**Compliance to Comments on the Exposure Draft**

|  |  |  |  |
| --- | --- | --- | --- |
| **SAI** | **Para reference (Pre revised GUID)/ General Comments** | **Comment** | **Action taken/Remarks** |
| Netherlands | General comment | The Netherlands Court of Audit (NCA) received a request for comments from INTOSAI on the Second Exposure Draft of GUID 5101 Guidance on Audit of Security of Information Systems. This memo contains the response from the IT audit cluster of the NCA. We first address the 2 specific questions in the request. We then provide a response for each section of the draft document. | No action required |
|  | General comment | We think this is a useful document for auditors less familiar with audits in the information security subfield. Overall, we think the document succeeds in getting auditors started without going into too much detail. In some places we would expect a little more or a little less level of detail, see our comments in paragraph 3 | No action required |
|  | General comment | We also note that the document can be positioned more clearly as a supplement to GUID 5100. Readers may otherwise be under the impression that this is an independently readable guidance, while the document provides additions, specific points of interest and examples that are useful in information security compliance audits. We also make suggestions for this in our commentary in paragraph 3 | Dealt with in para 3 |
|  | General comment | A third general observation is that the guidance could further emphasize that trends and technologies in information security are evolving extremely rapidly. Think of resilience of encryption against quantum computing or ever-changing modus operandi of cyber criminals. The document can point this out in several places, for example under “IV - The subject matter”. In addition, we suggest that the document be reviewed and updated more frequently than other guidances | The GUID has been drafted to provide guidance without being technology/IT system specific. Therefore, the document may not require frequent review. However, if there are any major changes in the overall technology ecosystem, it may require review.  No changes are required in the current GUID |
|  | General comment | We believe that the definitions included in Section III are sufficient to understand GUID. Explanations of technical terms that the reader may not be familiar with can be easily identified on the internet by anyone | No action required |
|  | Section I (Introduction) | Align this paragraph with GUID 5100 and use the introduction to position the document. The relationship to other GUIDs is currently covered in paragraph II. It is more clear to the reader if this is done in Section I. The points now included about the relevance of information security can then be mentioned last | Para 3 from Section II moved to Para 1 in Section I. The structure of the GUID now aligns with GUID 5100 |
|  | Section I (Introduction) | Explicitly state that the document has the same structure as the GUID 5100 | Since it has been explicitly stated that this GUID is a supplement to GUID 5100, stating that it has the same structure may be redundant.  Therefore, no change made to the GUID |
|  | Section II (Objectives of this GUID) | Make clear in this section that the document provides examples and specific points of interest, but does not claim to be complete | A clarification has been added in para 6 of Section II |
|  | Section III (Definitions) | No remarks | No action required |
|  | Section IV (The Subject Matter) Para 8 | The first sentence of paragraph 8 (“The information security audit work will be determined by the objectives and scope of the audit.”) seems redundant to us: after all, this applies to any audit | The sentence provides a context to the elements of scope elaborated subsequently in the paragraph. Therefore, the sentence is not redundant & is proposed to be retained.  Therefore, no change made to the GUID |
|  |  | Under item 8b we would add “risk acceptance thresholds” after “acceptance criteria” | Para 8b amended to include risk acceptance thresholds |
|  |  | Under item 8b we would add after item III as item IV: “Evaluation of the Information security risk management processes” | Evaluation of risk management has been added to item III that is on review & continual improvement |
|  |  | From item 8 a reference can be made to item 20 | Item 20 has been redrafted. So no reference to item 8 required |
|  | Section V (Planning Audit of Information Security) Para 9 | Under item 9, we would mention “new or amended laws and regulations.” | When new or amended laws/regulations are brought it, the IT system & organisation policies are appropriately changed. (If the entity has not made changes to the system/policies in aligning with the legal/regulatory amendments, such issue will not be under the scope of an Information Security audit). Therefore, this need is covered in item 9(a) – “development of new IT system or replacement/upgradation of an existing IT system” and item 9(g) significant changes in organisation policies & structures for IS management & implementation.  Therefore, no changes made to the GUID |
