E-ITS based security evaluation instrument (pilot version 2021-2)

Your name:
Date:
Organization:

Dimensions notation	*Dimensions and explanations*	Objective: To provide E-ITS-based questionnaire to organizations with a repeatable and comparable result for measuring the performance of information security management for both self-assessment and monitoring at different stages of the implementation lifecycle. Note: Mark the dotted statements below, • which currently describe the situation of your organization - in green, • which partly correspond to the description of the situation - in yellow, and • what could be the goal, but has not yet reached it - in red. • Leave white statements that do not apply to your organization.			
		1st level *Dealing with risks with the help of external parties. Every incident can lead to days of interruption, major data leaks can occur so that the risk owner does not know it or can only know it through external parties. Data exchange can pose significant risks to the data exchange partner.*	*2nd level* *Formal information security requirements have been implemented, but members of the organization are not aware of them and may not be monitored. People are not aware of incidents or do not know how to deal with them. Dealing with risks is accidental and highly dependent on the individual involved. The sustainability of information security is not guaranteed. The data exchange partner is also at high risk.*	*3rd level* *An essential set of security measures has been implemented to deal with known threats and to manage the associated risks. The sustainability of information security is not guaranteed, and the response to previously unknown threats is uncertain. When people change in an organization, there is a risk of falling back to the 2nd level quickly. The primary risks for the data exchange partner are managed.*	*4th level* *The institution is also ready to deal with completely new risks. People know their roles and what to do in an emergency. Emergencies have been tested and recovery tested. Possible interruptions do not significantly disrupt the operation of business processes and services. In the management of incidents, the competence of external parties is rather involved only in the case of large-scale incidents. Confidence and trust are guaranteed for data exchange partners.*
		INITIAL: Good practices have not been implemented, risks have not been recognized, management has not taken the initiative. Security activities are haphazard and rather	DEFINED: Processes and activities are started when they take place on an ad hoc basis. The documents have been prepared but are partly out of date or do not correspond to reality.	BASIC: Practical part works and is documented, resources are planned, roles and responsibilities are allocated. The regularity of activities has not yet been achieved.	STANDARD: There are clear over organizational policies and principles. Activities are monitored, tracked, standardized, and documented. There is continuous improvement. Exceptions are monitored.

		initiated at the grassroots level.			
ISMS	***Security management*** *In every organization, regardless of size and composition*	1. Information security measures and documentation have been updated during the last 3 years. 2. The need for information security management is recognized and with clear objectives	3. Information security management is initiated at the management level. 4. Critical business processes and related assets and the requirements for protection are mapped to provide services. 5. There is a primary security policy. 6. Information security roles and responsibilities are divided. 7. Some information security issues are at a declarative level because resources are insufficient, and the requirements are not recognized.	8. Resources have been allocated for the implementation of information security management. 9. Information security implementation plan is in place, basic measures have been implemented. 10. Information security is integrated into all processes, process managers monitor the implementation of measures in their process.	11. The principles of information security management are known to everyone, they are updated regularly (once a year). 12. Regular management information security reviews take place (protocols maintained).
ORP	***Organization and personnel*** *In every organization, regardless of size and composition*	13. Guidelines and rules have been updated and are not just formal 14. Introductory trainings take place 15. Ad hoc solutions are avoided in access management.	16. Information security roles are defined, and responsibilities are defined. 17. In addition to introductory trainings, there are other trainings related to information security. 18. Relevant and up-to-date user rules have been created (internal bylaws, computer user regulations). 19. Process managers know the requirements and protection	20. Management knows what the situation is in the organization of information security and what are the information security requirements of the institution. 21. Process managers are aware of the weaknesses and risks of their process and manage them in accordance with the organization's practices and guidelines. 22. Employees are aware of the rules and follow them. 23. Replacements have clear rules and allow work to continue. 24. There are certain rules for access management, they are followed and monitored.	25. Personnel policy covers the management of the entire employee life cycle. 26. Work organization is monitored and improved; constant information is provided. 27. The organization has a supportive information security culture. 28. Information security training is also integrated into all other training and information events.

