The Economics of Assurance Activities

Security Lancaster — Lancaster University

Contributors:
Dr. Jose M. Such (Principal Investigator),
Dr. Antonios Gouglidis,
William Knowles,
Gaurav Misra,
Prof. Awais Rashid
Security Lancaster
Infolab21 SCC
Lancaster University
Lancaster
LA1 4WA
United Kingdom

Cite as:
Such J.M., Gouglidis A., Knowles W., Misra G, Rashid A. The Economics of Assurance Activities. Technical Report SCC-2015-03, Security Lancaster, Lancaster University, 2015.

Acknowledgements:
This Cyber Security research project was funded by the UK Government.

Disclaimer:
This material is provided for general information purposes only. You should make your own judgement as regards use of this material and seek independent professional advice on your particular circumstances. Neither the publisher, nor the author, nor any contributors assume any liability to anyone for any loss or damage caused by any error or omission in the work, whether such error or omission is the result of negligence or any other cause.

Contents

Executive Summary

At the heart of the information assurance process lie the "assurance techniques" that are used in its assessments. Despite this, and against the backdrop of the year-on-year annual increases of security expenditures for organisations of all sizes, such assurance techniques remain largely unstudied holistically to understand them and their main characteristics, especially from the perspective of the economics of their use. This leaves some lingering questions unanswered: (i) which are these assurance techniques and what are their main characteristics? (ii) how are these techniques being used within particular assurance schemes? (iii) how do we ensure that the increasing number of trained professionals, products, and services in the information assurance space are deployed and utilised in a cost-effective manner?

This project intends to address this gap through a comprehensive review of the use of assurance techniques within 17 contemporary assurance schemes, and a large-scale stakeholder-supported study including 14 interviews as well as an on-line survey with 115 respondents on their perception of the use and value of such techniques in practice, in order to inform the design of future assurance schemes.

In order to mitigate against the subjectivity over what constitutes an assurance technique, a set of 25 assurance techniques were defined that spanned 6 categories: *Review*; *Interview*; *Observe*; *Test*; *Independent Validation*; *Individual Competence*. Relationships between assurance techniques were then described, e.g., where one contributed to another.

A framework was further defined to establish criteria for analysing assurance techniques, both independently, and within the context of specific schemes. The framework's design was informed by the stakeholder interviews. These interviews were also used to collate scheme-specific information. This resulted in a mapping of the usage of assurance techniques within each of the 17 assurance schemes. In order to facilitate the design of security evaluation criteria for future assurance schemes, a mapping was also made between the defined assurance techniques and the security control families of ISO/IEC 27001.

An online survey was then conducted which received responses from a further 115 stakeholders. An analysis of stakeholder characteristics found 64% of respondents to be security practitoners (e.g., penetration testers) and 91.81% of all stakeholders had over 5 years of industry experience. Stakeholder representation across our range of chosen assurance schemes was high, in particular for ISO/IEC 27001 and Cyber Essentials.

For individual qualifications, "Oral Examination" was perceived to be the most effective assurance technique, with multiple-choice examination the least effective. A further review found "Oral Examination" and "Employment History and Qualification Review" to be the most cost-effective combination for assessing individual competence.

An analysis of assurance techniques for assessing security controls was also conducted. A baseline "medium" size target was chosen for the survey (e.g., a company with 250 employees or infrastructure with 16 external IPs or 150 internal IPs). The analysis included factors such as the number of people required, expertise required, time required, effectiveness, cost, complementary assurance techniques, and stakeholder confidence in their answer.

Stakeholders perceived "Penetration Tests" and "Red Team Exercises" to be the most effective assurance techniques, but also categorised them as "Expensive". In contrast, both "Review of Client-Completed Self-Assessment Forms" and "Public Reviews" were perceived to be the least effective, but also the cheapest to conduct. A further analysis suggested the most cost-effective assurance techniques to be "Architectural Review" and "Vulnerability Scans" and "Penetration Tests". The least cost-effective assurance techniques were perceived to be "Public Review", "Emanation Security Analysis", "Fuzzing", "Static Analysis" and "Dynamic Analysis".

A case study for a "special" environment was also described, in the form of Industrial Control Systems (ICSs). Stakeholders interviewed as part of this process perceived an endemic lack of security risk management processes in ICS environments, with security assessments (where they occurred) often providing limited assurance about an environment's security. In order to encourage the development of ICS security risk management processes a series of practical "next steps" were identified.

A high level analysis of the economics of assurance schemes and incentives in the assurance scheme ecosystem, which could hamper/facilitate cost-effective assurance schemes and techniques, was also reported. A series of assurance scheme case studies were also conducted. Notably, this involved an analysis and comparison of the assurance ecosystem and incentives for ISO/IEC 27001 and Cyber Essentials certification.

Finally, the aggregate findings of the study were synthesised and consolidated into a series of conclusions and recommendations for improvement. This includes recommendations for assurance technique use in current and future assurance schemes.

Introduction

A notable trend in the body of literature on information assurance schemes is the focus on the operational benefits and challenges of using the scheme, or debate on the security controls that they outline. The assurance techniques used in the assessment of conformance to assurance schemes have largely escaped rigorous analysis. Where existing literature exists on assurance techniques, the focus has largely fallen on their role within software assurance. In particular, assurance techniques and their use within the Software Development Life Cycle (SDLC) [4]), or in rare cases, their use within specific product-focused assurance schemes (e.g., the classification of assurance techniques for use within Common Criteria [11]). The predominant body of work in this area has been instigated by the National Institute of Standards and Technology (NIST) project, Software Assurance Metrics And Tool Evaluation (SAMATE)[1], which is sponsored by the U.S. Department of Homeland Security (DHS). An abundance of publications have been produced under this umbrella; notably around the topic of source code analysis, with a particular focus on static analysis[2]. A comprehensive review of existing software security assessment tools is presented in [19], focusing on when they can be used, their required skills, and their benefits and drawbacks.

The role of economics within information assurance is a small but growing area of research focus; however, the majority of this research has focused on factors such as incentives (e.g., [3]), and limited attention has been paid to the economics of assurance techniques. Where this exists, the focus has again fallen on software assurance. For instance, [17] investigated the economic impact of having an inadequate infrastructure for software testing and [6] elaborated on existing approaches that are able to model and assess the cost and value of software. The scope of assurance techniques falls beyond software assurance, however, and it is in this broader application that this document is concerned: the multitude of assurance techniques, both non-technical (e.g., interviews and observation) and technical (e.g., penetration tests), which can be used in the assessment of security controls (be they technical, organisational or physical) or individual competence, and the economic factors inherent within this.

This study is the first one to report a comprehensive and extensive study of assurance techniques and their economics. Figure 1 depicts a high-level overview of the main steps of the methodology we used to produce this report. The initial process involved information gathering using three information sources. Firstly, publicly available information about the 17 assurance schemes shown in Table 1 and related literature was considered. Secondly, 14 interviews with security experts were conducted to retrieve information not publicly available, to validate information collected from publicly available information, and to check collected information for completeness. Interviews were also used to study the economics, incentives, and the assurance ecosystem, along with the ICS case study. Thirdly, an online survey was used to gather further information from 115 security professionals.

