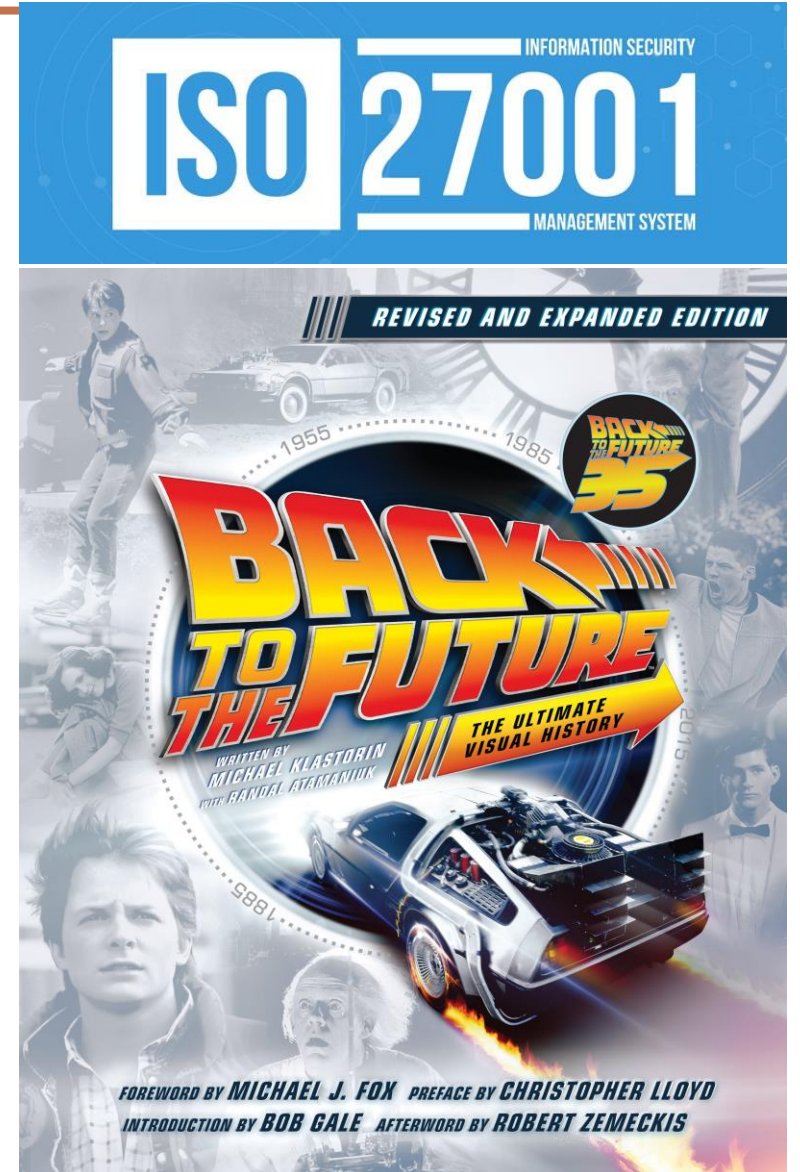
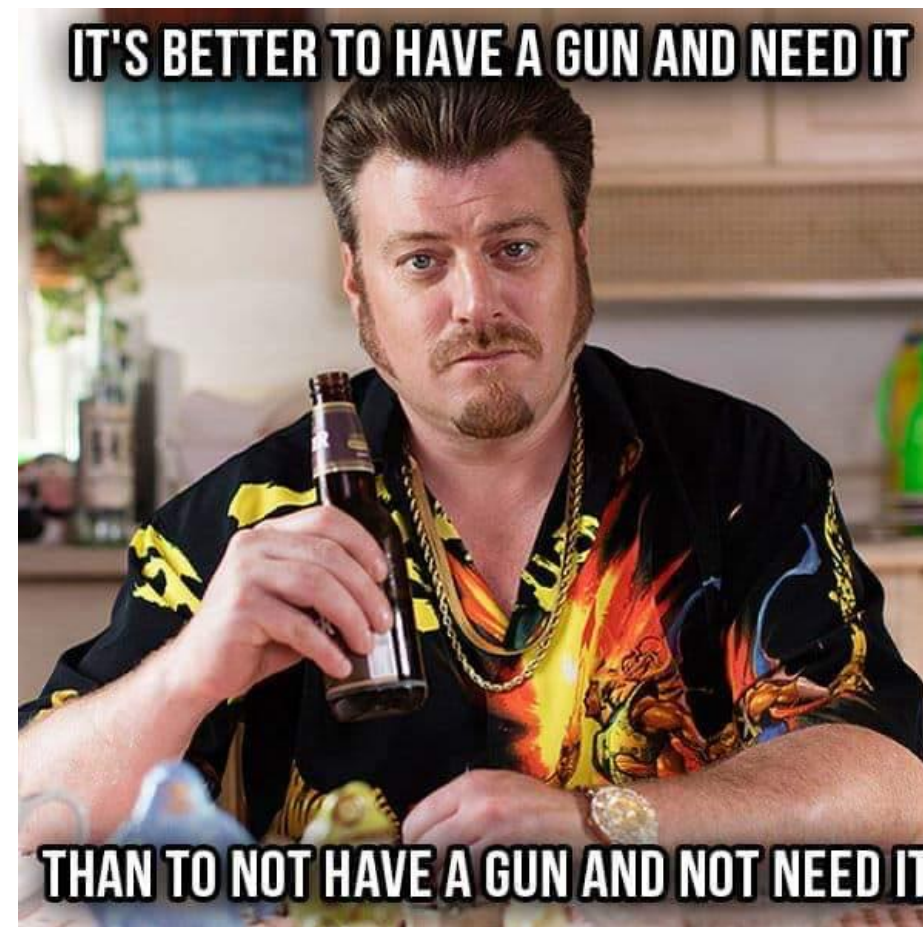


