Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

Lucrarea de laborator nr. 4

# La disciplina „Managementul și Auditul Securitații Informaționale”

Tema: “Evaluarea conformitații sistemului de SI cu recomandările ISO 27001 și GDPR. Domeniile ISO 27002”

A efectuat: st. gr. SI-211 A. Chihai

A verificat: E. Nemerenco

**Chișinău – 2024**

**ISO 27001:2022**

**Ce este ISO 27001?**

ISO 27001 este o standard internațională recunoscută pentru managementul securității informațiilor, concepută pentru a ajuta organizațiile să protejeze informațiile sensibile pe care le dețin împotriva amenințărilor de securitate cibernetică. Standardul stabilește cerințe pentru implementarea și menținerea unui sistem de management al securității informațiilor (ISMS), care să asigure identificarea, evaluarea și gestionarea riscurilor de securitate cibernetică.

4.0 CONTEXT OF THE ORGANIZATION  
  
4.1 UNDERSTANDING THE ORGANIZATION AND ITS CONTEXT  
Q. 1. Did the organization determine the purpose(s) of the ISMS?  
R. No  
  
R.   
  
Q. 2. Did the organization determine the internal and external issues that are relevant to the ISMS purpose?  
R. No  
  
R.   
  
Q. 3. Did the organization determine how internal and external issues could influence the ISMS ability to achieve its intended outcomes?  
R. No  
  
R.   
  
  
4.2 UNDERSTANDING THE NEEDS AND EXPECTATIONS OF INTERESTED PARTIES  
Q. 4. Did the organization determine interested parties?  
R. Yes  
  
Q. 5. Does the list of all of interested parties’ requirements exist?  
R. Yes  
  
  
4.3 DETERMINING THE SCOPE OF THE INFORMATION SECURITY MANAGEMENT SYSTEM  
Q. 6. Is the scope documented with clearly defined boundaries and applicability?  
R. Yes  
  
  
4.4 INFORMATION SECURITY MANAGEMENT SYSTEM  
Q. 7. Have you established, documented, implemented, maintained, and continually improved an information security management system, including needed processes and interactions, per ISO 27001 requirements?  
R. No  
  
R.   
  
R. - 5.0 LEADERSHIP  
  
  
5.0 LEADERSHIP  
  
5.1 LEADERSHIP AND COMMITMENT  
Q. 8. Are the general ISMS objectives compatible with the strategic direction?  
R. Yes  
  
Q. 9. Does management ensure the necessary ISMS resources are available as needed?  
R. No  
  
R.   
  
Q. 10. Does management ensure that ISMS achieves its intended outcomes?  
R. Yes  
  
  
5.2 POLICY  
Q. 11. Does an Information Security Policy exist with included objectives or a framework for setting objectives?  
R. Yes  
  
Q. 12. Is the Information Security Policy documented and communicated within the company and to other interested parties?  
R. Yes  
  
  
5.3 ORGANIZATIONAL ROLES, RESPONSIBILITIES AND AUTHORITIES  
Q. 13. Are roles, responsibilities, and authorities for information security assigned and communicated?  
R. Yes  
  
R. - 6.0 PLANNING  
  
  
6.0 PLANNING  
  
6.1 ACTIONS TO ADDRESS RISKS AND OPPORTUNITIES  
  
6.1.1 GENERAL  
Q. 14. Are internal and external issues, as well as interested parties' requirements, considered while addressing risks and opportunities?  
R. Yes  
  
  
6.1.2 INFORMATION SECURITY RISK ASSESSMENT  
Q. 15. Is there a documented process to identify information security risks, including the risk acceptance criteria and criteria for risk assessment?  
R. Yes  
  
  
6.1.3 INFORMATION SECURITY RISK TREATMENT  
Q. 16. Is the risk treatment process documented, including the risk treatment options and how to create a Statement of Applicability?  
R. Yes  
  
  
6.2 INFORMATION SECURITY OBJECTIVES AND PLANNING TO ACHIEVE THEM  
Q. 17. Are information security objectives and targets established at relevant functions of the organization, measured and monitored where practical, and consistent with the information security policy?  
R. Yes  
  
Q. 18. Is there a plan, or group of plans, in place to achieve the information security objectives and targets including designated responsibility, evaluation method, and the means & timeframe for the plan(s)?  
R. Yes  
  
  
6.3 PLANNING OF CHANGES  
Q. 19. Are changes in the ISMS done in a planned manner?  
R. No  
  
R.   
  