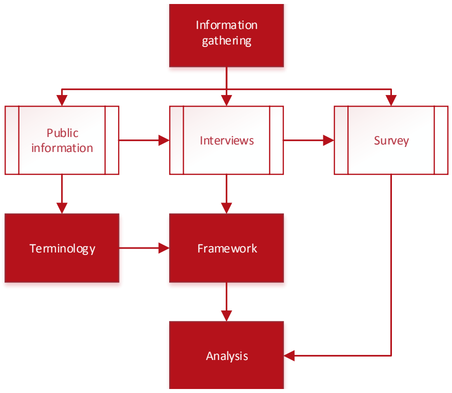


Figure 1: Methodology

Scheme	Scope	Target
CBEST/STAR	National (UK)	Organisational security
CEH	International	Individual qualification
CESG CAPS	National (UK)	Organisational security
CESG CAS	National (UK)	Organisational security
CESG CCP	National (UK)	Individual qualification
CESG CHECK	National (UK)	Individual qualification
CESG CLAS	National (UK)	Individual qualification
CESG CPA	National (UK)	Organisational security
CESG CTAS	National (UK)	Organisational security
CISSP	International	Individual qualification
Common Criteria	International	Organisation security
CREST	National (UK)	Individual qualification
Cyber Essentials	National (UK)	Organisational security
Cyber Scheme	National (UK)	Individual qualification
ISO/IEC 27001	International	Organisational security
PCI DSS	International	Organisational security
Tiger Scheme	National (UK)	Individual qualification

Table 1: Assurance Schemes Reviewed

All of the gathered information was used to: (i) define a consistent and coherent assurance terminology to clearly define assurance schemes, targets, techniques, evidence and the relationships between them; (ii) define a full assurance technique framework, including 25 assurance techniques classified into 6 assurance technique categories, and the relationships between them (e.g., how the outputs from some are used as inputs to others); (iii) analyse and study the current assurance technique landscape; and (iv) propose recommendations for future assurance schemes.

[1] http://samate.nist.gov/Main_Page.html

[2] A comprehensive list of SAMATE publications can be found at: http://samate.nist.gov/index.php/SAMATE_Publications.html

Terminology

The use of consistent terminology aids comprehension of meaning and facilitates the process of collecting reliable data within the survey. However, this study detected, through the review of related literature and publicly available information about assurance schemes, that there were inconsistencies and incoherences in the names and ways assurance techniques are referred to from different sources. Therefore, the first contribution of this study is a terminology to describe four basic components of assurance. Each component is described below, and their relationships collectively illustrated in Figure 2.

Assurance Scheme. This encompasses both standards and qualifications. For both, at least one assurance target is set. In some assurance schemes, there are explicitly defined assurance techniques that should be used to assess targets. For others, these are set and enforced through an external body (e.g., an accreditation body).

Assurance Target. An assurance target may be either a security control (e.g., asset management) or the competence requirements to assess such security controls (e.g., an individual must possess a certain qualification).

Assurance Technique (also known as an Assurance Activity). A method of assessing an assurance target. There are two types of assurance techniques. Those which assess security controls (e.g., penetration testing) and those that assess the competence requirements for using those assurance techniques (e.g., a multiple choice or lab-based exam).

Audit and Assessment Evidence. The use of an assurance technique to assess an assurance target generates audit or assessment evidence. Such evidence is used to assess compliance to an assurance scheme.

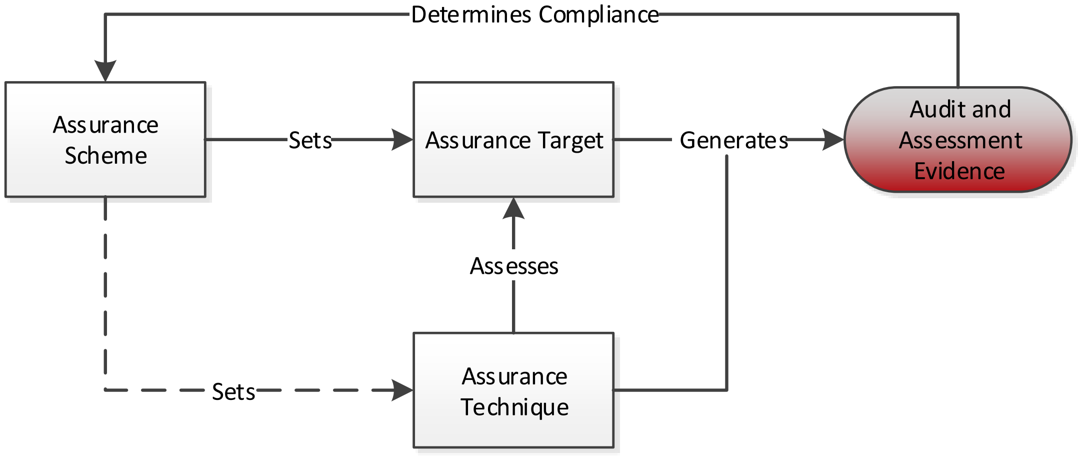


Figure 2: Assurance Activities

Assurance Techniques

Potential variations of assurance techniques are abundant. Therefore, the definition of a consolidated set of assurance techniques is paramount to allow for consistency within the survey and ensuing analysis. This study defines 25 high-level assurance techniques, which are split over 6 categories. Four of these categories represent the broad techniques for assessing assurance targets, in the traditional sense of a security control: Review; Interview; Observe and Test. This is supplemented by a fifth category, Independent Validation, which represents third-party assessment. The final category is Individual Competence, which contains assurance techniques that assess an individual's competence for using other assurance techniques (e.g., as part of a qualification).

This set of assurance techniques must be distinguished from two meta-techniques. The first of these is the **audit**, which is more appropriately defined as a process in which other assurance techniques are used to determine conformance to a specification. Assurance techniques in this context generate **audit evidence**. Such assurance techniques may be used directly by **auditors** (i.e., one or more individuals conducting an audit), although equally, an auditee (i.e., the client undergoing the audit) may also use assurance techniques, or procure services that use them (e.g., penetration tests), for which the audit evidence may be used by an auditor.

The second is **risk assessment**, which can be broken down into the consolidated steps of: asset identification; threat assessment; vulnerability assessment; risk evaluation (i.e., computing a measure of "risk"); and the recommendation of countermeasures. The assurance techniques that we have defined here are predominantly concerned with that of vulnerability assessment, although some assurance techniques contribute in full or part to the two prior steps (e.g., asset identification is a fundamental step of architectural reviews of operational systems, while threat assessment is explicitly defined here). The appropriate choice of assurance techniques here is paramount, as it is the outputs of these techniques that provide the variables for risk computation, which ultimately influences choices surrounding risk treatment (e.g., the implementation of new security controls). This importance for appropriate assurance technique choice can be extended when examining their role in **risk management**, which goes beyond the scope of a single risk assessment through monitoring and reviewing organisational risk over time. Controls may be implemented as part of the risk assessment process; the level of risk, pre and post-treatment, will then influence the choice of assurance techniques that are used within subsequent iterations of risk assessments. Therefore, if inappropriate assurance techniques are used it can have a wider impact on the risk management process.

The definition of the 25 high-level assurance techniques organised in 6 categories is provided below. Figure 3 visualises assurance techniques' categorisation and their relationships.

Review

Review of Documented Policies, Procedures, and Processes - The process of analysing the documented specifications (e.g., procedures and security properties) and processes (e.g., managerial) for a component or system under assessment.

Review of Client-Completed Self-Assessment Form - An analysis of a client submitted review of their implementation of assurance targets as set out within an assurance scheme. Self-assessment forms typically consist of a multitude of questions that a client must answer is multiple choice or narrative form.

Threat Assessment - A multi-stage process used to identify and rank the threats to computer software, a component, or IT system. Threat analysis builds upon the analysis of sub-processes such as asset identification and architectural reviews against a security policy.

Architectural Review - An analysis of the components (type, quantity, configuration, etc.) and their relationships within a piece of software, component, or system to determine if their implementation meets a desired security policy.

Configuration Review - A review of the way a system or its software has been configured to see if this leads to known vulnerabilities. Configuration reviews can be passive (e.g., manually checking software versions for known vulnerabilities) or active (e.g., automated build review scanners).

