

# FORVIS™

## What's New in ISO 27001:2022 & How to Prepare

February 2, 2023

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

**{ databrackets }**  
cybersecurity | compliance | certification

# TO RECEIVE CPE CREDIT

## ■ Individuals

- Participate in entire webinar
- Answer polls when they are provided

## ■ Groups

- Group leader is the person who registered & logged on to the webinar
- Answer polls when they are provided
- Complete group attendance form
- Group leader sign bottom of form
- Submit group attendance form to [cpecompliance@forvis.com](mailto:cpecompliance@forvis.com) within 24 hours of webinar
- If all eligibility requirements are met, each participant will be emailed their CPE certificate within 15 business days of webinar

# Meet the Presenters



**Tom Tollerton, CISSP**

Principal

FORVIS Cybersecurity Advisory



**Stephanie Jarvis, ISO Lead Auditor**

Senior Manager

FORVIS Advisory



**Srini Kolathur**

Director

databrackets



# Agenda

- Introductions
- Overview of the Changes Between ISO 27001:2013 & 27001:2022
- Clarifications & Simplifications of Mandatory Clauses
- New Controls in Annex A
- Addressing the Changes in Your ISMS
- Closing

# About FORVIS

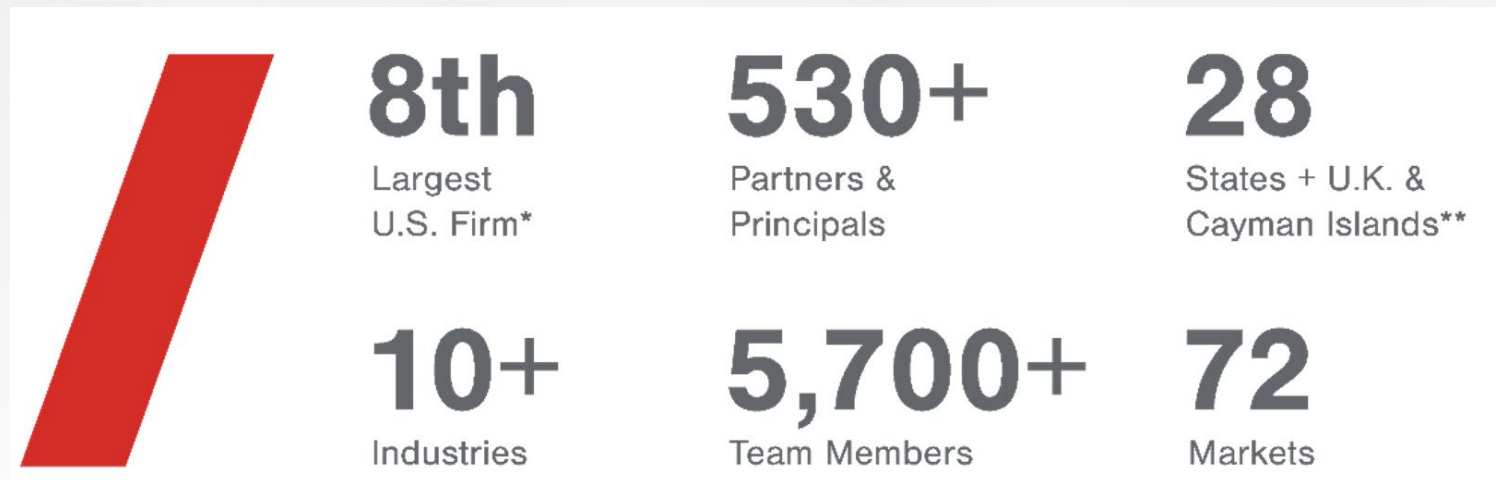
FORVIS assists organizations with various cybersecurity & ISO 27001 related services

- ISMS Buildout
- Gap/Readiness Assessment
- Policy/Procedure Development
- Internal Audit Support
- Project Management
- Education & Training
- vCISO Services

**FORVIS**

## Client-focused accounting and advisory services that help drive business forward.

FORVIS, LLP ranks among the nation's top 10 public accounting firms. Created by the merger of equals of BKD, LLP and Dixon Hughes Goodman LLP, FORVIS is driven by the commitment to use our forward vision to deliver an **Unmatched Client Experience™**.



**{ databrackets }**  
Cybersecurity | Compliance | Certification



We assist organizations in developing and implementing practices to secure sensitive data and comply with regulatory requirements.



## DIY PLATFORM

DIY assessments, employee training, customized policies & procedures and much more...



