ISO 27001:2022

The new global standard for Information Security management systems

November 2022

This presentation is brought to you by Qudos Management – a leading Australian management system consultancy practice and developer of the Qudos^3 IMS software solution.

For over 20 years, we have helped small, medium and large organizations to successfully develop management systems and achieve ISO certification.

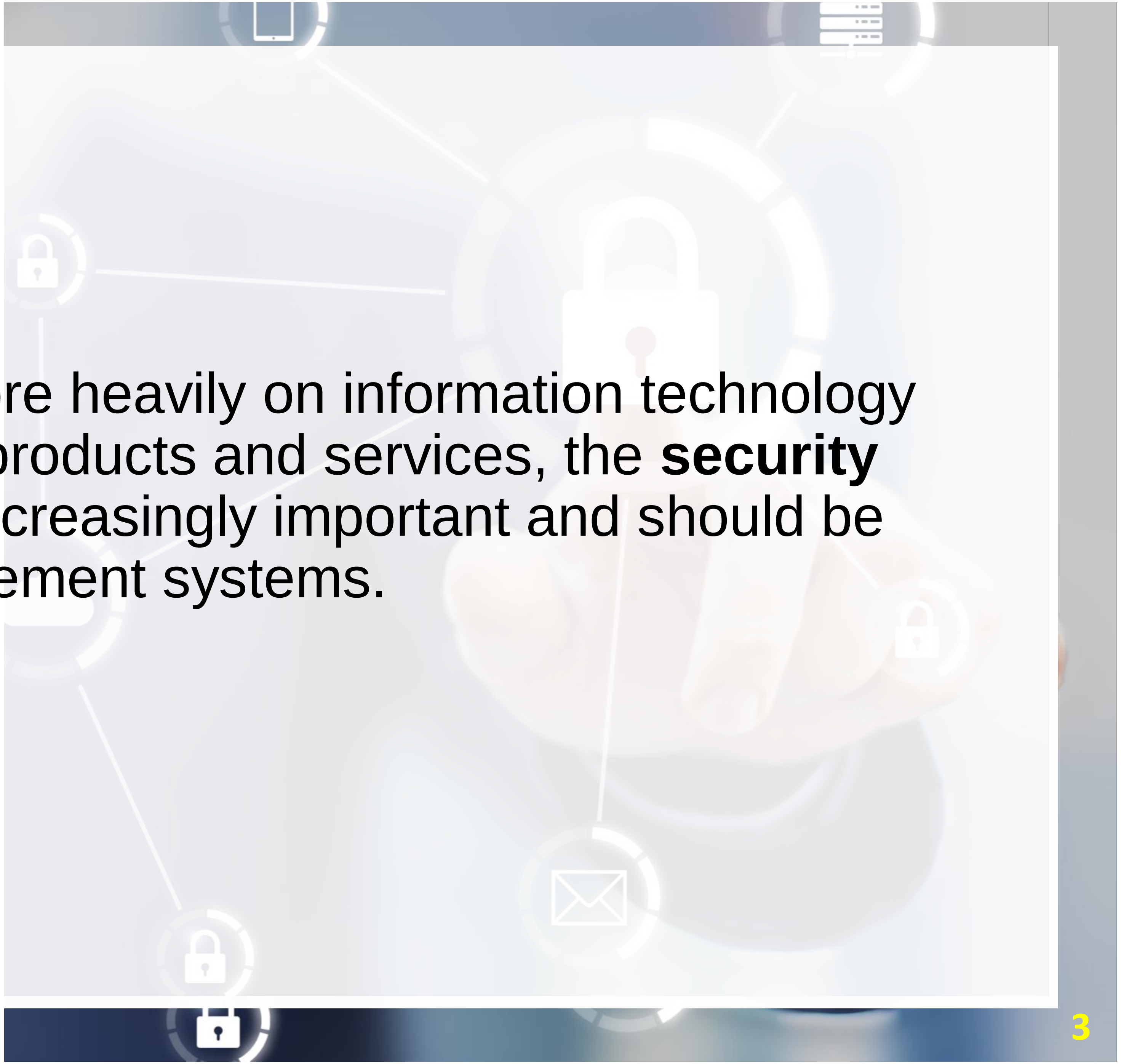
Summary of requirements	How currently addressed	Improvements	Status	Notes
4 CONTEXT OF THE ORGANIZATION				
4.1 Understanding the organization and its context				
Determine the factors that may affect the ISMS and its ability to achieve the intended results.	Situational analysis in place and updated to include InfoSec requirements.		🟩	• Consider external issues: Political, Economic, Social, Technological, Environmental, Legal (PESTEL) • Consider internal issues such as performance, culture and resources. • Business plan • SWOT analysis QMT Situational analysis / strategy plan, PESTEL /

; not specify a requirement for
iview of these factors. However, it
isable to do that e.g. schedule a
or include as an agenda item in
ew. The ISO 9001 Quality standard
irement and it would therefore be
grated system.

carried out in tandem with 4.1. It
nvolve the documentation of an
; Table'.

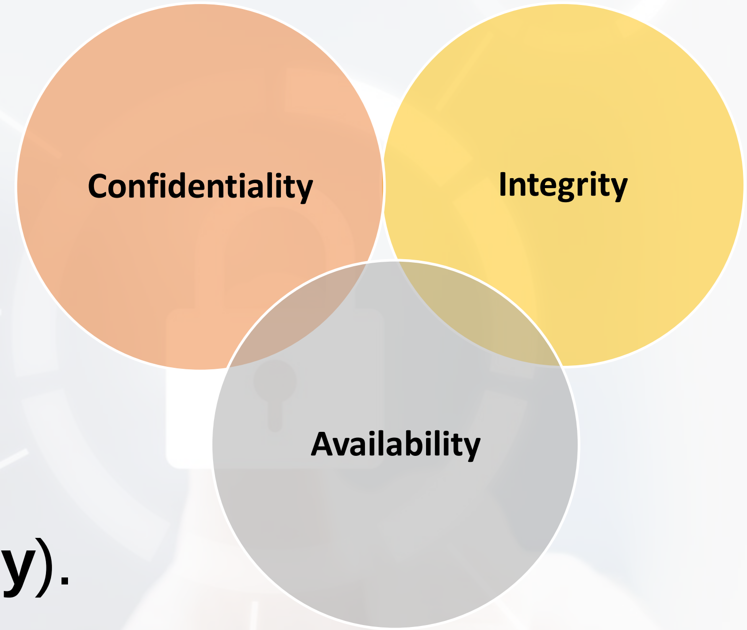
) 27001 does not specify a
monitoring and review of these
it might still be advisable to do that
eriodic review / or include as an
anagement review. The ISO 9001
does have a requirement and it
e required in an integrated system.

-column Interested parties table.



As we come to rely more heavily on information technology for the delivery of our products and services, the **security** of that information is increasingly important and should be included in our management systems.

What is Information Security?



Basically, we want our information to:

- Only be accessed by the right people (**Confidentiality**).
- Be correct with only authorised changes (**Integrity**).
- Be available to read and use whenever we want (**Availability**).

These 3 principles are often referred to by the acronym CIA, and they form the basis of information security.

Is it relevant to your business or organization?

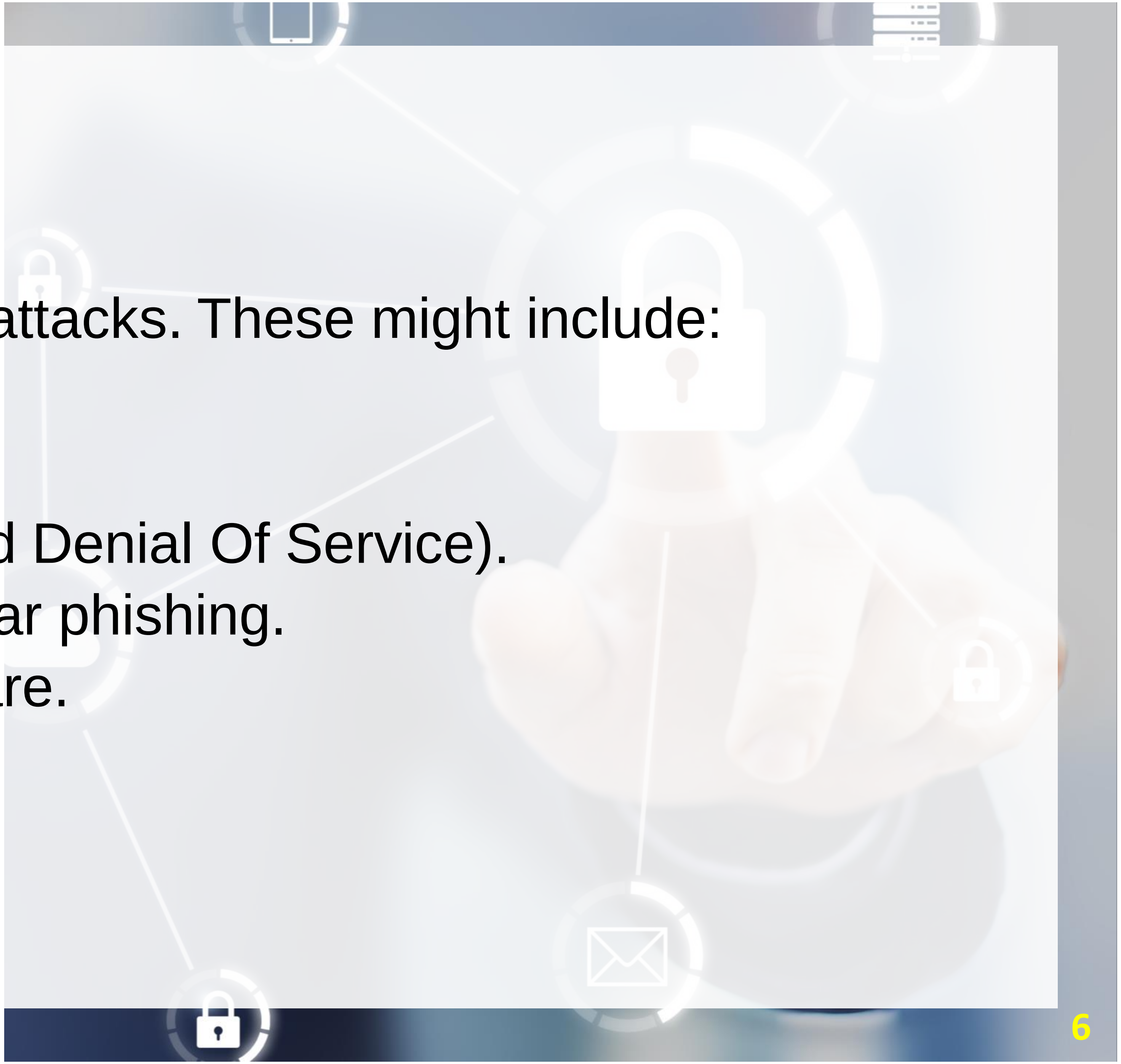
Yes, it’s relevant to every business.

