Risk Assessment & Treatment Considerations for your ISMS

Presented by: John Laffey, Technical Manager

PERRY JOHNSON
REGISTRARS, INC.

Please note:

- All participants have been muted.
- Please use the “Q & A” 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 under “Previously Recorded Webinars.”

PERRY JOHNSON REGISTRARS, INC.

Topics to be covered

- Establishing the context, approach, and criteria for risk management.
- Risk identification.
- Risk analysis.
- Risk evaluation.
- Selecting risk treatment
- Implementing risk treatment plans
- Evaluating levels of residual risks
- Assessing effectiveness of treatment
- Responses to questions asked during presentation

Context, Approach, and Criteria

- The internal and external context of your organization and scope of your ISMS will be key drivers in determining what criteria will be needed for risk evaluation, impact, and risk acceptance. For example, contractual or regulatory requirements applicable to your organization could have a large influence on what your risk acceptance criteria will be. The risk assessment process should be reflective of the industry sector and risks related to the organization, as well as expectations of stakeholders and current threat landscape.
- There are many different information security risk management strategies and approaches, and ISO 27001 does not prescribe that a particular one be used. The standard does require, however, that assessments be performed at planned intervals or when significant changes are proposed to occur.
- While the standard does not specify what the risk acceptance criteria should be, it does require that it is established and maintained. Additionally the standard also requires that risks associated with the loss of confidentiality, integrity, and availability of information be identified.

Risk Identification

- ISO 27001 requires that risks associated with the loss of confidentiality, integrity and availability for information within the scope of the ISMS be identified. This can be an overwhelming task when no formal approach has been planned for guiding the process.
- The standard does not require that a specific approach be used, but for illustrative purposes I will outline a commonly used method for assisting you with this task.
- This is not in any way implying that this method is the most effective way for your specific organization, or should be the method used.

Risk Identification cont.

- The first step is to identify the assets that are within the scope of the ISMS. Keep in mind that assets are not just hardware and software, but anything of value to the organization. For this example, lets assume that there are primary assets (business processes and information) and supporting assets (hardware, software, network, personnel, site, org structure). By identifying the primary assets – critical business processes and/or information – in the scope of the ISMS you can then identify the supporting assets which could potentially affect the confidentiality, integrity and/or availability of the primary assets.
- Identify an asset owner for all identified assets, this should be the person most appropriate for being responsible and accountable for the asset. In many cases the asset owner is the person best suited to determine the asset's value to the organization.
- Identify threats to the primary and supporting assets identified in the previous step. Keep in mind that threats may be accidental or deliberate, and of natural or human origin. To ensure a comprehensive list is created as well as limit the magnitude of work, consider using generic threat types such as 'unauthorized access', 'physical damage', 'technical failure'. Then where specific individual threats of a certain type warrant explicit identification, ensure that you do so. Factors that would influence if a specific threat be identified should include the criticality of the asset they are associated with, as well as the level of damage they could cause if realized.
- When determining threats please consider soliciting input from as many resources as you are able to, including; asset owners, users, related staff members, legal departments, legal bodies, physical and informational security specialists, etc. The more complete threat listing you can generate, the more informed and protected you can be.

Risk Identification cont.

- Identify existing controls already in place or planned to be implemented. This step may be simply a review of existing documentation of implemented controls in place, or if this is the initial iteration of the assessment and treatment process may be more involved. If no existing controls documentation exists, you will need to check with the individuals responsible for information security (IS officer, building manager, operations managers, etc.) to get a comprehensive list of controls already in place. The primary objective of this step is to avoid wasting time and/or money by duplicating controls. After completing this you should have a list of all existing or planned controls, as well as their implementation and usage status.
- Identify vulnerabilities related to identified assets. Vulnerabilities are weaknesses associated with assets or controls, that can be exploited by one or more threats. There are many resources that can be used to assist with vulnerability identification, including lists of common threats and associated vulnerabilities, automated vulnerability scanners, penetration testing, code review, etc. After performing this step you should have a list of vulnerabilities in relation to your assets, threats, and existing controls. ISO 27001 requires that a risk owner is identified for all risks, and these owners need to have the accountability and authority to manage their identified risk(s).
- To summarize, the goal of the identification process is to have a complete list of information assets with associated threats, vulnerabilities, and a listing of existing and planned controls as well as their implementation status. By gathering this information you will be prepared to perform your risk analysis.

Risk Analysis

- Again, there are many methods of risk analysis that can be used, ISO 27001 does not require a specific methodology be employed.
- Continuing with our example method, the next step is to identify consequences that the loss of confidentiality, integrity and availability may have on the assets identified. A consequence can be loss of effectiveness, adverse operating conditions, loss of business, reputation, damage, etc.
- By taking the list of assets and associated threats and vulnerabilities, scenarios can be drawn up by describing a threat exploiting a vulnerability. The scenarios should include operational consequences in terms of investigation and repair time, time lost, opportunity lost, health and safety, financial cost, image reputation and goodwill.

