Managing enterprise IT infrastructure and security - lab 3 report

Anna Marut, Bartosz Adamiec, Zuzanna Potrzebska, Adam Kasperski

Explaining the systematic approach to securing an enterprise IT infrastructure (a summary of the know-how obtained hitherto)

1. **Characterizing the company and its structure, eliciting the requirements.** Exemplary characteristics for analysis (that can be extended) - the mission, business objectives, and activity, the enterprise/organizational structure, drawing an organizational diagram as well as an IT infrastructure diagram - this basic information will be crucial in the project we are conducting because it helps to understand the business as a whole, understand the business needs, and how the business is constructed. This analysis may show us points of the business that the analyst needs to focus on in further steps. It will also be a base of information about the company that the analyst may come back to for the other steps of analysis.
2. **Defining the infrastructure and information assets.** The definition of infrastructure and information assets. Assigning transparent criteria to the information assets that the asset should meet (based on the analyst's expertise). Examples of such criteria may be e.g. resistance to bots or constant availability for the users. The infrastructure and information assets are showing us the companies most important aspects that the analyst needs to secure in their evaluation. Without knowing the assets to protect - the analyst won't be able to provide a sufficient and comprehensive examination of the company's security. The assets will be used in the further steps of the method (e.g. identifying the OSTs for the business).
3. **Identification and evaluation of information assets.** It is based on FIPS 199, Standards for Security Categorization of Federal Information and Information Systems. The impact of loss has three levels (low, moderate, and high) and in three categories (confidentiality, integrity, and availability). Low – if the loss of these three factors could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Moderate – if the loss of factors could be expected to have a serious adverse effect on organizational operations/assets, or individuals and high – if the loss of factors could be expected to have a severe or catastrophic adverse effect on organizational operations/assets or individuals. Each information asset should have a description and assigned the impact of the loss of confidentiality, integrity, and availability and the justification why a particular level was chosen. Confidentiality of information is its property of being available only to authorized entities. [ISO/IEC 17799:2000], Availability – assurance that cyber assets can be accessed and used by an authorized entity on any demand [ISO/IEC 17799:2000] Integrity of cyber assets – accuracy and completeness of the cyber assets [ISO 27000:2016]. The CIA Triad is considered the core underpinning of information security. As a result of this, a company can examine the potential loss of these factors in relation to the information assets of the particular company.
4. **Identification of general threats (GT).** Preparing a source list of general lists of IT threats to familiarize with e.g. ISO standards. Using this precious knowledge, the company can create its own list of general threats with descriptions explaining each

threat to be sure that everyone in the organization understands it in the same way. that are more relevant to the particular business. This phase is the development of a threat repository. If the company has already chosen one standard e.g. ISO 27001:2018 this step would be a little bit modified - no need to choose threats from many sources.

5. **Identification and analysis of company-specific threats.** It requires the preparation of threat transmission assets, information assets, and general threats that were collected at earlier steps. It is useful to name and describe the resulting specific, dedicated threats - organization-specific threats that were suited to the company. By doing so, it is analyzed what type of incidents can occur in the given context. This includes the identification and description of the relevant treats. Independent analysis of the likelihood of the loss of confidentiality, integrity, or availability of an asset IA when OST occurs and also the likelihood of the OST occurrence gives the information on what is probable or risky for the enterprise and what accidents are negligible. Also, the calculation of conditional likelihood should be done. Thanks to this analysis a company has an opportunity to plan the appropriate security strategy and better understand the potential IT risks in their organization.
6. **Risk evaluation.** Taking into account the Information asset, Organization-specific threat (OST), Impact (I), Conditional likelihood (CL) the calculation of the risk level can be done. Thanks to this evaluation, a company could look at IT threats broadly and take many factors into consideration.
7. **The list of risks sorted according to their level.** Finally, based on the calculated risk level for each threat and possible loss of confidentiality, integrity, and availability, the report of the result of the risk assessment can be prepared. The phase of Risk assessment that comprises risk identification, risk analysis, and risk evaluation that is an important point in ISO/IEC 27005:2011 is completed. It is worth remembering that risk assessment is often conducted with many iterations and the higher-level assessment to identify potentially high (critical) risks and tailor them to the needs of an enterprise.