R. - 7.0 SUPPORT  
  
  
7.0 SUPPORT  
  
7.1 RESOURCES  
Q. 20. Are adequate resources provided for all the elements of the ISMS?  
R. No  
  
R.   
  
  
7.2 COMPETENCE  
Q. 21. Is appropriate competence assessed, and training provided where needed, for personnel doing tasks that can affect the information security? Are records of competences maintained?  
R. Yes  
  
  
7.3 AWARENESS  
Q. 22. Is the personnel aware of the Information Security Policy, of their role, and consequences of not complying with the rules?  
R. Yes  
  
  
7.4 COMMUNICATION  
Q. 23. Are there identified needs for communication related to information security, including the responsibilities and what to communicate, to whom and when?   
R. Yes  
  
  
7.5 DOCUMENTED INFORMATION (7.5.1 GENERAL; 7.5.2 CREATING AND UPDATING; 7.5.3 CONTROL OF DOCUMENTED INFORMATION)  
Q. 24. Does the documentation of the ISMS include the Information Security Policy, objectives & targets, the scope of the ISMS, the main elements and their interaction, documents and records of ISO 27001 and those identified by the company?  
R. Yes  
  
Q. 25. Is it ensured that managing of documents and records exists, including who reviews and approves documents, and where and how they are published, stored, and protected?  
R. Yes  
  
Q. 26. Is documented information of external origin controlled?  
R. No  
  
R.   
  
R. - 8.0 OPERATION  
  
  
8.0 OPERATION  
  
8.1 OPERATIONAL PLANNING AND CONTROL  
Q. 27. Does the organization have established criteria for processes, and has it implemented controls over them according to these criteria?  
R. Yes  
  
Q. 28. Does the organization have the necessary documented information to be confident that its processes are being carried out as planned?  
R. Yes  
  
Q. 29. Are planned changes controlled? Are consequences of unplanned changes reviewed to identify mitigation actions if necessary?  
R. No  
  
R.   
  
Q. 30. Are outsourced processes identified and controlled?  
R. No  
  
R.   
  
  
8.2 INFORMATION SECURITY RISK ASSESSMENT  
Q. 31. Are the risks, their owners, likelihood, consequences, and the level of risk identified? Are these results documented?  
R. Yes  
  
  
8.3 INFORMATION RISK TREATMENT  
Q. 32. Does a risk treatment plan exist, approved by risk owners?  
R. Yes  
  
Q. 33. Is there a documented list with all controls deemed as necessary, with proper justification and implementation status?  
R. Yes  
  
R.   
  
  
9.0 PERFORMANCE EVALUATION  
  
9.1 MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION  
Q. 34. Is it defined what needs to be measured, by which method, who is responsible, who will analyze and evaluate the results?  
R. Yes  
  
Q. 35. Are the results of measurement documented, analyzed, and evaluated by responsible persons?  
R.   
  
  
9.2 INTERNAL AUDIT  
Q. 36. Does an audit program exist that defines the timing, responsibilities, reporting, audit criteria, and scope?  
R. No  
  
R.   
  
Q. 37. Are internal audits performed according to an audit program, results reported through an internal audit report, and relevant corrective actions raised?  
R. Yes  
  
  
9.3 MANAGEMENT REVIEW  
Q. 38. Is management review regularly performed, and are the results documented in minutes of the meeting?  
R. Yes  
  
Q. 39. Did management decide on all the crucial issues important for the success of the ISMS?  
R. Yes  
  
R.   
  