Risk Analysis cont.

- Depending on the approach adopted by your organization, a qualitative or quantitative risk analysis methodology may be in place. In short, a qualitative analysis approach will employ a more subjective rating system for potential consequences and likelihoods (low, medium, high), while a quantitative approach will use numerical values for consequences and likelihood. Each approach has it's merits, and can be effective methods of risk analysis.
- To determine the level of risk, the consequence and likelihood values are combined to assign a raw risk value.
- Now, with your risks and levels of risk identified, you can evaluate and prioritize them.

Risk Evaluation

- ISO 27001 requires that organizations evaluate their risks by comparing the risk analysis results against the criteria for performing information security risk assessments as well as the risk acceptance criteria that they have determined appropriate for their ISMS.
- This last step in the assessment process is to use the information gathered during the previous steps to make informed decisions and take action. The standard requires that untreated risks that are beyond the established acceptable level of risk must be treated. Additionally the risks must be prioritized for risk treatment.
- Additional considerations besides the established acceptable level of risk that may be used include the importance or criticality of the asset the risk is associated with, the degree of confidence in the risk assessment process, as well as contractual, legal and regulatory requirements.

Selecting Risk Treatment Options

- Broadly speaking there are four options typically available for treating a risk:
  1. Avoidance – Choose not to take on the risk by avoiding the actions that cause it.
  2. Mitigation – Take actions that reduce the risk by reducing the likelihood, consequences, or both.
  3. Transfer – Transfer or share some or all of the risk to a third party.
  4. Acceptance – Choose to take on the risk as it currently stands, this is common if the evaluated level of risk meets the acceptable level defined without treatment.

- These four options are not mutually exclusive, and it is very common to see a risk be reduced to an acceptable level at which point it is accepted by the organization.

Selecting Risk Treatment Options

- In terms of information security related risks and the requirements of ISO 27001, the primary method of treatment will be the implementation or modification of controls. While the standard requires that you reference the controls in Annex A to ensure that none have been omitted that may be applicable to your ISMS, please remember that you are free to implement controls not already present in Annex A as needed.
- The selection of controls needed should take into account the risk acceptance criteria established during the risk assessment phase, as well as legal, regulatory and contractual requirements.
- While the risk of not complying with legal, regulatory and contractual requirements will typically never be acceptable, for other identified risks it is expected that the cost of implementing and ongoing maintenance of selected controls will be evaluated against the value of the asset(s) they will protect and overall return on investment.

Selecting Risk Treatment Options

- In addition to financial constraints, the following factors should also be taken into consideration when selecting controls:
  - Time constraints – e.g. the proposed control would take an unacceptable amount of time to be implemented.
  - Technical constraints – e.g. the proposed control would impact the performance of key systems making them ineffective for business purposes.
  - Operational constraints – e.g. a proposed control would require additional oversight and management that cannot be supported.
  - Environmental constraints – e.g. a proposed control would require a new facility to accommodate the space requirements.
  - Legal constraints – e.g. an existing regulation requires data of a certain type to be encrypted in a particular manner.
- By considering all of these factors when selecting controls you will be in a good position to have an attainable risk treatment plan put together.

Evaluating Residual Risks

- After defining your risk treatment plan, you will need to determine residual risks. This is done through another iteration of the assessment on the identified risks, taking into account the expected effects of the proposed treatment. The level of risk expected to still remain after the treatment has been implemented is referred to as the residual risk. If residual risks exist that do not meet the established acceptance criteria, another iteration of risk treatment selection may be necessary.
- The risk treatment plan should also include person(s) responsible for implementation, expected date of completion of the implementation, current status of the implementation, and must be approved by all identified risk owners indicating their approval of the plan and acceptance of all expected residual risk.

Assessing Treatment Effectiveness

- The method of assessing the effectiveness of your treatment plan is going to depend on the nature of the risk being treated. For example if an identified risk was an unsecured door to an area with sensitive information and was treated by the installation of a lock or card access system, it would be reasonable to see something along the lines of it being tested and verified to be working as intended. If the risk involved unpatched systems being vulnerable to attack, the treatment evaluation may be a weekly report showing numbers of unpatched systems still in use and would require ongoing monitoring to determine if the actions being taken are reducing the risk to the required level.
- Other methods of evaluating treatment effectiveness may include internal or third-party audits, vulnerability scans, penetration testing, number of security incidents that have taken place, etc. Regardless of the nature of evaluation, the critical part is that it is being done and that actions are being taken in the event a treatment option is found to be ineffective. Additionally the status of the risk treatment plan is required to be discussed during the management review as outlined in the standard.

Questions & Answers

Thank you for attending!

- Contact us for further information at 800-800-7910
- Contact me directly at jlaffey@pjr.com