			requirements of their process and services.		
CON	***Concepts and methodologies*** *In every organization, regardless of size and composition*	29. The need for IT standardization of activities has been recognized	30. Predefined rules are followed when selecting and using cryptographic tools. 31. Pre-inspections are performed before the software and applications are deployed. Job hardware and software profiles have been created. 32. Impact assessments on the processing of personal data have been carried out and the necessary measures have been identified. A privacy policy has been established. 33. The principles of data backup have been prepared and data is being backed up.	34. There are clear rules for procuring, selecting, and deploying any software solution that follow the entire software lifecycle. 35. Job profiles have been created and consider the risks and protection requirements of business processes. 36. Data backup is tested regularly. 37. Users are aware of the possibilities and limitations of data backup.	38. The relevance of concepts, policies, strategies is monitored and regularly updated according to the needs and evolving requirements of the organization (regularity is evidenced by the documentation of reviews).
OPS	***Operational work*** *If external services are used for operational work, the corresponding requirements should be traceable in the form of an SLA.*	39. Personnel are competent to perform IT management. 40. Something is being logged. 41. Anti-malware programs have been implemented.	42. Change management is an agreed-upon process and is aligned with business processes. Update needs are monitored, and updates are monitored and implemented. 43. Before releasing the software, it is tested according to good practice separately from the work environment. 44. For teleworking, there are rules and agreements on how	46. IT management work is documented and traceable. 47. Terms of service have been agreed upon for IT management work. 48. There is a regular review of logs, log clocks are synchronized, and log collection is targeted. 49. For outsourced services, there is a contingency plan and a clear service level agreement that includes availability, integrity, and confidentiality clauses.	50. Change management is monitored and evaluated for effectiveness and efficiency. 51. There is a central system log infrastructure protected against unauthorized access, in which data is analyzed and alarmed in case of discrepancies. 52. An emergency plan has been prepared and tested for a remote maintenance failure and is regularly reviewed and updated. 53. Outsourced services are regularly monitored and evaluated. If changes are required, the services will be specified, and alternative options will be considered.

			tools are maintained for teleworking. 45. Rules have been agreed for outsourced services.		
DER	***Detection and response*** *Incident management and audits / reviews* *In every organization, regardless of size and composition*	54. When a security incident is reported, it is responded to by following agreed rules. 55. The obligation of information security audit is recognized.	56. A channel has been created for reporting security events and all security events are registered in the security event log. 57. A first aid guide for a security incident has been developed. 58. Formal documents are prepared for passing the information security audit. 59. The roles of people and communication channels in the event of an incident have been agreed.	60. The critical network segments are defined and monitored. 61. External sources are monitored for information analysis and risk estimation (reports). 62. Evidence of security events is preserved. 63. An escalation strategy and communication procedure has been established for a more significant security event. 64. The results of the information security audit are analyzed and included in the information security implementation plan. 65. An emergency concept has been created, including all business processes, and introduced to employees.	66. Regular inspections of detection systems are carried out and automatic alarms are implemented if possible. 67. Users and IT administrators regularly participate in information security exercises. 68. Regular internal and external audits of information security take place, which is the basis for management reviews and planning of future information security budget. 69. Emergency drills are conducted regularly, and Red Teaming is implemented.
APP	***Applications*** *If external services are used for operational work, the corresponding requirements should be traceable in the form of an SLA.* *Client applications, directory services, network services, business applications, groupware*	70. When deploying applications, the rights granted to the applications are monitored and restricted. 71. Application and database configurations are managed without clear rules. 72. When deploying groupware, each client configures it himself.	73. Users receive alerts about potential threats to user applications. 74. There are rules and a general security policy for directory services. 75. Allowed applications are defined. 76. Authentication is always required to use web applications. 77. A defined person is responsible for managing an organization's domain names. 78. Rules have been arranged for replacement (incl. E-mail exchange, access management).	79. Central computer management is used. The maintenance of office applications is organized by a trained role performer. 80. Directory services are managed only by the respective administrator. 81. Group policies have been implemented for directory services. 82. Each user account can be associated with a specific employee. 83. Passwords for administrative accounts are secure and unique. 84. Servers and client computers store passwords only in the form of hashes. 85. The access rights documentation corresponds to the actual situation. 86. The source code of web applications is protected against unauthorized access. 87. External networks use TLS and HTTPS to protect data communications. 88. The organization's domain names are renewed regularly and in a timely manner.	93. Lists of requirements have been created for the applications. The application is tested for compatibility before deployment. 94. When documents are sent, they are digitally signed to protect them from editing. 95. Web browsers are configured centrally. 96. Directory service activities are monitored and logged; log data is reviewed regularly. Logs are stored for 1 year. 97. The security of the webserver is checked regularly with penetration testing (e.g., during each audit). 98. When using the same domain name, the domain namespace is clearly divided into public and internal parts. 99. Database backup recovery and integrity are tested and checked regularly. 100. Restrictions on the automatic opening of e-mail attachments have been applied.

