E-ITS based security evaluation instrument (pilot version 2021-3)

Your name*:… ..
Role of the respondent*: …
Date of completion*:…
Institution*:…
Institution domain*: …
Number of computer jobs in the institution*: …
Number of geographical locations of the institution that depend on the ITC*: …
Other:…

Dimensions notation	Dimensions and explanations	**Objective:** To provide E-ITS-based Maturity Model 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 • accurately describe the situation in your org - in green, • somewhat describe the situation in your org with only a few shortcomings – in yellow, • partly describe the situation in your org and with significant shortcomings – in purple, and • 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	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.

		activities are haphazard and rather 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 3a years. 2. The need for information security management is recognized and with clear goals	3. Information security management is initiated at the management level. 4. Critical business processes and related assets for services and the necessary security needs (in the context of availability, integrity, and confidentiality) have been mapped. 5. There is a primary security policy. 6. Information security roles and responsibilities have been assigned.	7. Resources have been allocated for the implementation of information security management. 8. The information security implementation plan is in progress, the main measures have been implemented. 9. Information security is integrated into all processes, and process managers monitor the implementation of measures in their process.	10. The principles of information security management are known to everyone, they are updated regularly (once a year). 11. Regular management information security reviews take place (protocols maintained).
ORP	***Organization and personnel*** *In every organization, regardless of size and composition*	12. User rules have been drawn up. 13. Introductory trainings are taking place 14. Ad hoc solutions are avoided in access management.	15. Information security roles and responsibilities are divided. 16. In addition to introductory trainings, there are other trainings related to information security. 17. User rules are relevant and up to date (internal rules, computer user rules). 18. Process managers know the requirements and protection needs of their process and services. 19. Rules have been established for replacement (incl. E-mail exchange, access management).	20. Management knows the situation in the organization of information security and the information security requirements of the institution. 21. Process managers are aware of the vulnerabilities and risks of their process and manage them in accordance with the organization's practices and guidelines. 22. Employees are aware of and follow the rules. 23. Replacements have clear rules and allow work to continue. 24. There are certain rules for access management, they are followed and monitored.	25. The personnel policy covers the management of the entire life cycle of an employee. 26. Work organization is monitored and improved; constant information is provided. 27. The general culture of the organization supports information security. 28. Information security training is also integrated into other training and information events.
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 shall be followed in the selection and use of cryptographic tools. 31. Pre-inspections are performed prior to software and applications are deployed. 32. Job hardware and software profiles have been created. 33. Impact assessments on the processing of personal data have been carried out and the	35. There are clear rules for procuring, selecting, and deploying any software solution, which are followed the entire software lifecycle. 36. Job profiles have been developed and consider the risks and protection need of business processes. 37. Data backup is tested regularly. 38. Users are aware of the possibilities and limitations of data backup.	39. 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 documentation of reviews).

			necessary measures have been identified. A privacy policy has been established. 34. Data backup principles have been developed and data is being backed up.		
OPS	***Operational work*** *If external services are used for operational work, the corresponding requirements should be traceable in the form of an SLA.*	40. There are competent personnel to perform system administration. 41. Something is being logged. 42. Anti-malware programs have been implemented.	43. Change management is an agreed-upon process and is aligned with business processes. Update needs are monitored, and updates are monitored and implemented. 44. Before releasing the software, it is tested according to good practice separately from the work environment. 45. For teleworking, there are rules and agreements on how work equipment is maintained in the case of teleworking. 46. Rules have been agreed for outsourced services.	47. IT administrative work is documented and traceable. 48. Terms of service have been agreed for the performance of IT management work. 49. There is a regular review of logs, which presupposes that the collection of logs is targeted and that the log clocks are synchronized. 50. There is an emergency plan and a clear service level agreement for outsourced services, which includes availability, integrity, and confidentiality clauses.	51. Change management is monitored and evaluated for its effectiveness and efficiency. 52. There is a central system log infrastructure protected against unauthorized access, in which data is analyzed and alarmed in case of discrepancies. 53. An emergency plan for a remote maintenance failure has been prepared and tested and is regularly reviewed and updated. 54. Outsourced services are regularly monitored and evaluated. If changes are required, the services will be specified, and alternative options will be considered.
DER	***Detection and response*** *Incident management and audits / reviews* *In every organization, regardless of size and composition*	55. When a security incident is reported, it is responded to according to agreed rules. 56. The obligation to audit information security is recognized.	57. A channel shall be established for the notification of security events and all security events shall be registered in the register of security events. 58. A first aid guide for a security incident has been developed. 59. Formal documents are prepared for the information security audit. 60. The roles of people and channels of communication in the event of an incident have been agreed.	61. The critical network segments are defined and monitored. 62. External sources are monitored for information analysis and risk estimation (reports). 63. Evidence of security incidents is preserved. 64. An escalation strategy and communication procedure has been established for a more significant security event. 65. The results of the information security audit are analyzed and included in the information security implementation plan. 66. An emergency concept has been created, involving all business processes, and has been introduced to employees.	67. Regular inspections of detection systems are caried out and automatic alarms are implemented where possible. 68. Users and IT administrators regularly participate in information security exercises. 69. There are regular internal and external audits of information security, which are the basis for management reviews and planning of future information security budget. 70. Emergency drills are conducted on a regular basis and Red Teaming is implemented.
APP	***Applications*** *If external services are used for operational work,*	71. The rights granted to applications are monitored and limited during their deployment.	74. Users receive alerts for potential threats to user applications. 75. Directory service has rules and a general security policy.	80. The maintenance of the office software is organized by a trained role performer.	94. Lists of requirements have been created for applications. The application is tested for compatibility before deployment. 95. Documents are digitally signed to protect them from being sent.