27001: History, Transition and Future



Contents

1. Introduction and History Lesson
2. Overview of Changes
3. Details of Interesting Changes
4. Certification route and Transition
5. Ask Me Anything?



1. Introduction and History Lesson



1.1

What is thing called ISO 27001?



ISO 27001



ISO/IEC 27001 is the international standard for information security. It sets out the specification for an effective ISMS (information security management system).

ISO 27001's best-practice approach helps organisations manage their information security by addressing people, processes and technology.

Certification to the ISO 27001 standard is recognised worldwide to indicate that your ISMS is aligned with information security best practices.

Part of the ISO 27000 series, ISO 27001 sets out a framework for organisations to establish, implement, operate, monitor, review, maintain and continually improve an ISMS.

Things you might not know about ISO 27001?



10 things you might not know about ISO and 27001

1. ISO is one of the few democratic organizations in the world.
2. Certification are for 3 years.
3. ISO standards are only drawn up for business reasons
4. I couldn't find one presentation on the internet where someone had a bit of fun with this topic. The topic is as dry as the Atacama desert.
5. There are loads of 27000 standards you probably don't know about
6. There probably aren't 10 things that you don't know about ISO 27001



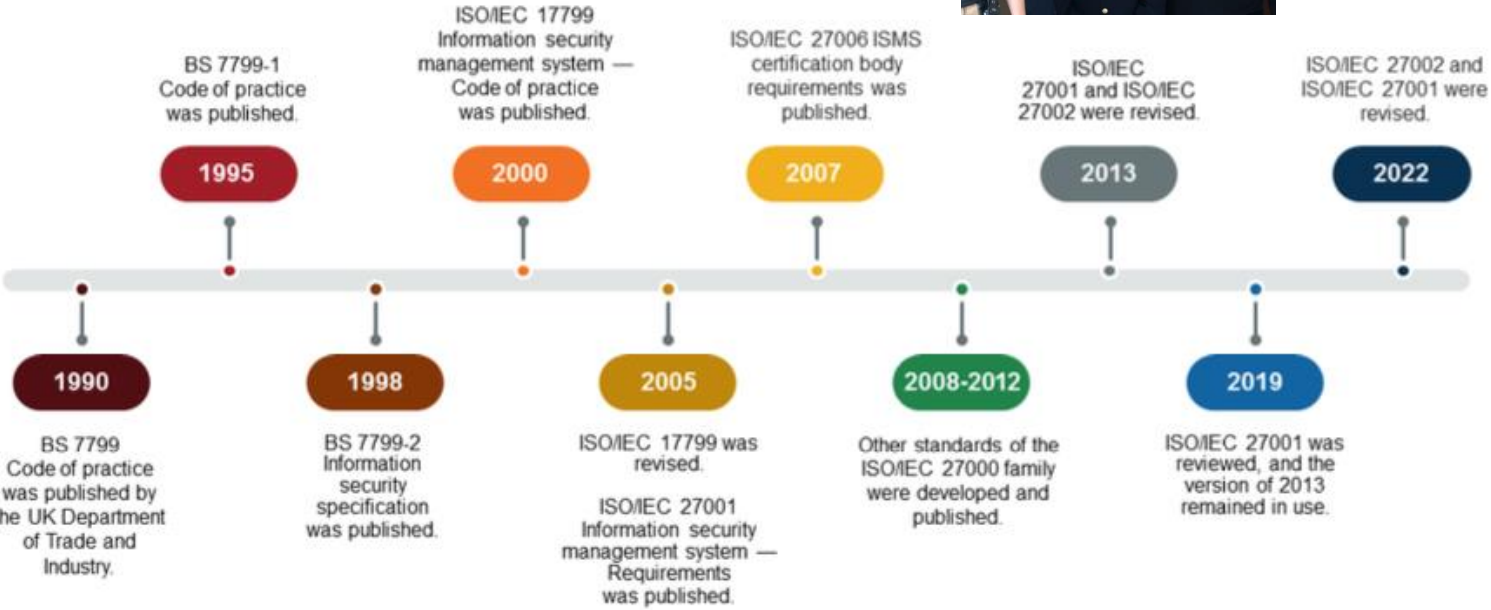


- Google says there are 46 standards in the family.
- Less than 5 can be certified against.
- The rest are reference standards.
- The core standards
 - 27001: ISMS
 - 27002: Controls
 - 27003: Implementation guide
 - 27004: Metrics
 - 27005: Risk Management
 - 27032: Cybersecurity
 - 27035: Incident Management
 - 27701: PIMS