Even if your organization is not planning to implement a full ISMS (or Information Security Management System) based on ISO 27001, there are elements of information Security that should be considered.

Cyber attacks

We all face the risk of attacks. These might include:

- Hacking
- DDOS (Distributed Denial Of Service).
- Phishing and Spear phishing.
- Malware or spyware.
- Ransomware.

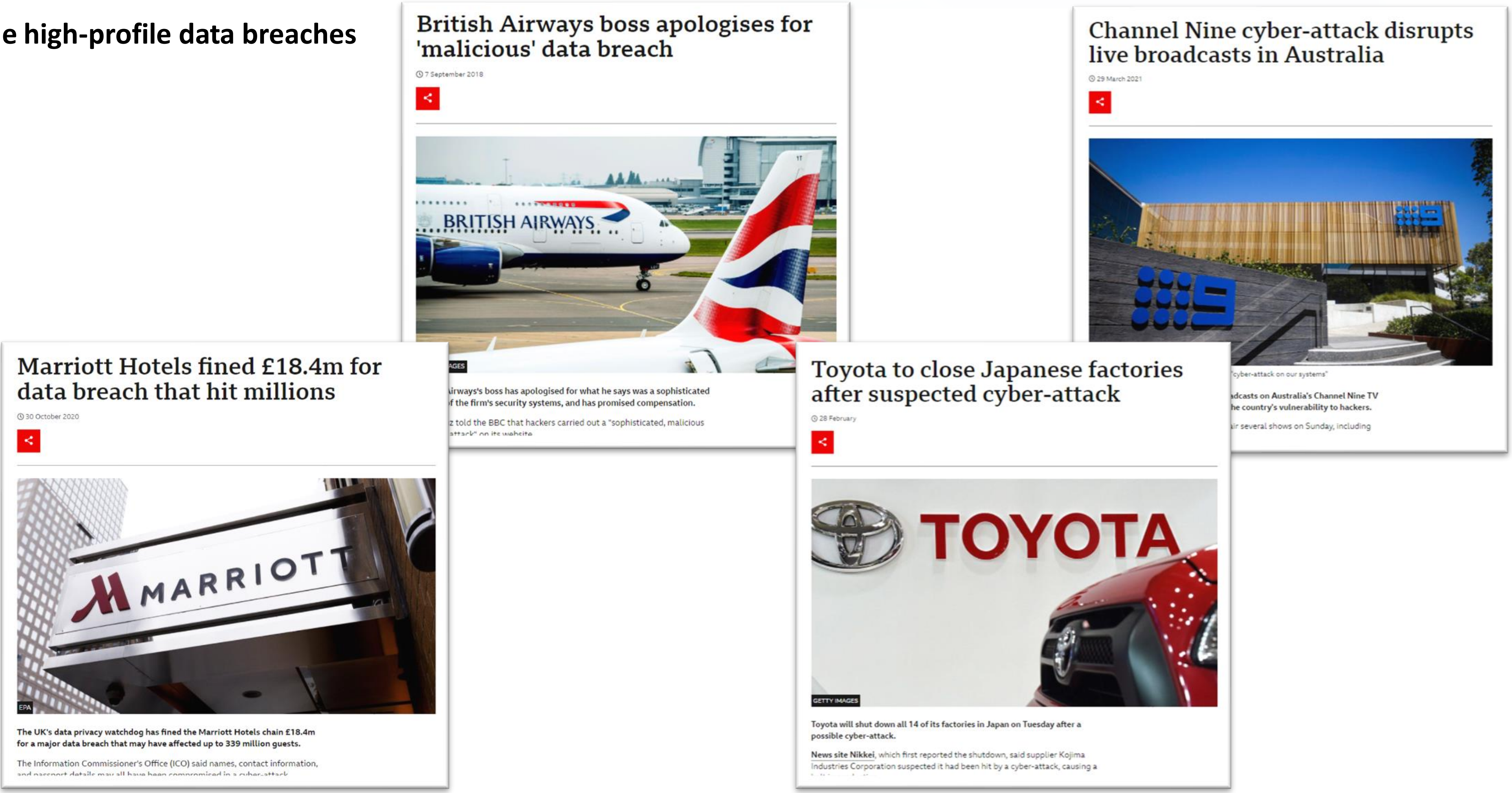


Such attacks may have many impacts, including:

- Loss of availability
- Loss of confidentiality.
- Reputational harm.
- Legal / regulatory non-compliance.
- Disruption to operations.

They may even present an existential threat to your business.

Some high-profile data breaches



British Airways boss apologises for 'malicious' data breach

7 September 2018

irways's boss has apologised for what he says was a sophisticated
f the firm's security systems, and has promised compensation.

z told the BBC that hackers carried out a "sophisticated, malicious
attack" on its website

Channel Nine cyber-attack disrupts live broadcasts in Australia

29 March 2021

"cyber-attack on our systems"

dcasts on Australia's Channel Nine TV
he country's vulnerability to hackers.

ir several shows on Sunday, including

Marriott Hotels fined £18.4m for data breach that hit millions

30 October 2020

The UK's data privacy watchdog has fined the Marriott Hotels chain £18.4m for a major data breach that may have affected up to 339 million guests.

The Information Commissioner's Office (ICO) said names, contact information, and passport details may all have been compromised in a cyber-attack