Choosing a security standard between ISO 27001:2018 and NIST SP 800-53 Revision 5, justifying the choice (comparison of strengths and weaknesses)

Comparison of Strengths and Weaknesses of both standards

	ISO 27001:2018	NIST SP 800-53 Revision 5
strengths	- Less technical and more risk-focused for organizations of all shapes and sizes - Provides certification, internationally recognized - Clear about its requirements and the documentation that the company is mandated to provide so it works well for companies wishing to design a long-running, comprehensive security platform to guard their assets.	- Good starting point - a good start before the certification - Flexible and voluntary - good for our small company - Easier to implement - needed when we are short on time - Well-defined organization and structure - there are three key components: the core, implementation tiers, and profiles with each function having categories, which are the

		activities necessary to fulfill each function
weaknesses	- Need to buy the standard - It is generally more pricey to implement for our small company	- NIST does not provide a certification process thus it could be difficult to prove compliance - Designed for the US Federal Agencies

Our choice with justification

For our case, it is more justified to choose the NIST SP 800-53 Revision 5 standard for the current moment. Why? Because there is no need for us to get certified against ISO at this point in the company's growth. We think that the NIST SP 800-53 Revision 5 standard will be a good base point to start the cybersecurity journey - in the future, there is a high chance to implement the ISO 27001:2018 standard because both of them are very beneficial for the company. But in the present state of the company (a small startup that is just starting its cybersecurity journey), we think that NIST SP 800-53 Revision 5 is just enough.

Selecting and describing security controls for 8 threats with the highest risk levels. Referring the controls to the threats. Indicating (potential) control areas that have not been addressed and explaining them.

Threat-specific controls

	Threat	Risk level	Security controls	Description
1	Clients data is unavailable due to DOS attack on CRM server	0,45	**SI-23** SYSTEM AND INFORMATION INTEGRITY - INFORMATION FRAGMENTATION **AU-2** AUDIT AND ACCOUNTABILITY - EVENT LOGGING **IA-4** IDENTIFICATION AND AUTHENTICATION - IDENTIFIER MANAGEMENT	● Fragment the client's data information distributes the fragmented information across a few system components. The fragmentation of information impacts the organization's ability to access the information in a timely manner. The extent of the fragmentation is dictated by the impact or classification level (and value) of the information, threat intelligence information received, and whether data tainting is used (i.e., data taintingderived information about the exfiltration of some information could result in the fragmentation of the remaining information). ● Identify the types of events that the system is capable of logging in support of the audit function. Coordinate the event logging function with other organizational entities requiring audit related information to guide and inform the selection criteria for events to be logged. Specify the event types for logging within the system along with the frequency of each identified event type. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents. Review and update the event types selected for logging every one year ● Prohibit the use of system account identifiers that are the same as public identifiers for individual accounts to

				manage the access to clients data that is extremely confidential data. Limiting the access reduces the probability of attacking and blocking the availability to the clients data. A good solution could be generating pairwise pseudonymous identifiers.
2	Accounting data is changed or removed due to SQL injection on CRM server	0,30	**SC-2** SYSTEM AND COMMUNICATIONS PROTECTION - SEPARATION OF SYSTEM AND USER FUNCTIONALITY **SI-16** SYSTEM AND INFORMATION INTEGRITY - MEMORY PROTECTION **SI-20** SYSTEM AND INFORMATION INTEGRITY - TAINTING	● Separate accountant functionality, including accounting interface services, from system management functionality. Prevent the presentation of system management functionality at interfaces to non privileged users. Store state information from applications and software separately. ● Implement controls to protect the system memory from unauthorized code execution ● Embed data or capabilities in the systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization
3	Clients data is leaked or changed due to third-party action based on opening infected email attachments that infected the CRM server	0,30	**SI-21** SYSTEM AND INFORMATION INTEGRITY - INFORMATION REFRESH **SI-22** SYSTEM AND INFORMATION INTEGRITY - INFORMATION DIVERSITY	● Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle every one year. Correct or delete inaccurate or outdated personally identifiable information ● De-identify the dataset upon collection by not collecting personally identifiable information. Prohibit archiving of personally identifiable information elements if those elements in a dataset will not be needed after the dataset is archived. Remove personally identifiable information elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release. Remove, mask, encrypt, hash, or replace direct identifiers in a dataset. Manipulate numerical data, contingency tables, and statistical findings so that no individual or organization is identifiable in the results of the analysis. Prevent disclosure of personally identifiable information by adding non-deterministic noise to the results of mathematical operations before the results are reported. Perform de-identification using validated algorithms and software that is validated to implement the algorithms. Perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified. ● The processing of personally identifiable information is an operation or set of operations that the information system