## CONSULTING

Professional services to help you with your Compliance needs



## MANAGED SECURITY

Managed compliance and security services that focus on your key business outcomes

# About ISO/IEC 27001

- ISO is the International Organization for Standardization
- Accredited Certification Bodies (CBs) perform the certification assessments

- ISO 27001 considers the **Information Security Management System (ISMS)**
- Certifications last three years between Full Audits
- Three security categories/principles
  - Confidentiality
  - Integrity
  - Availability

# Certification Process Overview

## Benefits

- Satisfying Client/Customer Requirements
- Demonstrate Commitment to Cyber Control
- Third-Party Assessment of Security Processes & Controls
- Benchmark for Improving Cybersecurity Processes
- Third-Party Management Tool

## Requirements

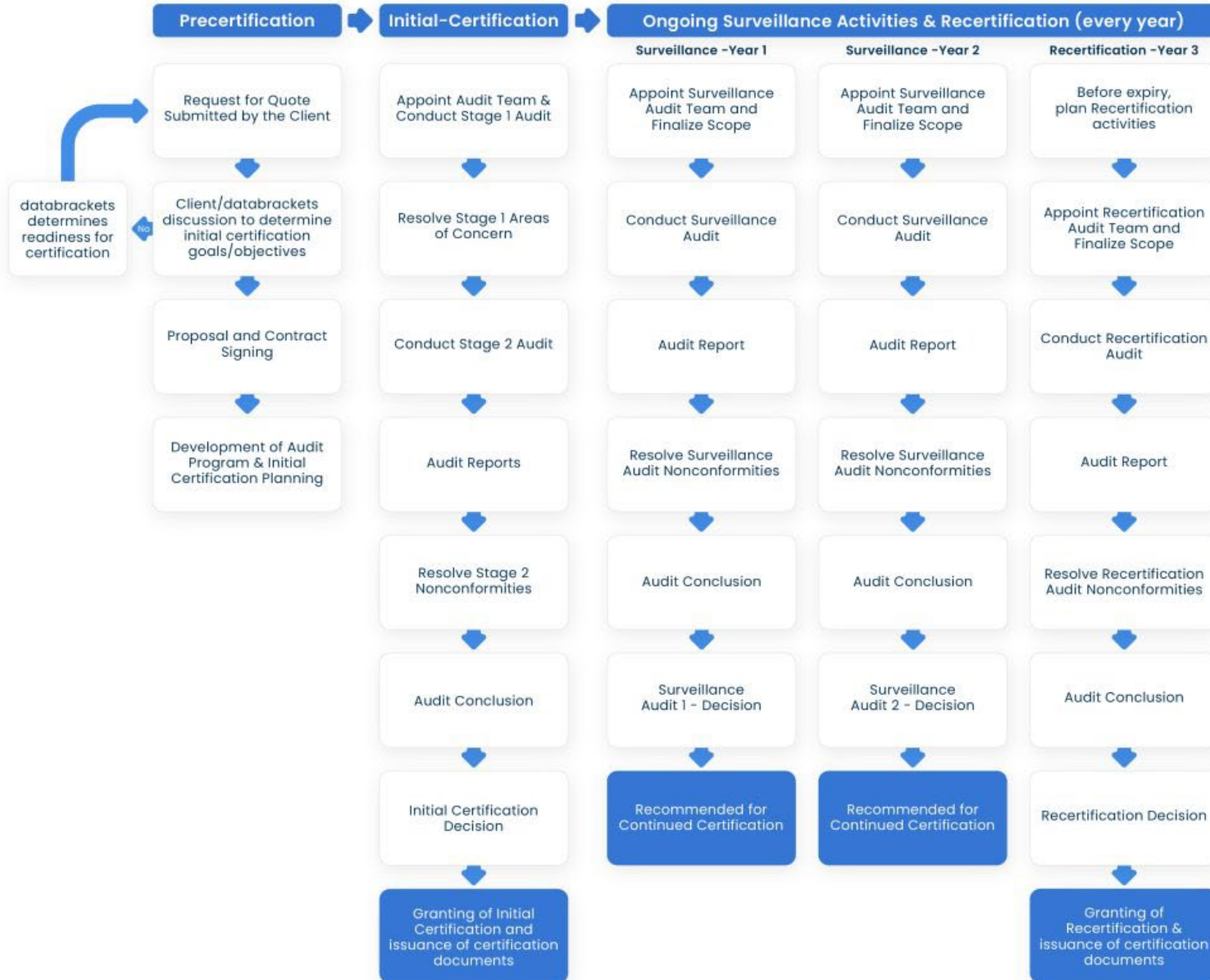
- Stakeholder Buy-in
- Time from Security & IT Leadership to Develop ISMS
  - Clear Scope
  - Accurate & Complete Policies & Procedures
- Ongoing Oversight of the ISMS (Business as Usual)