				89. Database security events are logged with a timestamp, the logs are protected against modification and overwriting. 90. Databases are backed up. 91. The groupware client is preconfigured for the user. 92. Server default account names and passwords have been changed; unnecessary default accounts have been deactivated.	
SYS	*IT systems* *If external services are used for operational work, the corresponding requirements should be traceable in the form of an SLA.* *Server, computer, mobile devices, other devices*	101. Only people with access rights can access the servers. 102. The servers use anti-malware software. 103. Printers and multifunction printer are in locations where the work is noticeable to other employees and where there are no unaccompanied guests. 104. There is a paper shredder or a container of paper documents to be destroyed near the printer or multifunction printer.	105. Configuration of server software, services, and accounts is documented. 106. It is documented which activities are logged on the servers and under what conditions the logs are viewed. 107. The client computer can only be used by a properly authenticated user. 108. The client computer has at least two user accounts: an administrative account and a regular user account. 109. For client computers have decided which cloud services and to what extent are allowed to be used. 110. The organization has a procedure in place to report the loss, theft, or malfunction of the laptop. 111. The organization has developed and established rules for the use of mobile phones.	114. Backup systems are physically separated from the servers to be backed-up and are in different fire compartments. 115. The user authenticates to the server only with a personalized user account. 116. Patches and updates have been tested on the test server for security, compatibility, and performance before being installed on the server. 117. It has been verified that the backed-up data can be restored on the server and can be used as intended after recovery. 118. Server malware control software is updated regularly. 119. Logs are analyzed regularly. 120. Before implementing the virtualization system, it has been checked whether: the host server of the virtual infrastructure has sufficient data connections for the virtualization system; the requirements for separation and encapsulation of applications running in the virtualization system are met; the virtualization system meets the requirements for availability and data transfer performance. 121. An administrative user account on client computers is used only to manage the client computer. No normal operations are performed under an account with administrative rights. 122. At least data that cannot be derived from other data is regularly backed up from client computers.	130. The server is connected to a uninterruptable power supply (UPS) with sufficient power and battery life, the battery life of which has been checked regularly. 131. Only services that are necessary for the purpose of the server are installed on the server. 132. Regular server security tests are documented. 133. Servers providing services outside the organization are in a demilitarized zone (DMZ). 134. All server configuration changes, and security activities can be tracked based on documentation (such as automatic logging). 135. The implementation of a server disaster recovery plan is practiced regularly. 136. The monitoring tools immediately inform the operating personnel if the prescribed limits are exceeded and if any faults occur. 137. Users have only such rights and have access only to the functions, services, and data they need to perform their tasks (the need-to-know principle). 138. The client computer's microphone and camera will not be used without the user's consent. Only authorized devices are connected to the client computer. Device authorization is documented. 139. Client computers are connected to a central monitoring system. 140. A reference installation has been created for client computers. During installation, the appropriately preconfigured reference installation is cloned into the client