|  |  | The consequences of disclosure of confidential findings and vulnerabilities is an aspect of information security audits to consider. Paragraph 29 of the draft already addresses this regarding the publication of results. We miss another comment on the requirements for the audit team in this regard: SAI investigators may have to deal with state confidential information in their audits. This requires explicit SAI considerations about screening of auditors by competent authority, such as national security agencies | Confidentiality is a fundamental value of the Auditor. It is applicable for every engagement & there need not be any requirement for screening the Auditor. Further, Audit of information security may not involve dealing with state confidential information (beyond the scope of a regular audit of information systems). Sensitivity to reporting any security weakness has already been covered in Para 29.  Therefore, no change made to the GUID |
|  | Section VI (Conducting Information Security Audits) Paras 17 to 28 | In this section several things get mixed up, at different levels of abstraction. We think this section could be better structured, possibly with some subheadings .  a. 17 contains an enumeration of quality aspects,  b. 18 and 26 deal with sources of evidence  c. 19 to 24 and 28 are about audit objects: sometimes referred to an audit object, such as culture/organization (19), risk management (20) and asset management (21) and sometimes to a specific control for an audit object, such as 2FA in IAM (22) and authenticity, integrity and non-repudiation of logging (23).  d. 25 deals with responsibilities in outscourcing.  e. 27 deals with reliance on third-party audits | Paragraphs in the section have been redrafted & re-sequenced for clarity. All paras deal with conducting IS audit |
|  | Section VI (Conducting Information Security Audits) Paras 18 | We suggest to dedicate item 18 only to vulnerability audits and pen testing (VA/PT): after all, that is a specific method to information security audits while the other data collection methods are generic. Regarding VA/PT, we miss some handles to get readers started. We suggest at least going deeper into the “arrangements and agreements” by pointing out the legal safeguards and indemnifications: VA/PT sometimes require activities that are illegal and VA/PT can also impose risks to the auditee, such as loss of data | The concerned paras relating to VA/PT have been redrafted |
|  | Section VI (Conducting Information Security Audits) Paras 20 to 21 | The items naming the audit objects, such as 20 and 21, seems more appropriate for Section IV (The subject matter) | Paragraphs in the section have been redrafted & re-sequenced for clarity. All paras deal with conducting IS audit |
|  | Section VII (Reporting on Audit of Information Security) | No remarks | No action required |
|  | Section VIII (Follow up) | In our view, item 34 should (also) be mentioned under item 9: “The need for an Audit of Information Security...” | Item 9 and Annex A includes illustrative lists of triggers that may necessitate an Information Security audit. Dynamic nature of IT sytems pointed out in Item 34 is already part of the lists, like point 9 (a), (b) & (g).  Therefore, no changes made to GUID |
|  | Annexure A | The enumeration may inspire SAIs but also seems somewhat arbitrary. One can think of many other factors that affect information security such as organizational culture, vulnerability management, change management, behavioural aspects, awareness training, SOC/SIEM et cetera. As far as we are concerned, the annexure is not really necessary | Annexure A has been deleted. The elements have been incorporated in the GUID |
|  | Annexure B | We wondered if this annexure is based on a model, standard or other guidance. If so, this can be referenced | It is not based on models, but includes all domains relating to information security.  Therefore, no change made to GUID |
|  |  | It would be nice if this table could be mapped to the domains described in item 8 in Section IV (“The Subject Matter”) | Para 8 items have been covered in the Annexure. A few changes have been made in the sequence to map the two |
|  |  | 'Whether the organization promotes a culture...' does not really fit under 'Information Security organization structure'. We would make a separate section 'Organization culture' for this (in line with the domains in item 8) | Security culture has been dealt along with organisation structure in item 8 as well.  Therefore, no change made to GUID |
|  |  | Number 8 seems to be missing from the table | Necessary correction has been carried out in the GUID |
| Norway | General comment | The GUID is not precise enough in terms of understanding the subject matter and complying with the ISSAI framework. The GUID is very focused on “checklist” auditing and does not cover how to audit security and information systems based on risk and materiality | Changes, where required, have been carried out where specific comments have been provided |
