

UIL Tool - Icon catalogue

**R. Hueting, S. Giorgi, A. Capaccioli (DBL), M. Bánfi, T. D. Soltész (MBE)**

# Risk assessment questionnaire

**Interview questions (target: pilot, possibly expertise / position in cyber security, risk management)**

1. Do you have any managerial improvement cycle applied for cybersecurity / risk management? If so, can you illustrate the activities in the following phases, *PLAN-DO-CHECK-ACT* (see figure below)? If a formal process cycle does not exist, what is the rationale? What tacitly defined informal steps are usually taken to respond to cyber security challenges?

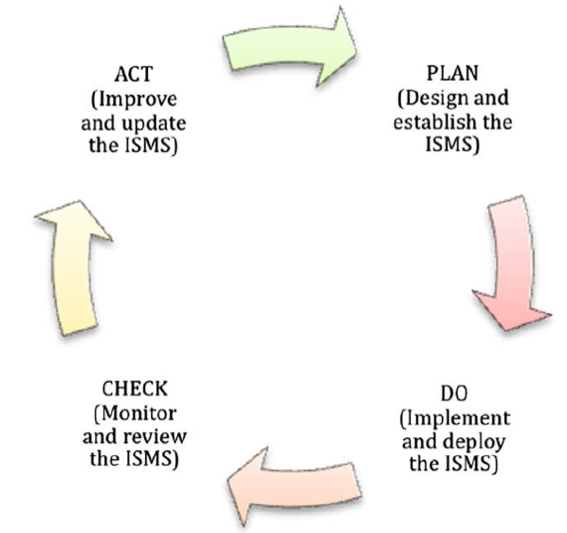


Figure 12. Information Security Management Systems (ISMS), Plan-Do-Check-Act (ISO/IEC 27001)

1. Describe the 3rd parties’ actors enabling the pilot’s services, and (if possible) what sensitive data is exchanged?
2. Rate the following risks for your pilot:   
   (PROB, probability of occurrence; IMPACT, possible monetary impacts. Likert Scale: 1, Very low; 2, Low; 3. Neither High nor Low; 4. High; 5. Very high)

|  |  |  |
| --- | --- | --- |
| **RISK** | **PROB**  **1 – Very Low to 5 Very High** | **IMPACT**  **1 – Very Low to 5 Very High** |
| Risks related to human failures / mistakes of resources employed, e.g.  -In-house staff deviating from the process (mistakes, including falling for social engineering attack)  -Staff at supplier side making mistakes/falling for social engineering attack.  -Failure of processes (e.g., background screening) |  |  |
| Corruption / malware mobile devices at work/home |  |  |
| Malware / virus in media devices, e.g. physical media transfer devices used by employees |  |  |
| Unauthorized access to network and network services. |  |  |
| Risk for physical access, damage and interference to the organization’s information and information processing facilities. |  |  |
| Sabotage of equipment/devices used for the storing / exchange of information. |  |  |
| Backup system failure. |  |  |
| Lack of redundant systems causing a major disruption or data breach[[1]](#footnote-1) |  |  |
| Unauthorised use of credentials allowing access to information systems. |  |  |
| Risk for eavesdropping[[2]](#footnote-2), intrusion via wireless networks and information theft. |  |  |
| Lack of security requirements in purchasing/procuring of new information systems or updates of existing ones. |  |  |
| Unauthorized access to information shared with suppliers. |  |  |
| Lack of response practices in case of cyber security / breach into the system. |  |  |
| Unauthorized physical access to premises (to steal or destroy devices or data) |  |  |

1. Are there any additional cyberthreats (including data loss / privacy issues) that you would like to add? Are there any specific threats targeting users with specific needs and limited access to the services implemented in your pilot? (Estimate threats probability and impact as in the previous question and write your answer in the table)

|  |  |  |  |
| --- | --- | --- | --- |
| **Any additional Cyberthreat** | **Please describe the Threat** | **Probability**  **(1 – Very Low to 5 -Very High)** | **Impact**  **(1 – Very Low to 5 - Very High)** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **Specific threats for specific user needs** | **Please describe the Threat** | **Probability**  **(1 – Very Low to 5 -Very High)** | **Impact**  **(1 – Very Low to 5 - Very High)** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. What protective measures are being adopted by your organization to prevent and counteract cyberthreats / unauthorized access to your systems / data loss?
   1. Are there any additional security measures that should be implemented to protect more vulnerable segment of users, i.e., specific needs and limited access.
2. Can you elaborate how the following KPIs can be affected in case of a successful cybersecurity attack against your pilot?
   1. COSTS.
   2. BRAND IMAGE.
   3. SALES / PROFITS

1. Data breach: confidential, sensitive, or protected information becomes exposed to an unauthorized person (Kaspersky, 2020). [↑](#footnote-ref-1)
2. Eavesdropping: theft of data / information while transmitted in network communications (Teng et al., 2012). [↑](#footnote-ref-2)