				or organization performs with respect to personally identifiable information across the information life cycle. Processing includes but is not limited to creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal. Processing operations also include logging, generation, and transformation, as well as analysis techniques, such as data mining. Organizations may be subject to laws, executive orders, directives, regulations, or policies that establish the organization’s authority and thereby limit certain types of processing of personally identifiable information or establish other requirements related to the processing. Organizations take steps to ensure that personally identifiable information is only processed for authorized purposes.
4	Clients data is changed or removed due to SQL injection on CRM server	0,30	**SI-18** SYSTEM AND INFORMATION INTEGRITY - PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS **SI-19** SYSTEM AND INFORMATION INTEGRITY - DE-IDENTIFICATION **PT-2** AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION	● Separate user functionality, including user interface services, from system management functionality. Prevent the presentation of system management functionality at interfaces to non privileged users. Store state information from applications and software separately. ● Implement controls to protect the system memory from unauthorized code execution ● Embed data or capabilities in the systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization
5	Accounting data is leaked or changed due to third-party action based on opening infected email attachments that infected the CRM server	0,27	**SI-18** SYSTEM AND INFORMATION INTEGRITY - PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS **SI-19** SYSTEM AND INFORMATION	● Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle every one year. Correct or delete inaccurate or outdated personally identifiable information ● De-identify the dataset upon collection by not collecting personally identifiable information. Prohibit archiving of personally identifiable information elements if those elements in a dataset will not be needed after the dataset is archived. Remove personally identifiable information elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release. Remove, mask, encrypt, hash, or replace direct identifiers in a dataset. Manipulate numerical data,

			INTEGRITY - DE-IDENTIFICATION **PT-2** AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION	contingency tables, and statistical findings so that no individual or organization is identifiable in the results of the analysis. Prevent disclosure of personally identifiable information by adding non-deterministic noise to the results of mathematical operations before the results are reported. Perform de-identification using validated algorithms and software that is validated to implement the algorithms. Perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.
6	Clients data is leaked or changed due to third-party action based on opening infected email attachments that infected the CRM server	0,27	**SI-18** SYSTEM AND INFORMATION INTEGRITY - PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS **SI-19** SYSTEM AND INFORMATION INTEGRITY - DE-IDENTIFICATION **PT-2** AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION	● Separate user functionality, including user interface services, from system management functionality. Prevent the presentation of system management functionality at interfaces to non privileged users. Store state information from applications and software separately. ● Implement controls to protect the system memory from unauthorized code execution ● Embed data or capabilities in the systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization
7	Clients data is changed or removed due to SQL injection on CRM server	0,23	**CM-10** CONFIGURATION MANAGEMENT - SOFTWARE USAGE RESTRICTIONS **SI-7** SYSTEM AND INFORMATION INTEGRITY - SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY **SI-15** SYSTEM AND INFORMATION	● Separate user functionality, including user interface services, from system management functionality. Prevent the presentation of system management functionality at interfaces to non privileged users. Store state information from applications and software separately. ● Implement controls to protect the system memory from unauthorized code execution ● Embed data or capabilities in the systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization

			INTEGRITY - INFORMATION OUTPUT FILTERING	
8	Accounting data is leaked or changed due to third-party action based on opening infected email attachments that infected the CRM server	0,2	**SI-18** SYSTEM AND INFORMATION INTEGRITY - PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS **SI-19** SYSTEM AND INFORMATION INTEGRITY - DE-IDENTIFICATION **PT-2** AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION	● Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle every one year. Correct or delete inaccurate or outdated personally identifiable information ● De-identify the dataset upon collection by not collecting personally identifiable information. Prohibit archiving of personally identifiable information elements if those elements in a dataset will not be needed after the dataset is archived. Remove personally identifiable information elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release. Remove, mask, encrypt, hash, or replace direct identifiers in a dataset. Manipulate numerical data, contingency tables, and statistical findings so that no individual or organization is identifiable in the results of the analysis. Prevent disclosure of personally identifiable information by adding non-deterministic noise to the results of mathematical operations before the results are reported. Perform de-identification using validated algorithms and software that is validated to implement the algorithms. Perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified

Common controls

Control ID and name	Applies to threats	Short description
SI-4 SYSTEM AND INFORMATION INTEGRITY - SYSTEM MONITORING	1, 2, 4, 7	Monitor the system to detect: Attacks and indicators of potential attacks and Unauthorized local, network, and remote connections. Identify unauthorized use of the system. Invoke internal monitoring capabilities or deploy monitoring devices. Analyze detected events and anomalies. All those activities may concur to encroach the integrity of the database and loosing of the clients' data.
SI-3 SYSTEM AND INFORMATION INTEGRITY - MALICIOUS CODE PROTECTION	1, 2, 3, 4, 5, 6, 7, 8	Implement malicious code for mobile code protection mechanisms at system entry and exit points to detect and eradicate malicious code. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures. Configure malicious code protection mechanisms to perform periodic scans every week of the system and real-time scans of files from external sources at the endpoint, send alerts to the security specialist in response to malicious code detection. Update malicious code protection mechanisms only when directed by a permitted authorized individual. Test malicious code protection functions in the schedule by introducing known benign code into the system. Verify that the detection of the code and the associated incident reporting occurs. Incorporate the results from malicious code analysis into organizational incident response and take into consideration

		the results and changes needed to implement.
CM-11 CONFIGURATION MANAGEMENT - USER - INSTALLED SOFTWARE	1, 3, 5, 6	Policy in the company is establishing the installation of software by authorized users. Enforce software installation policies and monitor policy compliance every half a year. Allow user installation of software only with verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. Monitor compliance from users with software installation policies using the help desk or any other automatic mechanism. .
SC-3 SYSTEM AND COMMUNICATIONS PROTECTION - SECURITY FUNCTION ISOLATION	1, 2, 4, 7	Isolate security functions from nonsecurity functions. Implement hardware separation mechanisms to bring in security function isolation. Minimize the number of non security functions. Implement security functions as they secure the integrity of the database.
SC-7 SYSTEM AND COMMUNICATIONS PROTECTION - BOUNDARY PROTECTION	1, 2, 4, 7	Monitor and control communications at the external managed clients interfaces to the system and at key users managed interfaces inside the company's system. Implement networks for common uses with publicly accessible system components that are separated from internal organizational networks.
SC-8 SYSTEM AND COMMUNICATIONS PROTECTION - TRANSMISSION CONFIDENTIALITY AND INTEGRITY	1, 5	Implement cryptographic mechanisms to prevent unauthorized licks of information; detect changes of information during transmission. Work on: confidentiality and integrity of information during preparation for transmission
SC-34 SYSTEM AND COMMUNICATIONS PROTECTION - NON-MODIFIABLE EXECUTABLE PROGRAMS	1, 2, 4, 7	For software products, load and execute the operating environment executed by hardware. By using nonmodifiable storage, the integrity of software from the point of creation of the read-only image is ensured.
SI-12 SYSTEM AND INFORMATION INTEGRITY - INFORMATION MANAGEMENT AND RETENTION	2, 3, 4, 6, 7	Manage information in the system in accordance to the applicable laws, orders, directives, regulations, policies, standards and operational requirements. The number of information which needs to be confirmed by the users.
PS-6 PERSONNEL SECURITY - ACCESS AGREEMENTS	2, 3, 4, 6, 7	Document and change if needed accesses. Review and update the accesses every quarter. Prepare and sign needed documents for the access Verify that access to classified information requiring special protection is granted only to people who have an access that is demonstrated by assigned official government duties;

