

# Determining the Scope of your Information Security Management System (ISMS) for ISO 27001

Presented by: John Laffey, Technical Manager



## Please note:

- All participants have been muted.
- Please use the “Question” section of the dashboard – questions will be answered at the end of the session as time allows.
- Copies of today’s presentation will be available for download shortly after the conclusion of the presentation.
- This webinar will also be available for viewing on our website [www.pjr.com](http://www.pjr.com) under “Previously Recorded Webinars”.



# Topics to be covered

- Overview of standard and purpose of defining the scope of your ISMS.
- Who and what to consider when determining your ISMS's scope.
- Strategies for determining and defining the scope of your ISMS.
- Scope for success – potential benefits and pitfalls of narrowing your ISMS scope.
- Responses to questions asked during presentation



# ISO 27001 overview


- ISO 27001:2013 (current revision as of this presentation) is a standard published by the International Organization for Standardization, or ISO, that provides a framework for the planning, implementation, and continual improvement of an information security management system.
- Many of the numbered clauses are common with other ISO standards, and the requirements of the standard are found here.
- ISO 27001 contains an annex that lists several control objectives and controls that must be evaluated when preparing risk treatment plan.
- Internationally recognized standard in information security that will provide assurance to customers and partners in your information security program.



# Purpose of formal scope definition

- The scope definition serves the purpose of stating exactly what it is that an organization does that is certified to be effectively controlled by the requirements of the standard.
- Without a formal scope definition, the statement of an organization being ISO 27001 certified could mean a great deal, or not much at all.
- The scope statement should state exactly what it is that an organization does that is certified to the standard.
- Example 1 (bad): XYZ company's information security system.
- This provides no details as to what products or services the company provides that has been found to meet the standards requirements.


# Purpose of formal scope definition cont.



- Example 2 (good): The development, operation, and administration of the scheduling and planning Software as a Service platform provided by company XYZ.
- This scope statement tells us that the fictional organization has been certified in not just the operation and administration of its SaaS platform, but also the development as well.
- This also means that the people and information systems associated with the development, operation, and administration of the system are in scope and need to meet the requirements of the standard as well.
- In the event this fictional company also provided other services, such as consulting, there should be no confusion or assumption that this separate service meets the requirements of the standard as it is not documented in the formal scope and wouldn't have been subject to the certification audit.

# Who and What to Consider when Deciding on Scope

- First – Understanding your organization and the issues that are most relevant to it, and the needs and expectations of people and organizations who have the most interest in it. Please note that the requirements of people and organizations interested in your company should include any legal or regulatory requirements your organization are subject to.
- For example - if your company provides financial consulting, it would make sense to ensure that the people, processes, systems, and information involved with your clients data is in scope. It would also make sense to ensure that your company is not in violation of any laws or regulations specific to financial consulting, or to the countries/states/counties etc. you operate your business in.
- It would not make sense for the same business to have a scope that only includes their sales department, who do not have access to or influence on any customer data or its security.
- In short, you want to be sure you are meeting the requirements and/or wishes of those who have the most influence on the ability to reach the organizations goals.



# Strategies for Determining and Defining the boundaries of your ISMS

- After considering the details and parties most relevant to your organization and its goals, you should have a good idea of what information should be within the scope of your system.
- Now the boundaries of the ISMS must be determined, which can be thought of as a perimeter serving as a demarcation between a trusted controlled environment, and the outside world.



# Strategies for Determining and Defining the boundaries of your ISMS

- In many cases the easiest and safest way to determine your boundaries is to include the whole organization. All of its people, processes, systems, and physical locations would be included. For smaller organizations with a single office, or those only offer one product or service, it will most likely be less resource intensive to take this approach.
- Determining the people and processes to be included in this case is easy, as it is everyone who is part of the organization.
- Similarly the physical perimeter for your location(s) are also easily identifiable.
- Determining the logical boundaries for your data network can be aided by identifying where the demarcation points for entry and exit exist, or where your organization has control and visibility of the network and where it does not.

# Strategies for Determining and Defining the boundaries of your ISMS

- For organizations that have determined that they wish to limit the scope of their ISMS, here are some strategies to use.
- If it exists, an organizational chart may easily identify the departments/people that are involved with the specific product or service that is in scope. However if there are individuals that are out of scope but occupy the same offices or buildings, they will have to be treated the same as any other person outside of scope and controlled as such. This could include separate physical areas secured to only allow in scope personnel have access, separate information systems, putting contracts in place with other organizational units to define and enforce information security related requirements etc.
- Any physical locations where in scope personnel work from, or that are involved with the data and systems used for the in scope good or service will need to be included in the scope.

# Strategies for Determining and Defining the boundaries of your ISMS

- For limited scopes, a strategy for determining the logical boundaries of the ISMS is to create a high-level data flow chart that illustrates a logical mapping of the associated data. It isn't necessary to identify each unique server/router/switch/storage array etc. at this point. For example if you have 27 database servers in geographically diverse locations where in scope data could end up, just identify database servers as a single point on the map. Start with all of the possible ways the data enters your systems/buildings, all of the potential places it will go to be stored/processed/archived, and all possible exit points. Also note the possible ways it can get between these locations. After you have created the high level map you can go back and drill down each potential system the data could end up at to each unique instance of the resource in order to end up with a comprehensive list of the systems that would need to be in scope.
- Working with this list of systems, you can then identify the physical locations they reside, methods of transport between them, and individuals with access to these systems.
- This is not the only method, and may not necessarily be the best method for your specific ISMS.



# Scope for Success – Potential benefits and pitfalls of narrowing your ISMS scope

- As illustrated in the previous slides, narrowing the scope of your ISMS can reduce its initial cost in resources, or potentially, increase it. Being able to roll out the ISMS at a single location can certainly be much less daunting than implementing at multiple, but due to the ease with which data networks can cross organizational and geographical boundaries it may not be realistic.
- I suggest that you should first determine what it is that your organization does that would have the greatest benefit for your interested parties by being controlled by an ISO 27001 certified ISMS, and then working from there to identify the people, processes, systems and data that are involved in it.
- The feasibility and sensibility of limiting the scope of your ISMS will greatly depend on the specifics of your organization and its context. The key point to remember is that, with a limited scope, organizational assets outside of the scope must be treated the same as those external to your company.



# Questions and Answers

- Thank you for attending!
- [jlaffey@pjr.com](mailto:jlaffey@pjr.com)