History Lesson



Important dates

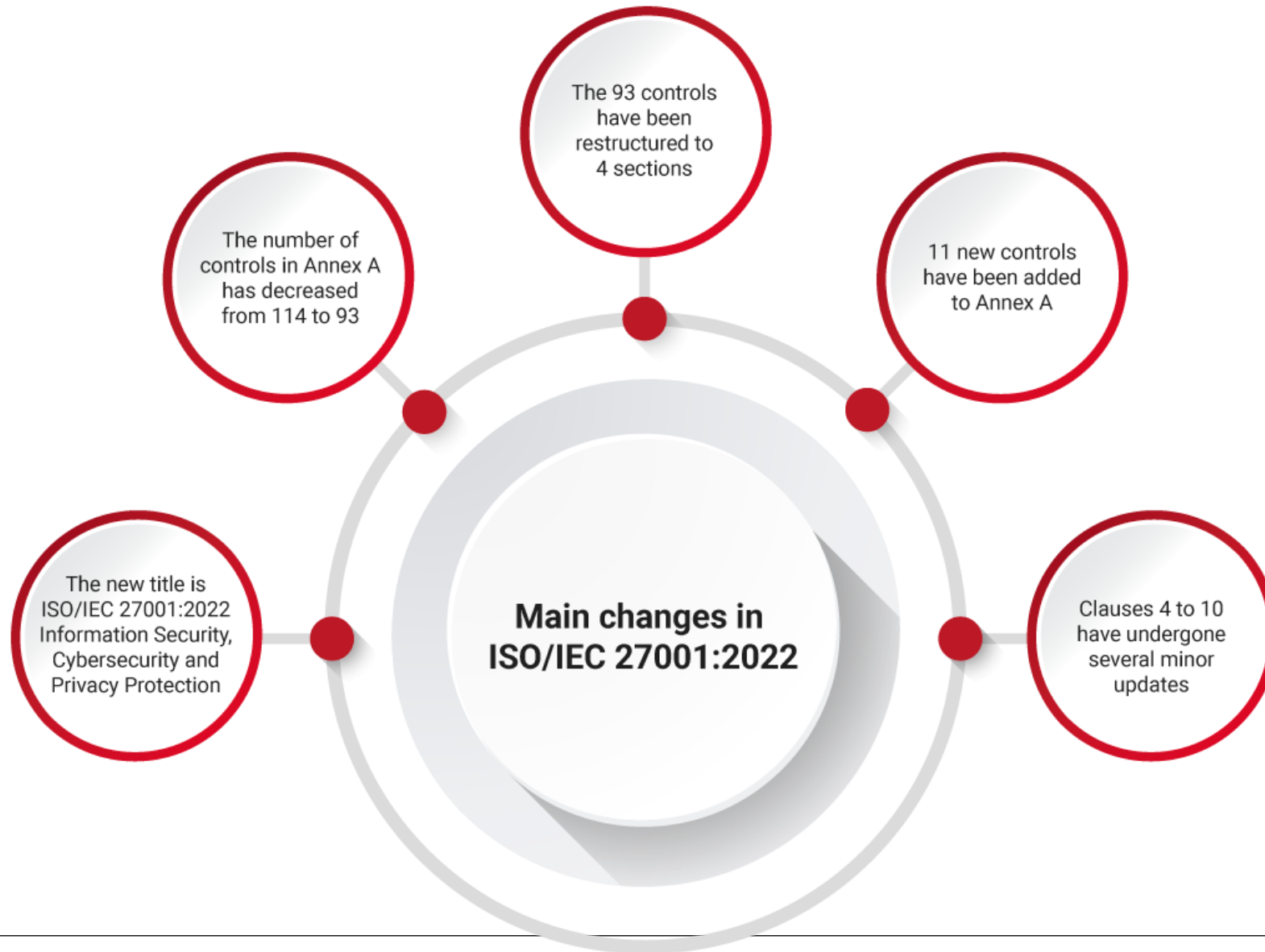


2022

Overview:
A change is
gonna come.



2. Overview of Changes



Is the change a big deal?



