DataGuard

ISO 27001 Implementation -

How to successfully prepare for your certification

21 October 2021
Christian Taube

CHRISTIAN TAUBE

Team Lead Information Security

Certified ISMS Security Officer
and Auditor according to ISO 27001

EXPERIENCE

Managing Director, LanguageWire München GmbH

Chief Solutions Officer, Xplanation NV (Leuven)

Co-founder, Technical Lead and Member of the Board, Matrix Communications AG (Munich)

Implementation of GDPR + ISO 27001 Compliance and successful audits according to TISAX® and ISO 27001 in international companies

TRAINING

M.A., studies in Stuttgart, Eugene (Oregon) and Munich

ICO-CERT
International Certification Organization

AGENDA

- Why information security?
- Overview: ISO 27001
- ISO 27001 implementation
- Deep Dive: ISO 27001 Audit
- Key takeaways & time for your questions!

WHY
INFORMATION SECURITY?

Fire in the data center

Le datacenter Strasbourg 2 (SBG2) du cloud français a été entièrement **ravagé par les flammes.**

3.4 million web pages taken down by fire at the largest French cloud operator

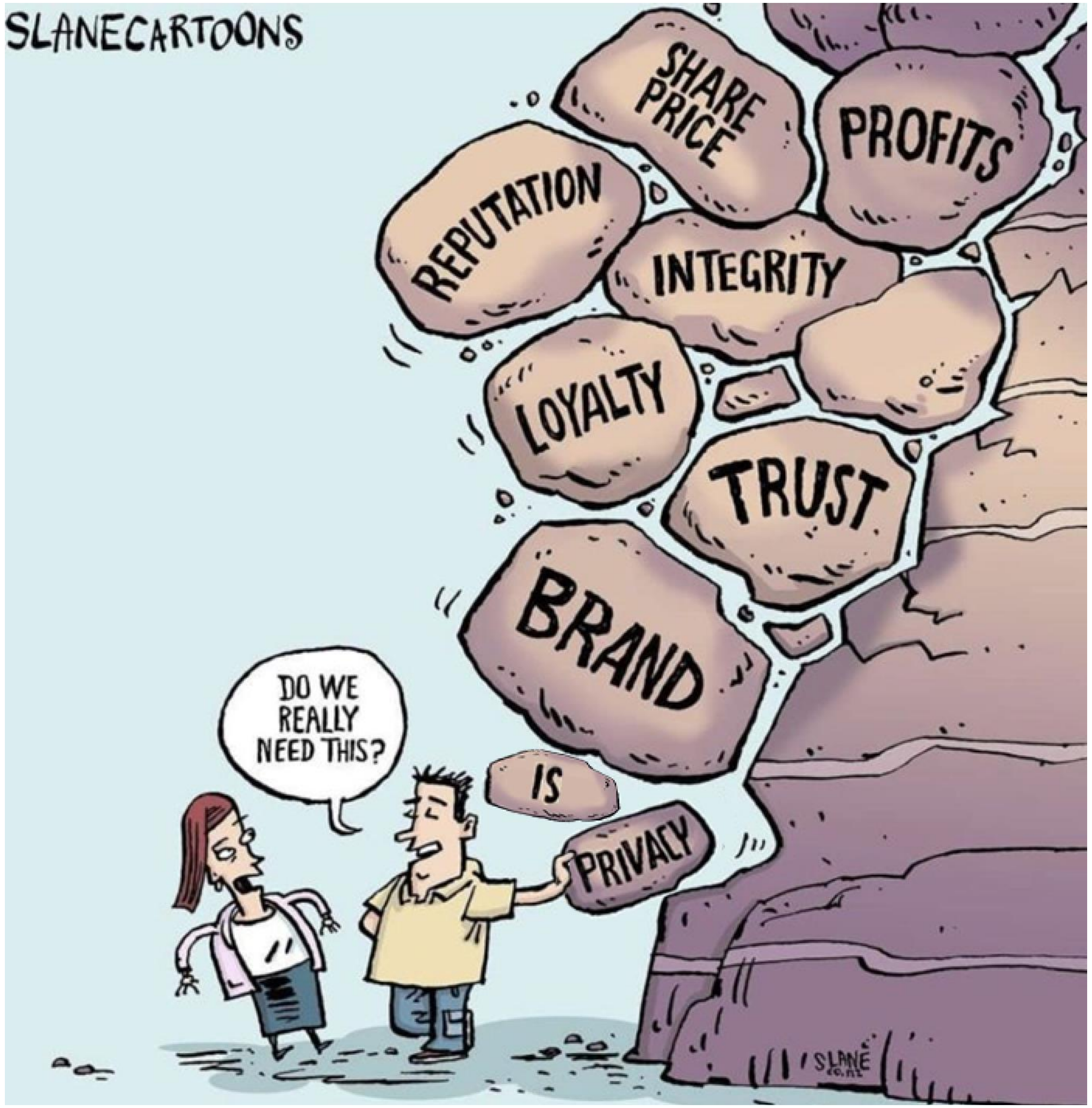
"According to the French web newspaper Le Journal du net, the destroyed data center only had alarm systems, but no sprinklers or similar automatic means of firefighting."