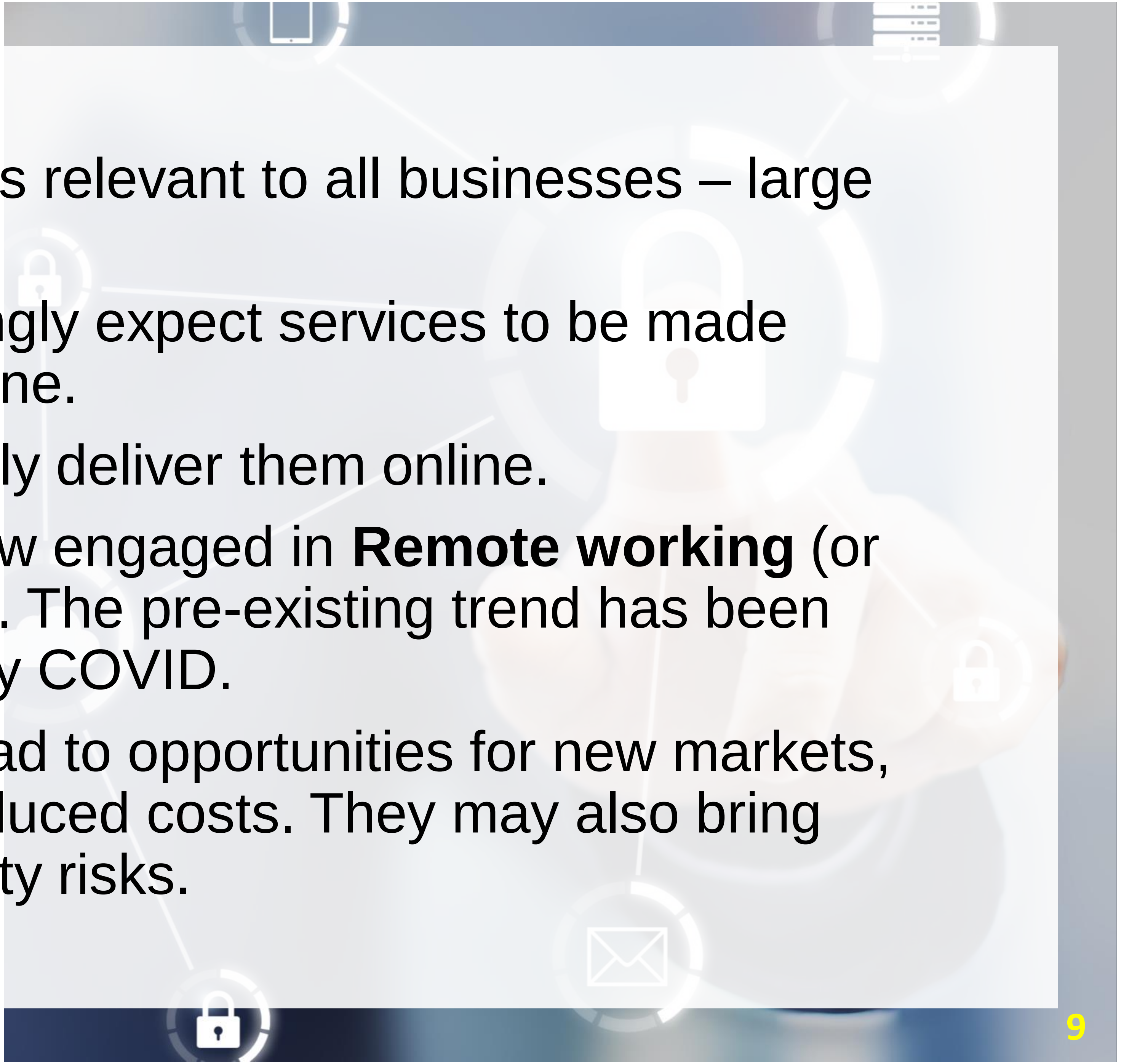
Toyota to close Japanese factories after suspected cyber-attack

28 February

Toyota will shut down all 14 of its factories in Japan on Tuesday after a possible cyber-attack.

News site Nikkei, which first reported the shutdown, said supplier Kojima Industries Corporation suspected it had been hit by a cyber-attack, causing a

Extracts from BBC News web site



- Information Security is relevant to all businesses – large and small
- **Customers** increasingly expect services to be made available to them online.
- **Suppliers** increasingly deliver them online.
- Many workers are now engaged in **Remote working** (or Teleworking or WFH). The pre-existing trend has been greatly accelerated by COVID.

These changes can lead to opportunities for new markets, better services and reduced costs. They may also bring new information security risks.

Customer requirement

We also see a growing number of clients facing a requirement from their clients to demonstrate that they have appropriate information security controls in place and often for ISO 27001 certification.

Legal / regulatory requirement

- Privacy Act (Australia) - with Notifiable Data Breaches amendment 2017.
- GDPR (General Data Protection Regulations) (EU and UK).
- Privacy Act (NZ) – similarities with GDPR.

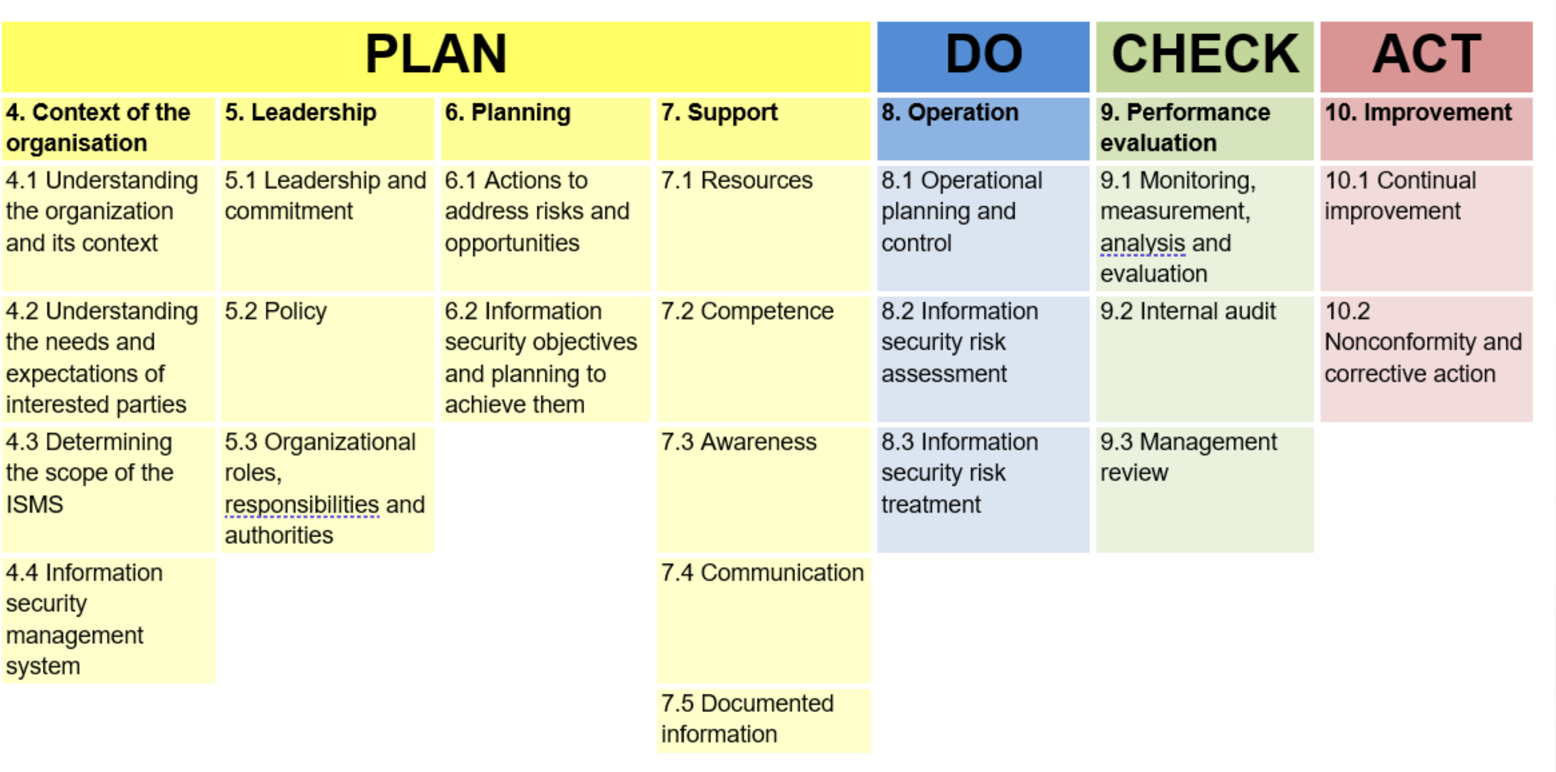
ISO 27001:2022 standard for Information Security Management Systems

The certification standard for information security.

It is based on the famous PDCA cycle and was one of the first standards to use ISO’s common high-level structure and terminology.

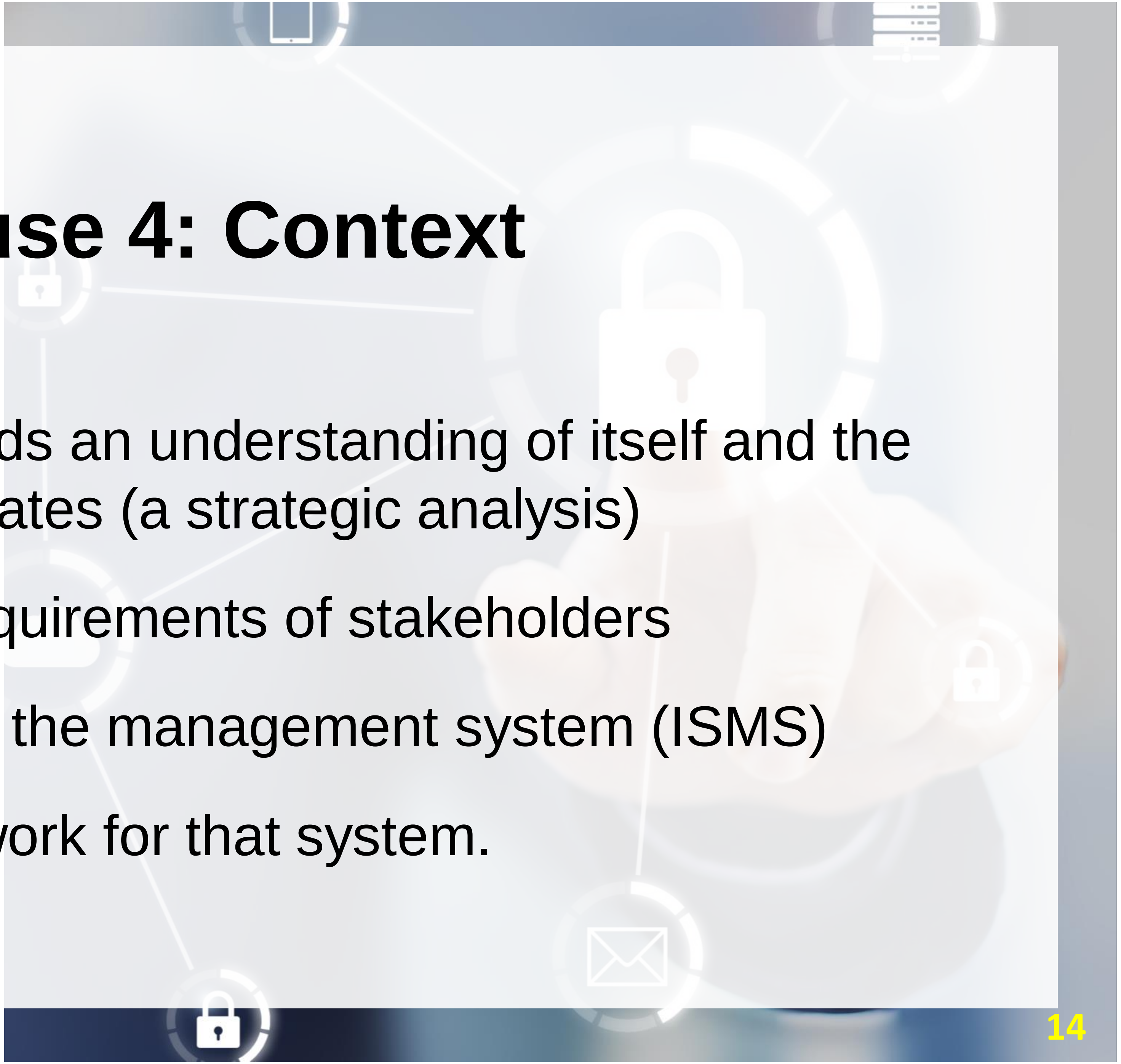
Therefore, the clause structure will be familiar to those used to ISO 9001.