Source Code Review - The examination of source code to discover faults that were introduced during the software development process. Source code reviews are predominantly manual; however, they may be supplemented with automated techniques (e.g., using static analysis tools).

Observe

Observe - The process of watching a live, operational system to identify real-world deviations from documented assurance targets.

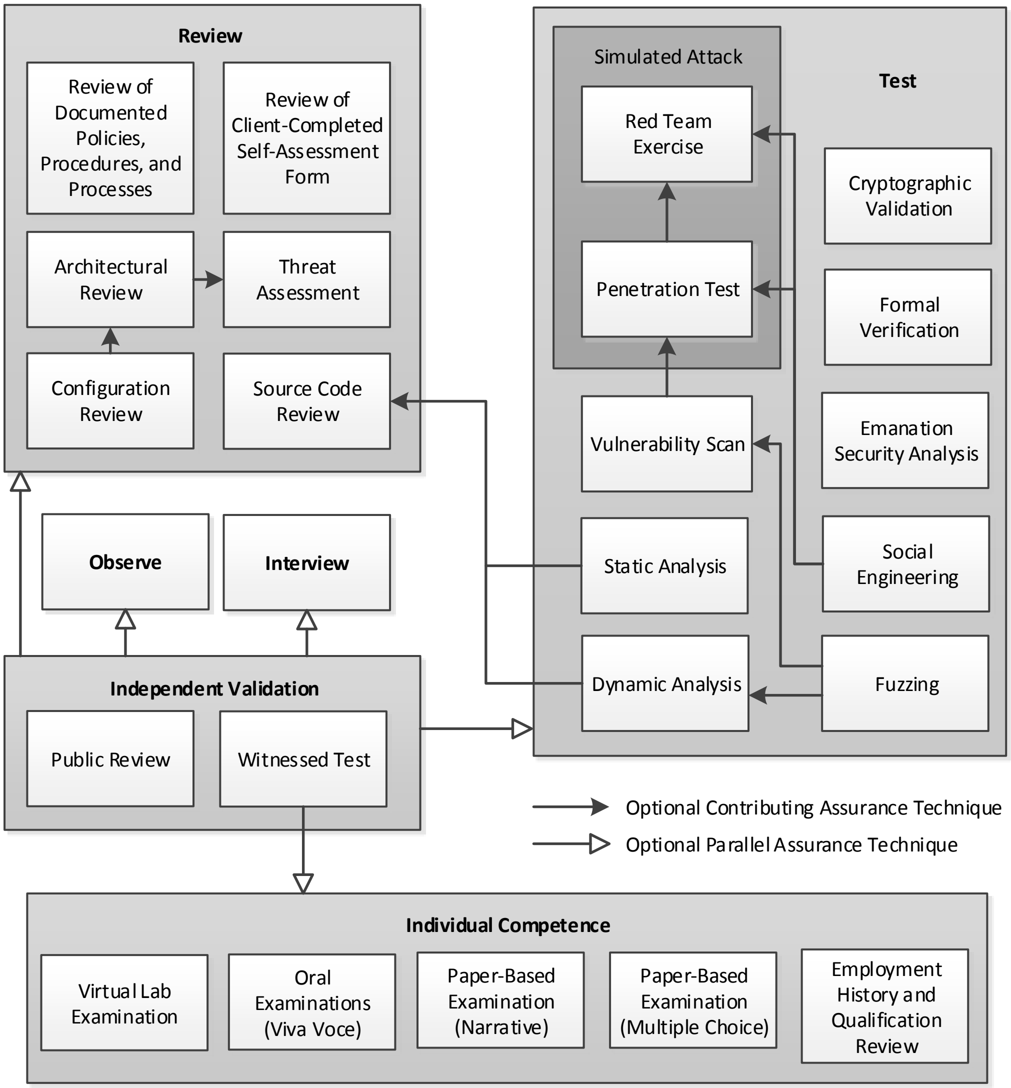


Figure 3: Assurance Activities

Interview

Interview - The process of questioning one or more individuals about security-related matters within the organisation being assessed through any medium (e.g., in person or virtually).

Test

Red Team Exercise - A simulated attack on a system that is given more freedom than is available during a penetration test, in order to more realistically simulate a real-world malicious attacker. This freedom is given in terms of the engagement's duration (e.g., often months in duration), available human resources (e.g., large teams built around individuals with different specialisms), allowed use of tools (e.g., a heavy use of social engineering is common), and restriction of defender knowledge to test their day-to-day responses to cyber threats.

Penetration Test - A simulated attack on a component or system using similar techniques to that of a real-world malicious attacker. A penetration test may build upon a vulnerability assessment; however, it differs in having an implicit or explicit goal that the assessment attempts to realise (e.g., compromise sensitive data or obtain a certain level of network access). Typically this requires vulnerabilities to be exploited, which would not be undertaken within a vulnerability assessment.

Vulnerability Scan - The process of using an automated scanner on a web application or network to identify vulnerabilities. Discovered vulnerabilities are not exploited.

Social Engineering - An attempt to manipulate one or more human users into performing an action that does not conform to operational procedures. This can be conducted in a manner that is goal-based (e.g., access data) or audit-based (e.g., the percentage of a department vulnerable to a spear phishing attack).

Static Analysis - Without executing computer software, static analysis attempts to debug and identify potential software vulnerabilities through an analysis of its source code. Static analyses are predominantly automated; however, they may contain some elements of manual interaction (e.g., in order to understand the context and implications of the results). Human-led analyses fall under source code review.

Dynamic Analysis - Once computer software has been executed, this technique attempts to debug and identify potential software vulnerabilities through active methods (e.g., inputting unexpected data through fuzzing) and passive methods (e.g., memory analysis).

Fuzzing - The process of injecting erroneous and unexpected data into an input field in order to trigger faults (e.g., crashes and exceptions) that could be leveraged to discover software vulnerabilities. Fuzzing may be dumb (i.e., random) or intelligent (i.e., with a knowledge of the protocol being tested).

Formal Verification - The use of mathematical techniques for assessing functional properties of information and communication systems.

Cryptographic Validation - A method used to analyse a cryptographic algorithm and/or its implementation within a component or system (e.g., entropy testing).

Emanation Security Analysis - One or more methods used to assess device emanations (e.g., electromagnetic or sound emanations) for the unintentional leakage and disclosure of information.

Independent Validation

Independent validation occurs when a third party is used to verify the assessment methodology of an assurance technique, or otherwise validate the results of its assessment of assurance targets.

Witnessed Test - The use of an independent witness to provide a second level of verification that the results of an assurance technique are as described.

Public Review - The process of opening a technology, component, or system to wider review by the public. Public reviews may be of documents (e.g., drafts of future cryptographic algorithms) or live systems (e.g., bug bounties).

Individual Competence

This category describes assurance techniques that assess an individual's competency for using other assurance techniques.

Virtual Lab Examination - The use of a virtual lab environment to simulate real-world scenarios for testing a candidate's competence.

Oral Examination (Viva Voce) - The process of questioning and answering using spoken word to determine a candidates competence.

Paper-Based Examination (Narrative Form) - An assessment that uses exam papers where questions must be answered in an essay style (i.e., written as a narrative).

Paper-Based Examination (Multiple-Choice - An assessment that uses exam papers where questions have multiple pre-prepared answers, of which the candidate must select one or a subset.

Employment History and Qualification Review - A review of the work history and experience of an individual. This includes the validation of pre-requisite qualifications.

Use of Assurance Techniques within Assurance Schemes

To further understand how assurance techniques are used in practice, it is required to study the role they play in particular assurance schemes. In this section, a descriptive analysis of the use of assurance techniques within assurance schemes is performed. Data for this was collected through an in-depth review of publicly available information about the 17 assurance schemes mentioned earlier, and targeted interviews to confirm and/or complete missing/incomplete information.