Details of Interesting Changes

**CHANGE
NOTHING
·
·
NOTHING
CHANGES**

I. The Name and structure has changed

1. Information Security, Cyber Security and Privacy Protection

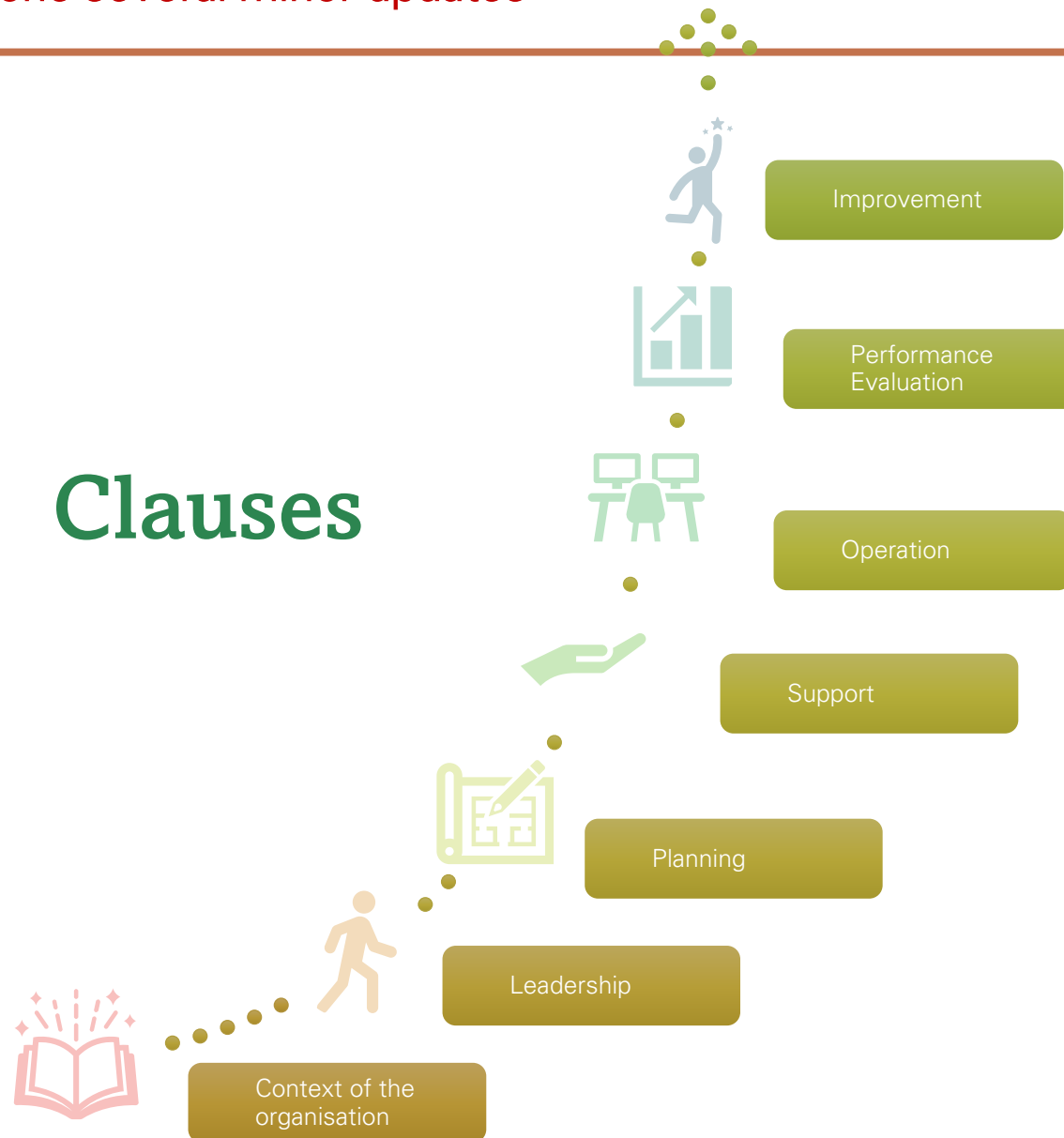
- “The first noticeable difference is that the information security standard document title has been simplified to the relatable “Information security, cyber security, and privacy protection – Information security management systems.”
- Legacy Name “Code of Practice” removed
- Attempt to align with NIST cybersecurity controls
- ISO 27701: Privacy bolt on these changes make it easier to create a Privacy Information Management System (PIMS)
- New Tech coming into the controls aligned to the Cyber security title



II. Clauses 4-10 have undergone several minor updates



Clauses



Small Changes - Clauses

Clause 3 “Definitions”

Contains links to the ISO online browsing platform and the IEC Electropedia which contain the terminology databases.

Clause 4.2 “Understanding the needs and expectations of interested parties”

Addition of item (c) stating “which of these requirements will be addressed through the information security management system” the impact being that more effort and clarity will be needed regarding the requirements of interested parties.

