ISO 27001 Information Security in plain English

August 2024

Qudos

info@qudos-software.com

Tel: 13 000 QUDOS

https://qudos-software.com

This presentation is brought to you by Qudos³ IMS software

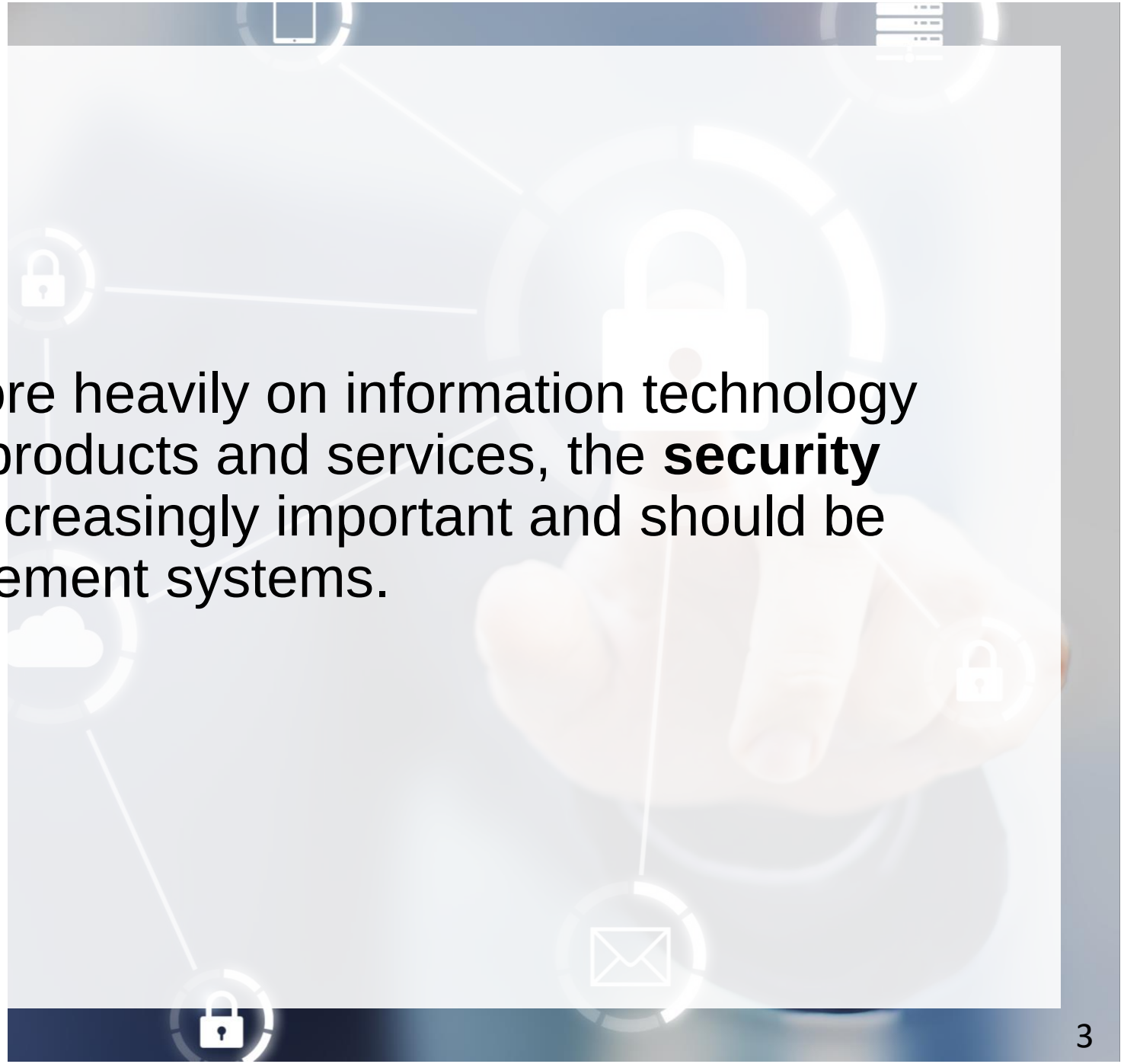
The comprehensive solution for a more effective and efficient management system.

info@qudos-software.com

Tel: 13 000 QUDOS

https://qudos-software.com

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?