*Source: FAZ online

Why information security?

Data privacy
as a fundamental value

Information security
as fundamental value

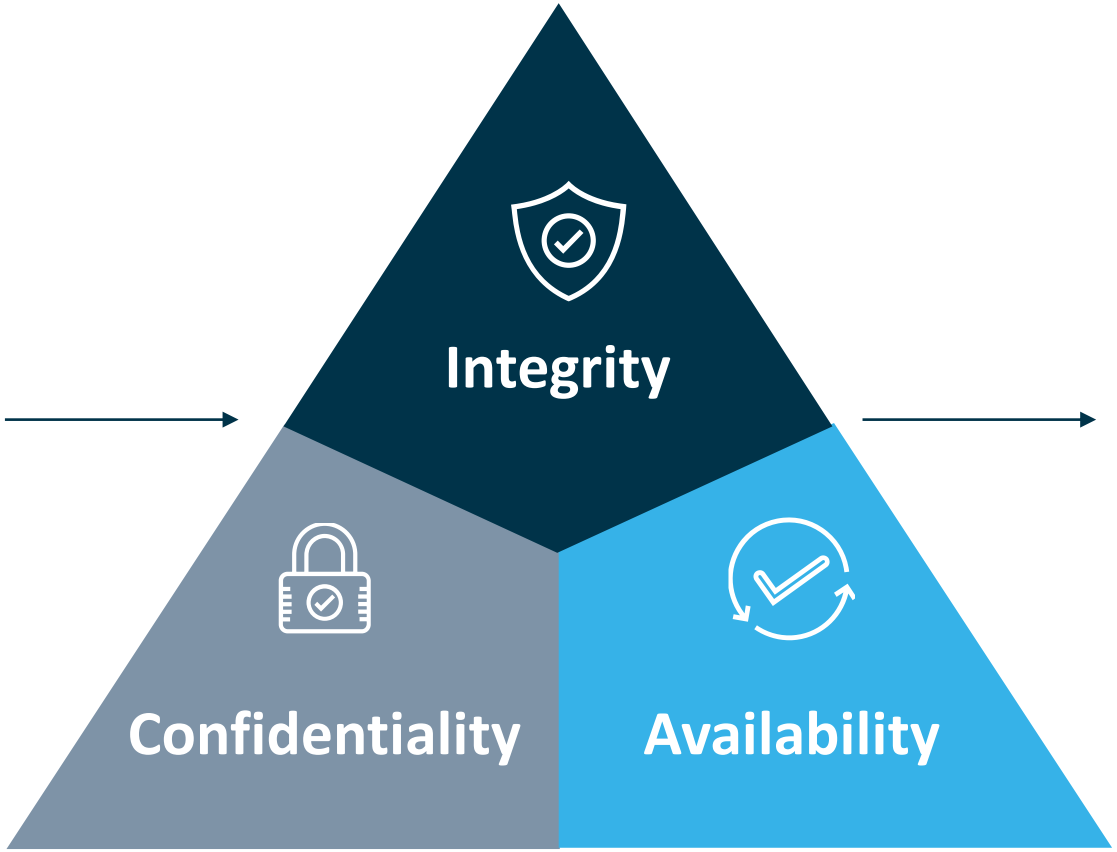


SURVEY #1:
Why does your organisation want to address information security?