- **Clause 4.4 “Information security management system”**

Additional wording has been introduced, requiring the inclusion of “the processes needed [for the maintenance and improvement of the ISMS] **and their interactions**, in accordance with the requirements of this document.” This addition allows for alignment to other ISO standards such as **ISO 9001:2015** and **22301:2019**.



**Clause 5.3 “Organisational roles, responsibilities and authorities”
Now amended and reads “Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organisation” adding clarity with regards to whom those roles should be communicated.**

A 3D rendered baby character with large green eyes, wearing a dark suit, white shirt, and dark tie. The baby is sitting at a wooden table with hands clasped in front of them. The background is a blurred indoor setting with a yellow chair back and a red and white checkered pattern.

Leadership

Risk and Objectives

Clause 6.1.3 “Information security risk treatment”

Update in Note 2 now reads “Annex A contains a list of possible information security controls.” rather than the original “comprehensive list of control objectives and controls.”

Clause 6.2 “Information security objectives and planning to achieve them”

Addition of item (d) which requires objectives to be monitored **throughout the lifecycle of the certification.**
Much more focus on objectives being used and monitored.



Communication, Planning and Monitoring changes

Clause 7.4 “Communication”

An additional amendment was made which has led to the removal of item (e), the requirement for setting up processes for communication, indicating that the way communications are affected has little impact on how they are received.

Clause 8.1 “Operational planning and control”

Now reads “The organisation shall ensure that externally provided process, products or services that are relevant to the ISMS are controlled.” The wording of this control now provides more clarity for implementing an ISMS compared to the original “The organisation shall ensure that outsourced processes are determined and controlled.” Additionally, the requirement to implement plans for achieving objectives was deleted, this is because it is covered in Clause 6.2.

Clause 9.1 “Monitoring, measurement analysis and evaluation”

The addition of the note from the existing standard “The methods selected should produce comparable and reproducible results to be considered valid” to the main body of text provides much-needed clarity as to what can be considered a “valid” result in the eyes of the standard.





New and restructured Clauses

Clause 6.3 "Planning of Changes"

- An entirely new clause but covering the pre-existing requirements of Change control, this clause is named "Planning of Changes." Ensures that when the organisation needs to perform changes to the information security management system, these changes must be conducted in a planned manner.

Clause 9.3 "Management Review"

- Restructuring of the clause has meant there are now three sub-clauses.
- The addition of item (c) to 9.3.2 Management review inputs which now includes "changes and needs and expectations of interested parties that are relevant to the information security management system."

Clause 10 "Improvement"

- The order of this clause has reversed so that 10.1 is now Continual improvement and 10.2 is now Nonconformity and corrective action.



