|  |  |  |
| --- | --- | --- |
| **SAI** | **Comments** | **Address of Comments** |
| **SAI Ecuador** | Regarding the exposure drafts of the "Guide on Cyber Security and Data Protection" being led by the SAI of Mexico and the "Guide on Audit of IT Management functions, including Governance, Contract Management and Sustainability"; we would like to indicate that we have no observations or comments on the documents. | Does not apply. |
| **SAI Egypt** | Regarding the study and review of the second Exposure Draft on **“Guide on Cyber Security and Data Protection”** led by the SAI Mexico under the INTOSAI Working Group on Information Technology (WGITA), the said draft is compatible with international standards issued in the cyber security and data protection field, for the following reasons:   * The draft included the most important definitions and concepts of cyber security and data protection. As well as, cyber security’s laws issued by (European Union - USA - Spain - Russia - China). * The draft provides a guiding steps that enable the auditor to verify the cyber security and data protection’s procedures, integrity and reliability policies on both of the organizational and national levels. Also, the draft addressed the obstacles that faces the auditor while carrying out relevant audits. * The draft outlines the considerations that should be taken to protect data and information from cyber attacks. | Does not apply. |
| **SAI Portugal** | As far as the Guideline on Cyber Security and Data Protection is concerned, we totally agree with it and don´t have any comments to make. However, we think that the Portuguese Regulations on the matter could be added to item 3.1.2 (regulations by Country) and, consequently, we also attach a word document with identification and links to the aforementioned regulations. | Change has been applied in the document, please refer to pages 26 and 27 where Portuguese Regulations have been included. |
| **SAI USA** | * Please refer to document attached titled GAO Comments | Under 2.1.2.1., when referring to some of the considerations that should be taken into account to further enhance the audit scope, SAI USA suggests to refer to the implementation of stronger security controls. Such addition has been made in page 11.  Under 2.2.1.1 SAI USA refers that *there seems to be some duplication of concepts in section 2.1.2.3 audit program development and 2.2.1 general audit process. Since there is an earlier section on planning the audit, should that part of the general audit process not be elaborated on again here? For example, both sections discuss defining the security baseline and defining a scoring method.* Given such comment, we have proceeded to eliminate the repeated information in section 2.2.1 and have referred instead to the information provided previously for section 2.1.2.3.  Please refer to pages 21 to 64 for comments received for Chapter 3. |
| **SAI Romania** | Regarding **the Cybersecurity and Data Protection Guideline,** we propose the following comments: 1) In Chapter 1, point 1.4 Key Cybersecurity and Data Protection Standards and Frameworks we propose to analyze the opportunity to introduce into the regulatory framework for EU countries the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing of the Directive 95/46/EC (General Data Protection Regulation)[[1]](#footnote-1). Proposed Comment:   |  |  | | --- | --- | | Criteria (with link) | Description | | [Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)](https://eur-lex.europa.eu/eli/reg/2016/679/oj) | This regulation requires entities to manage data securely by implementing "[appropriate technical and organizational measures](https://gdpr.eu/recital-78-appropriate-technical-and-organisational-measures/)". Technical measures mean anything from requiring employees to use two-factor authentication for accounts where personal data is stored to contracting with cloud providers that use end-to-end encryption.  Organizational measures are things like training staff, adding a data privacy policy to the employee handbook, or limiting access to personal data only to those employees who need it. |   The proposal also aims to harmonize with the provision of the **Cyber ​​Security and Data Protection Guide**, Chapter 2, point 2.1.2.2 *Risk Management and Security Frameworks* where the *"EU General Data Protection Regulation (GDPR)*" is mentioned as a framework that provides examples of management of cybersecurity risks and practices that could be used to help establish the scope of the audit. | Solicited change has been applied to the document and adjustments have been made accordingly. Express referral of the EU 2016/79 has been included as well as a appendix of acronyms and abbreviations. |
| **SAI** | **Comments** | **Address of Comments** |
