Risk Treatment Considerations for your ISMS

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 under “Previously Recorded Webinars”.

Topics to be covered

- Selecting risk treatment
- Implementing risk treatment plans
- Evaluating levels of residual risks
- Assessing effectiveness of treatment
- Responses to questions asked during presentation

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 and Answers

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