	the corresponding requirements should be traceable in the form of an SLA. *Client applications, directory services, network services, business applications, groupware*	72. Application and database configurations are managed 73. Groupware is up and running	76. Allowed applications are defined. 77. Authentication is required to process data defined for internal use only by web applications. 78. A specific person is responsible for managing an organization's domain names. 79. Central computer management is in use	81. Directory services (e.g., AD, LDAP) are only managed by the respective system administrator. 82. Group policies have been implemented for directory services. 83. Each user account can be associated with a unique user. 84. Passwords for administrative accounts are secure and unique. 85. Servers and client computers store passwords only in a hash form. 86. The documentation of access rights corresponds to the actual situation. 87. The source code of web applications is protected against unauthorized access. 88. External networks use encrypted communication protocols (TLS and HTTPS) to protect data. 89. The domain names of the organization have been renewed regularly and in a timely manner. 90. Database security events are logged with a timestamp, the logs are protected against modification and overwriting. 91. The databases are backed up. 92. The groupware client is preconfigured for the users. 93. The default server account names and passwords have been changed; unnecessary default accounts have been deactivated.	96. Web browsers are configured centrally. 97. The activities of the directory service are monitored and logged; the log data are reviewed regularly. Logs are stored for one year. 98. The security of the web server is checked regularly through penetration tests (e.g., during each audit). 99. When using the same domain name, the domain namespace is clearly divided into public and internal segments. 100. The recoverability and integrity of database backups are regularly tested and verified. 101. Restrictions on automatic opening of e-mail attachments have been applied.
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*	102. Only persons with access rights shall have access to the servers. 103. The servers use anti-malware software. 104. Printers and multifunction printer are in locations where the work is noticeable to other employees and where there are no unaccompanied guests. 105. There is a paper shredder or a container for paper documents to be	106. The configuration of the server software, services, and accounts are documented. 107. It is documented which activities are logged on the servers and under what conditions the logs are viewed. 108. The client computer can only be used by a properly authenticated user. 109. The client computer has at least two user accounts: an administrative account and a regular user account. 110. For client computers have decided which cloud services and	114. Before server deployment, a server usage plan is prepared, which defines the purpose of implementation, hardware requirements, integration with other applications (e.g., directory services) and backup arrangements). 115. Backup systems are physically separate from the servers to be backed up and are in different fire compartments. 116. The user authenticates to the server only with a personalized user account. 117. The patches and updates have been tested for security, compatibility, and performance on the test server before being installed on the server.	131. The server is connected to a uninterruptable power supply (UPS) with sufficient power and battery life, the battery life of which is checked regularly. 132. Only services that are necessary for the purpose of the server are installed on the server. 133. Regular server security tests are documented. 134. Servers that provide services outside the organization are in a demilitarized zone (DMZ). 135. All server configuration changes, and security activities can be tracked based on documentation (such as automatic logging). 136. The implementation of a disaster recovery plan is regularly practiced.