| **SAI Azerbaijan** | I am writing regarding your email on Exposure Drafts - Guidance on Audit of IT Management functions including Governance, Contract Management and Sustainability and Guide on Cyber Security and Data Protection.  Please be informed that we have reviewed your email.  ***We don’t have any suggestions regarding the submitted documents.*** | Does not apply. |
| **SAI Philippines** | |  |  | | --- | --- | | **Original Context/Text** | **Comments/Suggestions** | | 1.2 Structure of this Guideline Document  2. Guidance during audit phases  Includes audit guidance, how to start audits on cybersecurity and data protection (planning, execution, reporting, follow-up, termination, file and disposal). | Chapter 2 only covers planning, execution and reporting. To be consistent with the description and to cover the entire auditing process, we suggest including a brief discussion on follow-up, termination, filing and disposal. | | 2.1.3 Audit Skill Requirements | It is suggested to add the following as “nice-to-have” certifications:   * Certified Ethical Hacker (CEH) * Certified in Risk and Information Systems Control (CRISC) * CompTIA Cybersecurity Analyst (CySA+) | | 2.2.1.1 If the organization has not defined this security baseline, then the security baseline should can be selected using the following considerations: | Suggested Edits: If the organization has not defined this security baseline, then the security baseline should ~~can~~ be selected using the following considerations: | | National Cybersecurity Maturity Evaluation Models (Overview of analyzed maturity models table) | The links provided are no longer working. | | Provided that it is our intention to advocate for a part two of the document where we plan to extend on a series of subjects touched upon in this document (as the ones commented for sections 1.2. and 2) as well as other related subjects that where left aside for time purposes, note has been taken to touch upon the comments received in 1.2. and 2 for a part two of the present document.  For comments 2.1.3 and 2.2.1.1 please be referred to the group´s decision to expand on certain parts of the document in a second document to be promoted within the WG. Note has been taken to further expand on a part two of the document regarding certifications and certain regulations that given their importance are best to be left for referral in a second document followed by a thorough explanation of their content and relevance.  For comments regarding the malfunction of links, they have been revised and are working properly. |
| **SAI Kuwait** | |  |  | | --- | --- | | **Original Context/Text/Section** | **Comments/Suggestions** | | 4.2 Challenges, risks, and threats for critical infrastructure sectors | we suggest moving this section to chapter 1 or a separate chapter before chapter 2 (Guidance during audit phase) as it is considered as an introduction to cyber security risks before talking about how to audit cyber security. | | 3.15 Disaster Recovery by Function) (USA) | same above comment | | 3.14 General Disaster Recovery) (Australia) | same above comment | | 3.10 Specific Auditing of Critical National Infrastructure by Sectors) (USA) | same above comment | | 3.9 Semi-Specific Auditing of Critical National Infrastructure) (United Kingdom) | same above comment | | 3.8 General Auditing of Critical National Infrastructure | we suggest mentioning that there are some use cases for different SAIs reports (Canada, Korea, Turkey, Australia & Brazil) then list the details of each SAI report in an appendix or mention the links to these reports because they are considered as examples or references for the reader so no need to list the details of each report. | | Chapter 2 (Guidance during audit phases) | we suggest editing the title to (Cyber Security Audit guidance) because it is dedicated to cybersecurity. | | Chapter 2 (Guidance during audit phases) | Some pages of the draft are numbered, and others are not. | | It is considered that comments referred for sections 4.2, 3.15, 3.14, 3.10 and 3.9 are not applicable. If we were to move content of Chapter 4 to Chapter 1, there is a risk for Chapters 4 and 3 (observed in the same way by SAI Kuwait) to be left with no content and for Chapter´s 1 content to lose alignment with its proposed objective.  For comment 3.8 it is considered to be correct to leave the explanation provided for each of the listed reports as their intention is to provide the reader with an in depth understanding of the different ways the Auditing of Critical National Infrastructure has been approached. Rather than referring the reader to the corresponding links, because they make up the main nucleus of our section, we believe best to provide the reader with the whole details.  It is considered for the current name of Chapter 2 to be correct. This is because the main title of the document is Cybersecurity and Data protection. Therefore, referring a particular section with the name the document holds as a whole can cause confusion.  Last comment has been applied. All pages have been numbered. |