For each of the 25 assurance techniques, data was gathered about which of the 17 assurance schemes uses them. Then, for each assurance technique within each assurance scheme, the following data was gathered:

- **Intended Outcome**: A qualitative description of what an assurance technique is intended to achieve for a particular assurance scheme and how the results are reported (e.g., pass or fail for an examination, or the choice of metrics to report vulnerabilities).
- **Lifecycle Stage**: The stage of a component or system's lifecycle in which an assurance technique is predominantly used. Five criteria are outlined:
  - Pre-Deployment - Before a component or system has been put into an operational environment.
  - Operational - Once the system is live.
  - Acquisition - An assessment prior, during, or after a component or system has been procured, but before it is deployed operationally by the purchasing organisation.
  - End of Life - When a system is being is being removed from active use.
  - N/A - Not applicable (e.g., for assurance techniques that assess individual competence).
- **Qualifications and/or Certifications needed:** The required prerequisites to be allowed to conduct an assurance technique. These can be applied at two levels: that of the individual (e.g., personal qualifications or security clearance) or that of the organisation (e.g., to be a certification body or other "approved" company).
- **Sensitivity of Input Material:** This study uses the data classifications mentioned below and outlined by the UK Cabinet Office's 2013 publication, "Government Security Classifications" [18] (readers are referred to the UK Cabinet Office publication for a full description of each classification).
  1. OFFICIAL
     (a) OFFICIAL-SENSITIVE COMMERCIAL
     (b) OFFICIAL-SENSITIVE PERSONAL.
  2. SECRET
  3. TOP SECRET
- **Extent of Contribution:** Three criteria are defined to determine a level of extent that an assurance technique contributes to the collective assurance targets set out by an assurance scheme.
  1. Xsig - An assurance technique is mandatory and its contribution to the scheme is significant. The term significant is qualified as an assurance technique that provides assessment to a large proportion of security controls or requirements, or any assurance technique that is a necessary prerequisite to another Xsig activity, regardless of the proportion of security controls and requirements assessed.
  2. Xmin - An assurance technique is mandatory; however, it's contribution to the scheme in minor. The term minor is qualified as an assurance technique that is only applicable to the assessment of a small proportion of security controls or requirements, and is not a necessary prerequisite to an Xsig assurance technique.
  3. Xop - An assurance technique is suggested, but an alternative could be used in its place to assess the outlined security controls and requirements.

Appendix A: Assurance Technique Characteristics per Assurance Scheme details all the results obtained. The criteria represent the columns, and each row describes the characteristics of an assurance technique within the context of a particular scheme. A tabular approach enables ease of analysis, and if interactive, the sorting and filtering by particular characteristics. Such functionality enables it to serve as a valuable descriptive resource on the contemporary usage of assurance techniques, both for the design of future schemes, and if in the public domain, those wishing to procure assurance techniques for use within assurance schemes.

Next, a high level analysis of the table in Appendix A is reported. First, Figure 4 lists all the assurance techniques and how often they are used within assurance schemes (only reported values where explicit mentions of use of assurance technique was found within an assurance scheme). It can be seen that *Review of Documented Policies, Procedures and Processes* was found to be the most widely used assurance technique across all the organisational security schemes that were surveyed during this research. On the other hand, none of the assurance schemes reviewed included *Static Analysis, Dynamic Analysis* and *Public Reviews*.

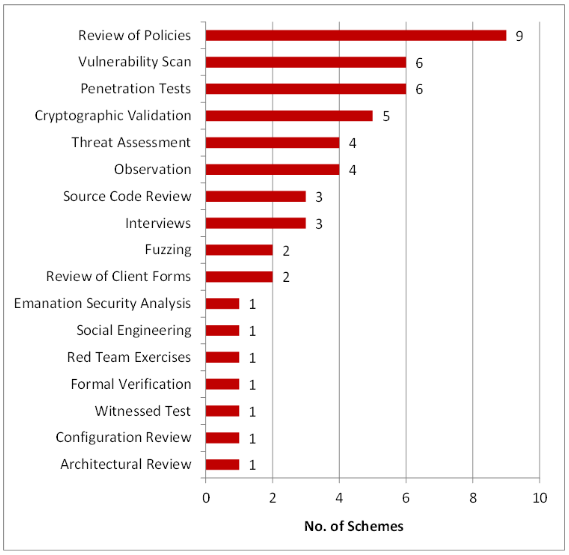


Figure 4: Number of Assurance Schemes in which each Assurance Technique is employed.

Having a closer look at individual variables reported in Appendix A, the *intended outcome* variable contains a qualitative description of what the technique is aiming to achieve for that particular assurance scheme. This information is important to contextualize the effectiveness of any technique, as the effectiveness of an assurance technique is perceived with respect to its intended outcome. It can be seen that the intended outcome of the assurance technique often depends on the assurance scheme it is employed in. For example, *Review of Documented Policies, Procedures and Processes* is used to perform an assessment statement to outline risks and recommendations when it is used as part of the CESG Tailored Assurance Scheme (CTAS). On the other hand, it is used ensure compliance with established standards and provide audit trails for other assurance schemes like ISO/IEC 27001 and CESG Assured Services (CAS). Thus, the same technique can be used for different objectives depending on the assurance scheme.

An interesting observation regarding the *Lifecycle stage* is that **most techniques are used for Operational** systems regardless of the assurance scheme they are used in. One notable exception to this is the *Common Criteria* assurance scheme. It can be seen from the table that assurance techniques like *Review of Documented Policies, Procedures and Processes, Source Code Review, Penetration Testing, Vulnerability Scans* and *Cryptographic Validation* are used in the **Pre-Deployment** phase even though they are used for **Operational** systems when employed in other assurance schemes.

Regarding *extent of contribution*, a general observation is that most assurance techniques that are explicitly mentioned to be used within particular assurance schemes are mandatory and its contribution to the scheme is significant (Xsig). There are only few exceptions to this (16 out 92 cases), in which assurance techniques were deemed to be either mandatory but with a minor contribution (7 cases) or were optional (9 cases). Notable cases were those of *Penetration Testing* and *Vulnerability Scans*, which are both optional in ISO/IEC 27001, yet they were rated among the most cost-effective assurance techniques by the security practitioners that filled out the aforementioned on-line survey. Another interesting observation is that an assurance technique can be a significant part of an assessment for a particular assurance scheme while it may be optional for an assessment for a different assurance scheme. For example, *Source Code Review* are mandatory and a **significant** part of a *Common Criteria* evaluation but they are an **optional** part of a *CTAS* evaluation and they may or may not be employed. Moreover, in other assurance schemes such as *PCI DSS*, for example, *Source Code Reviews* are not employed at all.

Assurance Techniques and Security Controls

Assurance schemes like Cyber Essentials clearly dictate the assurance technique to be used to assess the security controls it mandates (e.g., review of self-assessment forms to check the 5 Cyber Essentials security controls). However, there are many other assurance schemes in which this is unclear. Furthermore, the effectiveness of an assurance technique is obviously relational to the security control (i.e., assurance target) in which it is assessing.

A preliminary mapping of assurance techniques to the high-level security families of ISO/IEC 27001 has been produced. It is believed that such a mapping will aid in the development of compliance evaluation criteria for the security controls outlined in future assurance schemes. ISO/IEC 27001 was chosen due to its widespread international adoption and position as the de facto MSS for information security, and the frequent use as a baseline for other assurance schemes. However, there are mappings of ISO/IEC 27001 to other schemes, like Appendix H of [14], which is a mapping between the security controls of ISO/IEC 27001 to NIST 800-53, and then from NIST 800-53 to ISO/IEC 15408 (Common Criteria).