OVERVIEW:
ISO 27001

Protection of your information assets

The information security management system protects the



of your information assets from risks and vulnerabilities

The ISO 27001 standard...

- is the leading international standard for information security
- offers a process- and risk-oriented framework for the development of an ISMS (= **I**nformation **S**ecurity **M**anagement **S**ystem)
- provides for certification
- can be used by any company or organisation and is therefore
  - To be interpreted individually
  - More specific information on the implementation of an ISMS according to ISO 27001 can be found in ISO 27002
- contains 6 normative chapters and 14 control objectives, which contain a total of 114 individual controls

Control Objectives of ISO 27001

- A.5 Management Direction / Information Security Policy
- A.6 Organisation 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 Operational security
- A.13 Communications security
- A.14 System acquisition, development and maintenance
- A.15 Supplier relationships
- A.16 Information security incidents
- A.17 Business continuity management
- A.18 Compliance

Comprehensive management system - not just IT security!

SURVEY 2:
Which (other) certification(s) are you pursuing?

Implementing ISO 27001

Step 1: Assembling your team

✓ Selection of a Project Manager/Success Manager/“project driver“

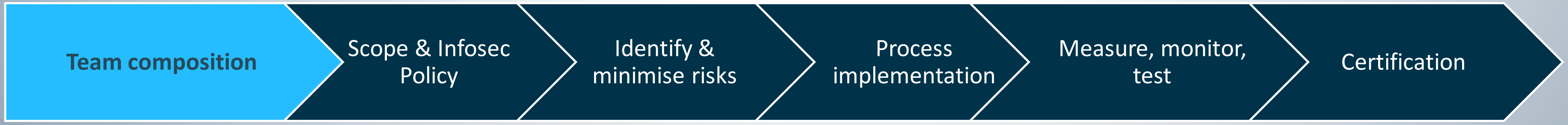
✓ Putting together the right team

✓ Joint definition of goals, vision and desired time frame for the project

✓ Definition of roles and responsibilities, e.g., based on RACI matrix: *„Responsible, Accountable, Consulted, Informed*"

✓ Determining the stakeholders who need to be involved

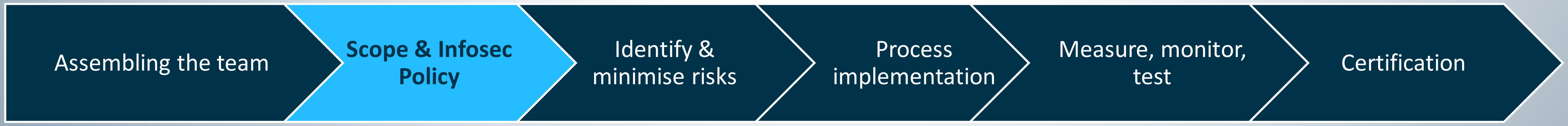
Deliverables: **Project team responsibility matrix, drafts of statement of applicability and of scope documentation**



Step 2: Scope of application & information security policy

- ✓ Obtain support and commitment from management (especially: resources)
- ✓ Definition of the ISMS application scope (e.g., entire company vs. development only)
- ✓ Information security policy: which objectives does the team want to achieve, and how?
- ✓ Documentation of your approach to information security

Deliverables: Information security policy, employee training plan, draft records to track the effectiveness of your actions



Assembling the team

Scope & Infosec Policy

Identify & minimise risks

Process implementation

Measure, monitor, test

Certification

Step 3: Identify and minimise risks

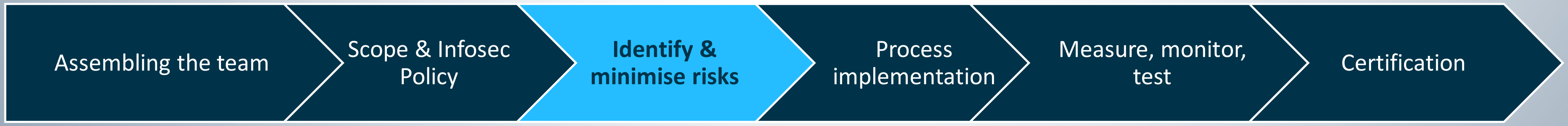
✓ Definition of rules for the evaluation of your risks,