|  |  |  |
| --- | --- | --- |
| **SAI** | **Comments** | **Address of Comments** |
| **NAO UK** | For all document:   * There are no page number for pages 1 to 30. Given the length and complexity of this document it would aid those using it to have page numbers inserted through the document. * For consistency through the guide, review and change “cyber security” to “cybersecurity”. * Section 2 of the Guide:   + contains a lot of generic information. It could be enhanced to include further guidance on specific audit tests, the reasons for these tests and examples of typical supporting evidence that auditors can ask for.   + A sample but simple easy to follow audit program covering the key areas of a cybersecurity and data protection audit would be useful. * Section 3 of the Guide. This section of the document is very rich in content. The section is a mix of country specific case studies and reference to specific documents / maturity models. The non-specialist reader is provided with little support to navigate all this content and so it is difficult to extract key messages and learnings from all this content. In this regard it would be good if you could provide more assistance to the reader in relation to this section. Some thoughts on the additional assistance that could be offered are as follows:   + In this section you reference the National Cyber Security Framework Manual produced by the NAO accredited CCD COE. It would help if you could explain why you have chosen to highlight the work of this research body.   + You also reference a variety of other documents (e.g. ENISA Cyber Security Strategies; Swedish National Cybersecurity Strategy; various maturity models). Again it would help the user to know why you are using these reference sources;   + In this section you also refer to cybersecurity related legislation, best practices and certifications for specific countries. This has a lot of information in it and so, once again, it is hard for the non-specialist reader to extract key messages from this area of the document. In this regard:     - It would help to provide some justification as to why you have chosen to feature these countries;     - It would also be valuable to compare and contrast what is being done in various countries and to highlight any matters that would assist SAI auditors in undertaking their own audit reviews;   + On pages 28 and 29 you note various maturity models. Useful to explain the relative merits of each of these and some introductory guidance on how a SAI Auditor might seek to use this;   + The “Pillar-Based assessment for cybersecurity agencies” on pages 65 to 69 is very difficult to extract value from. It feel that may need a whole guide of its own if this is to be of value to the general IT Auditor;   + Similarly the section on “Assessing the maturity level of CSIRT” feels as if it would need a training course for the reader if it was to be useable. * The Guide also needs to be reviewed for general readability. In some of the sections (please see below), the sentences do not flow logically. They will need to be reviewed and redrafted please for better readability. * Links to sources of information should be provided please, where possible. | * + All pages of the document have been numbered.   + The us of the term “cyber security” throughout the whole document has been changed to “cybersecurity” and a note has been included (please see footnote 1).   + For comments regarding Section 2, as referred for previous comments, please be referred to the group´s decision to expand on certain parts of the document in a second document to be promoted within the WG. The idea of this document is to be a generic introduction to cybersecurity and data protection, under the understanding that a second part of the document will further expand on specific subjects left to a generic explanation in this version.   + An introductory step to step guide can be found in 2.1.2.3. further enhanced in 2.2.1.   + For comments regarding section 3, please be kindly referred to the general intention behind this document, to provide auditors / audit public an overview of the state that cybersecurity and data protection guard under a global reach. Such intention has been expressed at the beginning of section 3. The reason as to why some regulations have been highlighted is to provide the reader with examples and mainly, to provide an oversight (as the word is used) of how information referred in section 3 has been applied in other countries.   + The public to which this document is directed to and its objective are referred under section 1.2 “This document is *not meant to be an exhaustive* guide *for auditors* but could be used as a *starting point* to assist *auditors* in *identifying criteria* for *further review*”.   + The suggestion to undertake a compare and contrast exercise has been taken note of for a detailed part two of the document.   + For the comments regarding the pillar-based assessment, please be referred to our intention to provide the reader with a general overview of subjects important when touching upon cybersecurity and data protection. This is meant to be an introductory document as have correctly pointed out, many parts of the document are worth expanding on a second part of the document.   + The appendix has been moved to the end of the document for prompt and precise referral by the reader for the terms used along the document.   + The document has been adjusted as suggested for better readability.   + Referential links have been included in the document.   + Based on the information provided above, as highlighted in the beginning of the document under 1.5, information provided under such section as well as the rest is meant to provide the reader with an audit starting point.   + Please know we have taken note of the specifications pointed out to be worked in a second part of the document more specific than generic as the present document has thought to be worked as. |
|  | There is a table on this page of best practice documents. The first column is headed “Criteria (with link)”. Not sure what is meant, in this context, by criteria.  Can you better align the link to the relevant document in column 1 with the “Description” in column 2. In some cases these merge so it is difficult to determine to which document the description relates? | * + For better understanding purposes, the word “criteria” has been replaced for “Practice”.   + Alignment has been made as suggested. |
|  | **Please delete**  NIST SP 800-161, Rev 1 (Draft): Supply Chain Risk Management Practices for Federal Information Systems and Organizations  **Replace with**  [NIST SP 800-161, Rev 1 (final): Supply Chain Risk Management Practices for Federal Information Systems and Organizations](https://www.bing.com/ck/a?!&&p=e312d294ffa3c2a7JmltdHM9MTY2MDkxNzk2OSZpZ3VpZD1lZTJhZTNjYi03ZmM2LTQ2NWEtOTkxNy1hNzk3YTc1YTY0MmYmaW5zaWQ9NTI0MA&ptn=3&hsh=3&fclid=12b302bc-1fc8-11ed-a7ab-7b0d672781b7&u=a1aHR0cHM6Ly9jc3JjLm5pc3QuZ292L3B1YmxpY2F0aW9ucy9kZXRhaWwvc3AvODAwLTE2MS9yZXYtMS9maW5hbA&ntb=1) | * + Replacement has been made and link has been updated accordingly. |

|  |  |  |
| --- | --- | --- |
| **SAI** | **Comments** | **Address of Comments** |
| **NAO UK** | “*Cybersecurity and Data Protection Best Practices and Key Methodologies*”  **Delete link**  NIST SP 800-53A Rev 4: Assessing Security and Privacy Controls in Federal Information Systems and Organizations. Please remove link. The guide has been replaced and will be withdrawn on 25 January 2023. It has been replaced by Revision 5.  **Replace with**  Link to Revision 5 - [SP 800-53A Rev. 5, Assessing Security and Privacy Controls in Info Sys and Orgs | CSRC (nist.gov)](https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final) | * + For all referrals, name has been adjusted and link has been replaced. |
|  | “*Defining the terms of engagement”*  **Insert**  “The audit should consider the cyber security requirements and goals of an organization. **This will entail analysing industry trends to identify emerging cybersecurity risks and engaging with senior management to understand their expectations.**  Understanding the organization’s cyber security requirements and goals will help with identify**ing** risks to the organization and defin**ing** the audit objective.” | * + Changes have been applied with the following precisions:   + “Analysing” as proposed was spellchecked for the term “analyzing”.   + As commented before, instead of using the word cyber security as two words, throughout the whole document it was been unified as one. |
|  | *“Risk-based Approach to Cyber Security”*  **Insert** **between steps 1 and 2**  **“Undertake risk assessment - Assess the vulnerability of key assets and the key controls to mitigate against the risks identified.”**  **Insert Step 7**  **Reporting - Collate audit findings and make recommendations for change or improvement, including recommendations for addressing residual risks or identified weaknesses not mitigated by controls”** | * + Changes have been applied with the following precisions:   + A new step two was introduced titled “Risk assessment”.   + Given that there was already a step 7, a step 8 was introduced named “Reporting”. |
|  | *Define the security baseline*  “The security baseline will provide the basis for assessing the entities performance. The  security baseline should be based on the following:”  **Change to** **entity’s** | We consider for this change not to be applicable as we are referring in plural to entities performance and not only to one specific entity in singular. |
|  | “*Perform audit procedures”* – 1st bullet point  **Insert**  “Requirements that deviate from the **security** requirements should be supported by a risk assessment.” | * + Change has been applied. |
