertake Gap Analysis	
2. System Planning	Identify Interested Parties	
2. System Planning	Operational Risk Assessment	
2. System Planning	Information Security Manual - Planning	
2. System Planning	Information Security Manual - Support	
2. System Planning	Information Security Manual - Operations	
2. System Planning	Information Security Manual - Improvement	
2. System Planning	Information Security Risk Analysis	
2. System Planning	Branding/design of completed ISMS Manual	
3. Draft System Documents	Information Security Policy	
3. Draft System Documents	Management System Registers	
3. Draft System Documents	Management System Procedures	
4. Implementation Planning	Plan implementation	
4. Implementation Planning	Set objectives and targets	
4. Implementation Planning	Compile legal and other requirements	
5. Awareness Training	Define awareness requirements	
5. Awareness Training	Carry out awareness training	
6. Implementation Activities	Plan training requirements and activities	
6. Implementation Activities	Implement training requirements and activities	
7. Review	Internal audits	
7. Review	Management Review Meeting	
8. Stage 1 Audit	Engage certification company for stage 1 audit	
8. Stage 1 Audit	Complete stage 1 audit	
9. Address Gaps	Address any gaps raised at stage 1 audit	
10. Stage 2 Audit - Certification	Undertake stage 2 audit and receive certification	