PERRY JOHNSON
REGISTRARS, INC.

ISO 27001 Fundamental Concepts

Presented by John Laffey

PJR Technical 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 -

- Defining your scope per the requirements of ISO 27001 and the effect your scope can have on a certification audit.
- Risk assessment and treatment, statement of applicability, and how they fit together.
- Information assets, what they are and what do you need to do with them according to ISO 27001.
- How to address hosted infrastructure and services as part of your ISMS.
- Responses to questions asked during presentation

PERRY JOHNSON
REGISTRARS, INC.

Scope definition – What does ISO 27001 require?

- The standard requires that the organization shall determine the boundaries and applicability of the information security management system to establish it’s scope.
- Additionally, the standard requires that the organization **consider**:
  - The external and internal issues that are relevant to the organization’s purpose and that affect it’s ability to achieve the intended outcome’s of it’s ISMS.
  - The information security related requirements of the organization’s interested parties.
  - The interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.
- Lastly the standard requires that the scope be available as documented information.

PERRY JOHNSON
REGISTRARS, INC.

Scope definition – What do those requirements mean ?

- The organization shall determine the boundaries and applicability of the information security management system to establish it’s scope.
  - The types of boundaries that should be determined include physical, informational and organizational.
  - Physical boundaries are typically addresses of offices/buildings where the organizations activities are carried out.
  - Informational boundaries would be defined by the specific information handled by the organization that is desired to be in scope of the ISMS, this could be all of the information an organization handles as well.
  - Organizational boundaries – Are there only specific departments or functions included in the scope? Be sure to define them clearly.

Scope definition – What do those requirements mean ?

- The standard requires that the organization **consider** The external and internal issues that are relevant to the organization’s purpose and that affect it’s ability to achieve the intended outcome’s of it’s ISMS.
    - An example of an external issue would be legislative and regulatory requirements applicable to the industry or region you or your customers reside in. GDPR would be an example of an external issue relevant to an organization that collects information about individuals in the EU as part of their operations.
    - An example of an internal issue would be something related to what the purpose of the organization is. More specifically if an organization develops software that it sells, utilizing outsourced developers could be an internal issue that is relevant to the both the organizations purpose and its ability to achieve the intended outcomes of the ISMS.

PERRY JOHNSON
REGISTRARS, INC.

Scope definition – What do those requirements mean?

- The information security related requirements of the organization’s interested parties.
  - An interested party is defined as a person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity in ISO 27000.
  - Examples of interested parties and their information security related requirements include:
    - Owners of an organization may require that no information security related breaches take place that could cause financial and reputational damages to the organization.
    - Regulatory bodies may require that information security related legislation such as HIPAA be adhered to.
    - Customers of an organization may require that the organization safeguard the confidential or personal information disclosed to the organization as part of the goods or services being provided.

PERRY JOHNSON
REGISTRARS, INC.

Scope definition – What do those requirements mean?

- The interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.
  - In most modern information systems there will be portions that are provided by a third party, an example would be an internet provider. In this example it is expected that the organization would be able to identify the points of demarcation between its internally managed systems and the providers internet connection, and account for any risks that may arise from the company receiving information across this link and the inability for the organization to directly control or monitor the myriad of devices the information may pass through on its route from the sender.
  - The risks that arise from such interfaces and the treatment options available to the organization are going to be different from risks related to systems that the organization has control of, but they must still be considered and addressed.

Scope definition – What do those requirements mean?

- The standard requires that the scope be available as documented information.
    - Documented information could include written descriptions, charts and diagrams, network maps, lists, or any other method of describing the scope of the ISMS. It must be available as documented information, and must be controlled per the requirements of ISO 27001 clause 7.5.

Scope definition – Impact it could have on your certification audit

- The definition of the scope is going to the locations and number of people under the organization’s control that are included in the ISMS.
- The primary drivers of determining the duration of your certification audit are the risk level of the activities being performed, complexity of the ISMS, number of in-scope employees, and number of locations.
- It is recommended that you contact a registrar during the planning stages of implementing your ISMS in order to ensure the scope of the ISMS can be agreed upon, and to have a good idea of how long the certification process will take.

PERRY JOHNSON
REGISTRARS, INC.

Risk assessment, treatment, and statement of applicability (SoA)

- The standard requires that an information security risk assessment process be defined and applied that includes the risk acceptance criteria and the criteria for performing information security risk assessments.
- The standard requires that this process will result in an output of identifying information security risks within the scope of the ISMS, identifying the owners of those risks, analyzing the potential consequences and likelihood of the risks coming to fruition, and prioritizing the treatment of the risks.