## Timeline

- Readiness Assessment Process can take 8 to 12 weeks
- Certification Audit 3 to 6 Weeks
- Point-in-Time
- Surveillance Audit Annually
- Recertification Audit – Every Three Years



# ISO 27001 AUDIT AND CERTIFICATION PROCESS FLOW CHART



# Summary of Changes in ISO/IEC 27001:2022

- Structure of the standard aligns with new Harmonized Structure (HS) of other ISO standards introduced since May 2021
- Focus on concision in Annex A: merging controls & consolidating control categories
- Minimal changes to Mandatory Clauses 4–10
- Increased focus on Process
  - Clause 4.4: Implementation of ISMS must include “processes needed & their interactions”
  - Clause 6.3: Changes to the ISMS must be “carried out in a planned manner”

# Control Changes – By The Numbers

- **11 new controls**
- **Total number of controls in Annex A has decreased from 114 to 93**
- **23 controls renamed; 57 merged into 24**
- **93 controls have been restructured into four control categories**
  - A.5 Organizational controls (37 controls)
  - A.6 People controls (8 controls)
  - A.7 Physical controls (14 controls)
  - A.8 Technological controls (34 controls)

# 11 New Security Controls

A.5.7

Threat Intelligence

A.5.23

Information Security for Use of Cloud Services

A.5.30

ICT Readiness for Business Continuity