  
10.0 IMPROVEMENT  
  
10.1 CONTINUAL IMPROVEMENT  
Q. 40. Is the ISMS continuously adjusted to maintain its suitability, adequacy, and effectiveness?  
R. Yes  
  
  
10.2 NONCONFORMITY AND CORRECTIVE ACTION  
Q. 41. Does the organization react to every nonconformity?  
R. Yes  
  
Q. 42. Does the organization consider eliminating the cause of the nonconformity and, where appropriate, take corrective action?  
R. Yes  
  
Q. 43. Are all nonconformities recorded, together with corrective actions?  
R. Yes  
  
R. Requirements Readiness (in %):  
  
R. 71.21  
  
R. - ANNEX A. (Note: only the controls marked as applicable in the Statement of Applicability must be implemented.)  
  
R. - A.5 ORGANIZATIONAL CONTROLS  
  
  
A.5 ORGANIZATIONAL CONTROLS  
Q. 44. Are there published policies, approved by management, reviewed, and updated to support information security?  
R. Yes  
  
Q. 45. Are all information security responsibilities defined?  
R. Yes  
  
Q. 46. Are duties and responsibilities properly segregated considering situations of conflict of interest?  
R. Yes  
  
Q. 47. Is management actively requiring all employees and contractors to comply with information security rules?  
R. Yes  
  
Q. 48. Are contacts with relevant authorities defined?  
R. Yes  
  
Q. 49. Are contacts with special interest groups or professional associations defined?  
R. Yes  
  
Q. 50. Is information related to information security threats collected and analyzed to produce threat intelligence?  
R. Yes  
  
Q. 51. Do projects consider information security aspects?  
R. Yes  
  
Q. 52. Does an Inventory of Assets exist, and does every asset in the inventory have a designated owner?  
R. No  
  
R.   
  
Q. 53. Are rules and procedures for handling of information and other associated assets defined?  
R. No  
  
R.   
  
Q. 54. Are company assets returned by employees and contractors when their employment is terminated?  
R. Yes  
  
Q. 55. Are criteria to classify information defined?  
R. No  
  
R.   
  
Q. 56. Are there procedures which define how to label and handle classified information?  
R. Yes  
  
Q. 57. Is the information transfer properly protected?  
R. Yes  
  
Q. 58. Is there an Access Control Policy, and do users have access only to the resources they are allowed to use?  
R. Yes  
  
Q. 59. Are access rights provided via a formal registration process?  
R. Yes  
  
Q. 60. Are there rules for passwords and other secret authentication information to be provided in a secure way, as well as for password management systems, and users, on how to manage and protect them?  
R. Yes  
  
Q. 61. Is there a formal access management process to handle, review, and update access to information systems and users' access rights?   
R. Yes  
  
Q. 62. Is there a policy on how to treat the risks related to suppliers and partners?  
R. No  
  
R.   
  
Q. 63. Are relevant security requirements included in the agreements with the suppliers and partners?  
R. No  
  
R.   
  
Q. 64. Do the agreements with providers and suppliers include security requirements?  
R. No  
  
R.   
  
Q. 65. Are suppliers regularly monitored, and are changes involving arrangements and contracts with suppliers and partners taking into account risks and existing processes?  
R. Yes  
  
Q. 66. Are cloud services acquired, used, managed, and canceled according to information security requirements?  
R. Yes  
  
Q. 67. Are incidents managed properly?  
R. Yes  
  
Q. 68. Are security events assessed and classified properly?  
R. Yes  
  
Q. 69. Are procedures on how to respond to incidents documented?  
R. Yes  
  
Q. 70. Are security incidents analyzed properly?  
R. Yes  
  
Q. 71. Do procedures exist which define how to collect evidence?  
R. No  
  
R.   
  
Q. 72. Are requirements for continuity of information security defined, implemented, exercised, and tested?  
R. Yes  
  
Q. 73. Is ICT readiness managed according to business continuity objectives and ICT requirements?  
R. Yes  
  
Q. 74. Are legislative, regulatory, contractual, and other security requirements listed?  
R. No  
  
R.   
  
Q. 75. Do procedures exist to protect intellectual property rights?  
R. Yes  
  
Q. 76. Are records protected properly?  
R. No  
  
R.   
  
Q. 77. Is personally identifiable information protected properly?  
R. Yes  
  
Q. 78. Is information security regularly reviewed by an independent auditor?  
R. No  
  
R.   
  
Q. 79. Do the managers regularly review if the security policies and procedures are performed properly in their areas of responsibility, and that information systems are in compliance with the information security policies and standards?  
R. Yes  
  
Q. 80. Are operating procedures for IT processes documented?  
R. Yes  
  
R. - A.6 PEOPLES CONTROLS  
  
  
A.6 PEOPLES CONTROLS  
Q. 81. Does the organization perform background checks on candidates for employment or for contractors?  
R. Yes  
  
Q. 82. Are there agreements with employees and contractors that specify information security responsibilities?  
R. Yes  
  
Q. 83. Do employees and contractors attend trainings to better perform their security duties, and do the awareness programs exist?  
R. Yes  
  
Q. 84. Does the organization have a formal disciplinary process?  
R. No  
  
R.   
  