PERRY JOHNSON REGISTRARS, INC.

Risk assessment, treatment, and statement of applicability (SoA)

- After risks have been identified, analyzed, and prioritized for risk treatment the organization must utilize their risk treatment process and apply it to any unacceptable levels of risks identified.
- Part of this process must include determining all necessary controls that require implementation in order to treat those risks.
- Annex A. of the standard contains a comprehensive list of controls, and the organization must refer to this list when determining necessary controls to ensure that no necessary controls have been omitted.

Risk assessment, treatment, and statement of applicability (SoA)

- After referencing the controls listed in Annex A., and determining all necessary (applicable) controls, a statement of applicability can be created.
- The SoA is required to document all of the controls from Annex A, justification for inclusion, status of implementation, and justification for exclusion if necessary.

Risk assessment, treatment, and statement of applicability (SoA)

Example Statement of Applicability Excerpt

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.

Risk assessment, treatment, and statement of applicability (SoA)

- To summarize, your risk assessment identifies the information security risks that require treatment. When determining the controls necessary to treat your risks to an acceptable level you reference all of the controls in Annex A. and document if they are applicable to you, justify their (ex)inclusion, and the current implementation status of the control. The document that you record this information on becomes your statement of applicability.

Information Assets – What are they and what does ISO 27001 require you to do with them?

- Information assets are comprised of the information an organization handles or processes, as well as the supporting information systems that are utilized for the processing, storage, and transmission of the information.
- Information assets can also include people in addition to hardware, software, and networking equipment.
- Identifying and determining the value of information assets in terms of criticality to business operations is a key component to an effective risk assessment process. Determining an assets value not just by the cost of procurement but by the criticality to the organization allows risks related to the asset to be properly evaluated for treatment. It would make sense that similar risks identified relating to the main operating system of an organization would be treated with a higher priority than risks to an internal system used to display upcoming holidays.
- The standard also requires that an inventory of information assets is drawn up and maintained, and that assets in the inventory have a designated owner. The asset owner should ensure that the asset is inventoried, has appropriate classification and define access restrictions and proper handling procedures.

Information Assets – What are they and what does ISO 27001 require you to do with them?

- Another benefit of identifying all of your information assets is to ensure that when conducting your risk assessment you are taking into account all of the identified information assets and not overlooking any systems or potential threat vectors.
- By having asset owners assigned who are knowledgeable and familiar with the information assets and the role they play in the organization overall, you have a great list of resources to consult with when conducting your risk assessment.
- Having a comprehensive and complete list of your information assets also provides clarity and confidence in knowing exactly what information your organization has in its possession, ensuring you can identify all applicable information security related requirements to this information.

Hosted services and infrastructure and how to address them in your ISMS

- Utilizing third party hosted services and infrastructure as part of an organizations information systems has become a common practice for many organizations. In some cases the majority of an organization's information systems and processing may be taking place on these third party provided platforms.
- In terms of ISO 27001 and its requirements, the most important thing to understand is that the organization is still responsible and required to ensure the protection of the information being processed and stored on these systems.

Hosted services and infrastructure and how to address them in your ISMS

- While an on-site visit to the third parties facilities is not typically feasible or appropriate for your certification audit, be prepared to demonstrate whatever due diligence your organization has conducted in order to have confidence that the third party platform is meeting your information security requirements.
- There are also controls that specifically speak to suppliers to the information security system and monitoring and measuring their performance, as well as ensuring that information security related requirements are clearly spelled out and agreed upon in contracts or agreements.

Hosted services and infrastructure and how to address them in your ISMS

- Be prepared to demonstrate what controls you have implemented and are responsible for as they apply to the hosted platform. For example, if a third party is providing you with hosted infrastructure it is still expected that you are considering all of the controls in Annex A. A more specific example would be related to physical security at the third party owned facilities where the systems you are utilizing are physically housed. You still must determine what your organizations requirements are in terms of physical security and be able to demonstrate how you are ensuring that they are being met by the third party.

Hosted services and infrastructure and how to address them in your ISMS

- As a organization seeking ISO 27001 certification, you must still be responsible for, and able to demonstrate the manner in which information security threats are being identified and treated whether it be on systems you own or on those provided by third parties.

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