✓ ... the impact of a risk on your business model, and

✓ ... the probability of a risk actually occurring

✓ Determining the acceptable level of risk
(depends heavily on the nature of your business and your risk tolerance)

Deliverables: Risk management processes, risk assessment and treatment plans, and gap assessment of information security controls



Assembling the team

Scope & Infosec Policy

Identify & minimise risks

Process implementation

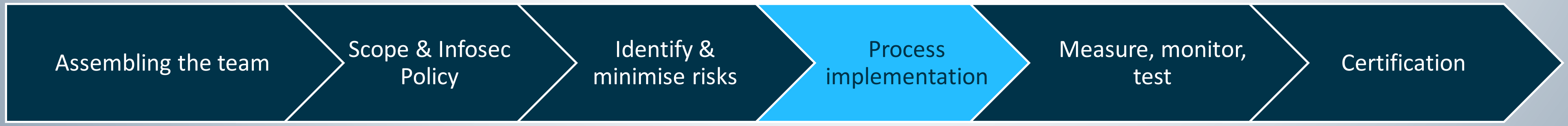
Measure, monitor, test

Certification

Step 4: Implement your processes

- ✓ Start the concrete implementation of your processes to protect your information assets
- ✓ Employee awareness, e.g. through training, also plays an important role
- ✓ Definition of review steps and mandatory procedures
- ✓ Extension and/or adaptation of your documentation: In the context of the actual implementation of your processes, you will gain more clarity and, if necessary, new insights

Deliverables: Information Security Management System (ISMS) manual, new information security policies, updated internal information security audit plan, updated risk assessment and treatment plans



Assembling the team

Scope & Infosec Policy

Identify & minimise risks

Process implementation

Measure, monitor, test

Certification

Step 5: Measure, monitor, check

✓ Review your information security management system

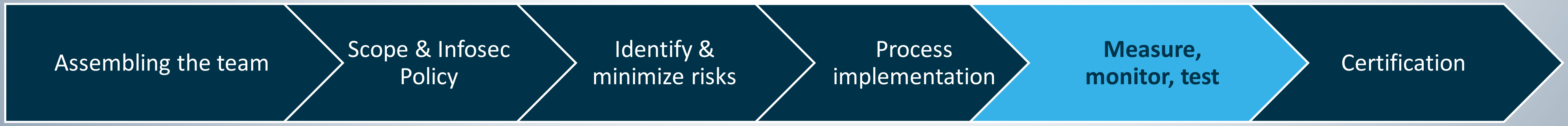
✓ Carry out internal audits and, if necessary, deriving appropriate measures

✓ Define your key performance indicators (KPIs)

✓ Prepare of your annual report and a presentation for your stakeholders

✓ Put ISMS to the test at least 1 x year, through review by management and internal audits ➔ Address new circumstances, new risks, new threats in a timely manner

Deliverables: Metrics & Key Performance Indicators (KPIs), internal audit report(s), annual management report and presentation for key stakeholders, corrective action plan(s) and continual improvement plan(s)



Assembling the team

Scope & Infosec Policy

Identify & minimize risks

Process implementation

Measure, monitor, test

Certification

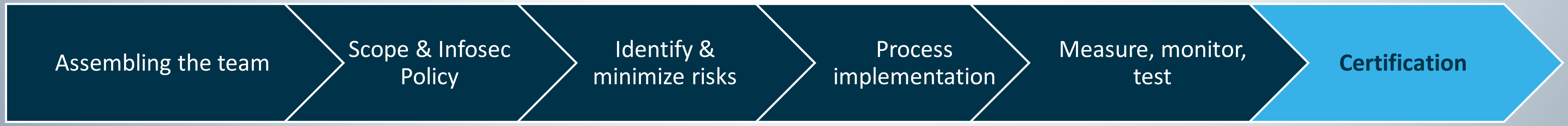
Step 6: Certification

✓ Select your auditor

✓ Before the audit, you should be sure that you can live in and with your processes. Audit costs will be charged either way!