Q. 85. Are there agreements covering information security responsibilities that remain valid after the termination of employment?  
R. Yes  
  
Q. 86. Does the organization list all the confidentiality clauses that need to be included in agreements with third parties?  
R. Yes  
  
Q. 87. Are there rules defining how the organization's information is protected considering teleworking sites?  
R. No  
  
R.   
  
Q. 88. Are information security events and weaknesses reported in properly by employees and contractors?  
R. No  
  
R.   
  
R. - A.7 PHYSICAL CONTROLS  
  
  
A.7 PHYSICAL CONTROLS  
Q. 89. Do secure areas that protect sensitive information exist?  
R. Yes  
  
Q. 90. Are the entrances to secure areas protected?  
R. No  
  
R.   
  
Q. 91. Are secure areas located in a protected way?  
R.   
  
Q. 92. Are premises monitored for unauthorized access?  
R. Yes  
  
Q. 93. Are the alarms, fire protection, and other systems installed?  
R. Yes  
  
Q. 94. Are working procedures for secure areas defined?  
R. Yes  
  
Q. 95. Is there orientation for users about what to do when they are not present at their workstations?  
R. No  
  
R.   
  
Q. 96. Is the equipment properly protected?  
R. Yes  
  
Q. 97. Are the organization assets properly protected when they are not at the organization premises?  
R.   
  
Q. 98. Are there procedures that define how to handle, protect, transport, and dispose of storage media, inside and outside the organization premises, in line with the classification rules and information sensitivity?  
R. Yes  
  
Q. 99. Does the equipment have protection against energy variations?  
R. Yes  
  
Q. 100. Are the power and telecommunication cables adequately protected?  
R. Yes  
  
Q. 101. Is the equipment maintained regularly?  
R. Yes  
  
Q. 102. Is information properly removed from media or equipment that will be disposed of?  
R. Yes  
  
R.   
  
  
A.8 TECHNOLOGICAL CONTROLS  
Q. 103. Are rules for the secure handling of mobile devices, and for protecting equipment when not in the physical possession of its users, defined?  
R. No  
  
R.   
  
Q. 104. Are privileged access rights managed with special care?  
R. Yes  
  
Q. 105. Is the access to information in systems restricted according to the access control policy?  
R. Yes  
  
Q. 106. Is the access to source code restricted to authorized persons?  
R. Yes  
  
Q. 107. Is secure log-on required on systems according to the Access Control Policy?  
R. No  
  
R.   
  
Q. 108. Are resources monitored and plans made to ensure their capacity to fulfill users' demands?  
R. No  
  
R.   
  
Q. 109. Are anti-virus software, and other software for malware protection installed and properly used?  
R. No  
  
R.   
  
Q. 110. Is information about vulnerabilities properly managed, and are information systems regularly reviewed to check their compliance with the information security policies and standards?  
R. Yes  
  
Q. 111. Are configurations of relevant IT assets properly handled?  
R. Yes  
  
Q. 112. Is data that is no longer required properly disposed of?  
R. Yes  
  
Q. 113. Is data masking applied according to applicable requirements?  
R. Yes  
  
Q. 114. Do systems, networks, and devices include data leakage prevention measures?  
R. Yes  
  
Q. 115. Is a backup policy defined and performed properly?  
R. Yes  
  
Q. 116. Does IT infrastructure have redundancy (e.g.: secondary location) included in its planning and operation?  
R. Yes  
  
Q. 117. Are relevant events from IT systems logged periodically, and are logs protected properly?  
R. Yes  
  
Q. 118. Are systems, networks, and applications monitored, and proper actions  taken when anomalous behaviors are found?  
R. Yes  
  
Q. 119. Are clocks on all IT systems synchronized?  
R. No  
  
R.   
  
Q. 120. Is the use of utility tools controlled and limited to specific employees?  
R. No  
  
R.   
  