Controls

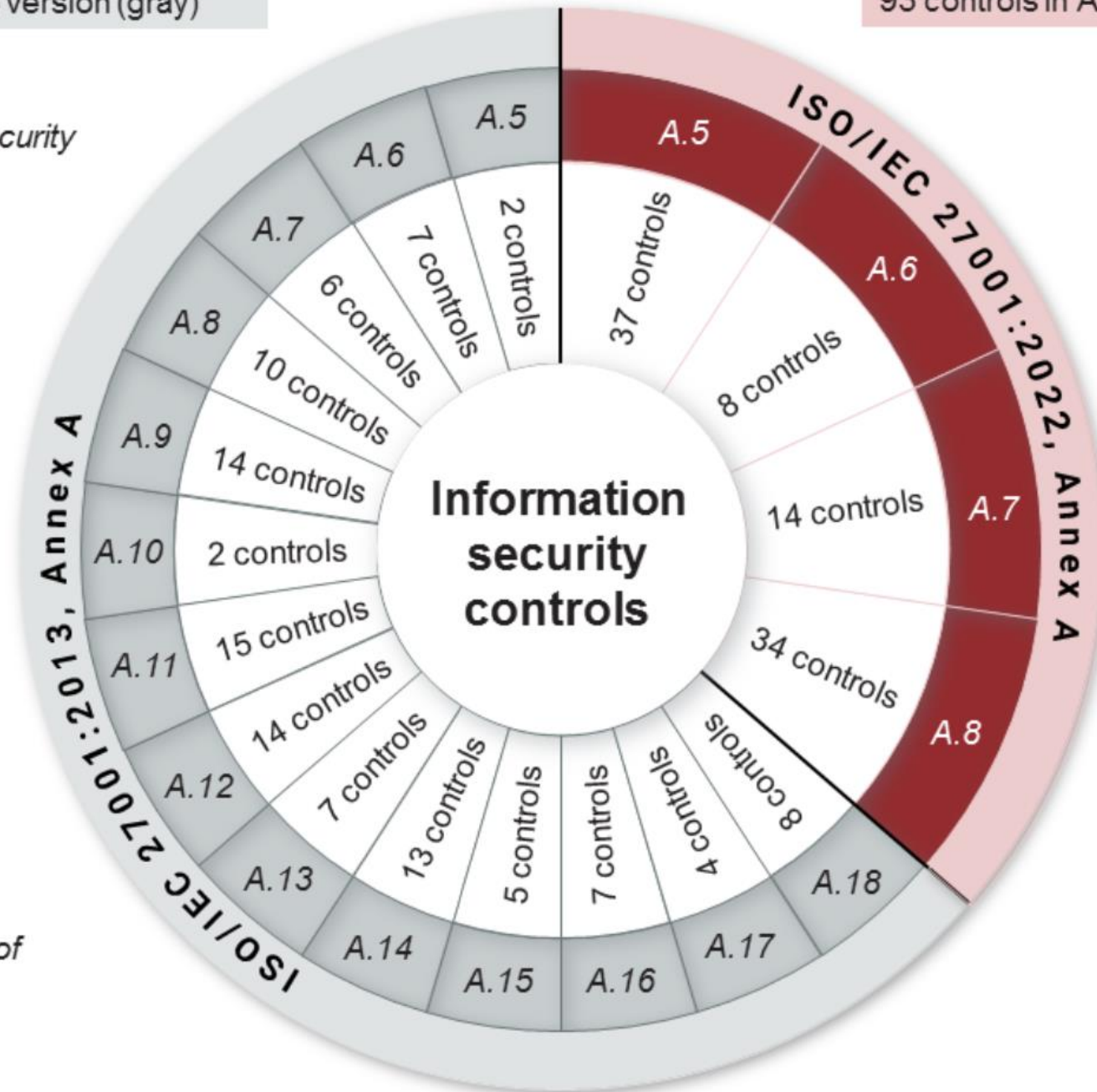
Controls Revamp

- Numbering and Structure changed completely into 4 sections:
 - Organisational (ISO 27001 5.1-5.37)
 - People (ISO 27001 6.1-6.8)
 - Physical (ISO 27001 7.1-7.13)
 - Technological (ISO 27001 8.1-8.34)
- Controls Merged and Updated
- New Controls have been added



Sample Footer Text

- A.5 Information security policies
- A.6 Organization of information security
- A.7 Human resource security
- A.8 Asset management
- A.9 Access control
- A.10 Cryptography
- A.11 Physical and environmental security
- A.12 Operations security
- A.13 Communications security
- A.14 System acquisition, development and maintenance
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security aspects of business continuity management
- A.18 Compliance














- A.5 Organizational controls
- A.6 People controls
- A.7 Physical controls
- A.8 Technological controls

What does the merging practically mean?

- There are actually more than 114 controls because there are now more focus points in each control
- There are now much more in each merged control so you might forget things unless you read the details: e.g. Access Reviews, key management.
- Badly trained auditors might miss important controls that are in the detail.
- Could lead to inconsistencies and mistakes.



11 New Controls in ISO 27001:2022

-  5.7 Threat intelligence
-  5.23 Information security for use of cloud services
-  5.30 ICT readiness for business continuity
-  7.4 Physical security monitoring
-  8.9 Configuration management
-  8.10 Information deletion
-  8.11 Data masking
-  8.12 Data leakage protection
-  8.16 Monitoring activities
-  8.23 Web filtering
-  8.28 Secure coding

New Controls

Perceptions on new controls

- **Monitoring and Physical monitoring** is interesting as they asking for monitoring and not just that you have logs, cameras and store and lock things. Have client that have logs and cameras and don't actually look at them unless things go wrong.
 - Focus on telling you to implement technologies now – it was previously hinted at but now its much more direct.:
 - DLP
 - Web filtering
 - **Threat intelligence** is an interesting control. Can be done on a very basic to a very advanced level.
 - **Cloud specific control** had to be added and lots of security people were not happy just to have it in supplier management.
 - **Configuration management** big focus area in other standards for years (NIST, PCI-DSS)
 - **Data Masking and Data Deletion** focused on the data journey and protection
 - **ICT readiness for business continuity** – BCP/DR in ISO has an interesting history as it was split out then sort of brought back in.
 - **Secure coding** – also was covered as art of secure engineering principles but widened out a lot more.
-

Marketing Talk: Experts say

- All in all, this new version of ISO 27001 provides more clarity within Clauses 4-10 by making small amendments as well as taking into consideration more current cyber security requirements such as threat intelligence.
- The standard has also worked to address duplication by merging a number of controls to simplify the process of implementing and maintaining an ISMS.
- The transition is not difficult if you understand the changes.