Appendix B: Mapping of Assurance Techniques to Assurance Controls outlines the mapping between 20 assurance techniques and the 35 ISO/IEC 27001 (Annex A) control families. Assurance techniques within ISO/IEC 27001 broadly fall into two categories: First, those used or procured (from a third party) by a client (i.e., the auditee) which generate audit evidence. Second, those used by an auditor. In some cases, assurance techniques may bridge the two categories (e.g., for internal audits). It is important to clarify for the reader, that in standards such as ISO/IEC 27001, auditors are free to use any assurance technique they deem adequate for assessing an assurance scheme's requirement, although exceptions to this occur in other schemes, where particular requirements mandate certain assurance techniques be used in their assessments for certain security controls (e.g., in PCI DSS).

The following mapping is not intended to dictate assurance technique usage in either category. Instead, it is intended to provide guidelines on the most appropriate assurance techniques for particular security controls, with the intention of facilitating the design of security evaluation criteria for future assurance schemes. To provide a robust framework for this analysis, a set of principles was defined.

Core Principle: An assurance technique contributes directly to an audit and is conducted by the auditor, or the assurance technique is used by the auditee or a third-party to generate audit evidence. Sub-principles:

1. Where possible, assurance technique usage is pragmatic (i.e., they provide a valid contribution, or can be seen to provide one in the design of future assurance schemes, while ignoring "potential" or "abstract" inclusions).
2. An assurance technique may provide audit evidence while not being a direct assessment of a security control. An example is a threat assessment. This may include the definition of organisational requirements and identification of assets, which can contribute to control families such as "A.6.1 Internal Organisation".
3. Relationships between assurance techniques were defined in Figure 2. If an assurance technique is set which has "optional contributing" assurance techniques, it does not mean they also must be enabled in this mapping, and vice versa. An example is penetration testing, where multiple sub-techniques can contribute, and may or may not be used depending on the assessor.
4. Assurance techniques are associated with control families, based upon their potential to assess that control family. A more granular level of effectiveness exists beyond this; the mapping does not dictate that two assurance techniques are equally effective for assessing that control family.

A preliminary review of the quantity of assurance techniques within each control family was conducted. A table representing these figures can also be found in *Appendix B: Mapping of Assurance Techniques to Assurance Controls*. The table shows a clear trend in the range of 5 to 10 assurance techniques. A qualitative review of these assurance techniques demonstrates the dominance of the "big three" audit techniques (review, interview, observe). This, however, is not surprising given that ISO/IEC 27001 is used to enforce an ISMS, where processes reign over the specifics of security controls. For the control families at the higher end of this range, we begin to see greater use of assurance techniques where an element of user behaviour is considered in the security controls contained. For example, social engineering appears frequently here. Control families where there are technical controls (a minority) there is as would be expected, a large number of assurance techniques that could potentially be used in their assessment; however, contraints of real-world environments may restrict the use of some of these (e.g., due to closed source software).

Perceptions of Assurance Techniques

Expert knowledge from 115 security professionals was gathered via an on-line survey focusing on economic-related variables, including experts' perceptions of requirements (number of people, expertise, and time) and cost to conduct each assurance technique as well as effectiveness and complementary assurance techniques. Note that these variables can largely vary depending on the assurance target being assessed. Indeed, many of the techniques depend on the nature and size of the organization to be assessed, the environment and conditions of evaluation, etc.

In order to enable meaningful comparisons across techniques and with a view to maximising fairness of any such comparison, survey respondents where suggested to consider a commercial medium-size scenario for all assurance techniques as follows:

"For each assurance technique, assume a commercial target of medium size. Examples: company with 250 employees; infrastructure with 16 external IPs or 150 internal IPs; web application with one database and 100 static or dynamic pages; product like a Firewall, Router or Switch."

Stakeholder Composition

Primary Role: Figure 5 shows the distribution of the different roles that the respondents of the survey have in their day to day jobs. As can be seen from the figure, 64% of respondents in our sample are Security Practitioners. This is an advantage for our research as the practitioners actually perform the assurance techniques, which are analyzed in this project, and have a fair idea about how they work and therefore have provided valuable insight from their point of view.

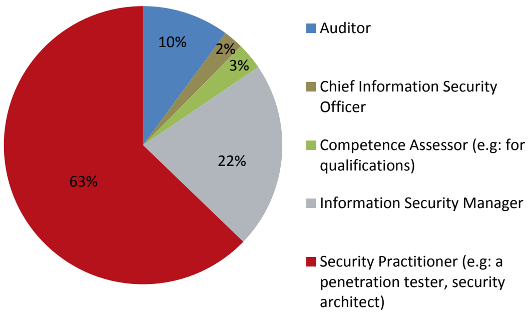


Figure 5: Primary Role of Survey Participants

Assurance Experience: Figure 6 shows the number of years respondents spent in the information security industry. Notably, **56,45% respondents have spent over 15 years in the security industry**, and 91.81% over 5 years.

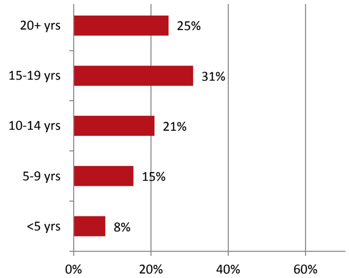


Figure 6: Number of years spent in security industry

Assurance Schemes: Respondents were also asked about the assurance schemes they are involved in their day-to-day role. Figure 7 shows the results. As can be seen in the figure, we found a reasonably large variety of assurance schemes that the respondents are familiar with, covering most of the assurance schemes reviewed in this document.

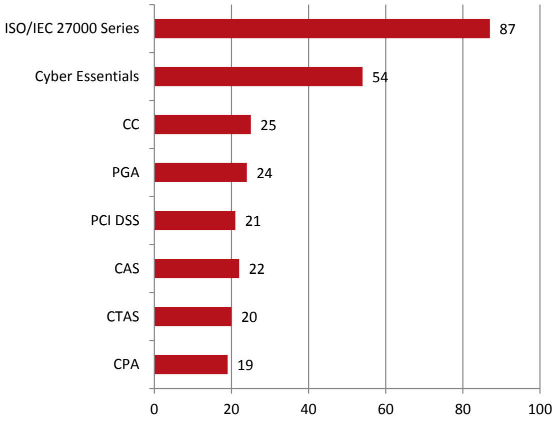


Figure 7: Assurance Schemes

Individual Qualifications: Figure 8 shows the number of instances of each of the individual qualifications encountered. It is to be noted here that the total number of responses to this question is more than the total number of respondents, because respondents were allowed to choose multiple qualifications to be able to list all their qualifications.

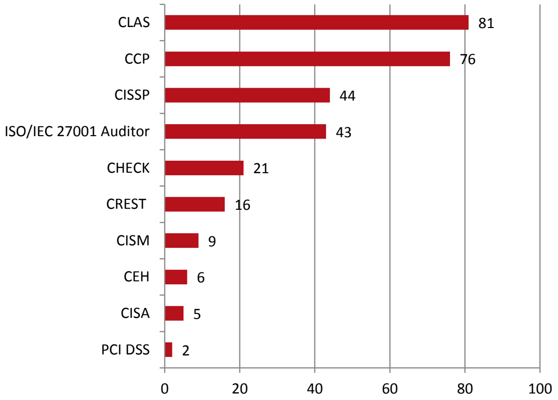


Figure 8: Individual Qualifications

Confidence Level: Respondents were asked to select their level of confidence in the answers they provided for each of the assurance technique. The results are shown in Table 2. The respondents were able to select 3 levels, namely, **Low, Medium** and **High**. *Architectural Reviews* and *Penetration Testing* have been found to be the two assurance techniques where the highest proportion of respondents answered with **High** level of confidence (62% and 61% respectively).