SC-5 SYSTEM AND COMMUNICATIONS PROTECTION - DENIAL-OF-SERVICE PROTECTION	2	Protection of the denial of service events like: attack on CRM server. Monitor indicators of denial-of-service attacks against, or launched from, the system. Monitor the system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks.
SC-23 SYSTEM AND COMMUNICATIONS PROTECTION - SESSION AUTHENTICITY	2	Protect the communications sessions. It is important to establish grounds for confidence at both ends of communications sessions in the ongoing identities of other parties and the validity of transmitted information. Authenticity protection includes protecting against “man-in-the-middle” attacks, session hijacking, and the insertion of false information into sessions. Invalidate session identifiers upon user logout or other session termination. Generate a unique session identifier for each session with randomness and recognize only session identifiers that are system generated. Only allow the use of certified authorities for verification of the establishment of protected sessions.
SA-9 SYSTEM AND SERVICES ACQUISITION - EXTERNAL SYSTEM SERVICES	2, 3, 4, 6, 7	Require that providers of external system services comply with organizational security and privacy requirements. Define and document organizational oversight and user roles and responsibilities with regard to external system services. Employ processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis. Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services. Verify that the acquisition or outsourcing of dedicated information security services is approved by the Security Specialist. Establish, document, and maintain trust relationships with external service providers. Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system. Provide the capability to check the integrity of information while it resides in the external system.
SC-35 SYSTEM AND COMMUNICATIONS PROTECTION - EXTERNAL MALICIOUS CODE IDENTIFICATION	2, 3, 4, 5, 6, 7	Include system components that proactively seek to identify network-based malicious code or malicious websites. Like decoys, the use of external malicious code identification techniques requires some supporting isolation measures to ensure that any malicious code discovered during the search and subsequently executed does not infect organizational systems. Virtualization is a common technique for achieving such isolation.
SI-8 SYSTEM AND INFORMATION INTEGRITY - SPAM PROTECTION	3, 5, 6	Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.
AT-2 AWARENESS AND TRAINING - LITERACY TRAINING AND AWARENESS	1, 2, 3, 4, 5, 6, 7, 8	Provide security and privacy literacy training to system users (including managers, senior executives, and contractors) as a part of initial training for new users and a year thereafter; and when required by system changes. Update literacy training and awareness content. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.
AC-1 ACCESS CONTROL	1, 2, 3, 4, 5, 6, 7, 8	Develop, document, and disseminate to the CEO: access control policy that: Addresses purpose, scope, roles, responsibilities, management commitment,

- POLICY AND PROCEDURES		coordination among organizational entities, and compliance and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; Procedures to facilitate the implementation of the access control policy and the associated access controls. Designate the security specialist to manage the development, documentation, and dissemination of the access control policy and procedures. Review and update the current access control for policies and procedures every 3 months.
CP-3 CONTINGENCY PLANNING - CONTINGENCY TRAINING	1, 2, 3, 4, 5, 6, 7, 8	Provide contingency training to system users consistent with assigned roles and responsibilities within one year of assuming a contingency role or responsibility, when required by system changes, and one month thereafter. Review and update contingency training content and following organization-defined events. Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations. Employ mechanisms used in operations to provide a more thorough and realistic contingency training environment.
CA-6 ASSESSMENT, AUTHORIZATION, AND MONITORING - AUTHORIZATION	1, 2, 3, 4, 5, 6, 7, 8	Assign a senior official as the authorizing official for the system. Assign a security specialist as the authorizing official for common controls available for inheritance by organizational systems. Ensure that the authorizing official for the system, before commencing operations: Accepts the use of common controls inherited by the system and Authorizes the system to operate. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems. Update the authorizations every year. Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats. Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.
IA-2 IDENTIFICATION AND AUTHENTICATION - IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	1, 2, 3, 4, 5, 6, 7, 8	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users. Implement multi-factor authentication for access to privileged accounts. Implement multi-factor authentication for access to non-privileged accounts. When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources. Implement replay-resistant authentication mechanisms for access to privileged accounts and non-privileged accounts. Accept and electronically verify Personal Identity Verification-compliant credentials.
IR-2 INCIDENT RESPONSE - INCIDENT RESPONSE TRAINING	1, 2, 3, 4, 5, 6, 7, 8	Provide incident response training to system users consistent with assigned roles and responsibilities: within one year of assuming an incident response role or responsibility or acquiring system access; when required by system changes; and one month thereafter. Review and update incident response training content quarterly.
IR-3 INCIDENT RESPONSE - INCIDENT RESPONSE TESTING	1, 2, 3, 4, 5, 6, 7, 8	Test the incident response capability using automated mechanisms. Coordinate incident response testing with organizational elements responsible for related plans. Use qualitative and quantitative data from testing to: determine the effectiveness of incident response processes; continuously improve incident response processes; and provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.