Relationship of clauses with the PDCA cycle

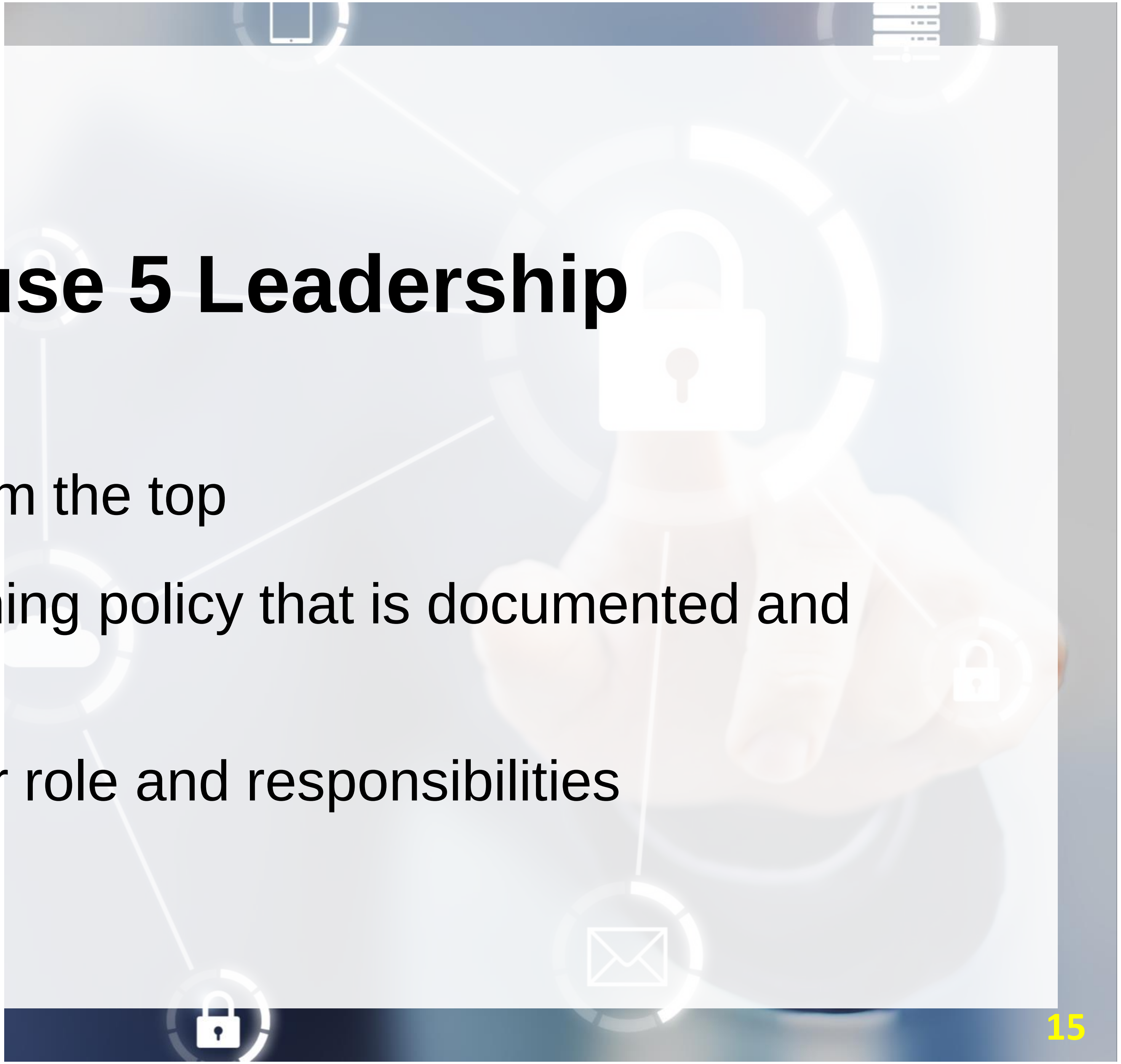


PLAN				DO	CHECK	ACT
4. Context of the organisation	**5. Leadership**	**6. Planning**	**7. Support**	**8. Operation**	**9. Performance evaluation**	**10. Improvement**
4.1 Understanding the organization and its context	5.1 Leadership and commitment	6.1 Actions to address risks and opportunities	7.1 Resources	8.1 Operational planning and control	9.1 Monitoring, measurement, analysis and evaluation	10.1 Continual improvement
4.2 Understanding the needs and expectations of interested parties	5.2 Policy	6.2 Information security objectives and planning to achieve them	7.2 Competence	8.2 Information security risk assessment	9.2 Internal audit	10.2 Nonconformity and corrective action
4.3 Determining the scope of the ISMS	5.3 Organizational roles, responsibilities and authorities		7.3 Awareness	8.3 Information security risk treatment	9.3 Management review	
4.4 Information security management system			7.4 Communication			
			7.5 Documented information			

ISO 27001 Clause 4: Context



- The organization builds an understanding of itself and the world in which it operates (a strategic analysis)
- It understands the requirements of stakeholders
- It sets boundaries for the management system (ISMS)
- It sets out the framework for that system.



ISO 27001 Clause 5 Leadership

- The system is led from the top
- There is an over-arching policy that is documented and communicated
- Everyone knows their role and responsibilities