|  | *Considerations*  “This section will outline the considerations of IT risk and complexity, and integration /use in Compliance, Performance and Financial Audits.”  NAO comment: The sub-section does not quite match the description above or cover performance or financial audit considerations. It covers IT risk and complexity, multi-organisation audits and the advantages and disadvantages of penetration testing. | * + The precision has been made spelling “multi-organisation” as “multi-organization”. |
|  | *IT Risk and Complexity*  **Insert word**  “Cyber security is important for any organization and the cyber security audit should consider the organization’s cyber security risks. A good indicator of cyber security risks is an organization’s attack surface. The attack surface is the amount of ICT equipment and software used by an organization. The greater the attack surface, the greater **the** opportunities for  adversaries in finding vulnerabilities to exploit.” | * + Change has been applied. |
|  | *Multi-organization Audits*  **Insert / delete**  “The auditor may need to adjust the**ir** approach when auditing **~~of~~** multiple organizations.” | * + Changes has been applied. |
|  | *Reporting*  **Insert**  “The audit team will review the audit evidence in order to reach a conclusion or issue an opinion. The audit should evaluate whether the audit evidence obtained is sufficient and appropriate so as **to reduce** the audit risk to an acceptably low level.” | * + Changes have been applied. |
|  | *Cybersecurity and data protection legislation*  **Delete words / insert**  “According to the **~~established in the~~** North Atlantic Treaty Organization Cooperative Cyber Defen**c**e Centre of Excellence (NATO CCD COE), cybersecurity in a country could be understood as the following: “ | * + Specific referral of this part of the document is not found but precision has been made in page 23. |
|  | *The Three Dimensions: Governmental, National, and International*  **Delete word**  “Any approach to a NCS strategy needs to consider the ‘three dimensions’ of activity: the governmental, the national (or societal) **~~social~~** and the international.” | * + Change has been applied. |
|  | Table – 4th row  **Amend** heading from **RGPD** to **GDPR** | * + Change has been applied. |
|  | **Delete / insert words** (after the Table)  “They conducted this performance audit from November 2018 to September 2020 in  accordance with generally accepted government auditing standards. Those standards require that they plan and perform the audit to obtain sufficient, appropriate evidence to provide a  reasonable basis for their findings and conclusions based on **~~our~~ their** audit objectives. They believe that the evidence obtained provides a reasonable basis for **~~our~~ their** findings and conclusions based on **~~our~~** **their** audit objectives.” | * + This section cannot be found. |
|  | *Critical Infrastructures*  **Delete words**  “**~~Due that~~** One important activity in the development of a National Cybersecurity Strategy (NCS) is to identify and classify Critical National Infrastructure (CNI) and Critical Information Infrastructure.” | * + Change has been applied. |
|  | *Critical Information Infrastructures (CII)*  **Delete curly bracket at end of sentence**  “It is an important component of Critical National Infrastructure, especially to the extent different national functions rely on information and communications technology (ICT) for their operation.**~~}2~~** | * + Change has been applied. |
|  | **Insert**  “Thus, based on the analysis of the different SAI’s audit reports the most important principles for effectively formalizing and assess**ing** a CNI/CII includes:”  **Delete letter**  “Use**~~d~~** of international frameworks or standards to assess CNI/CII.”  **Insert word**  “Assess risks using the method of benchmark, in order to identify certain risk  assessment policy and methodological approaches that other countries have used  successfully, **~~these~~ this** is focused on nations that have similar national goals and  circumstances.” | * + Changes have been applied. |
|  | **Delete**   * “The audit team has determined the modules to be tested according to the following **~~(:)~~** criteria:” * “Materiality (The impact of the application on the activities of the Institution and **~~--~~** financial statements, etc.),” | * + Changes have been applied. |
|  | **Insert**  “However, instances of cyber terror, such as the paralysis of Nonghyup computer networks (April 2011) and EBS personal information leakage of near**ly** 4 million users (May 2012) continuously occur, proving that the security of the nation and society are at **~~threat~~** **risk**. Based on the foregoing it is necessary to **~~implement~~** conduct audits in ICT systems including critical infrastructures.” | * + Changes have been applied. |