|  | General comment | The wording in some of the paragraphs is a bit ambiguous and difficult to understand. Simplifying the language is advisable for the GUID to provide useful guidance for everyone to understand | Changes, where required, have been carried out where specific comments have been provided |
|  | General comment | The GUID uses IT security and information security interchangeably. Cyber security is also mentioned but not defined. Information security is the only one of these three terms that is defined. If they are all to be used in the GUID, they should all be included in the definitions paragraph with an explanation of what the differences between them are | Cyber security has also been included in the definitions. Any reference to IT security in the GUID has been removed, as it is only a component of information security |
|  | General comment | Our understanding is that the GUID will give additional guidance on how to conduct a compliance audit when the subject matter is on information security. ISSAI 400 contains the principles in compliance auditing. ISSAI 4000 is the compliance audit standard containing all the requirements you must follow to be ISSAI compliant, and the standard gives you all the steps in a compliance audit | Changes, where required, have been carried out where specific comments have been provided |
|  | General comment | After assessing GUID 5101, we do not find that this GUID give us additional guidance to conduct a compliance audit when the subject matter is information security. In addition, we recommend you to look at ISSAI 4000 and GUID 4900 and align the GUID after compliance audit terminology | Changes have been made in the GUID to align terminology |
|  | General comment | The first step in an audit, is that the auditor identifies areas that are significant for the intended user (ISSAI 4000/64). What is specific when it comes to information security? Are there areas with potential risk of non-compliance that are significant for the intended user ? | These have been covered in Section V.  Therefore, no change made to GUID |
|  | General comment | When identifying the intended user and responsible party (ISSAI 400/35 and ISSAI 4000/101) is there anything particular to take into consideration when it comes to information Security ? | GUID 5101 provides additional guidance. There is no additional information on intended user(s) & responsible party required for Information Security audit.  Therefore, no change made to GUID |
|  | General comment | Subject matter – The subject matter shall be measured or evaluated against criteria (ISSAI 400/31 and ISSAI 4000/107). Please identify audit criteria in a different paragraph than the paragraph about the subject matter . These are two different elements in an audit | The section is on compliance of subject matter to applicable authorities. Identifying criteria in the section ensures clarity on the issue. It is also in sync with ISSAI 4000/107  Therefore, no change made to GUID |
|  | General comment | Despite this we will not recommend using ISO/IEC 27001. Not all SAIs use this as source for audit criteria because it is not mandatory for public sector entities to comply with this standard in many countries | The references also clarifies that these are to be used only where applicable.  Therefore, no change made to GUID |
|  | General comment | Audit criteria –Applicable authorities are laws and regulations, not only policy, procedures, standard and practises. Look at ISSAI 400, ISSAI 4000 and GUID 4900 for more information about audit criteria | Paras 7 & 8 modified |
|  | General comment | Type of engagement – is this guidance for direct reporting engagement (ISSAI 100/29, ISSAI 400/15 and ISSAI 4000/37-42)?  Type of assurance – is this guidance for audit with reasonable assurance or limited assurance (ISSAI 400/41 and ISSAI 4000/33 - 36)?  There are general principles (ISSAI 400) and requirements (ISSAI 4000) of compliance audit such as objectivity and ethics, audit risks, risk of fraud, professional judgment and scepticism, quality control, documentation, and communication. We recommend you to discuss these principles and requirements and consider if there is anything special to highlight for the IT-security area | GUID 5101 intends to provide additional guidance. Where there are no differences from the principles & standards, no mention has been made in the GUID. References have been made to areas like audit risks, documentation, communication etc where additional guidance was required.  Therefore, no change made to GUID |
|  | General comment | In the chapter about the audit process, we recommended you highlight the methods and techniques that are used in this type of audit, because it differs from other compliance audits . The methods and techniques depend on the audit objectives and the audit questions | Methods & techniques have been mentioned in para 18 and in other paras in Section VI.  Therefore, no change made to GUID |