Q. 121. Is installation of software strictly controlled?  
R. Yes  
  
Q. 122. Are the networks controlled to protect information in systems and applications?  
R. Yes  
  
Q. 123. Are security requirements for network services defined, and included in agreements?  
R. Yes  
  
Q. 124. Are the networks segregated considering risks and assets classification?  
R. Yes  
  
Q. 125. Is access to external websites controlled?  
R. No  
  
R.   
  
Q. 126. Does a policy to regulate encryption and other cryptographic controls exist?  
R. No  
  
R.   
  
Q. 127. Are rules for the secure development of software and systems defined?  
R. No  
  
R.   
  
Q. 128. Is application information, including transaction information, transferred through public networks appropriately protected?  
R. Yes  
  
Q. 129. Are principles for engineering secure systems applied to the organization system's development process?  
R. Yes  
  
Q. 130. Is software code developed according to defined principles?  
R. Yes  
  
Q. 131. Is the implementation of security requirements tested during system development, and are the criteria for accepting the systems defined?  
R. Yes  
  
Q. 132. Is the outsourced development of systems monitored?  
R. Yes  
  
Q. 133. Are development, testing, and production environments separated and properly secured?  
R. No  
  
R.   
  
Q. 134. Are changes that could affect the information security of new or existing systems properly controlled and tested?  
R. Yes  
  
Q. 135. Are test data carefully selected and protected?  
R. No  
  
R.   
  
Q. 136. Are audits of production systems planned and executed properly?  
R. No  
  
R.   
  
R. Number of controls complied with:  
  
Q. Number of controls complied with:  
R. 64  
  
Q. Enter your e-mail address  
R. [adrian.chihai@isa.utm.md](mailto:adrian.chihai@isa.utm.md)

**GDPR**

**Ce este GDPR?**

Regulamentul General privind Protecția Datelor (GDPR) este o legislație europeană care reglementează modul în care organizațiile colectează, utilizează și protejează datele personale ale cetățenilor din Uniunea Europeană (UE). Adoptat în 2016 și intrat în vigoare pe 25 mai 2018, GDPR urmărește să ofere cetățenilor controlul asupra informațiilor lor personale și să consolideze drepturile lor în ceea ce privește protecția datelor.  
  
PRINCIPLES RELATED TO PROCESSING OF PERSONAL DATA  
Q. 1. Is the legal basis for each processing activity documented? (“The organisation should maintain a log of each processing activity it engages in, as well as the corresponding legal basis. The processing activity has a valid legal basis only if one or more of the following apply: (a) the data subject provides valid consent; (b) processing is necessary for entering into or the performance of a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or other individual; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or third party, to the extent it does not infringe on the fundamental rights and freedoms of the data subject, particularly where the data subject is a child” - Article 6(1) EU GDPR.)  
R. Yes  
  
Q. 2. Is the purpose for each processing activity documented? (Every processing activity should be documented. "Processing" is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." - Article 4(2) EU GDPR.)  
R. Yes  
  
Q. 3. Will the personal data be processed for a purpose other than what was intended at the time of collection? (Departments within the organisation should consult the Data Protection Officer/Legal Counsel/other relevant personnel prior to processing personal data for a secondary purpose. "Personal Data" is defined as "any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" - Article 4(1) EU GDPR.)  
R. No  
  
R. Once you have defined a purpose for processing, make sure to stick to it and not change it without reassessing the legal basis. For example, if the processing activity you want to change is based on an existing consent, before changing the processing activity, you should obtain the consent again. Make sure that such processing is also lawful - the processing activity has a valid legal basis only if one or more of the following apply: "(a) the data subject provides valid consent; (b) processing is necessary for entering into or the performance of a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or other individual; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or third party, to the extent it does not infringe on the fundamental rights and freedoms of the data subject, particularly where the data subject is a child” - Article 6(1) EU GDPR <https://advisera.com/eugdpracademy/gdpr/lawfulness-of-processing/>  
  
Q. 4. Do consent-collecting mechanisms require some action (e.g., ticking a box) or affirmative statement by the data subject? (In order for the consent to be valid it should be freely given, specific, unambiguous, and should require some affirmative action from the data subject. Silence, pre-ticked boxes, opt-out or inactivity do not constitute a valid consent.)  
R. Yes  
  