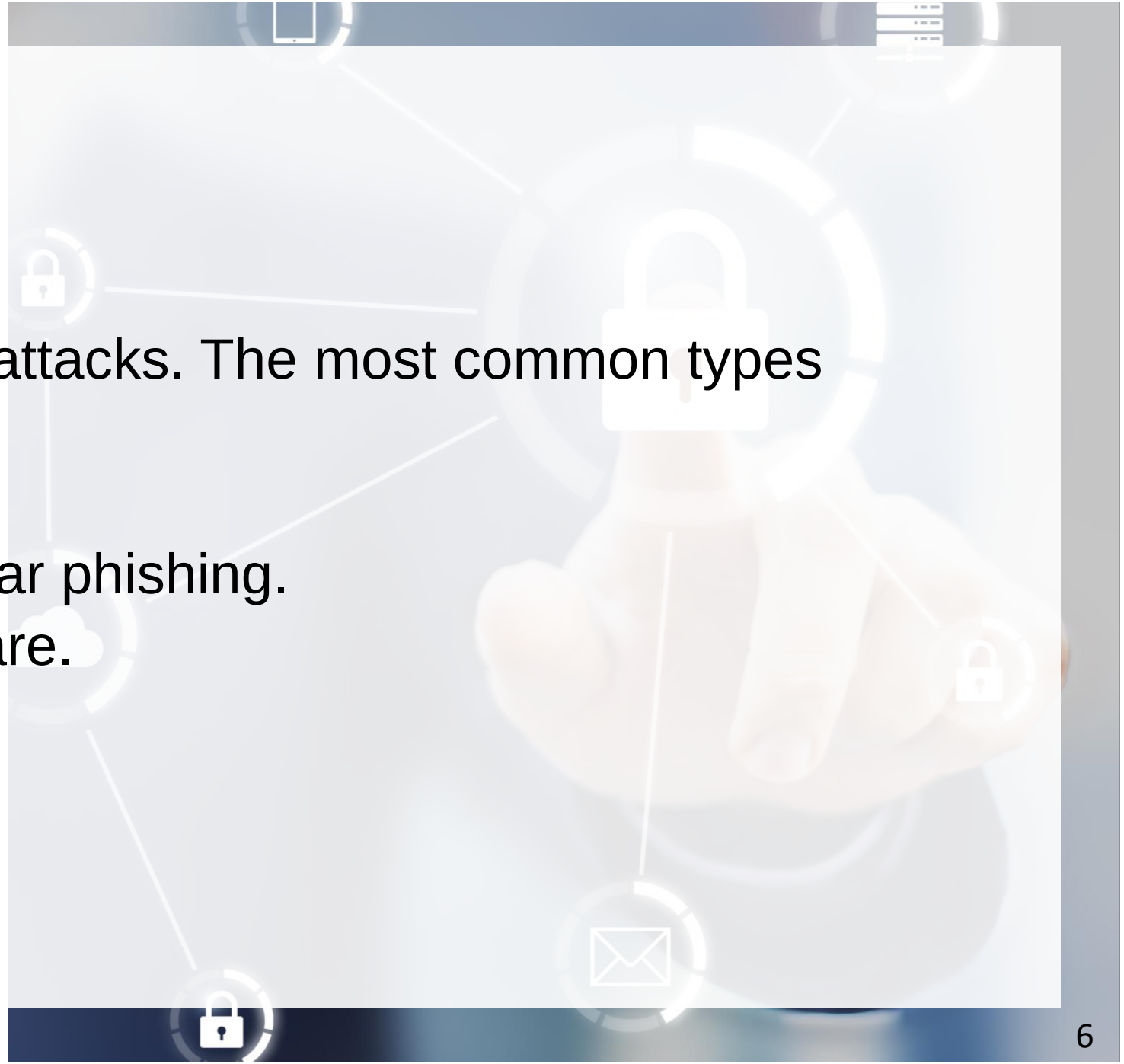
Yes, it’s relevant to every business.