✓ Audit: Stage 1 - Documentation only ; Stage Level 2 - On site

Deliverables: Certification audit preparation plan, corrective action plans addressing non-conformities



Assembling the team

Scope & Infosec Policy

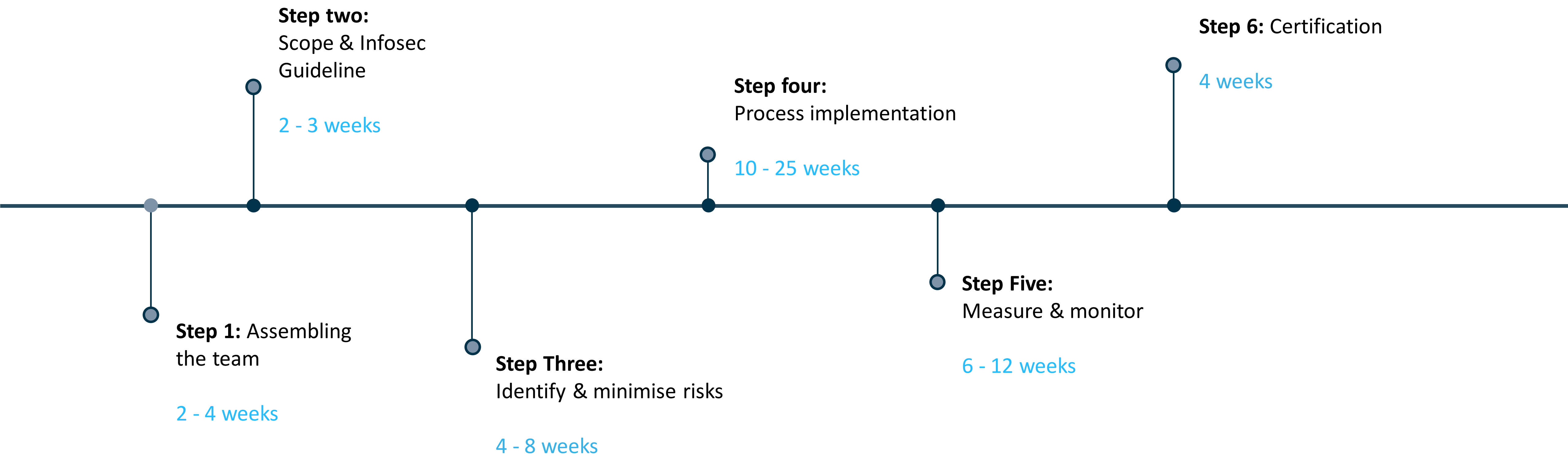
Identify & minimize risks

Process implementation

Measure, monitor, test

Certification

Timeline: The path to ISO 27001 certification



Step 1: Assembling the team

2 - 4 weeks

Step two:
Scope & Infosec Guideline

2 - 3 weeks

Step Three:
Identify & minimise risks

4 - 8 weeks

Step four:
Process implementation

10 - 25 weeks

Step Five:
Measure & monitor

6 - 12 weeks

