ISO 27001 – Expectations for Auditing of Annex A Controls

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!

PERRY JOHNSON REGISTRARS, INC.

Topics to be Covered -

- Overview of Annex A and its use
- Statement of applicability and its role during your audit
- Examples of controls from annex a being audited
- Responses to questions asked during presentation

PERRY JOHNSON REGISTRARS, INC.

Annex A – Reference Control Objectives and Controls

- Annex A is a table in the standard that contains controls and control objectives to be used when determining necessary controls for your ISMS.
- There are 114 controls grouped into 14 different categories.
- These controls cover everything for organization of policies, to physical security, to network security and encryption amongst others.
- This table is a great reference when conducting your risk assessment to ensure you are considering all possible risks that may be applicable to your organizations ISMS.

PERRY JOHNSON REGISTRARS, INC.

Statement of Applicability

- The statement of applicability is a document that lists all of the controls of annex a, a justification for inclusion or exclusion of the control, and status of implementation.
- The statement of applicability may also contain additional controls beyond what is in annex a, however all of the controls in annex a must be documented at a minimum.
- Though not required by the standard, it is helpful to also include a reference describing how the control has been implemented.

PERRY JOHNSON REGISTRARS, INC.

Statement of Applicability Example

Control	Inclusion Justification	Implementation Status	Exclusion Justification
A.8.2.1 Classification of Information	Risk Assessment Results	Implemented – See Policy #XYZ	NA
A.8.2.2 Labelling of Information	Risk Assessment Results, Contractual Requirements	Implemented – See Procedure #XYZ	NA
A.8.2.3 Handling of Assets	Risk Assessment Results, Contractual Requirements	Implemented – See Procedure #XYZ	NA

PERRY JOHNSON REGISTRARS, INC.

Objectives of Example Controls

- The control objective for A.8.2.1 as documented in ISO 27001:
  - “Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification”
- The control objective for A.8.2.2 as documented in ISO 27001:
  - “An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization”
- The control objective for A.8.2.3 as documented in ISO 27001:
  - “Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

PERRY JOHNSON REGISTRARS, INC.

Example Policy and Procedure

- Assume for our example the following in regard to the three controls we are looking at.
  - The organization has a policy defining three levels of classification; public, private, and confidential.
  - For each classification the policy describes the characteristics of information falling into each category, as well as examples.
  - The organization has a procedure for labelling and handling information based on its classification.
  - The procedure states that confidential and private information must be labelled as such in a watermark or header.
  - Handling requirements including transmission, retention, encryption, authorization, and destruction requirements are defined.

PERRY JOHNSON REGISTRARS, INC.

Auditing Effective Implementation of These Controls

- After verifying that a classification scheme has been adopted by the organization you can expect your auditor to do the following:
  - Inquire who handles the more restrictive classifications of information. Interview those who do and verify that they are handling the information in accordance with policy and procedure.
  - Verify with system admins where applicable that appropriate access control is implemented with regards to restricted information, as well as encryption if/where needed.
  - During interviews with staff and tours of office facilities auditors will be keeping an eye out for printed materials that are unattended or can be seen by those passing by to ensure that the information is not available to unauthorized individuals when it should not be as well as labelled appropriately where necessary.

PERRY JOHNSON REGISTRARS, INC.

Auditing Effective Implementation of These Controls cont.

- Additionally expect that all staff who may be randomly selected for interviews to assess awareness of the ISMS will be questioned about this policy.
  - This policy along with a few others is expected to be known by all staff.
  - A baseline knowledge of the policy and procedure is required for individuals to be able to identify different types of information and know how to handle them.
  - It is not expected that all staff would have the policy memorized, but could show awareness of it and be able to identify the level of classification for the information they were currently working with.

PERRY JOHNSON REGISTRARS, INC.

Objectives of Example Controls

- The control objective for A.9.2.1 as documented in ISO 27001:
  - “A formal user registration and de-registration process shall be implemented to enable assignment of access rights”

- The control objective for A.9.2.2 as documented in ISO 27001:
  - “A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services”

PERRY JOHNSON REGISTRARS, INC.

Example Procedure

- Assume for our example the following in regards to the two controls we are looking at
  - The organizations registration and de-registration process states that all requests must be submitted to the IT department by a member of HR. New user account requests must include name, start date, manager, position of employee.
  - The process also states that a user access request form must be filled out and submitted to IT by HR or individuals manager. The request form includes all systems the individual needs access to, as well as permission levels.

PERRY JOHNSON REGISTRARS, INC.

Auditing Effective Implementation of These Controls

- After verifying the procedure in place to add users and assign them access rights and permission you can expect your auditor to:
  - Interview members of staff who are responsible for assigning access rights and creating new accounts, verifying they understand the procedure and what is required.
  - Choose a sampling of recently hired staff and verify the necessary requests are on file along and that they were approved by the required individuals.
  - Verifying the permissions assigned to the sampled users match the requests on file by reviewing system configurations.
  - Reviewing a random sampling of user accounts for access and permissions and verifying that a request is on file matching levels currently granted.

PERRY JOHNSON REGISTRARS, INC.

Thank You for Attending!

Download these slides & view a recording at www.PJR.com.
Feel free to contact John Laffey with questions at jlaffey@pjr.com.

PERRY JOHNSON REGISTRARS, INC.

Questions & Answers

- Contact us for further information at 800-800-7910