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. The most common types include:

- 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.

Data breaches are frequently in the news

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"

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

...air several shows on Sunday, including

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

30 October 2020

EPA

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

GETTY IMAGES

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 was greatly accelerated by the COVID epidemic.

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

Customer requirement

A growing number of businesses face requirements from their clients to demonstrate that they have appropriate information security controls in place - and often for evidence of 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.

PLAN				DO	CHECK	ACT
4. Context of the organisation	**5. Leadership**	**6. Planning**	**7. Support**	**8. Operation**	**9. 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	6.3 Planning of changes	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 Operations

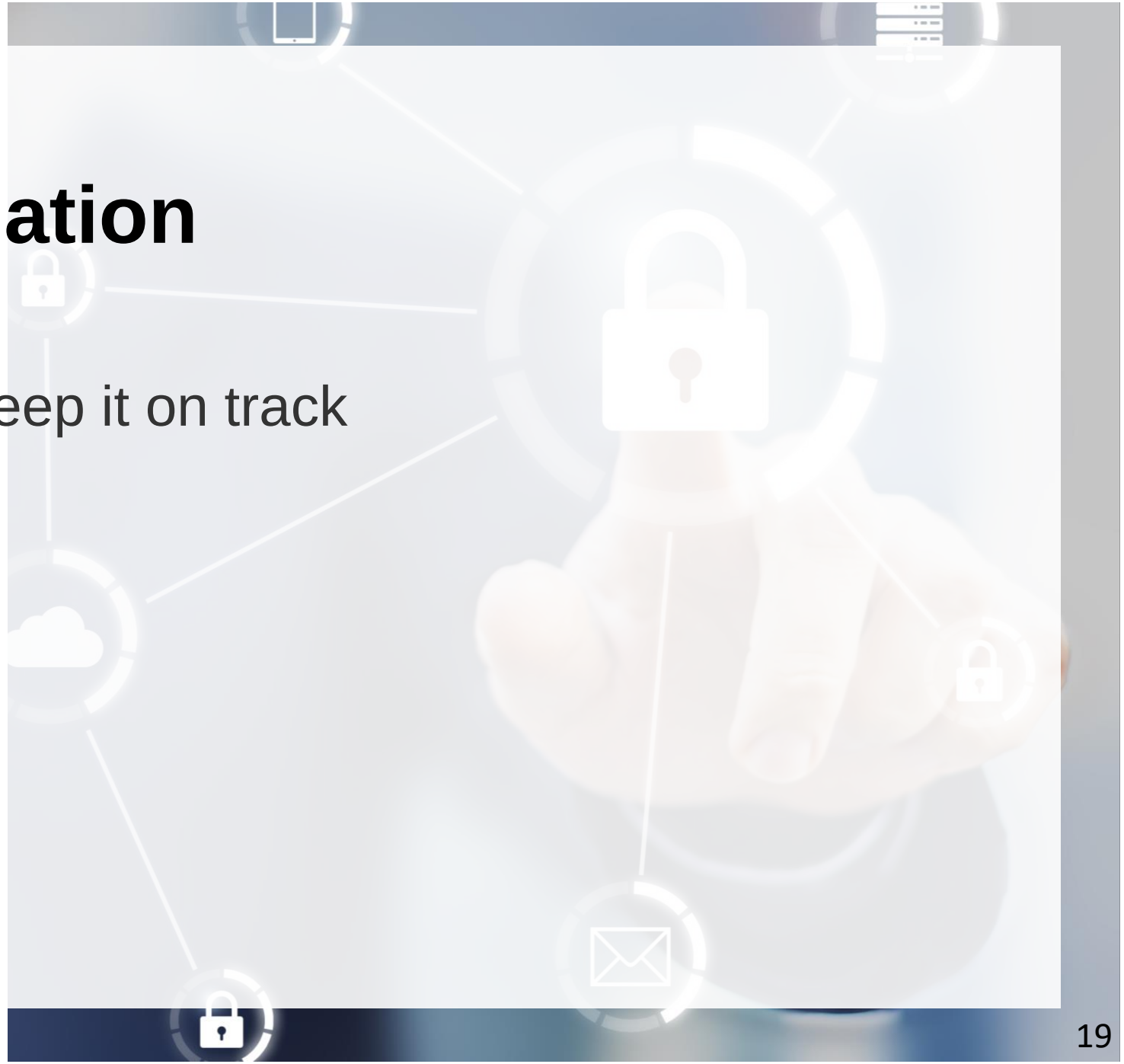
- Plan and control the necessary processes
- Perform risk assessments
- Treat risks