Assurance Technique	Confidence Level			**Total**
	Low	Med	High	Resp.
Review of Policies, etc.	4%	40%	**56%**	72
Review of Client Forms	16%	**53%**	31%	64
Architectural Review	-	38%	**62%**	64
Configuration Review	6%	**55%**	39%	56
Source Code Review	18%	**47%**	35%	49
Observation	12%	**64%**	24%	41
Interviews	9%	41%	**50%**	54
Red Team Exercises	7%	**52%**	41%	42
Penetration Tests	5%	34%	**61%**	56
Vulnerability Scan	7%	42%	**51%**	55
Social Engineering	25%	**40%**	35%	40
Threat Assessment	4%	46%	**50%**	54
Static Analysis	30%	**67%**	3%	30
Dynamic Analysis	28%	**65%**	7%	29
Fuzzing	41%	**48%**	11%	27
Formal Verification	16%	**53%**	31%	32
Cryptographic Validation	26%	**52%**	22%	31
Emanation Security Analysis	35%	**54%**	11%	26
Witnessed Test	10%	**63%**	27%	30
Public Review	**46%**	**46%**	8%	26

Table 2: Confidence of respondents in their input

Assurance Techniques Characteristics

Assurance Technique	**Number of People**				**Total**
	1	**2**	**3**	**4+**	**Resp.**
Review of Policies	**54%**	37%	8%	1%	73
Review of Client Forms	**81%**	13%	3%	3%	64
Architectural Review	**74%**	17%	6%	3%	64
Configuration Review	**61%**	30%	5%	4%	57
Source Code Review	**43%**	33%	10%	15%	49
Observation	**61%**	32%	5%	2%	41
Interviews	35%	**56%**	9%	-	54
Red Team Exercises	11%	30%	28%	**31%**	43
Penetration Tests	18%	**64%**	16%	2%	56
Vulnerability Scan	**80%**	16%	4%	-	55
Social Engineering	40%	**42%**	5%	13%	40
Threat Assessment	**72%**	22%	2%	4%	54
Static Analysis	**70%**	20%	7%	3%	30
Dynamic Analysis	**62%**	24%	7%	7%	29
Fuzzing	**66%**	26%	-	8%	27
Formal Verification	31%	**41%**	13%	15%	32
Cryptographic Validation	**58%**	26%	7%	9%	31
Emanation Sec. Analysis	**46%**	**46%**	8%	-	26
Witnessed Test	**50%**	33%	17%	-	30
Public Review	**48%**	28%	8%	16%	25

Table 3: Number of people required

Number of People Required: The results are shown in Table 3. It can be seen from the results that most respondents believed that almost all the assurance techniques can be successfully performed for the scenario given with **2 people**. Furthermore, a vast majority stated that *Review of Client-Completed Self-Assessment Forms*, *Architectural Reviews*, *Vulnerability Scans*, *Threat Assessment*, and *Static Analysis* can be successfully performed for the scenario given with **only 1 person**.

A notable exception is *Red Team Exercises* where more than 50% of the respondents (59% to be exact) believe that it requires **more than 2 people** to complete this technique. For all other techniques, at least 50% of the respondents believe that at most 2 people are required for the technique to be completed for the given example scenario.

Expertise Required: Table 4 shows the results obtained regarding the level of expertise respondents thought was required to perform the particular assurance techniques successfully. Looking at the results, we find that different levels of expertise are required for different techniques in the type of scenario we described to the respondents. Techniques such as *Architectural Review, Interviews, Threat Assessment* and *Cryptographic Validation* seemingly require **Senior** professionals (72%, 66%, 61% and 61% respectively).

Assurance Technique	**Expertise Required**				**Total**
	P	**P(W)**	**S**	**Pr**	**Resp.**
Review of Policies	33%	**35%**	32%	-	72
Review of Client Forms	**45%**	26%	27%	2%	64
Architectural Review	8%	9%	**72%**	11%	64
Configuration Review	21%	**46%**	33%	-	57
Source Code Review	19%	18%	**45%**	18%	49
Observation	27%	**46%**	22%	5%	41
Interviews	11%	16%	**66%**	7%	55
Red Team Exercises	9%	10%	**50%**	31%	42
Penetration Tests	12%	29%	**52%**	7%	56
Vulnerability Scan	**44%**	40%	16%	-	55
Social Engineering	20%	**40%**	35%	5%	40
Threat Assessment	6%	20%	**61%**	13%	54
Static Analysis	27%	33%	**40%**	-	30
Dynamic Analysis	21%	34%	**45%**	-	29
Fuzzing	30%	**33%**	**33%**	4%	27
Formal Verification	12%	25%	**47%**	16%	32
Cryptographic Validation	6%	10%	**61%**	23%	31
Emanation Sec. Analysis	8%	**46%**	35%	11%	26
Witnessed Test	7%	37%	**53%**	3%	30
Public Review	**36%**	28%	24%	12%	25

Table 4: Expertise required to perform each technique — P: Practitioner; P(W): Practitioner with Supervision; S: Senior; Pr: Principal.

Another interesting observation is that some techniques are more likely to be performed by **Practitioners** if they are provided with supervision. Looking at the table, we find a big jump in the proportion of respondents who think that techniques like *Configuration Review, Social Engineering* and *Emanation Security Analysis* can be performed by **Practitioners with supervision** as compared to without supervision. This is an important aspect to consider as it has implications in terms of the resources required for the performance of the technique which would eventually contribute towards its cost. There also seems to be 3 assurance techniques that could be conducted most of the time by **practitioners alone or with little supervision**: *Review of Client-Completed Self-Assessment Forms*, *Vulnerability Scans*, and *Public review.*

Assurance Technique	**Time required to complete this technique**						**Total Responses**
	<1 day	1 day	2 days	2-10 days	10-20 days	20+ days	
Review of Policies	3%	9%	12%	**61%**	11%	4%	66
Review of Client Forms	19%	28%	**30%**	20%	3%	-	64
Architectural Review	3%	13%	19%	**50%**	13%	2%	62
Configuration Review	9%	16%	18%	**40%**	17%	-	57
Source Code Review	2%	2%	10%	**31%**	**31%**	24%	49
Observation	3%	12%	39%	**44%**	2%	-	41
Interviews	18%	11%	31%	**33%**	7%	-	55
Red Team Exercises	-	14%	29%	**36%**	15%	6%	42
Penetration Tests	2%	-	16%	**59%**	21%	2%	56
Vulnerability Scan	14%	24%	**38%**	22%	2%	-	55
Social Engineering	10%	15%	27%	**42%**	3%	3%	40
Threat Assessment	-	19%	**33%**	**33%**	11%	4%	54
Static Analysis	3%	-	**57%**	20%	10%	10%	30
Dynamic Analysis	-	10%	**38%**	**38%**	7%	7%	29
Fuzzing	-	18%	30%	**37%**	11%	4%	27
Formal Verification	3%	6%	13%	**50%**	10%	18%	32
Crypto Validation	-	10%	10%	**42%**	16%	22%	31
Emanation Sec. Analysis	-	8%	**42%**	**42%**	4%	4%	26
Witnessed Test	3%	3%	**54%**	37%	3%	-	30
Public Review	-	12%	8%	**44%**	12%	24%	25

Table 5: Time required to complete each assurance technique

Time Required: Table 5 shows the results of the question which asked the respondents to enter the amount of time they thought it would take to complete the particular technique successfully for the type of scenarios given.

The duration of any assurance technique can be a good measure of the effort required to complete it. From the results shown in the table, we find that most of the techniques can be completed **within 10 days**.

There are two assurance techniques for which a vast majority believe that they can be completed **within 2 days**. These techniques are *Review of Client-Completed Self-Assessment Forms* and *Vulnerability Scans* (77% and 76% respectively).