			112. Only system administrators have access to server system files. 113. When the user is away and not in use, the user locks the screens of their devices (computer, phone, tablet).	123. Client computers have centrally managed anti-malware software installed. 124. The user is granted write access only to a specifically specified file system area. Users do not have write access to operating system and application folders. 125. The personal firewall is activated on the laptop. 126. Device names do not provide information about the user's identity and do not contain elements referring to an organization (mobile phones). 127. Configuring printers and multifunctional printers through the control panel and the webserver is password protected. The password is known only to authorized users. 128. Access to the Intranet for IoT devices is as limited as possible. The devices themselves are protected against unauthorized physical access. 129. Employees know what data is allowed to be stored on removable media and under what conditions.	computer. The reference installation contains all configuration changes, updates, and security patches, and has been pre-tested and documented. 141. The digital assistants on the client computers are deactivated. 142. Laptop disks are encrypted. 143. Files downloaded on the client computer are not opened automatically. 144. Multiple authentications (such as 2FA) is used to log on to the computer. 145. Logging on to the organization's Intranet is only possible on approved laptops (e.g., through certificate-based device authentication). 146. The user cannot change the security settings of web applications and e-mail clients on their own. 147. Access from the laptop to the internal network is encrypted via a virtual private network (VPN). 148. The SIM card of a smartphone or tablet is protected by a PIN code other than the default setting. 149. The wireless interfaces of mobile phones (e.g., WLAN or Bluetooth) are deactivated when not in use or during breaks. 150. If IoT devices (such as security cameras) belong to a more general-purpose system (such as a building management system), they only exchange data with that system. When a LAN network device belongs to a larger IT system, the device's direct access to the Internet is blocked.
IND	***Industry*** *If external services are used for operational work, the corresponding requirements should be traceable in the form of an SLA.*	151. There is a service agreement with an external operator of industrial automation.	152. The initial passwords for the operational technologies have been replaced. 153. Data exchange partners and data categories for industrial automation components are documented. 154. A support service agreement has been	155. Industrial automation is part of an integrated security policy. 156. It is defined and documented which data and events of the automation components are logged, how long the log data is stored and who can access the logs. 157. Unnecessary interfaces, services, functions of drive technology and industrial automation components have been deactivated or uninstalled.	160. A zone concept has been developed for the use of industrial automation. The operating technology infrastructure is documented. 161. Access to maintenance interfaces is restricted to authorized persons. 162. Complete documentation of industrial automation is available in case of faults. 163. Measurement and control data transmitted in public networks are protected by secure data communication protocols. 164. Sensors are calibrated regularly, calibration is documented.

	Operational and control equipment, industrial automation (incl. SCADA, robots, smart houses)		concluded with the supplier of the robotic device.	158. Industrial automation components are separated from office IT systems; communication of components with other components is needs-based and as minimal as possible. 159. When performing remote maintenance on a robotic device, the maintenance provider cannot access other systems or robotic devices in the organization.	165. Safety automation devices are managed in accordance with legal regulations and safety standards. 166. The value limits of the safety automation variables are defined, and the reaching of the limit is alarmed.
NET	***Networks and communications*** *If external services are used for operational work, the corresponding requirements should be traceable in the form of an SLA.* *Networks, network components, communications*	167. There is a certain role for managing computer network. The network is documented.	168. The principles of network topology have been documented and updated at least during the last 3 years. 169. There are documented rules for managing and operating network devices. 170. The wireless LAN usage policy specifies which internal and external networks the wireless LAN client may be connected to.	171. The network is documented, and updates are added immediately (up to date). 172. The network is segmented according to the protection requirements. 173. The default passwords for all network components have been changed. 174. Security updates and security patches issued by the network equipment manufacturer are installed as soon as possible after publication. 175. Network management solutions are backed up (settings, logs, event notifications). 176. IEEE 802.11i-2004 (WPA2 encryption mechanism) or later (WPA3) is used. WEP and WPA are disabled. 177. All network management components and associated network components are time-synchronized and use the same time zone. 178. The default passwords have been replaced with strong enough passwords before using the telephone switching office.	179. During the regular network management review, the up-to-dateness of the network management documentation, compliance with the status and the actual procedures are checked (more than one review report). 180. Significant events related to network components and network management tools are automatically reported to the responsible IT staff immediately after the event. 181. Configurations of network management tools and network components are backed up and are part of the organization's recovery plan. 182. Wireless LAN access is only allowed through a firewall. 183. Firewalls are monitored, logs are stored, and defined events are automatically notified.
INF	***Infrastructure*** *If external services are used for operational work, the corresponding requirements should be traceable in the form of an SLA.*	184. The buildings meet fire safety requirements and anti-burglary measures have been implemented.	185. The spatial plan has considered the existence of secure zones and established separate access systems and principles (e.g., door locking). The special requirements of the protected premises have been considered	188. Access and key management are in place; rules are documented and recognized. 189. Unused cables are discarded. 190. Workplace documents are stored according to agreed rules. 191. Cabling and piping plans are valid. 192. Cabling is intelligibly marked and documented.	193. Regular fire safety drills. 194. Server room sensors and equipment are monitored and tested regularly, results are documented, and equipment is upgraded if necessary. 195. The network documentation is updated based on changes and reviewed regularly.

	Buildings, premises, cabling		(lack of piping, gas extinguishing, etc. in the server rooms). 186. Guest supervision is in place. 187. A proper server room has been set up, with access restricted to the appropriate roles.		