Top NCR's Issued during ISO 27001 Audits

PRESENTED BY: JOHN LAFFEY – PJR INFORMATION SECURITY PROGRAM MANAGER

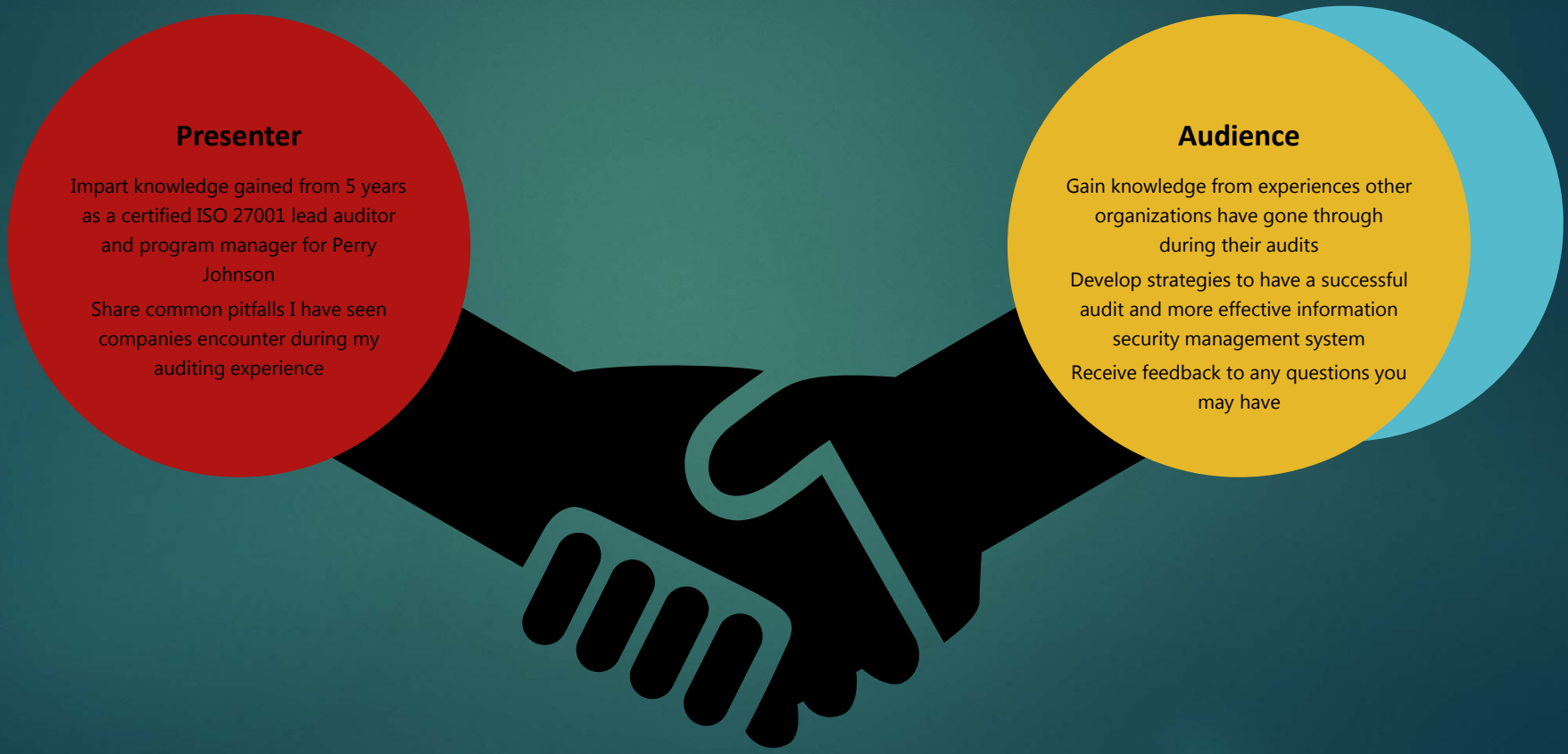
Before we Begin:

- All participants have been muted for call clarity
- The slides from this presentation will be available shortly from www.pjr.com – 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!

Agenda

- Objectives of this presentation
- Top NCR's issued during 27001 audits and strategies to avoid them
- Responses to questions asked during presentation

Objectives for this presentation



Presenter

Impart knowledge gained from 5 years as a certified ISO 27001 lead auditor and program manager for Perry Johnson

Share common pitfalls I have seen companies encounter during my auditing experience

Audience

Gain knowledge from experiences other organizations have gone through during their audits

Develop strategies to have a successful audit and more effective information security management system

Receive feedback to any questions you may have

Risk Assessment Process

Top NCR's Issued

01

Process does not define acceptable Level of risk

Organizations do not realize they must clearly define an acceptable level of risk – required by clause 6.1.2.a.1

Organizations are hesitant to put a level of risk in stone as acceptable – adjust the way you evaluate risk not your acceptable risk level

02

Not being conducted at planned intervals or when changes are made

Organizations do a great job with initial assessment during implementation and don't revisit it.