It is also noteworthy that an important fraction of our respondents think that *Source Code Review*,*Formal Verification*, *Cryptographic Validation*, and *Public Review* may take **more than 20 days** to be completed. Thus, we observe a large and varied spectrum of completion times where some assurance techniques may be completed within a day while others may take more than 2 months according to some respondents.

Assurance Technique	Effectiveness					**Total Responses**
	Excellent	Very Good	Good	Fair	Poor	
Review of Policies	6%	18%	**46%**	30%	-	71
Review of Client Forms	3%	3%	33%	**34%**	27%	64
Architectural Review	6%	41%	**45%**	8%	-	63
Configuration Review	2%	26%	**46%**	26%	-	57
Source Code Review	6%	25%	**49%**	10%	10%	49
Observation	2%	22%	32%	**44%**	-	41
Interviews	4%	31%	**33%**	27%	5%	55
Red Team Exercises	16%	36%	**38%**	5%	5%	42
Penetration Tests	13%	**50%**	32%	5%	-	56
Vulnerability Scan	5%	33%	**34%**	24%	4%	55
Social Engineering	7%	15%	**37%**	33%	8%	40
Threat Assessment	4%	33%	**46%**	17%	-	54
Static Analysis	-	20%	30%	**47%**	3%	30
Dynamic Analysis	-	17%	31%	**52%**	-	29
Fuzzing	-	22%	22%	**52%**	4%	27
Formal Verification	-	31%	**38%**	28%	3%	32
Cryptographic Validation	6%	26%	**45%**	23%	-	31
Emanation Sec. Analysis	-	15%	**39%**	38%	8%	26
Witnessed Test	3%	20%	**40%**	27%	10%	30
Public Review	4%	12%	27%	**38%**	19%	26

Table 6: Effectiveness of Each Assurance Technique

Assurance Technique	Cost					**Total Responses**
	Extremely Expensive	Very Expensive	Expensive	Moderate	Cheap	
Review of Policies	-	-	14%	**69%**	17%	72
Review Client Forms	-	-	5%	36%	**59%**	64
Architectural Review	-	5%	28%	**58%**	9%	64
Configuration Review	-	2%	21%	**67%**	10%	57
Source Code Review	18%	20%	**29%**	**29%**	4%	49
Observation	-	-	17%	**63%**	20%	41
Interviews	2%	2%	25%	**55%**	16%	55
Red Team Exercises	2%	17%	**52%**	24%	5%	42
Penetration Tests	2%	10%	**52%**	34%	2%	56
Vulnerability Scan	-	2%	20%	29%	**49%**	55
Social Engineering	-	2%	23%	**55%**	20%	40
Threat Assessment	-	4%	28%	**57%**	11%	54
Static Analysis	-	3%	23%	**64%**	10%	30
Dynamic Analysis	-	-	35%	**55%**	10%	29
Fuzzing	4%	7%	15%	67%	7%	27
Formal Verification	22%	**25%**	22%	31%	-	32
Cryptographic Validation	13%	26%	**29%**	26%	6%	31
Emanation Sec. Analysis	4%	23%	31%	**34%**	8%	26
Witnessed Test	-	10%	**40%**	37%	13%	30
Public Review	4%	8%	15%	31%	**42%**	26

Table 7: Cost of the Assurance Techniques

Effectiveness: We asked the respondents to state how effective they thought the assurance techniques were *"in achieving its objectives"*. The results are shown in Table 6 and they show that most of the assurance techniques have **at least Good** effectiveness according the respondents (13 out of 20 techniques). However, there are 5 assurance techniques for which the majority (at least 50%) of respondents think that the effectiveness is **Fair at best**. These techniques are *Review of Client-Completed Self-Assessment Forms, Static Analysis, Dynamic Analysis, Fuzzing* and *Public Review.*

Penetration Tests are the only assurance technique for which the majority of the respondents (50%) feel that the effectiveness is **Very Good**. The two assurance techniques which have a considerable proportion of respondents rating the effectiveness as **Excellent** are *Penetration Tests* and *Red Team Exercises.* These can be considered to be the best perceived techniques in terms of effectiveness by the respondents in our sample.

The two assurance techniques which have a comparatively higher proportion of respondents who rated their effectiveness as **Poor** are *Review of Client-Completed Self-Assessment Forms* and *Public Reviews.* These are considered the least effective assurance techniques by the respondents.

Cost: Respondents could also express their opinion on the cost of conducting each assurance technique in the type of scenarios given. The results are shown in Table 7.

We find that *Review of Client-completed Self-assessment Forms* is considered to be by far the **cheapest** assurance technique by a large majority of the respondents (59%) in the described scenario, followed by *Vulnerability Scans*, and *Public Review.*

There is also a group of assurance techniques, whose cost for the scenarios described is perceived to be **moderate**: *Review of Documented Policies, Procedures and Processes, Architectural Review, Configuration Review, Observation, Interviews, Social Engineering, Threat Assessment,* and *Dynamic and Static Analysis.*

There are 4 techniques which are considered to be **at least expensive** by over 60% of the respondents. These techniques are *Source Code Review (67%), Red Team Exercises (71%), Penetration Testing (66%)* and *Formal Verification (69%).*

Complementary Assurance Techniques

One of the primary objectives of this research was to identify assurance techniques which are complementary to each other, providing insights on which are the assurance techniques that are used together more often than others. To this aim, we asked the respondents of the on-line survey to list up to 3 complementary assurance techniques for every assurance technique they were familiar with, which when performed together could achieve high effectiveness.

Appendix C: Complementary Assurance Techniques contains all the details of the results obtained, reporting individual bar charts showing the number of complementary assurance techniques suggested by respondents for each of the 25 assurance techniques studied. For the sake of clarity and brevity, only aggregated high-level results are reported here.

Most Commonly Chosen Techniques: Table 8 summarises the number of times each assurance technique was chosen by respondents as the first, second and third most complementary technique for other assurance techniques.

Assurance Technique	1st	2nd	3rd	Total
Review of Policies	4	5	4	13
Observation	3	2	2	7
Architectural Review	0	4	3	7
Interviews	3	1	2	6
Penetration Tests	3	0	2	5
Source Code Review	1	1	2	4
Static Analysis	3	0	0	3
Configuration Review	1	1	1	3
Vulnerability Scan	1	1	0	2
Dynamic Analysis	1	1	0	2
Review of Client Forms	0	0	2	2
Fuzzing	0	2	0	2
Witnessed Test	0	0	2	2
Threat Assessment	0	1	0	1
Formal Verification	0	1	0	1
Red Team Exercises	0	0	0	0
Social Engineering	0	0	0	0
Cryptographic Validation	0	0	0	0
Emanation Security Analysis	0	0	0	0
Public Review	0	0	0	0

Table 8: Most commonly chosen complementary techniques

Being chosen as the most common complementary technique can be interpreted as an added value to the utility of the assurance technique. If a particular assurance technique is a complementary technique for another assurance technique, the chances of it being included in different assurance schemes is higher. This supports the analysis in the previous section, which presented *Review of Documented Policies, Procedures and Processes* and *Penetration Tests* as the two most commonly used assurance techniques across various assurance schemes. The likelihood of their being chosen as complementary techniques may be a contributing factor of such widespread use across schemes.

Groups of Complementary Techniques: On further analysis of the individual distributions of the complementary techniques, 3 main clusters of assurance techniques have been identified.