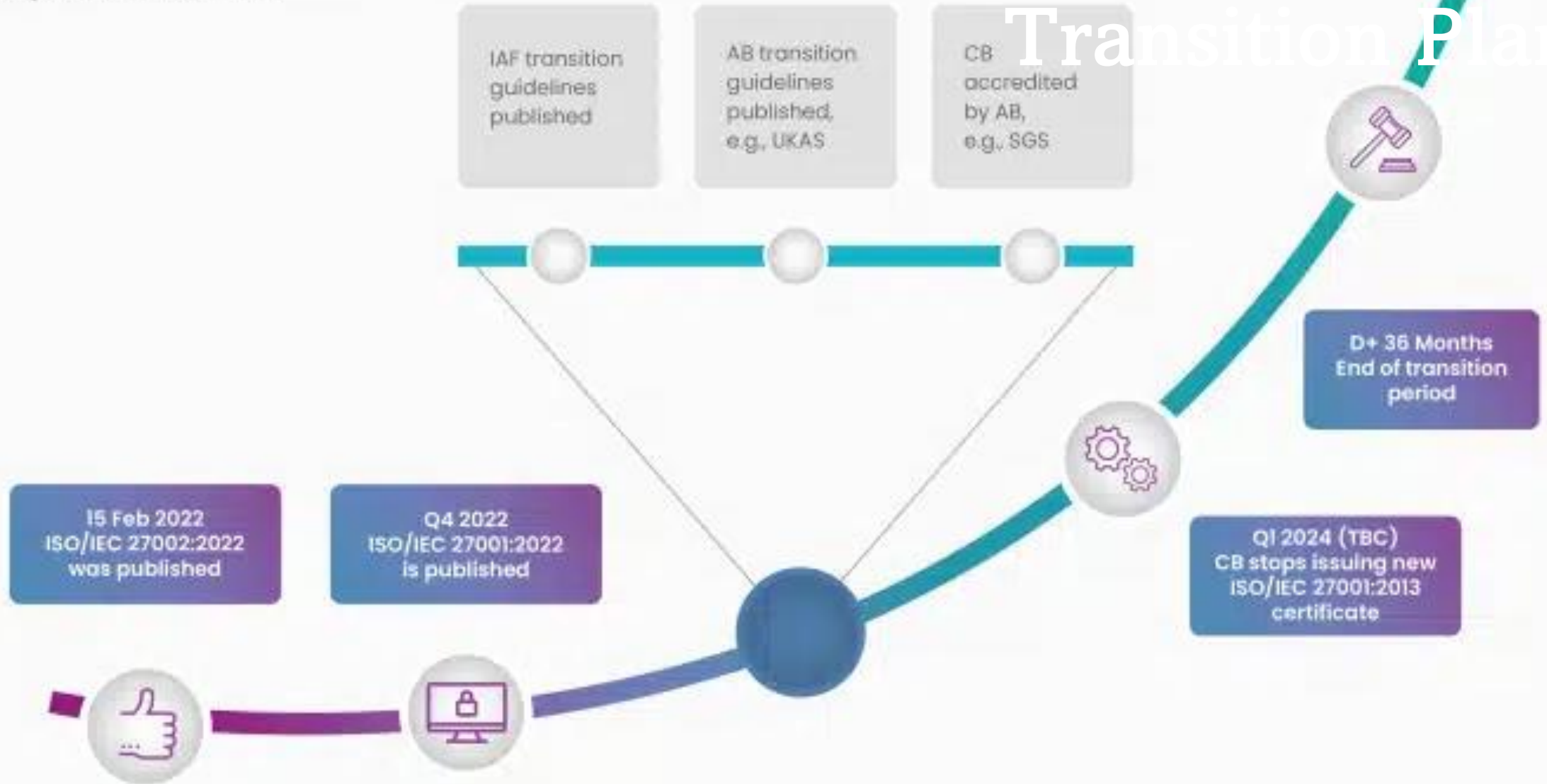


Transition to ISO/IEC 27001:2022

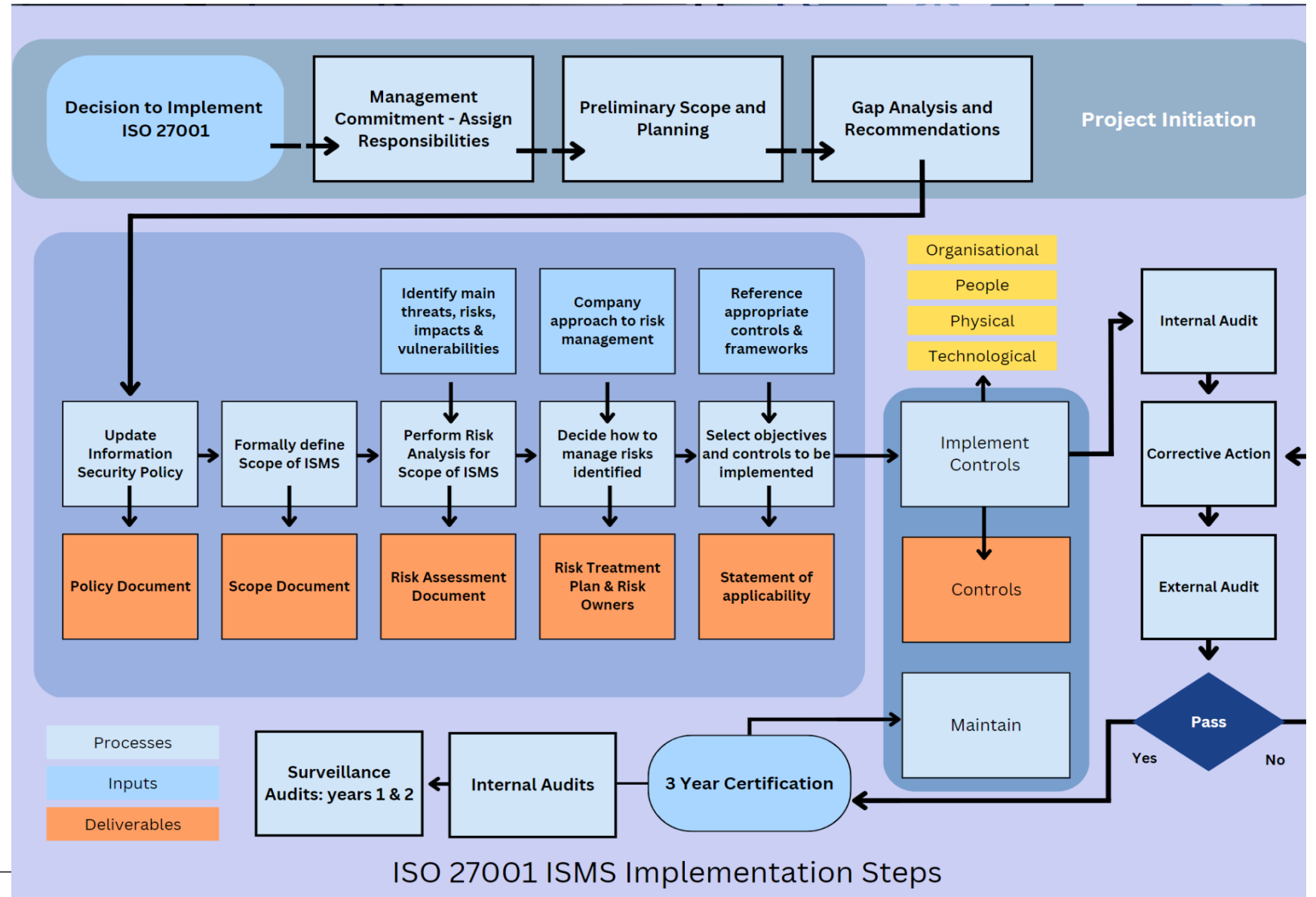
Sample Footer Text

3-year transition period
Proposed timeline >>

Transition Plan



ISO Journey : Practical Approach



5 main reasons companies get certified.



- They have no choice.
- They will make more money from it.
- They will lose money if you don't get certified.
- It make them better at what you do.
- It will make them more secure?

Ideal clients are a combination of many of those reasons.

Your Questions

1. Which organization should comply or rather implement ISO27001

- Anyone smallest client was 3 staff members and largest multinational companies- it applies to all and can be done affordably as prices have shot down.

2. For certification for an Organisation, you have be certified with the BSI or PECB and obviously comes with a cost. With the new standard, is there any way a company can self certify or have a Lead Implementer sign off for the review performed?

- Internal audits and getting another party to gap analysis/internal audit you can allow for this but the effect is limited and internal ones always have doubt to an external party.

3. How do i make this a pragmatic implementation

- By following the steps above
- Understanding it as well as you can – experience, training courses – clauses ate critical.