Q. 5. Where processing involving special categories of data is based on consent, is explicit consent obtained (e.g., in writing or verbally) from the data subject? ("Special categories" of data are "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" - Article 9(1) EU GDPR.)  
R. Yes  
  
R. - RIGHTS OF THE DATA SUBJECTS WHILE PROCESSING AND ACCESSING THEIR INFORMATION  
  
  
RIGHTS OF THE DATA SUBJECTS WHILE PROCESSING AND ACCESSING THEIR INFORMATION  
Q. 6. Is a process in place to respond to requests for access to information held about a data subject?  
R. Not applicable  
  
Q. 7. Is a process in place to rectify/delete information about a data subject pursuant to a request?  
R. Yes  
  
Q. 8. Is a process in place to communicate updates of personal data to third parties who have received the data?  
R. Yes  
  
Q. 9. Is there a process in place to allow a data subject to revoke consent for a particular processing activity at any time? (According to Article 7(3) of the EU GDPR, revoking consent should be as easy for the data subject as giving consent.)  
R. Not applicable  
  
Q. 10. When consent for a particular processing activity is revoked, are there processes in place to ensure processing is stopped, including any processing by third parties?  
R. Yes  
  
Q. 11. Is there a process in place to comply with requests to restrict the processing of data if requested by a data subject, including any processing by third parties?  
R. Yes  
  
Q. 12. Is a process in place to comply with requests from a data subject to have their personal data transferred directly to another controller, if technically possible? (The process should be documented.)  
R. Yes  
  
Q. 13. Is a process in place to stop processing for direct marketing purposes when an objection is received?  
R. Yes  
  
Q. 14. If engaged in automated decision making, including profiling, is there a process by which a data subject may request a manual review of the decision or profiling activity? ("Profiling" is defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements" - Article 4(4) EU GDPR.)  
R. Not applicable  
  
Q. 15. Has a representative within the European Union been designated? (A European Union representative should be designated where the organisation offers goods or services to, or monitors the behaviour of, data subjects who are within the European Union. A "representative" is defined as "a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation" - Article 4(17) EU GDPR.)  
R. Not applicable  
  
R. - TRANSFERS OF DATA TO THIRD PARTIES  
  
  
TRANSFERS OF DATA TO THIRD PARTIES  
Q. 16. Do contracts with third parties specify that the third party, and any subcontractor that may be utilised, must have data protection and security protection clauses/annexes in place?  
R. Yes  
  
Q. 17. Are records kept of all processing activities your company engages in? (This requirement does not apply if your company employs fewer than 250 individuals, unless your processing activities could result in a high risk to the rights of the data subject or involve special/sensitive categories of information.)  
R. Yes  
  
Q. 18. Are all data transfers documented, including cross-border transfers?  
R. Yes  
  
Q. 19. Is a data transfer mechanism in place in the event that personal data is to be transferred to a third country or international organisation?  
R. Yes  
  
R. - PRIVACY NOTICES  
  
  
PRIVACY NOTICES  
Q. 20. Is a Privacy Notice provided to data subjects no later than at the time information is collected from those data subjects?  
R. Yes  
  
Q. 21. Is a Privacy Notice provided to data subjects at every point of collection?  
R. No  
  
R. A Privacy Notice should be provided to data subjects at every point of collection. See here an example of a Privacy Notice <https://advisera.com/eugdpracademy/documentation/privacy-notice/>  
  
Q. 22. If data is to be processed for a secondary purpose, are data subjects notified of the new purpose prior to processing?  
R. No  
  
R. If data is going to be processed for a secondary purpose, you should notify the data subjects of the new purpose prior to processing; or, if the processing is based on consent, obtain the consent again for the secondary purpose as well. See here an example of a Data Subject Consent Form <https://advisera.com/eugdpracademy/documentation/data-subject-consent-form/>  
  
Q. 23. Does the Privacy Notice clearly specify how data subjects can exercise their rights under the GDPR?  
R. No  
  
R. A Privacy Notice must clearly specify how data subjects can exercise their rights under the GDPR. See here an example of a Privacy Notice <https://advisera.com/eugdpracademy/documentation/privacy-notice/>  
  