ISO 27001 Clause 6 Planning

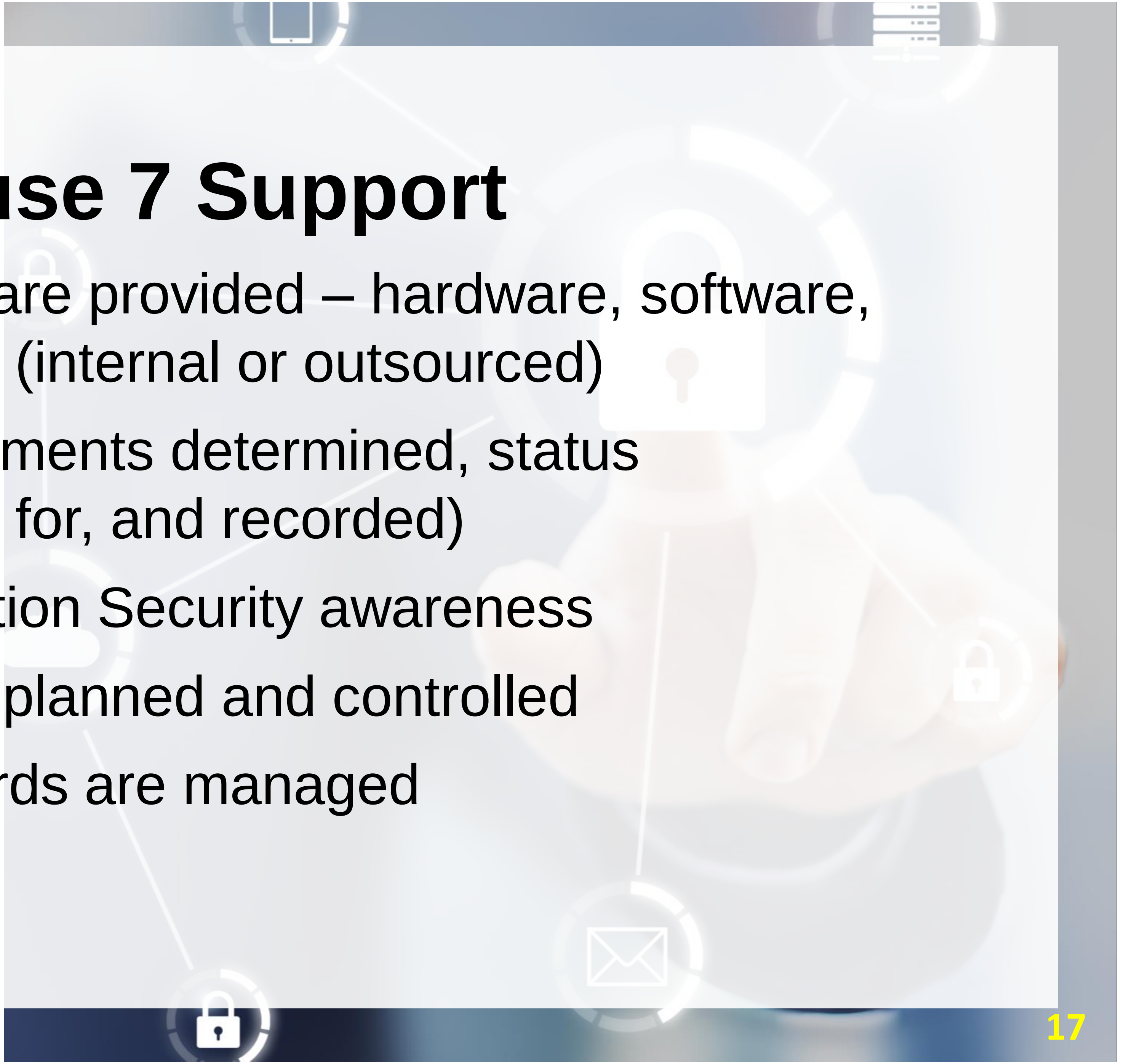
- Actions are planned to address risk and opportunities
- Determine plans on how to assess and treat risks
- Measurable objectives are established

There is a blog on our web site about SMART objectives – with 50 examples.

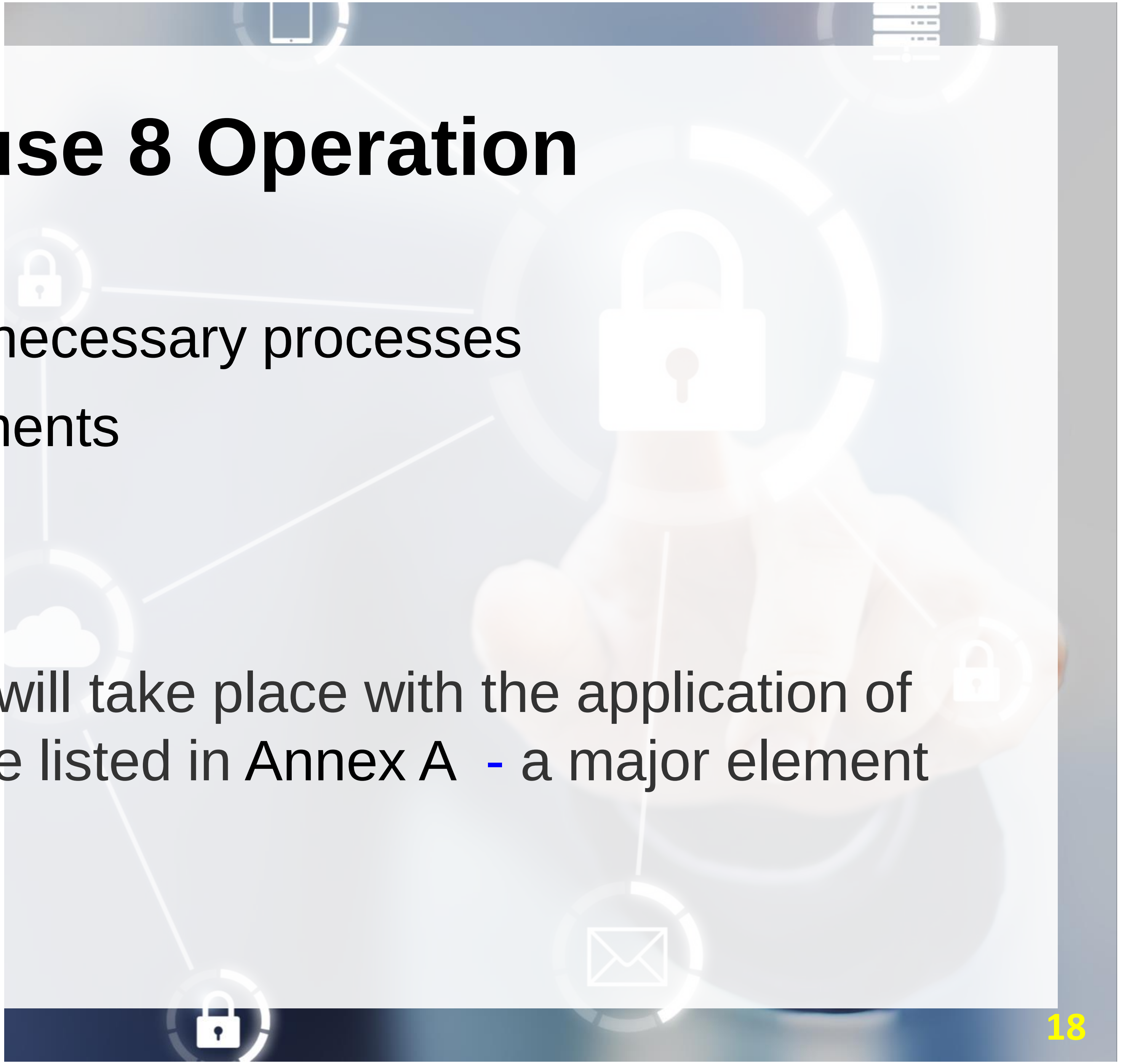
https://qudos-software.com/smart-objectives/

ISO 27001 Clause 7 Support

- Adequate resources are provided – hardware, software, infrastructure, people (internal or outsourced)
- Competence (requirements determined, status determined, provided for, and recorded)
- People have Information Security awareness
- Communications are planned and controlled
- Documents and records are managed



ISO 27001 Clause 8 Operation



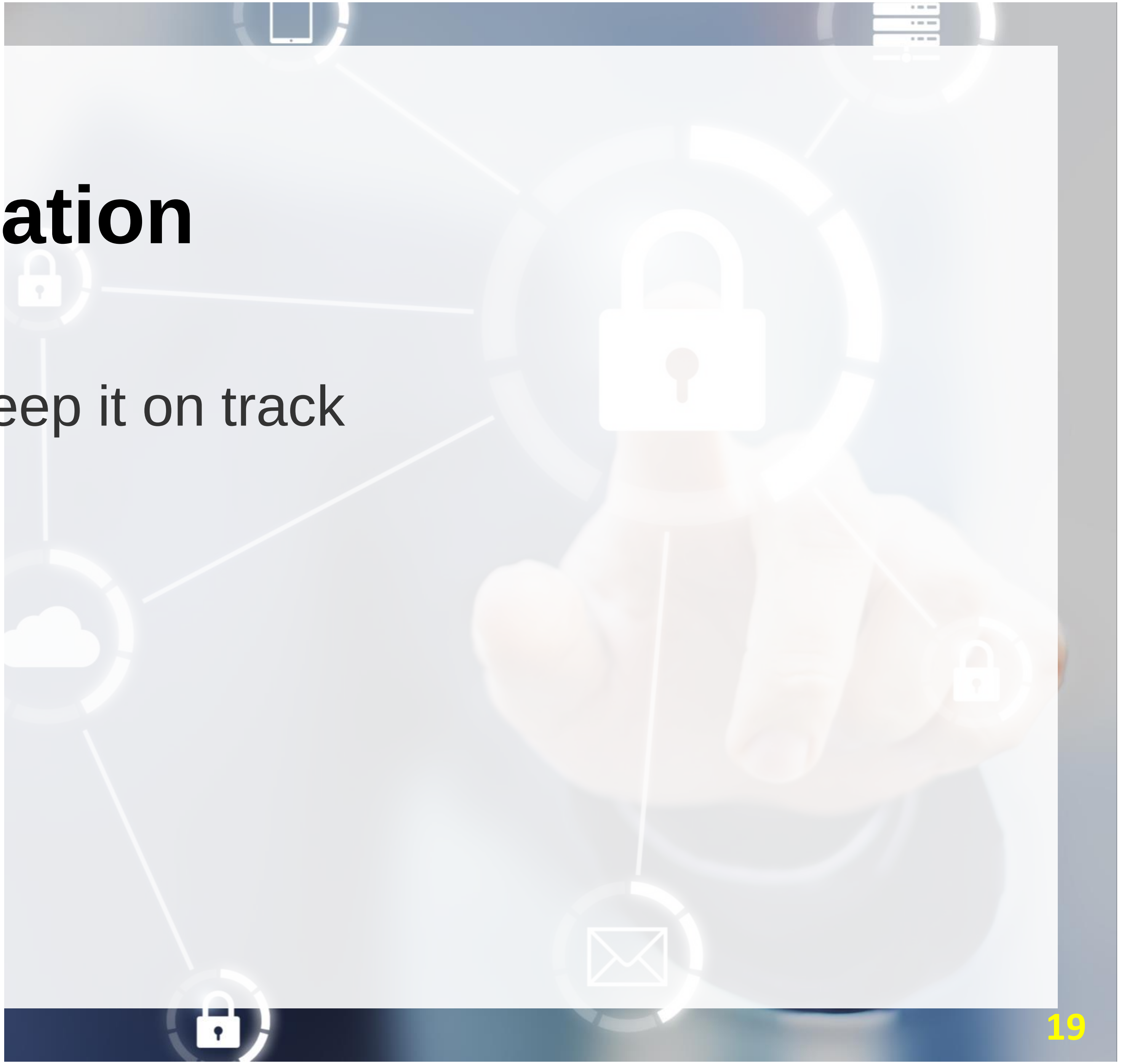
- Plan and control the necessary processes
- Perform risk assessments
- Treat risks

The treatment of risks will take place with the application of controls including those listed in Annex A - a major element of ISO 27001.