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

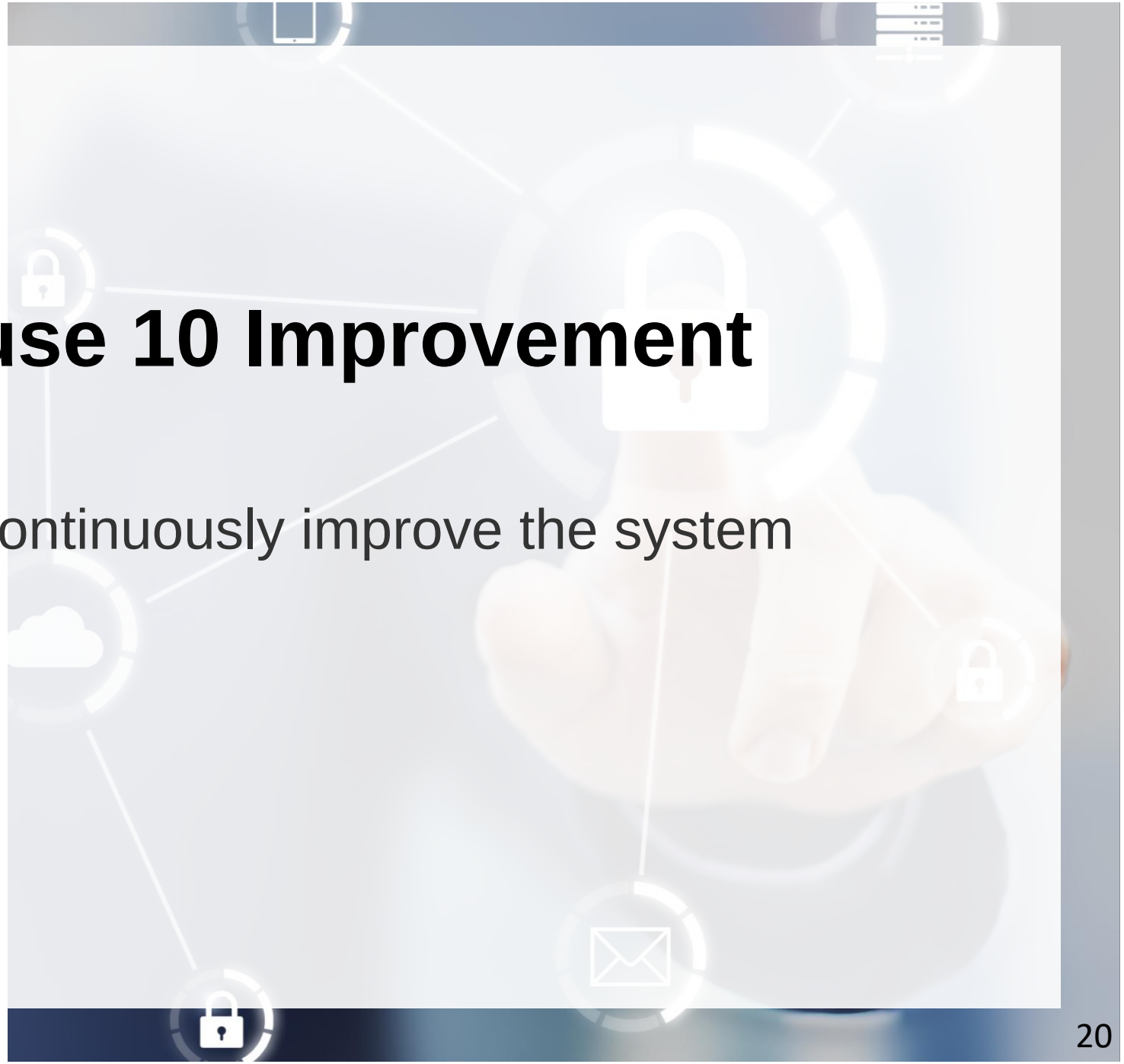
Check the system to keep it on track

- Operational checks
- Internal audits
- Management review



ISO 27001 Clause 10 Improvement

Deal with issues and continuously improve the system



The big difference…Annex A Controls

In addition to the regular clauses, ISO 27001 includes **Annex A** with controls to be considered and addressed as applicable. There are 93 controls in 4 domains or sets 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

Including requirements for policies, asset management, access controls, gathering threat intelligence and more.

Annex A6:

People controls

Annex A7:

Physical controls

Annex A8:

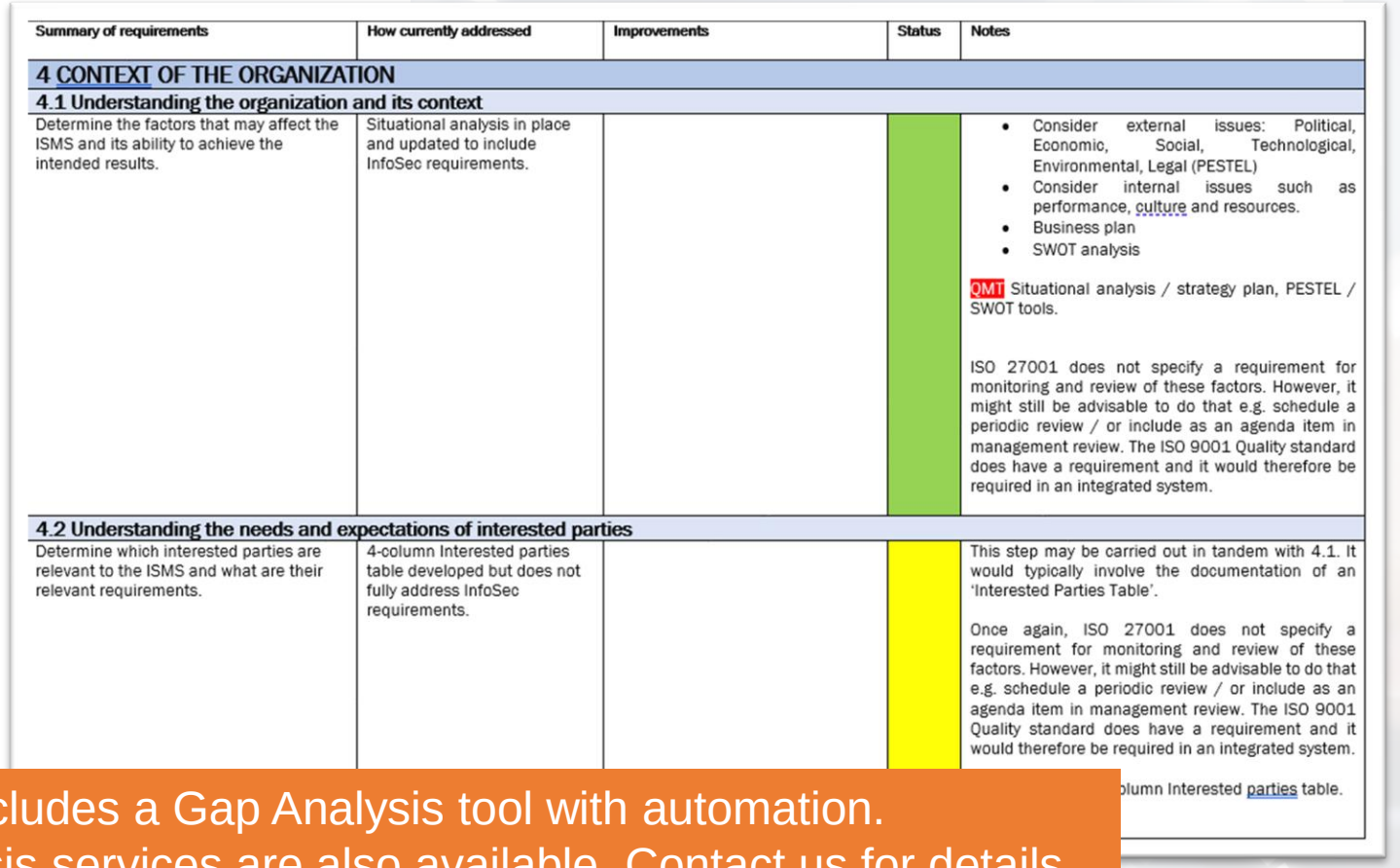
Technological Controls

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.

- **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



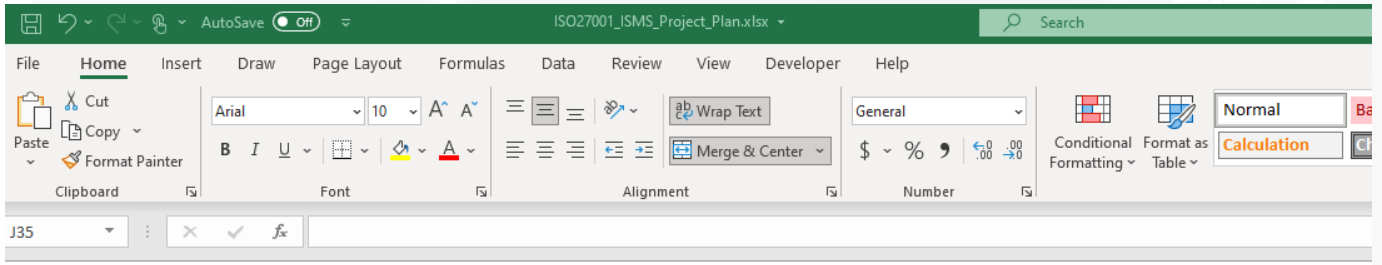
Summary of requirements	How currently addressed	Improvements	Status	Notes
4 CONTEXT OF THE ORGANIZATION				
4.1 Understanding the organization and its context				
Determine the factors that may affect the ISMS and its ability to achieve the intended results.	Situational analysis in place and updated 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. olumn Interested parties table.

Qudos[3] 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 in Qudos ISO 27001 InfoSec Toolkit – included in Qudos[3] IMS software.



ISO 27001 InfoSec Management System Project Plan

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

Activity		Responsible Person	Time period - Months 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												

This presentation contains just a summary of the standard and its requirements.

Contact us about:

- ISO 27001 Information security gap analysis service
- ISMS system development services
- **Qudos³** IMS software – including ISO 27001 toolkit

E: info@qudos-software.com
T: **13 000 QUDOS**
W: qudos-software.com
Follow us on LinkedIn