|  | **Brazil**  Background information on national cyber security strategy / audit arrangements is required to set the scene and ensure consistency with the previous sections of the Guide.  *Objective*  The sentences in this section do not flow logically. The paragraph needs to be reviewed and redrafted for better readability please.  *Conclusions*  It’s not quite clear how the conclusions relate to the scope of the audit done. | * + The information provided is set to provide the reader an overview of the different way nations apply different frames of references as they work to identify CNI/CII. For referential / background information please refer to section 3.5 of the document.   + Precisions have been made for better readability.   + Precisions have been made to better transmit the message referring to the expectations held by the Court following the resulting from the applied assessments. |
|  | “Objective” section  **Delete / insert words**  “The **~~objective~~ strategy** is intended to shape **~~and assurance~~** the Government’s policy, while also offering a coherent and compelling vision to share with the public and private sector, civil society, academia and the wider population.” | * + Changes have been applied. |
|  | “*Scope and Methodology*” Section   * This section needs redrafting as the information presented does not flow logically. * There is a need for more information on the audit being referred to here, including the actual scope of the audit and the methodology. | * + Please have in mind that this document is meant to provide the reader with a general overview of various aspects regarding cybersecurity and data protection.   + As for the specific section pointed out for “scope and methodology”, such section is referred when presenting the different cases in which SAIs perform a general audit of critical infrastructure, to encourage cybersecurity audits. Under the section of scope and methodology, our intention is to provide the reader with the extend to which the examples set forth have proceed to approach the different levels of government and other relevant actors involved. |
|  | “Frameworks and Guides”   * A link to the audit report being referred to is required to enable users of the Cybersecurity and DP Guide follow through on the reference made to specific sections / pages of the said audit report. * The National Cyber Security strategy referenced in the document is out of date.   The strategy referenced here is out of date. The latest strategy can be accessed via the link below:  [National Cyber Strategy 2022 - GOV.UK (www.gov.uk)](https://www.gov.uk/government/publications/national-cyber-strategy-2022) | * + Precision has been made. Please refer to page 43 of the document with the precision that based on a prior comment the term cyber security was aligned to the term cybersecurity. |
|  | **USA**  **Delete words**  “Threats to the systems supporting critical infrastructures are evolving and growing. These cyber-based assets are susceptible to unintentional and intentional threats. Unintentional, or non-adversarial**~~,~~** threat sources include equipment failures, software coding errors, or the  accidental actions of employees. They also include natural disasters and the failure of other critical infrastructures since **~~due to~~** the sectors are often interdependent.” | * + Change has been applied. |
|  | “Conclusions”  Reference was made to “SCCs” in the conclusion but it is not clear what this means and no reference to SCCs was made in the other sections of the write-up under 3.10.1 USA | * + Please refer to the Appendix of the document, specifically page 81 where SCCs are referred to as Sector Coordinating Council. |
|  | National Resilience / Disaster Recovery  **Delete/insert words**  “Organizational resilience is important to assure users and managers that the expected level of service will be provided. Outages are also often unavoidable driving factors in organizations; therefore, preparation is key to be able to continue operations while protecting people, assets, and the organization's reputation; employing process resiliency tactics helps  organizations to address these issues and limit the impacts. **~~We were~~ They are** classified into two main types:” | * + Please see precision in page 49. |
|  | **Delete/insert words**  Entities Responsible **~~of~~** **~~the~~** **for** National Cybersecurity**~~.~~** | * + Change has been made. |