|  | Para 1 | This paragraph is copied from GUID 5100 – it should be rewritten to be more relevant for Information Security Audits . Sentence no 2 is unclear – is the GUID saying that if you conduct an IS audit you also need to include information security in that audit? | The paragraph is specific to information security.  The sentence states that there is a need to ensure controls. Where there is a risk of lack of such controls, audit of information security may be needed.  Therefore, no change made to GUID |
|  | Para 2 | Suggested phrasing: Information security breaches may lead to severe legal, reputational/ credibility, financial, productivity damage, and exposure to further intrusions. Security breaches may be caused by weaknesses and vulnerabilities that lead to accidental exposure, or disclosure of information by insiders, loss of availability or unauthorised changes in systems and data due to cyber-attacks | The paragraph has been redrafted |
|  | Para 3 | The reference to ISSAI 4000 is missing. If a SAI uses ISSAI 4000 as their authoritative standard, there are requirements and not only principles the SAI must follow to be ISSAI compliant.IT-security aspects – it is better to use information security to avoid inconsistencies. See also comment under question 2 | SAIs may have their own standards. ISSAI 400 covers the requirements |
|  | Para 4 | Repetition of paragraph 3 – delete or merge | Retained because para 3 has been moved to introduction.  Therefore, no change made to GUID |
|  | Para 5 | This paragraph is confusing. Just refer to ISSAI 400, paragraph 20 which states the three different perspectives of compliance audit | The paragraph has been redrafted in sync with ISSAI 400/9 |
|  | Para 6 | Ok, however a bit redundant | No action required |
|  | Section III (Definitions) a | Ok, but should probably also include definitions for cyber security and IT security if these terms are to be used throughout the GUID | Cyber security has been defined |
|  | Section IV (The Subject Matter) | This section should be under Planning an audit of Information Security – after sources of criteria and risk assessment | The GUID follows the structure of ISSAI 4000, with subject matter & scope (ISSAI 4000/43-44) followed by the planning process (Chapter 6 of ISSAI 4000)  Therefore, no change made to GUID |
|  | Para 7 | Difficult sentence to understand. Suggest rephrasing. Please look at subject matter and audit criteria in the email | Sentence has been rephrased |
|  | Para 8 | Again, difficult to understand. Suggest rephrasing to make the point clear. The subject matter should always be determined by risk and materiality. The audit objective and audit questions are key to the scope. Further, audit questions contain audit criteria and are a concretisation of the audit objective. The list of elements may be counterproductive and seen as exhaustive. If examples of subject matters are needed, we suggest that they are moved to the annexure. We are also unsure about the use of ISO/IEC 27001. Not all countries use this as a source of audit criteria | It is clarified that the list is illustrative. ISO has been referred only where it is applicable. The sentence has been redrafted to provide clarity |
|  | Para 9 | Is this the overall risk assessment to determine risk and materiality of the audit, or is this risk assessment when determining criteria and scope? The list of examples: revise language and consider moving to annexure | It is clarified in the GUID that it is illustrative. Moving it to annexure may reduce readability |
|  | Para 10 | Should this have been 9 h)? Would we normally recommend that auditors use the risk assessment done by the auditee instead of performing both an overall risk assessment and a more detailed risk assessment when criteria are deduced? Normally, the entity’s own risk assessment is part of knowing the entity | The para has been redrafted for clarity |
|  | Para 11 | This paragraph is a bit vague and could be explained in more detail. Why is information security important? What is the importance of the information values that the auditee has? | The para is structured on GUID 5100. It further adds that materiality considerations specific to information system as provided in GUID 5100 would apply.  Therefore, no change made to the GUID |
|  | Para 12 | Long and complicated sentence. As it is now, it does not make sense. Should not the GUID give guidance on how to deduce objective and scope from criteria? And not standards for audit risk assessment and planning of audits. We already have standards for this – the ISSAI framework | The paragraph has been redrafted |
|  | Para 13 | There is some confusion here on what is audit standard and what is criteria. Audit standards govern the auditors’ work, i.e. the ISSAI framework – in this context ISSAI 400 and 4000. Audit criteria are laws, regulations, standards etc. that the auditees are obliged to adhere to and to which the auditor benchmark the audit findings. This is not clear in these paragraphs. Consider revising | The word ‘standards’ in the para refers to information security standards & not audit standards. The word has been removed to avoid confusion |