Major changes to systems are made without risk assessment being conducted.

03

Risk owners not identified

Clause 6.1.2.c.2 states that a risk owner must be identified for each risk however I have seen this omitted from many assessments.

04

Risks not prioritized for treatment

Clause 6.1.2.e.2 of the standard requires that risks be prioritized for treatment, however I often see this missed as well.

Access Control

Top NCR's Issued

1

User access provisioning, A.9.2.2:

It is required that a formal process be in place to add or remove access rights, on many occasions I have seen user accounts with privileges that had not gone through a formal process.

2

Review of user access rights, A.9.2.5

It is required that users access rights are reviewed at **regular** intervals, I have written several NC's against this requirement.

3

Removal or adjustment of access rights, A.9.2.6

It is required that users access is revoked upon termination or modified upon job change. I believe this is a critical control and in many cases have found active user accounts of terminated employees.

Physical and Environmental Security

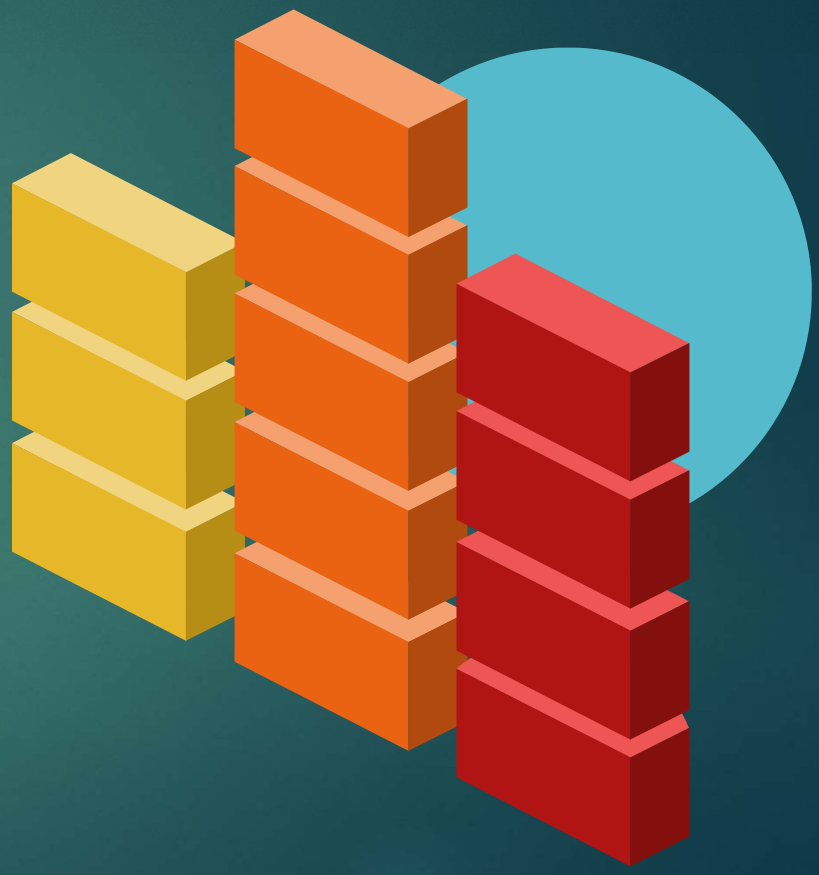
Top NCR's Issued

Unattended user equipment – A.11.2.8

This control requires unattended equipment has appropriate protection. This control requires user education and buy in, unattended computers should not be unlocked. I have written this NCR more than any other.

Clear desk and screen policy – A.11.2.9

It is required that a clear desk and screen policy is adopted, this includes printed sensitive material and awareness of your surroundings if you deal with sensitive information. Includes printed materials left on printers, material that requires shredding, etc.



Compliance

Top NCR's Issued

Identification of applicable legislation and contractual requirements – A.18.1.1

Requirements identified and documented

This control explicitly states that ALL legislative, statutory, regulatory, and contractual requirements concerning information security be documented and maintained. This can be a daunting task, however it is necessary to have a truly effective ISMS.

Approach to meeting requirements documented

This control also states that the approach to meeting each requirement is documented, this again can be a daunting task. This is amongst the most frequent NCR I have written.

Thank you for Attending!

DOWNLOAD THESE SLIDES AT WWW.PJR.COM

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

Questions & Answers

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