A.7.4

Physical Security Monitoring

A.8.9

Configuration Management

A.8.10

Information Deletion

A.8.11

Data Masking

A.8.12

Data Leakage Prevention

A.8.16

Monitoring Activities

A.8.23

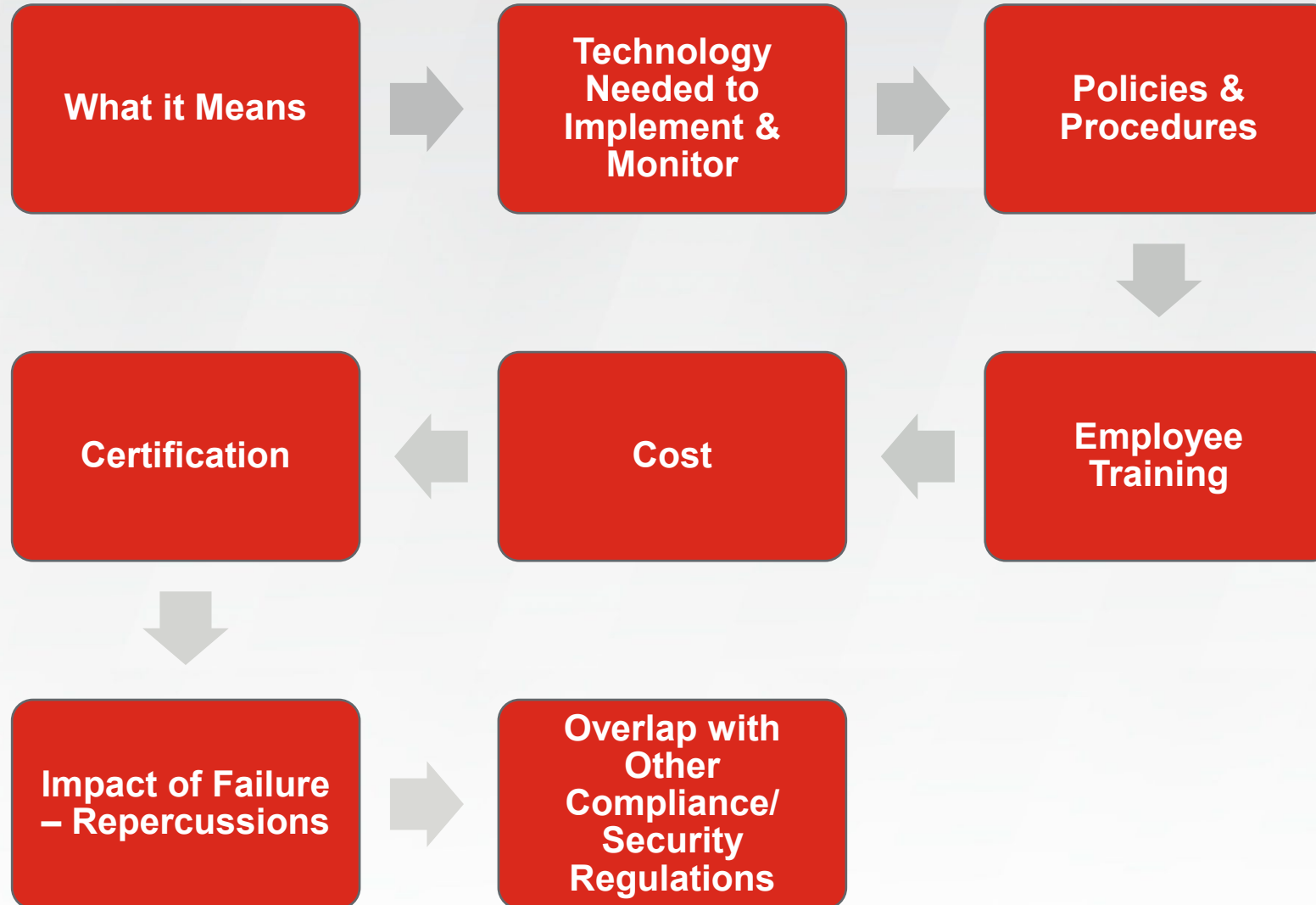
Web Filtering

A.8.2

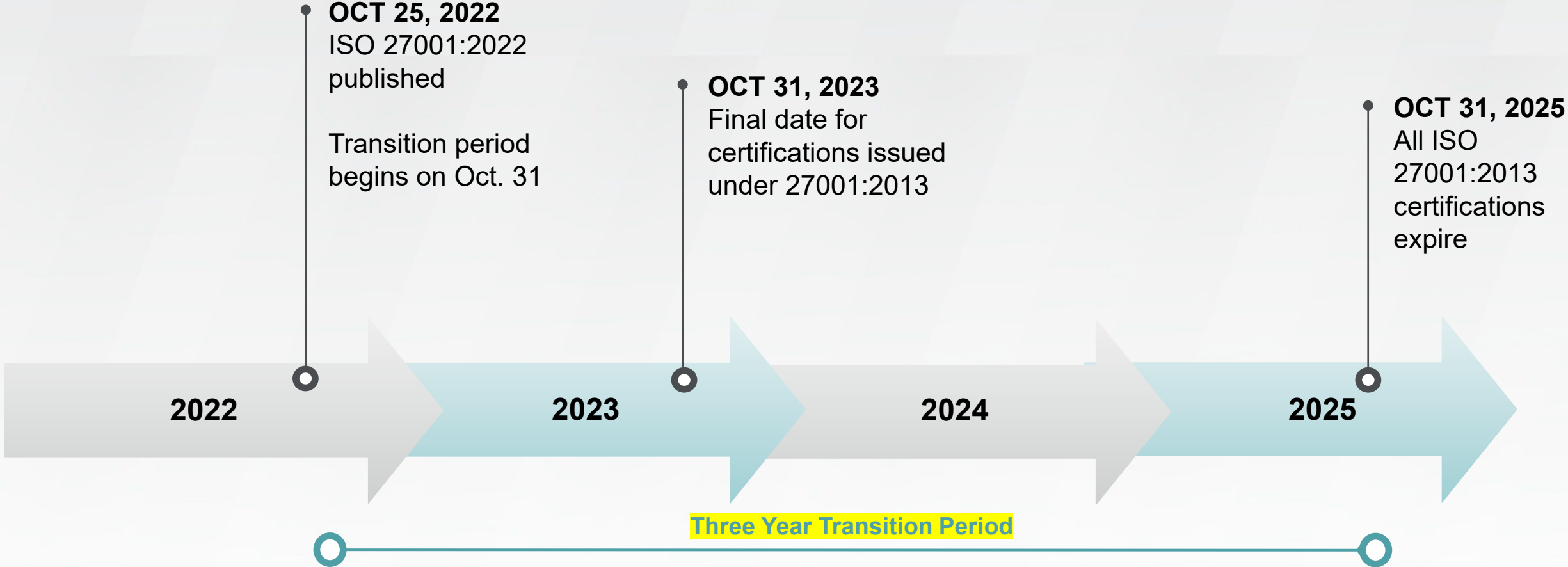
Secure Coding



# Example: Data Leakage Prevention



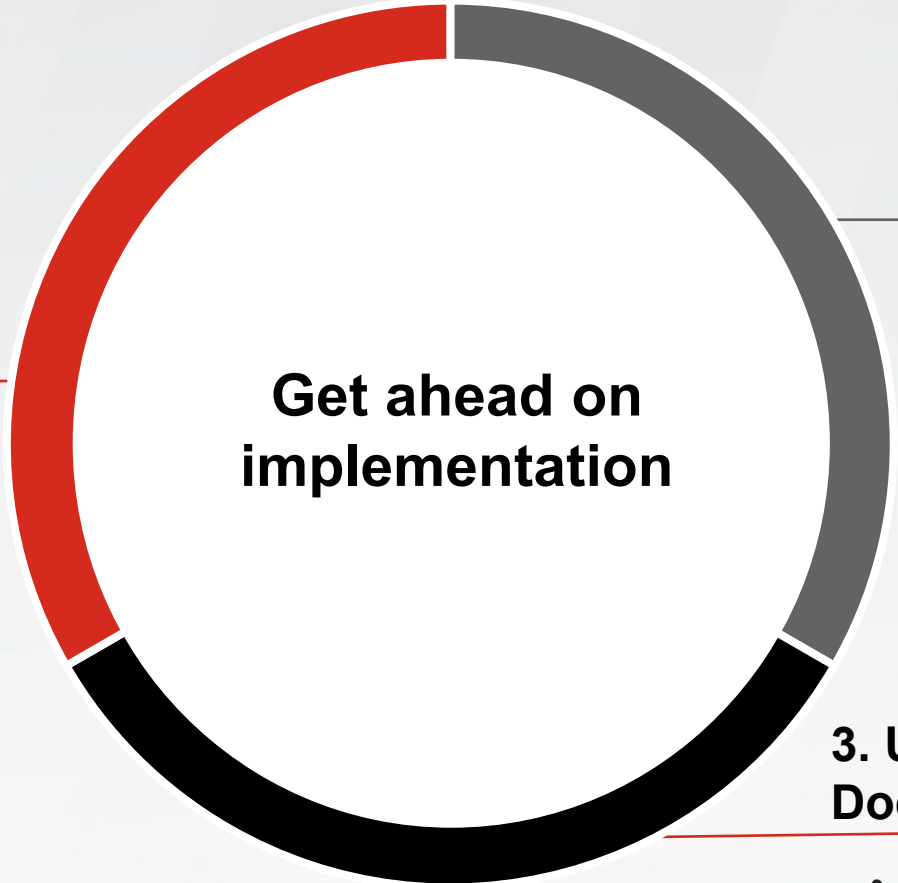
# Transition to ISO 27001:2022



# Integrating 27001:2022 into Your ISMS

## 1. Education & Awareness

- Become familiar with the changes
- Make key stakeholders aware of fundamental changes
- Begin communicating expected timeline for transition



**Get ahead on  
implementation**

## 2. Risk Analysis/Treatment

- Control Gap Analysis against new & changed controls
- Update Statement of Applicability, as needed

## 3. Update Processes & ISMS Documentation

- Documentation updates, including evidence of new or modified process changes
- Prepare for transition audit or recertification audit

# Common Questions

- / Will the new requirements be difficult to integrate?**
- / Does the new version of ISO 27001 impact my current certification?**
- / I don't currently have ISO 27001 certification. Do I need it? Is it worth it?**
- / Are there alternatives to ISO 27001?**

**Complete Summary of Changes Publicly Available Here:**  
<https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:dis:ed-3:v1:en>



# Questions

---

**FORV/S**

FORVIS is a trademark of FORVIS, LLP, registration of which is pending with the U.S. Patent and Trademark Office.

**{ databrackets }**  
Cybersecurity | Compliance | Certification

# CONTINUING PROFESSIONAL EDUCATION (CPE) CREDIT



**FORVIS, LLP** is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: [www.nasbaregistry.org](http://www.nasbaregistry.org)

# CPE CREDIT

- CPE credit may be awarded upon verification of participant attendance
- For questions, concerns, or comments regarding CPE credit, please email FORVIS at [cpecompliance@forvis.com](mailto:cpecompliance@forvis.com)

# Thank you!

[forvis.com](https://forvis.com)

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by FORVIS or the author(s) as to any individual situation as situations are fact specific. The reader should perform its own analysis and form its own conclusions regarding any specific situation. Further, the author(s) conclusions may be revised without notice with or without changes in industry information and legal authorities. FORVIS has been registered in the U.S. Patent and Trademark Office, which registration is pending.

# FORVIS

Assurance / Tax / Advisory