|  | Para 14 | This paragraph should be the first under planning and should focus on laws and regulations as authorities to draw criteria from | Section V.1 is on source of criteria. The structure of the sections is that it identifies international information security frameworks/standards in the initial part. It then provides guidance to SAIs on choosing the appropriate framework.  Therefore, no change made to the GUID |
|  | Para 16 | Repetitive. This is covered in the introduction | The para has been deleted |
|  | Para 17 | Content ok but very verbose – simplify the language to make the point clear | The para has been redrafted |
|  | Para 18 | Move definitions of Pen testing and vuln assessment to definitions section. Remove the example (e.g. relating to audit logs of various types) as it is not necessary. It is important to remember that the methods and techniques which are used depend on the audit objectives and the audit questions | PA/VT has been moved to definition. The example quoted improves clarity. So it has been retained |
|  | Para 19 | The scope of the audit should be covered under planning | The para has been redrafted |
|  | Para 20 | These are all pertaining to the scope of the audit, which is determined in the planning of the audit. The scope of the audit and specific audit procedures are usually risk-based; hence the auditor should determine what to focus on during the audit based on risk. This is too detailed and suggestive. It presents as an audit program. Examples should be moved to annexure to emphasise that they are only examples and not mandatory audit procedures | The para has been redrafted. Providing examples in the GUID improves readability. ISSAI 4000 also includes several examples which provides clarity to the reader |
|  | Para 29 | Include ISSAI 4000 | SAIs may have their own standards. ISSAI 400 covers the requirements |
|  | Para 30 | There are other alternatives to management letters. For example, some SAIs has the mandate to redact sensitive information. Consider rephrasing to include other alternatives | Para has been rephrased |
|  | Para 31 | Again, language is a bit difficult. Please use clear language to make the GUID more user friendly | Para has been redrafted |
|  | Para 32 | What is meant by technical solutions here? This sentence is difficult to understand. Should the auditor assess technical solutions and conduct a cost-benefit analysis, or should the entity do this ? | The para has been redrafted for clarity |
|  | Para 33 | The need to comply with ISSAI 400 is already covered. Remember also that there are “principles” in ISSAI 400. In ISSAI 4000 there are “requirements”. | SAIs may have their own standards. ISSAI 400 covers the requirements |
|  | Para 34 | What does this paragraph mean? Usually, the SAI will have one follow-up of a compliance audit. The extent and scope of the follow-up is determined based on the risk that the auditee has not complied with the recommendations and has not mitigated risks and vulnerabilities. If the audit is carried out on a regular basis, the follow-up is done in the next cycle | The para clarifies dynamic nature of information technology, which needs to be factored in while planning follow-up  Therefore, no change made to GUID |
|  | Annexure A | We don’t understand the point of this annexure | Annexure A has been deleted. The elements have been incorporated in the GUID |
|  | Annexure B | We don’t understand the point of this annexure. It is already stated earlier that ISO 270001/2 is the basis of this GUID – audit procedures could be drawn from this or other standards based on risk assessment. The annexure does not provide any guidance on how to audit | The annexure provides high level audit questions, which would be useful in information security audits  Therefore, no change made to GUID |
| USA | General comment | Yes, this GUID provides useful guidance for supreme audit institutions (SAI) for carrying out such compliance audits | No action required |
|  | General comment | Yes, the GUID includes all definitions needed to understand and use it | No action required |
|  | Para 9 | We suggest clarifying the bolded terms used on page 7 of the PDF (see text block below). Rephrasing these sentences to explain the terms more clearly, thus showing how the examples used in each bullet relate to the remainder of the sentence, might be helpful to readers.  Paragraph 9: The need for an Audit of Information Security may be triggered, depending on the results of an audit risk assessment, by one or more events, such as (illustratively, refer Annexure A also):  (a) development of a new IT System or replacement/**upgradation** of an existing IT System by the audited entity, especially in a critical business area;  (b) **non-upgradation**/replacement of a long-standing legacy IT system, where the underlying technological infrastructure is outdated and not currently supported through security patches/ updates;  (c) **non-conduct** of periodic internal/ external security testing, including and security testing of operational IT systems, especially those which have undergone significant application or infrastructural upgrades. | The paragraph has been redrafted to bring in more clarity |