Step 6: Certification

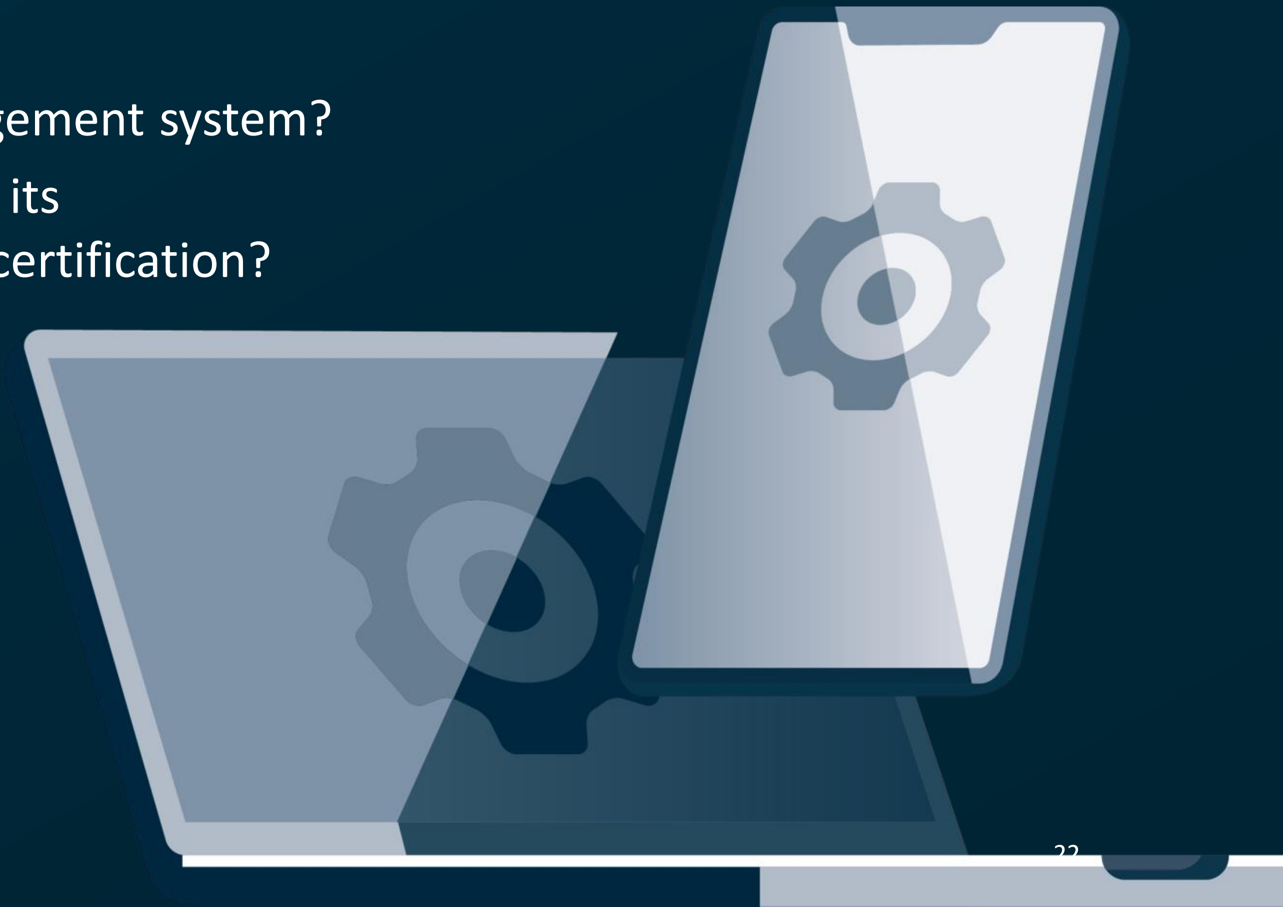
4 weeks

DEEP DIVE:
ISO 27001 AUDIT

ISO 27001 Certification Audit - Stage 1

Is your management system certifiable?

- Gather necessary information on the scope
- Check your documentation for conformity and comprehensiveness
- Key questions:
    - Status of the implementation of the management system?
    - Does the existing management system and its degree of implementation generally allow certification?
    - Are important details still missing?
- Outcome:
  Audit plan for the remainder of the certification audit > tage 2,
  based on the acquired knowledge
  about the organization