- Don't go down rabbit holes and waste time.
- Either using templates or using a solution.
- Getting someone In to guide you – tyre kicking

Certification is not a silver bullet. Security must always be the main focus!



Alliances

As part of the Alliances Projects: Community Development initiative and mission, we are consolidating what is good in terms of core certifications, academia and eventually experience based mentorships to raise awareness of when these opportunities will arise.

A partnership with PECB Training Leader and award winner **Bevan Lane, Director – Infosec Advisory Group** means we are able to create and plan an annual training session on the PECB courses as highlighted below:

- [ISO/IEC 27001 Lead Implementer – 4 day course](#)
- [ISO/IEC 27005 Risk Manager – 3 day course \(Intermediate course\)](#)
- [ISO/IEC 27701 Privacy Information Management Systems \(PIMS\) 4 day course](#)

PECB | ISO/IEC 27001 LEAD IMPLEMENTER



PECB | ISO/IEC 27005 RISK MANAGER

Course Agenda

- Day 1:** Introduction to ISO/IEC 27005 and risk management
- Day 2:** Risk assessment, risk treatment, and risk communication and consultation based on ISO/IEC 27005
- Day 3:** Risk recording and reporting, monitoring and review, and risk assessment methods

PECB | ISO/IEC 27701 PRIVACY INFORMATION MANAGEMENT SYSTEM



Ask me Anything

