# Navigating ISO/IEC 27001: Top Common Errors to Avoid

PRESENTED BY: JOHN LAFFEY – PJR INFORMATION SECURITY PROGRAM MANAGER



# Before we Begin:

- All participants have been muted for call clarity
- The slides from this presentation will be available shortly from <u>www.pjr.com</u> – under 'Training', click 'Past Webinar Slides'
- A recording of this webinar (and all past webinars) will be available for review on YouTube
  - Search 'Perry Johnson Registrars' to view them free!



### Presenters

- John Laffey ISMS Program Manager for PJR and lead auditor for 27001.
- Dejan Kosutic CEO at Advisera and leading expert on cybersecurity and ISO 27001





- Frequently encountered issued during 27001 audits and strategies to avoid them
- Responses to questions asked during presentation



#### **Risk Assessment Process**





#### **Risk Treatment Process**

#### 01

Excluding controls that are applicable

**Obtaining approval of the** treatment plan and residual information security risks

02

Creating a statement of applicability that includes all requirements of the standard 03

Creating risk treatment plans





#### **Access Control**



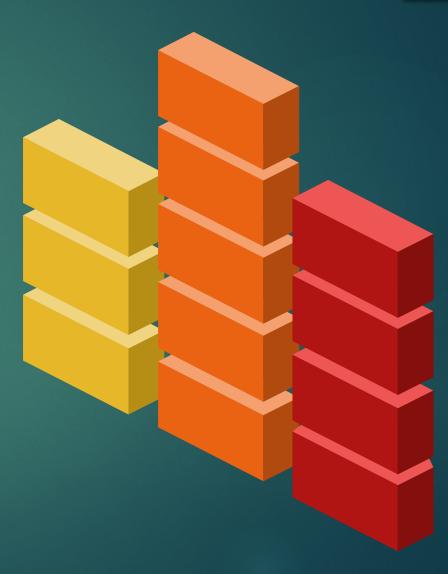


#### **Physical Controls**



Clear desk and clear screen policy – A.7.7

#### Physical security monitoring – A.7.4





#### Compliance

#### Legal, statutory, regulatory and contractual requirements A.5.31



Requirements identified and documented



#### Approach to meeting requirements docum

## Questions & Answers



- Contact us at 1-800-800-7910 for further information regarding 27001 certification
- Reach out to me at <u>ilaffey@pjr.com</u> with any further questions or comments



# Thank you for Attending!

DOWNLOAD THESE SLIDES AT <u>WWW.PJR.COM</u>

VIEW A RECORDING OF THIS PRESENTATION ON YOUTUBE ON OUR CHANNEL – PERRY JOHNSON REGISTRARS