IR-4 INCIDENT RESPONSE - INCIDENT HANDLING	1, 2, 3, 4, 5, 6, 7, 8	Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery. Coordinate incident handling activities with contingency planning activities. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.
IR-5 INCIDENT RESPONSE - INCIDENT MONITORING	1, 2, 3, 4, 5, 6, 7, 8	Track and document incidents. Documenting incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics as well as evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources, including network monitoring, incident reports, incident response teams, user complaints, supply chain partners, audit monitoring, physical access monitoring, and user and administrator reports.
IR-6 INCIDENT RESPONSE - INCIDENT REPORTING	1, 2, 3, 4, 5, 6, 7, 8	Require personnel to report suspected incidents to the organizational incident response capability within 3 hours. Report incident information to the Security Specialist. Report incidents using automated mechanisms. Report system vulnerabilities associated with reported incidents to the Security Specialist. Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.
IR-8 INCIDENT RESPONSE - INCIDENT RESPONSE PLAN	1, 2, 3, 4, 5, 6, 7, 8	Develop an incident response plan that: Provides the organization with a roadmap for implementing its incident response capability. Describes the structure and organization of the incident response capability. Provides a high-level approach for how the incident response capability fits into the overall organization. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions. Defines reportable incidents. Provides metrics for measuring the incident response capability within the organization. Defines the resources and management support needed to effectively maintain and mature an incident response capability. Addresses the sharing of incident information. Is reviewed and approved by the Security Specialist. Explicitly designates responsibility for incident response to the Security Specialist. Distribute copies of the incident response plan to the senior developers. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing. Communicate incident response plan changes to the Security Specialist. Protect the incident response plan from unauthorized disclosure and modification.
SC-16 TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES	1, 2, 3, 4, 5, 6, 7, 8	Associate security and privacy attributes with information exchanged between systems and between system components. Verify the integrity of transmitted security and privacy attributes. Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process. Implement mechanisms or techniques to bind security and privacy attributes to transmitted information.

Potential not addressed control areas with explanation

Control family	**Description and why we did not use it**

MA - MAINTENANCE	The MA controls have requirements for maintaining organizational systems and the tools used. It is partially covered in other controls since we have already described the maintenance in more specific controls dedicated to the particular attacks.
MP - MEDIA PROTECTION	The Media Protection control family includes controls specific to access, marking, storage, transport policies, sanitization, and defined organizational media use. In our eight threats, we do not have cases directly connected to the media.
PE - PHYSICAL AND ENVIRONMENTAL PROTECTION	The Physical and Environmental Protection control family is implemented to protect systems, buildings, and related supporting infrastructure against physical threats. In our eight threats, we do not investigate cases connected to physical accidents and natural disasters like emergency shutoff, power, lighting, fire protection, and water damage protection.
PL - PLANNING	Planning controls are specific to an organization's security planning policies. This is a very general and short family of controls connected to general planning like scope, roles, responsibilities, organizational compliance. In this step of accessing controls to our topmost serious threats, we prefer to focus on more specific security controls to ensure IT security.
PM - PROGRAM MANAGEMENT	The Program Management control family is specific to managing the security program and operations. This includes, for instance, a critical infrastructure plan, information security program plan, plan of action milestones and processes, risk management strategy, and enterprise architecture. In this step, we decided to focus on controls that are strongly connected to specific attacks on concrete servers. We know that management is very important and it should not be covered in a poor way.
RA - RISK ASSESSMENT	The Risk Assessment control family relates to an organization's risk assessment policies and vulnerability scanning capabilities. As we know from the lecture and also other courses, risk assessment is a very significant step and should be considered separately and in this step focus more on particular attacks.
SR - SUPPLY CHAIN RISK MANAGEMENT	This is the last family control in the NIST. This is the final phase and taking into consideration that we did not investigate the risk assessment it is logical that we omitted Supply Chain Risk Management, especially that it is not strongly related to our top risky threats.