|  | **Delete/insert**  Note: There is a need for a review and redraft please of the section highlighted in yellow.  “These police organizations dedicated to the computer world pursue and prevent bank fraud, identity theft, cyberbullying or **~~cyber~~ online** bullying, child pornography, identity theft through different social networks and hacks that result in loss or kidnapping of information. Their functions are diverse: they are in charge of combating virtual terrorism, carrying out cyber patrolling to avoid computer crimes or fraud against computer systems, banking institutions, it is in charge of carrying out the pertinent investigations through any case of the different types of existing computer crimes, finding dedicated bands to cyberbullying, and child prostitution through the Internet as a means of contact, analyzes and identifies the different types of computer crimes and scams carried out through the Internet.” | * + Precision has been made regarding “cyber bullying” to “online bullying”.   + Redraft has been done to the pointed paragraph of the document. |
|  | **Delete**  (Information in the paragraphs below does not flow logically and we do not consider that it adds value. Role of CSIRT has already been described in previous paragraph)  **“~~This section describes the role of cyber incident response teams (CSIRT) in charge of~~**  **~~responding to computer security incidents, in cybersecurity matters, to achieve advances in~~**  **~~cyberspace security; different types of cyber incident response teams (CSIRT) are reviewed,~~**  **~~which are those who manage the most critical and significant events that threaten the~~**  **~~confidentiality, integrity or availability of critical information networks and play a crucial~~**  **~~role in improving cyber resilience.~~”**  **“~~Guides are presented to evaluate a computer security incident response team (CSIRT), whose objective is for an audit institution to identify the elements of review to understand the nature, the scope and operation of an IT security incident management service, both to newly trained~~**  **~~teams and to a high degree of maturity.~~ “** | * + Change has been made. |
|  | Cert/CSIRT functions  **Delete** – last bullet (contains no information)  **Delete/Insert words**  “All CSIRTs work differently depending on the entities they provide protection to. However,  in general terms, most of these groups have an attack team, which is responsible for studying  the behavior of cybercriminals and the main attack vectors, and a defense team, whose  objective is to analyze the traffic of the networks to be alert under the presence of a computer  eventuality. Additionally, these teams have great challenges such as sharing information,  adding synergies with other CSIRTs to be able to share information in forums (such as  APCERT or FIRST) and being able to offer an effective and rapid response to any threat **~~that~~**  **~~puts~~** **to** the most critical information or the interruption of services and/or business." | * + Changes have been applied. |
|  | Computer Emergency Response Team (CERT) and Computer Security Incident Response Team (CSIRT)  **Delete/insert words**  “Distinctions are made between CERT and CSIRT: A CERT is conceived as a study center and a place where methods and procedures are established to improve incident response teams; a CSIRT **~~as~~** **team are** those responsible for responding to incidents. | * + Change has been applied. |
|  | The paragraph below needs to be reviewed and redrafted as it contains gaps. The number of areas of cybersecurity and the number of bullet points that followed are not consistent.  “In a study made by the European Union (EU) v, it is shown a board with the complete  description of the estate of the actual cybersecurity frames and its capacities for each member.  The report considers five main areas of cybersecurity politics of each state of EU:  - Legal foundations of cybersecurity  - Operating Entities.  - Public-private partnerships  - Education.” | * + Change has been made. |
|  | *Assessing the maturity level of a CSIRT*  **Delete stray characters**  “The objective of the maturity level evaluation is to analyze how well a CISRT team governs, documents, performs, and measures its function **~~viii,~~.** **T**his analysis compares the level where the CISRT is currently, which allows organizations to visualize the information and consider it as a baseline to detect existing gaps, carry out in-depth reviews, issue opinions and take actions focused on continuous improvements. | * + Change has been applied. |

|  |  |  |
| --- | --- | --- |
| **SAI** | **Comments** | **Address of Comments** |
| **NAO UK** | SIM3 Model  **Delete – stray characters (**in last sentence)  “… skills and competence measured against a defined reference model **~~ix~~**.” | * + Change has been applied. |
|  | Financial service sector  **Delete word**  Regardless of which sector is being audited, the team must understand the systems and technology used in that sector, and the potential threats and vulnerabilities. This may be accomplished **~~by~~** in several ways, including reviewing any documentation developed by organizations within the sector, completing physical reviews of companies or locations, and interviewing organizations within the sector. | * + Change has been applied. |

1. <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [↑](#footnote-ref-1)