Clause 9 Evaluation

Check the system to keep it on track

- Operational checks
- Internal audits
- Management review

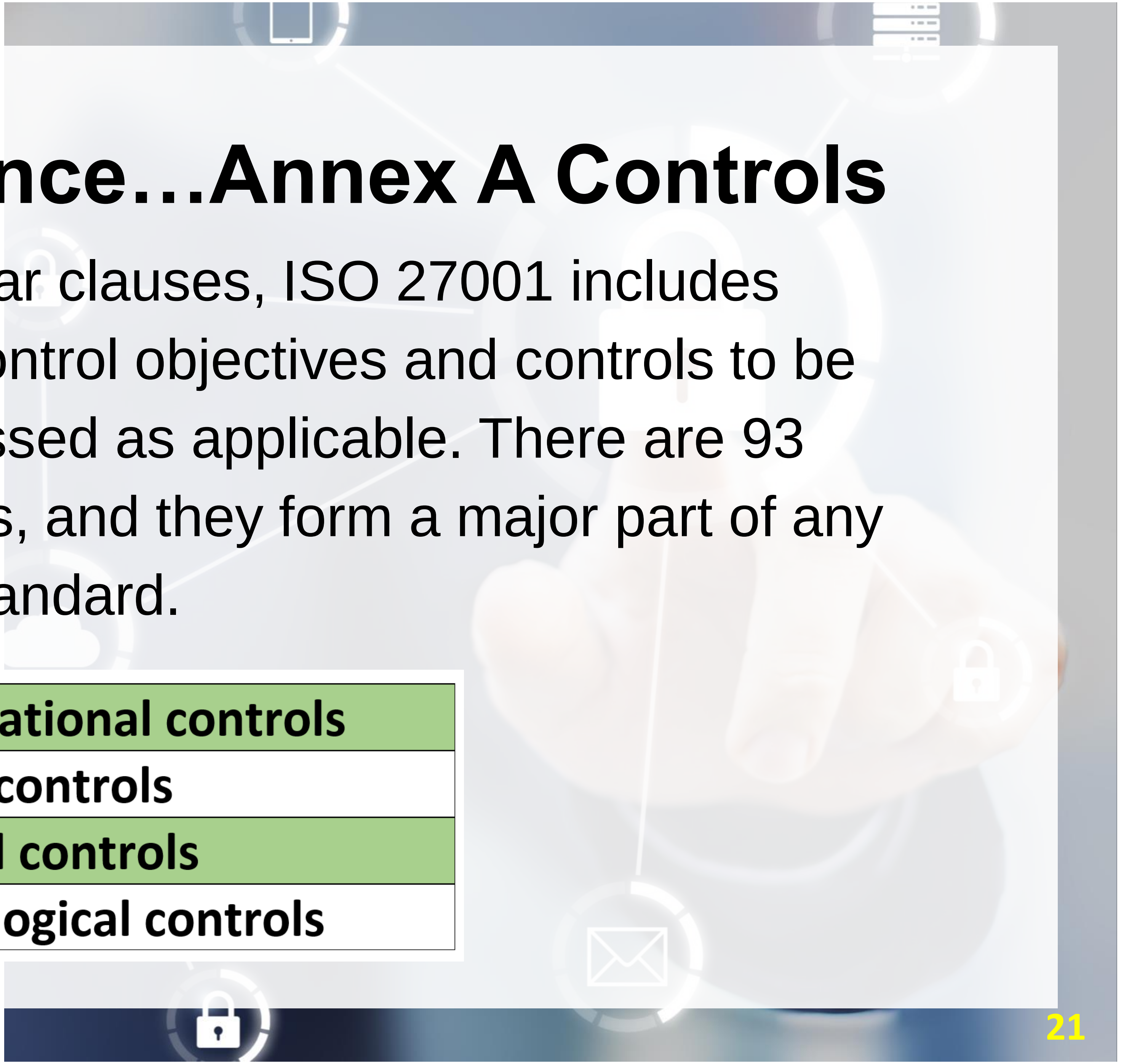


ISO 27001 Clause 10 Improvement

Deal with issues and their root causes, and continuously improve the system

The big difference…Annex A Controls

In addition to the regular clauses, ISO 27001 includes **Annex A** which lists control objectives and controls to be considered and addressed as applicable. There are 93 controls in 4 categories, and they form a major part of any ISMS based on that standard.



A5 Organizational controls
A6 People controls
A7 Physical controls
A8 Technological controls

Annex A5:

Organizational controls

These controls include:

- The development of policies
- Threat intelligence
- Asset management
- Access control
- Information classification and labelling
- Cloud services

Security Classification

Restricted
Confidential
Internal
Public
Unclassified

ISO 27001 Information Security

Information Security Policy

We will establish, maintain, and continually improve an ISMS (information security management system) to manage the risks facing information belonging to our organization and relevant interested parties. We aim to protect that information from all threats (whether internal or external, deliberate, or accidental), and safeguard its confidentiality, integrity, and availability. Specifically, we will ensure that:

- Business requirements for the availability of information and information systems are met

ccess

tection from unauthorized disclosure, theft, or

ess) will be maintained by protecting against

ned, and tested, to ensure that information
verse events

le to all employees and relevant contractors

to the ICT Manager and investigated

ented to identify any weaknesses in the
sified assets

nce with the ISO 27001 standard.

inistering our ISMS, it is the responsibility of
e Policy.

Annex A6:

People controls

These controls include:

- Screening of workers
- The disciplinary process
- Confidentiality / NDAs
- Remote working

Annex A7:

Technological controls

These controls include:

- Physical security for offices etc.
- Physical security monitoring
- Clear desk and clear screen
- Storage media
- Secure disposal

Annex A8:

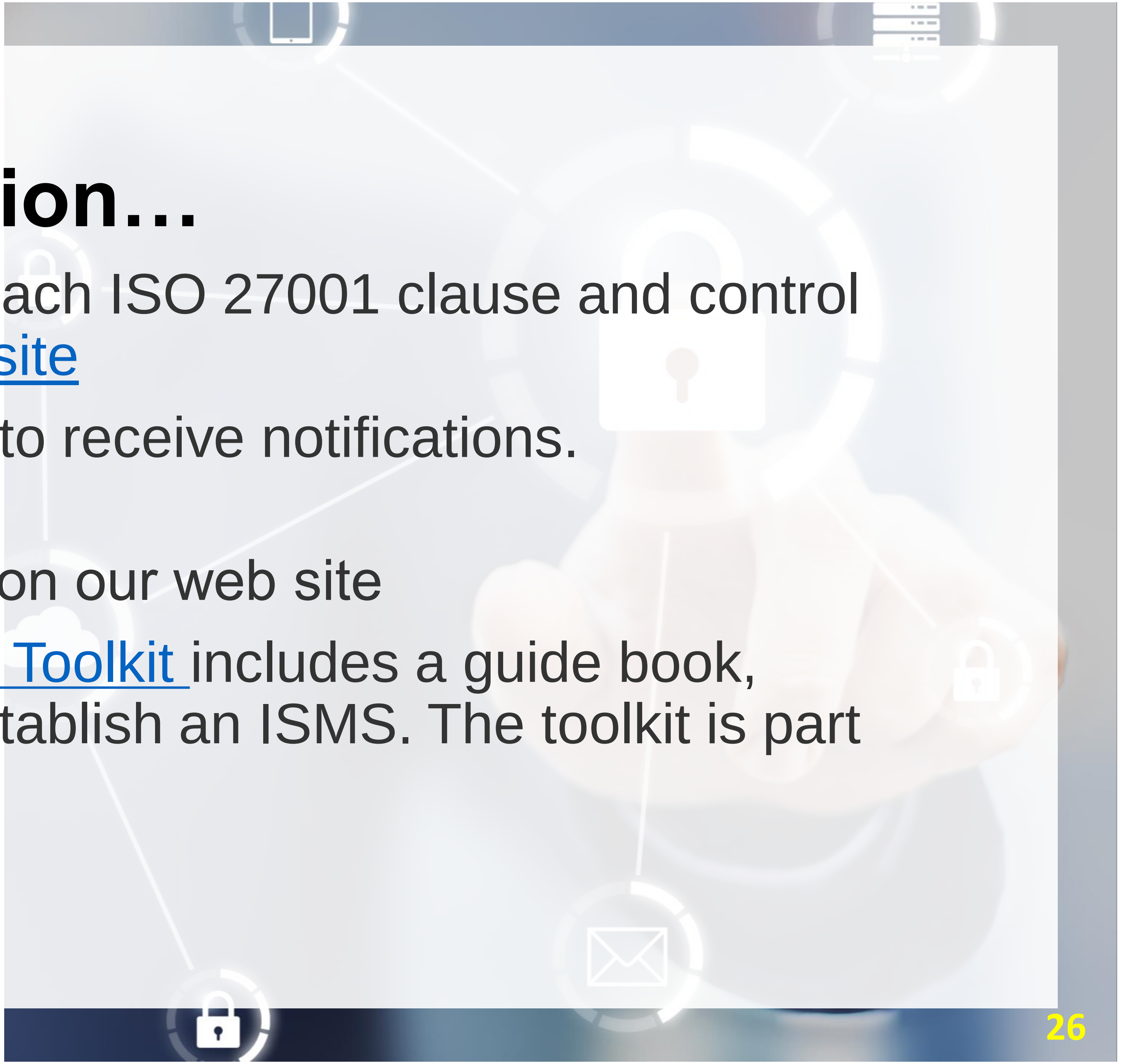
Physical controls

These controls include:

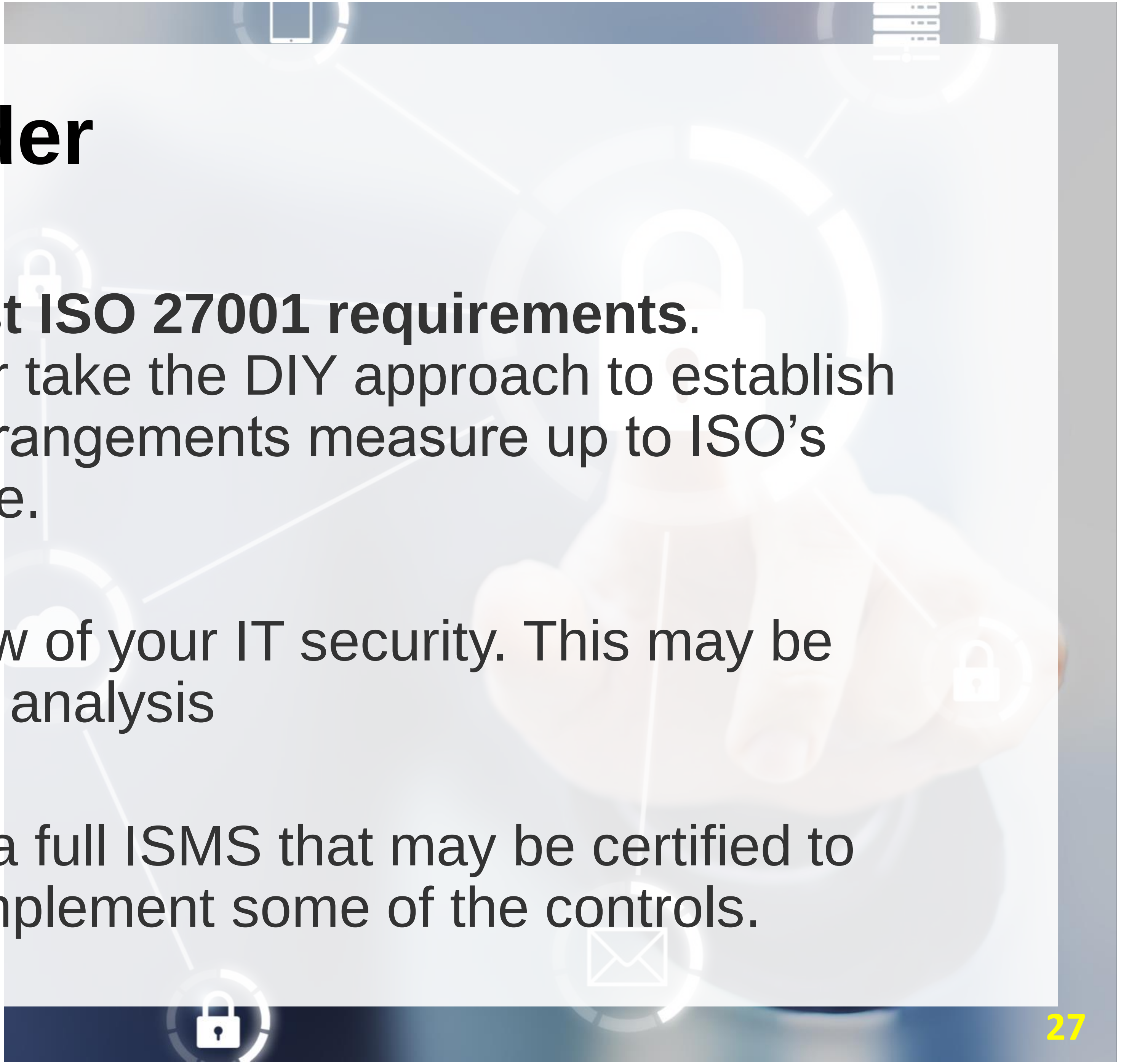
- Endpoint user devices.
- Protection against malware
- Information deletion
- Data masking
- Information backup

For more information…

- A series of blog posts on each ISO 27001 clause and control are published on our web site
- Sign up for our newsletter to receive notifications.
- Follow us on LinkedIn
  A ‘Follow us’ link button is on our web site
- Qudos ISO 27001 InfoSec Toolkit includes a guide book, documents and tools to establish an ISMS. The toolkit is part of Qudos^3 IMS software.

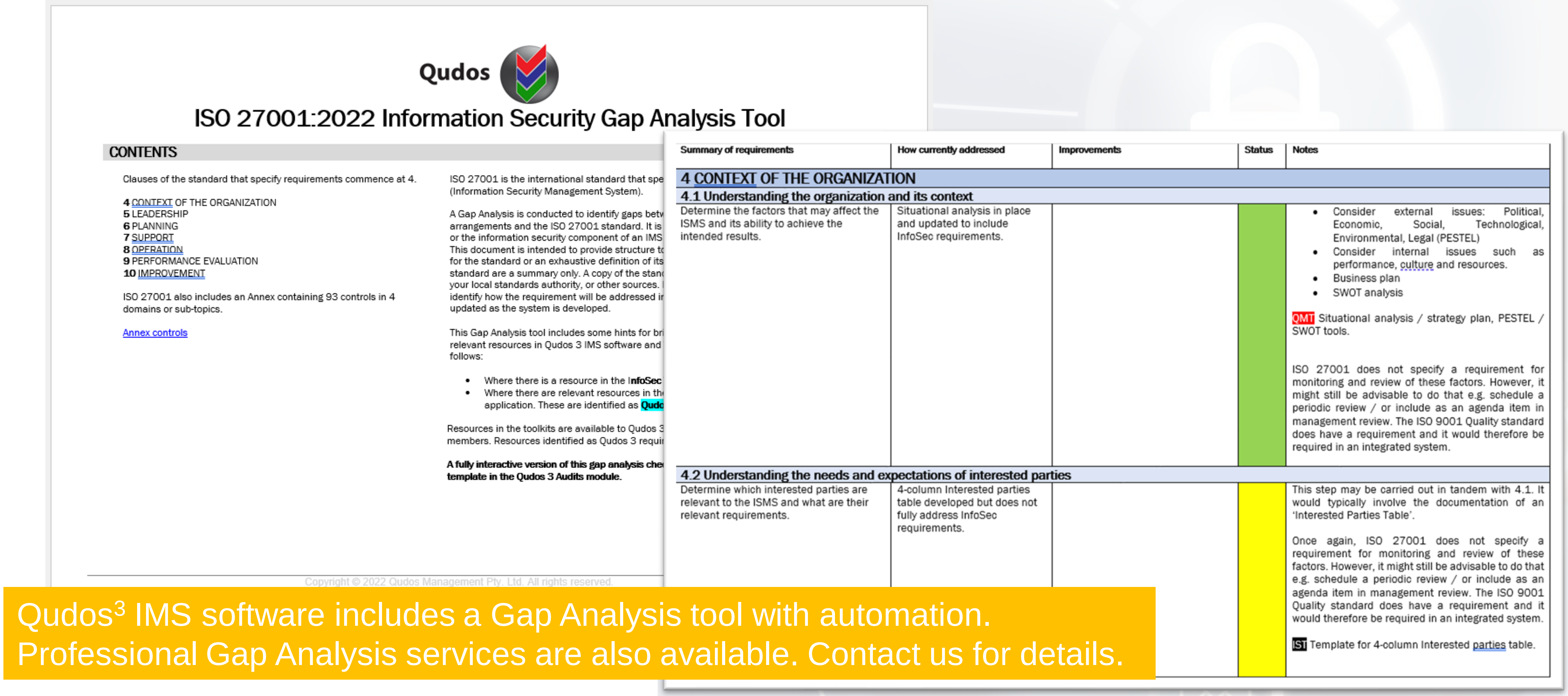


Steps to consider



- **Gap Analysis against ISO 27001 requirements.** Engage a specialist or take the DIY approach to establish where your current arrangements measure up to ISO’s model of good practice.
- **IT Security review** An independent review of your IT security. This may be done alongside a gap analysis
- **Plan your system** Whether you choose a full ISMS that may be certified to the standard or just implement some of the controls.