		destroyed near the printer or multifunction printer.	to what extent are allowed to be used. 111. The organization has procedures in place for reporting the loss, theft, or failure of a laptop computer. 112. The organization has developed and established rules for the use of mobile phones. 113. Only system administrators have access to server system files.	118. It has been verified that the backed-up data can be restored to the server and can be used as intended after recovery. 119. Server malware control software is updated regularly. 120. Logs are analyzed regularly. 121. The prerequisites for the implementation of the virtualization system have been met and verified (the virtual infrastructure host server has sufficient data connections for the virtualization system; the requirements for separation and encapsulation of applications running in the virtualization system have been met; the virtualization system meets availability and data transfer performance requirements). 122. An administrator user account on client computers is used only to manage the client computer. No normal operations are performed under an account with administrator rights. 123. At least the data that cannot be derived from other data is regularly backed up from client computers. 124. Centrally managed anti-malware software installed on client computers. 125. The user is granted write access only to a specified file system area. Users do not have write access to operating system and application folders. 126. The personal firewall is activated on the laptop. 127. Device names do not identify the user and do not contain elements referring to the organization (e.g., mobile phones). 128. Configuring printers and multifunctional printers through the control panel and web server is password protected. The password is known only to authorized users. 129. Access to the intranet for IoT devices shall be as limited as possible. The devices themselves are protected against unauthorized physical access.	137. The monitoring tools immediately inform the operating staff if the prescribed limits are exceeded and if any faults occur. 138. Users have only such rights and access only to the functions, services, and data they need to perform their tasks (the principle of knowledge). 139. The client computer's microphone and camera will not be used without the user's consent. Only authorized devices will be connected to the client computer. Device authorization is documented. 140. Client computers are connected to a central monitoring system. 141. A reference installation has been created for client computers. During installation, the appropriately preconfigured reference installation is cloned into the client computer. The reference installation contains all configuration changes, updates, and security patches, and has been pre-tested and documented. 142. The digital assistants on the client computers have been deactivated. 143. Laptop disks are encrypted. 144. Files downloaded on a client computer are not opened automatically. 145. Multiple authentication (e.g., 2FA) is used to log on to the computer. 146. Logging in to the organization's intranet is only possible on approved laptops (e.g., through certificate-based device authentication). 147. The user cannot independently change the security settings of web applications and email clients. 148. Access from the laptop to the internal network is encrypted via a virtual private network (VPN). 149. The SIM of a smartphone or tablet is protected by a PIN that is different from the default setting. 150. The radio interfaces of mobile phones (e.g., WLAN or Bluetooth) are deactivated when not needed or when interrupted. 151. If IoT devices (e.g., security cameras) belong to a more general-purpose system (e.g., a

				130. Employees are aware which data is allowed to be stored on removable media and under what conditions.	building management system), they only exchange data with that system. If the device of the object network belongs to a larger IT system, the direct access of the device 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.* *Operational and control equipment, industrial automation (incl. SCADA, robots, smart houses)*	152. There is a service contract with an external operator of industrial automation.	153. The data exchange partners, and data categories of the industrial automation components are documented. 154. A support service agreement has been concluded with the supplier of the robotic device.	155. The default passwords for the operational technologies have been replaced. 156. Industrial automation is part of an integrated security policy. 157. The data and events of the automation components are logged and documented (log storage duration, access to logs). 158. Unnecessary interfaces, services, functions of operational technology and industrial automation components have been deactivated or uninstalled. 159. The components of industrial automation are separated from the office IT systems, the interaction of the components with other components is needs-based and as minimal as possible. 160. When performing remote maintenance of a robotic device, the maintenance service provider has not the access to other systems or robotic devices in the organization.	161. A zoning concept has been developed for the use of industrial automation. The operating technology infrastructure is documented. 162. Access to maintenance interfaces shall be restricted to authorized persons. 163. Full documentation of industrial automation is available in case of faults. 164. Measurement and control data transmitted in public networks are protected by secure data communication protocols. 165. Sensors are calibrated regularly, calibration is documented. 166. Safety automation equipment is managed in accordance with legal regulations and safety standards. 167. 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*	168. There is a certain role for managing computer network. 169. Network topology is documented.	170. The network topology principles are documented and updated at least during the last 3 years. 171. There are documented rules for managing and operating network devices. 172. The wireless LAN usage policy specifies which internal and external networks the wireless LAN client may be connected to.	173. The network is documented, and updates are added immediately (up to date). 174. The network is segmented according to the protection requirements. 175. The default passwords for all network components have been changed. 176. Security updates and security patches issued by the network equipment manufacturer are installed as soon as possible after publication. 177. Network management solutions are backed up (settings, logs, event notifications). 178. An up-to-date cryptographic mechanism is used to secure wireless communications (e.g., WPA3). The use of easy-to-break encryption protocols (e.g., WEP, WPA) are blocked.	181. 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). 182. Significant events related to network components and network management tools are automatically reported to the responsible IT staff as soon as they occur. 183. Configurations of network management tools and network components are backed up and are part of the organization's recovery plan. 184. Wireless LAN access is only allowed through a firewall.

				179. All network management components and their associated network components have time synchronization and use the same time zone. 180. The default passwords have been replaced with strong enough passwords before using the telephone switching office.	185. Firewalls are monitored, logs are maintained, and defined events are automatically reported.
INF	*Infrastructure* *If external services are used for operational work, the corresponding requirements should be traceable in the form of an SLA.* *Buildings, premises, cabling*	186. The buildings comply with fire safety requirements and anti-burglary measures have been implemented.	187. 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 (lack of piping, gas extinguishing, etc. in the server rooms). 188. Guest supervision is in place. 189. A proper server room has been set up, with access restricted to the appropriate roles.	190. Access and key management are in place; rules are documented and recognized. 191. Unused cables are discarded. 192. Workplace documents are stored according to agreed rules. 193. Cabling and piping plans are in place. 194. Cabling is clearly marked and documented.	195. Regular and practical fire safety drills have been conducted. 196. Server room sensors and equipment are monitored and tested regularly, results are documented, and equipment is upgraded if necessary. 197. The network documentation is updated based on changes and reviewed regularly.