R. - DATA BREACHES  
  
  
DATA BREACHES  
Q. 24. Is a process in place to ensure the appropriate Supervisory Authority is notified within 72 hours of a confirmed data breach?  
R. Yes  
  
Q. 25. Do agreements/contracts with third parties specify that the third party has to notify you (the controller) without undue delay after becoming aware of a data breach or potential data breach involving personal data? (All contracts with third parties involving the handling of personal data should include provisions to notify you (the controller) in the case of a data breach.)  
R. Yes  
  
Q. 26. Are internal policies in place defining what is considered to be a data breach and when and if notification to data subjects or Supervisory Authorities is required? (Internal policies should specify what constitutes a data breach under the GDPR, and what kinds of scenarios could result in a "risk to the rights and freedoms" of an individual, thus requiring notification to the relevant authorities or data subjects.)  
R. Yes  
  
Q. 27. Is a log kept of all data breaches that occur, along with the effects and remedial actions taken? (The GDPR requires the controller to document all data breaches that occur in order to demonstrate compliance with Article 33, paragraph 5: “The controller shall document any personal data breaches, comprising of the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.”)  
R. Yes  
  
Q. 28. Are assessments of processing activities conducted by the relevant personnel to determine the data protection measures that should be in place, proportionate to the risks involved with the processing activity? ("Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary." - Article 24(1) EU GDPR.)  
R. No  
  
R. You should conduct assessments of processing activities to determine that the data protection measures that should be in place are proportional to the risks involved with the processing activity. These assessments should be conducted by the relevant personnel. You should review and update the protection measures where necessary. See here an example of Guidelines for Data Inventory and Processing Activities Mapping <https://advisera.com/eugdpracademy/documentation/guidelines-for-data-inventory-and-processing-activities-mapping/> and the Inventory of Processing Activities <https://advisera.com/eugdpracademy/documentation/inventory-of-processing-activities/>  
  
Q. 29. Is privacy assessed at the beginning stages of development of any processing activity?  
R. No  
  
R. You should assess the privacy at the beginning stages of development of any processing activity. See here an example of the Information Classification Policy <https://advisera.com/eugdpracademy/documentation/information-classification-policy/>  
  
Q. 30. Are measures such as data minimisation and pseudonymisation implemented across all applicable organisational units? ("Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects." -  Article 25(1) EU GDPR.)  
R. No  
  
R. You should implement measures such as data minimisation and pseudonymisation across all applicable organisational units both at the time of the determination of the means for processing and at the time of the processing itself. The measures should be implemented in an effective manner and should integrate the necessary safeguards into the processing in order to meet the requirements of the EU GDPR and protect the rights of data subjects. See here an example of Anonymisation and Pseudonymisation Policy <https://advisera.com/eugdpracademy/documentation/anonymization-and-pseudonymization-policy/>  
  
R. - DATA PROTECTION IMPACT ASSESSMENT (DPIA)  
  
  
DATA PROTECTION IMPACT ASSESSMENT (DPIA)  
Q. 31. Are Data Protection Impact Assessments (DPIAs) completed for processing activities involving special categories of information, automated decision making, or profiling?  
R. Yes  
  
Q. 32. Are DPIAs completed prior to implementing new technologies, processes, or projects?  
R. Yes  
  
R. According to our readiness assessment tool, the processes of your organisation are compliant with the requirements of EU GDPR (in %):  
  
R. 67  
  
Q. Enter your e-mail address  
R. [adrian.chihai@isa.utm.md](mailto:adrian.chihai@isa.utm.md)

**Concluzie**

În concluzie, evaluarea conformității sistemului de securitate a informațiilor (SI) cu recomandările ISO 27001 și GDPR, în special în domeniile ISO 27002, este un proces esențial pentru organizații în vederea asigurării securității și protecției datelor. Implementarea și respectarea acestor standarde și reglementări sunt cruciale pentru gestionarea riscurilor de securitate a informațiilor și pentru protejarea confidențialității, integrității și disponibilității datelor.

Prin evaluarea conformității, organizațiile pot identifica lacunele și deficiențele în sistemul lor de securitate a informațiilor și pot lua măsuri corective pentru a le remedia. Astfel, se poate îmbunătăți nivelul de securitate al sistemului și se pot minimiza riscurile de securitate cibernetică și de nerespectare a regulamentelor privind protecția datelor.