Gap Analysis



Qudos

ISO 27001:2022 Information Security Gap Analysis Tool

CONTENTS

Clauses of the standard that specify requirements commence at 4.

ISO 27001 also includes an Annex containing 93 controls in 4 domains or sub-topics.

Annex controls

ISO 27001 is the international standard that spe
(Information Security Management System).

A Gap Analysis is conducted to identify gaps betw
arrangements and the ISO 27001 standard. It is
or the information security component of an IMS
This document is intended to provide structure to
for the standard or an exhaustive definition of its
standard are a summary only. A copy of the stanc
your local standards authority, or other sources. I
identify how the requirement will be addressed ir
updated as the system is developed.

This Gap Analysis tool includes some hints for bri
relevant resources in Qudos 3 IMS software and
follows:

- Where there is a resource in the I**nfoSec**
- Where there are relevant resources in the
application. These are identified as **Qudo**

Resources in the toolkits are available to Qudos 3
members. Resources identified as Qudos 3 requir

A fully interactive version of this gap analysis chec
template in the Qudos 3 Audits module.

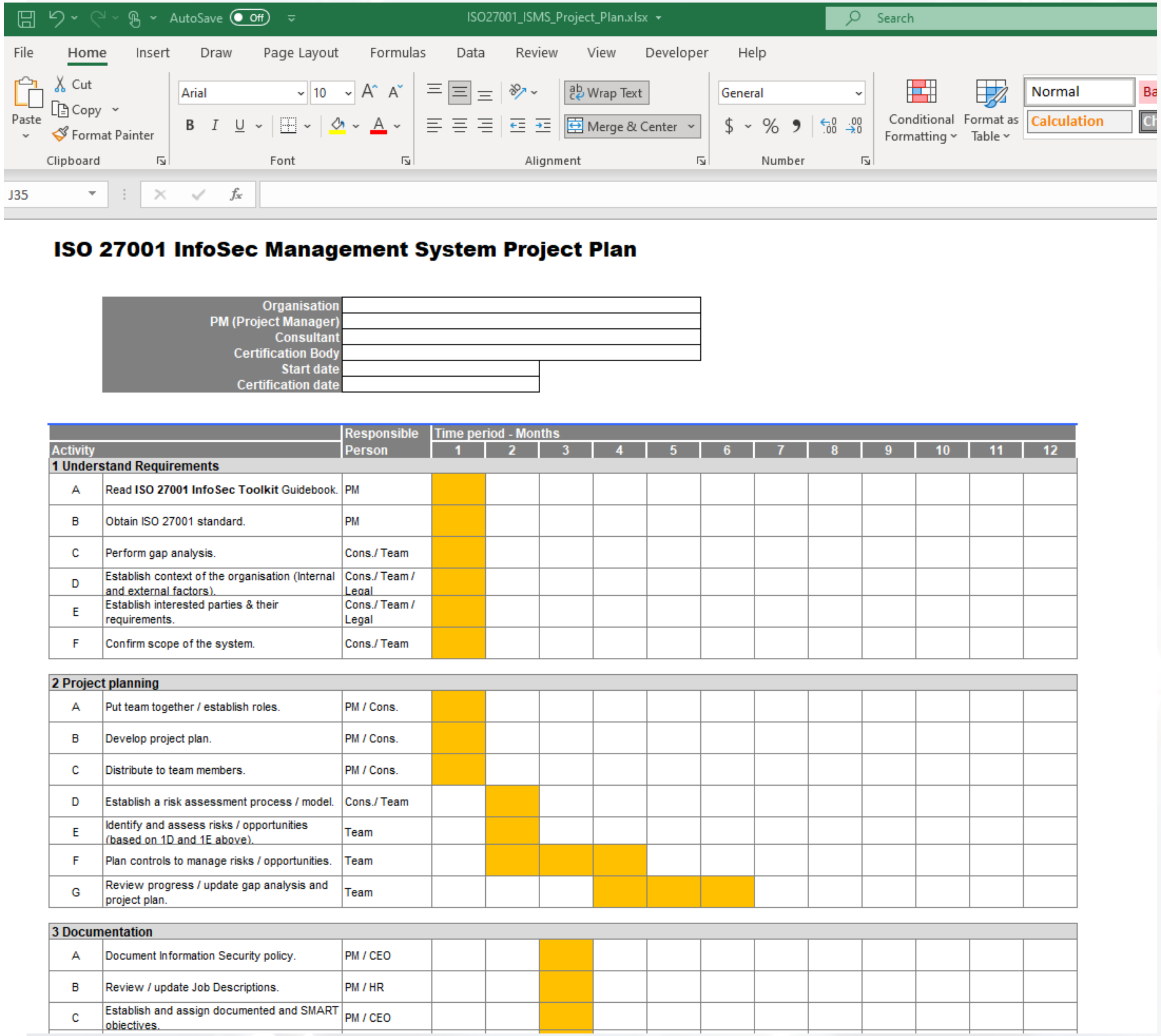
Summary of requirements	How currently addressed	Improvements	Status	Notes
4 CONTEXT OF THE ORGANIZATION				
4.1 Understanding the organization and its context				
Determine the factors that may affect the ISMS and its ability to achieve the intended results.	Situational analysis in place and updated to include InfoSec requirements.		🟩	• Consider external issues: Political, Economic, Social, Technological, Environmental, Legal (PESTEL) • Consider internal issues such as performance, culture and resources. • Business plan • SWOT analysis QMT Situational analysis / strategy plan, PESTEL / SWOT tools. ISO 27001 does not specify a requirement for monitoring and review of these factors. However, it might still be advisable to do that e.g. schedule a periodic review / or include as an agenda item in management review. The ISO 9001 Quality standard does have a requirement and it would therefore be required in an integrated system.
4.2 Understanding the needs and expectations of interested parties				
Determine which interested parties are relevant to the ISMS and what are their relevant requirements.	4-column Interested parties table developed but does not fully address InfoSec requirements.		🟨	This step may be carried out in tandem with 4.1. It would typically involve the documentation of an 'Interested Parties Table'. Once again, ISO 27001 does not specify a requirement for monitoring and review of these factors. However, it might still be advisable to do that e.g. schedule a periodic review / or include as an agenda item in management review. The ISO 9001 Quality standard does have a requirement and it would therefore be required in an integrated system. IST Template for 4-column Interested parties table.

Qudos³ IMS software includes a Gap Analysis tool with automation.
Professional Gap Analysis services are also available. Contact us for details.

ISMS Project Plan

Develop a Project Plan with timeframe and responsibilities.

Extract shown from a model plan included with in Qudos^3 IMS software.



ISO 27001 InfoSec Management System Project Plan

Organisation	
PM (Project Manager)	
Consultant	
Certification Body	
Start date	
Certification date	

		Responsible	Time period - Months											
Activity		Person	1	2	3	4	5	6	7	8	9	10	11	12
1 Understand Requirements														
A	Read **ISO 27001 InfoSec Toolkit** Guidebook.	PM	🟨											
B	Obtain ISO 27001 standard.	PM	🟨											
C	Perform gap analysis.	Cons./ Team	🟨											
D	Establish context of the organisation (Internal and external factors).	Cons./ Team / Legal	🟨											
E	Establish interested parties & their requirements.	Cons./ Team / Legal	🟨											
F	Confirm scope of the system.	Cons./ Team	🟨											
2 Project planning														
A	Put team together / establish roles.	PM / Cons.	🟨											
B	Develop project plan.	PM / Cons.	🟨											
C	Distribute to team members.	PM / Cons.	🟨											
D	Establish a risk assessment process / model.	Cons./ Team		🟨										
E	Identify and assess risks / opportunities (based on 1D and 1E above).	Team		🟨										
F	Plan controls to manage risks / opportunities.	Team		🟨	🟨	🟨								
G	Review progress / update gap analysis and project plan.	Team				🟨	🟨	🟨						
3 Documentation														
A	Document Information Security policy.	PM / CEO			🟨									
B	Review / update Job Descriptions.	PM / HR			🟨									
C	Establish and assign documented and SMART objectives.	PM / CEO			🟨									

Contact us about:

- ISO 27001 Gap analysis service
- IT Security review
- ISMS System development services
- Qudos^3 management system software – including ISO 27001 toolkit

- **Email:** info@qudos-software.com
- **Tel: +61 (7) 3063 0444** or **13 000 QUDOS**
- **Web:** qudos-software.com

Qudos