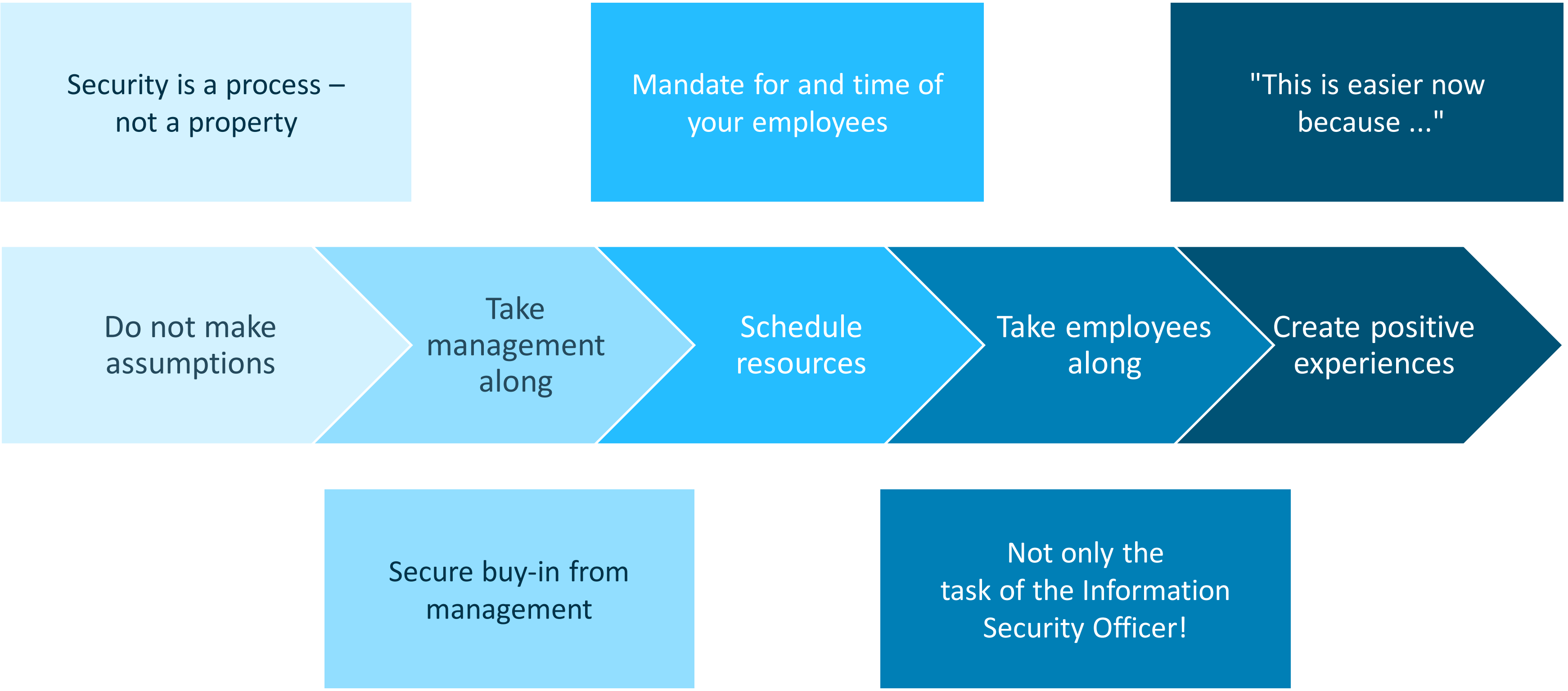
ISO 27001 Certification Audit - Stage 2

Is your management system effective?

- Samples of evidence for all requirements and in all processes or departments within the scope of application based on:
  - Requirements of the standard
  - Documents of the organisation
  - Basics (e.g. laws, further, industry-specific, required standardisations)
- Closing meeting: Evaluation of the results, first audit result and, if necessary, notification of deficiencies / deviations
- Determine corrective actions, if necessary
- Subsequently: Verification of root cause analysis and of the measures taken, by the audit team

WHAT ARE KEY TAKEAWAYS?

Top 5 takeaways for a successful ISO 27001 audit



Security is a process – not a property

Mandate for and time of your employees

"This is easier now because ..."

Do not make assumptions

Take management along

Schedule resources

Take employees along

Create positive experiences

Secure buy-in from management

Not only the task of the Information Security Officer!

QUESTIONS?

Thank you for your interest!

Do you have further questions?

This is how you can reach me.

Email:

ctaube@dataguard.de

LinkedIn:

https://www.linkedin.com/in/christiantaube/