1. **Observation, Interviews and Review of Documented Policies, Procedures and Processes:** Looking at Figure C1 in *Appendix C: Complementary Assurance Techniques* for *Review of Documented Policies, Procedures and Processes*, Figure C3 for *Observation* and Figure C4 for *Interviews*, we find that all these techniques are the top two most commonly selected complementary techniques of each other. This suggests that these techniques have a higher chance of being performed together for assurance schemes. Looking at *Appendix A*, we find that all these three assurance techniques in both the **PCI DSS** and **ISO/IEC 27001** assurance schemes.
2. **Vulnerability Scans and Penetration Testing:** Looking at Figure C6 in *Appendix C: Complementary Assurance Techniques*, we find that *Vulnerability Scans (25)* are the most common complementary technique for *Penetration Tests*. Similarly, we can see in Figure C7 that *Penetration Tests (25)* are the most common complementary assurance technique for *Vulnerability Scans*. Looking at *Appendix A*, we find that both these techniques are used in 5 assurance schemes, namely, **ISO/IEC 27001 (though optionally), PCI DSS, Common Criteria, CTAS** and **CPA**.
3. **Static Analysis and Dynamic Analysis:** From Figure C9 and C10 in *Appendix C: Complementary Assurance Techniques*, we see that *Static Analysis* and *Dynamic Analysis* are the most commonly chosen complementary assurance technique for each other. Looking at *Appendix A*, it seems none of assurance schemes reviewed uses these techniques.

Cost-Effectiveness of Assurance Techniques

Collected data on perceived cost and effectiveness obtained via the on-line survey was then used to derive a measure of cost-effectiveness. Details about this measure as well as all the calculations performed to get cost-effectiveness values for each assurance technique are in *Appendix E: Cost-Effectiveness Calculations.* Because of their difference in nature, it was decided to split the analysis between assurance techniques targeting security controls and assurance techniques targeting individual competences.

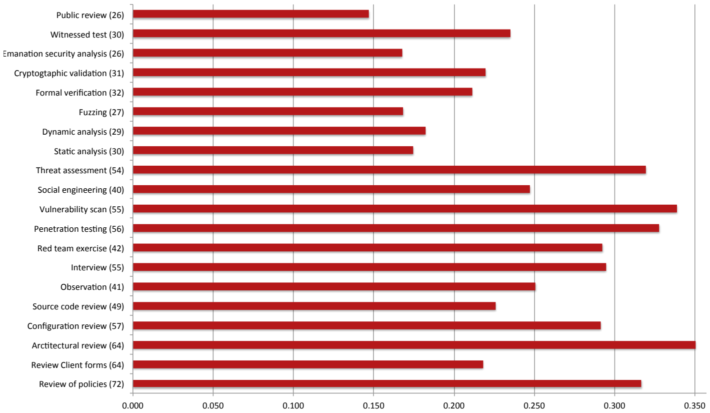


Figure 9: Cost-effectiveness of assurance techniques.

Figure 9 depicts cost-effectiveness for each of the 20 analysed assurance techniques for security controls. Architectural review, penetration testing, and vulnerability scans were perceived to be the most cost-effective assurance techniques. The least cost-effective assurance techniques were perceived to be public review, fuzzing, static and dynamic analysis, and emanation security analysis. It is also worth highlighting the confidence level of respondents, which varied in overall from 35.80% to 81.30% (see Appendix E). The most confident responders were those who provided information about the architectural review, review of policies, interview, penetration testing, vulnerability scan and threat assessment activities. On the other side, the least confident responders appears to be the ones that evaluated the static and dynamic analysis, fuzzing, emanation security analysis, and public review activities, hence the least cost-effective assurance techniques were also the ones respondents were less sure about.

Cost-Effectiveness of Assurance Techniques Combinations

We further elaborate on the combinations of assurance techniques that can provide higher levels of effectiveness and cost effectiveness. In order to identify such combinations of assurance techniques, we filtered information retrieved via the on-line survey. Specifically, we identified assurance techniques that when performed together can be highly effective. The data used for the identification of these sets was performed on the basis of metrics, i.e., the overall effectiveness, and cost effectiveness of individual assurance techniques. Specifically, combinations were restricted to sets of four assurance techniques (the ones highest rated by respondents). We expressed the effectiveness and cost effectiveness of each combination, by the product of the individual assurance activity values per se. Further information regarding the calculation of effectiveness and cost-effectiveness of individual combinations is provided in *Appendix E: Cost-Effectiveness Calculations.*

Figure 10 depicts the effectiveness of a list of combined assurance techniques, and Table 12 in *Appendix D: Combinations of Assurance Techniques* labels the list of assurance techniques in each of the combinations. Looking into Figure 10, "Comb 4." ranks first amongst all the identified sets of combined assurance techniques. More specifically, "Comb. 4" consists of the following individual assurance techniques: Penetration Tests; Architectural Review; Reviewing Documented Policies, Procedures, and Processes; Vulnerability Scans. In the second place, there is "Comb. 5" that refers to Vulnerability Scans; Architectural Review; Configuration Review; Penetration Tests, and "Comb. 10", which includes Architectural Review; Configuration Review; Penetration Tests; and Reviewing Documented Policies, Procedures, and Processes. "Comb. 3" ranks third, i.e., Red Team Exercises; Penetration Tests; Reviewing Documented Policies Procedures, and Processes; and, Vulnerability Scans. Finally, "Comb. 11" consists of the forth top ranked combination that refers to Threat Assessment; Architectural Review; Interviews; and, Reviewing Documented Policies, Procedures, and Processes.

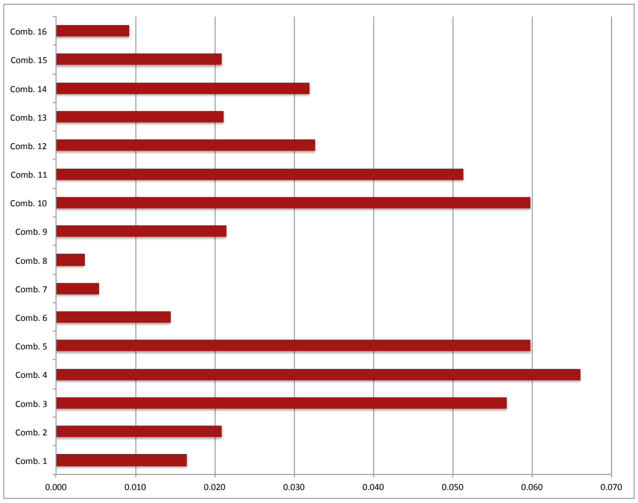


Figure 10: Effectiveness of combined assurance techniques

Amongst the list of identified combinations, the least effective combination is "Comb. 8", which consists of a combination of the following assurance techniques: Dynamic Analysis; Fuzzing; Source Code Review; and Static Analysis.

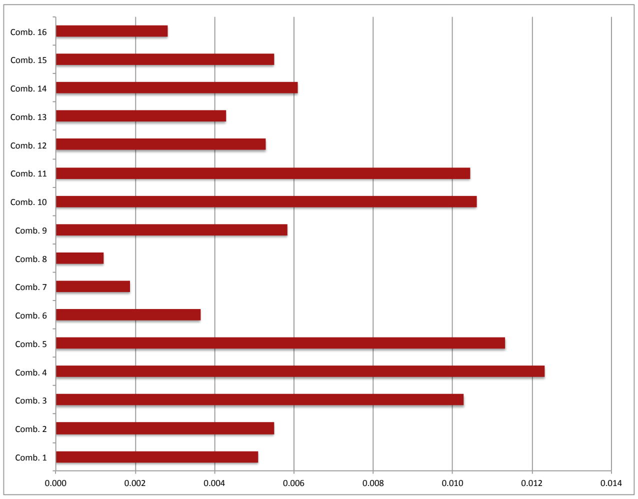


Figure 11: Cost-effectiveness of combined assurance techniques

Figure 11 depicts the cost-effectiveness of each of the identified combinations of assurance techniques. It seems that "Comb. 4" (i.e., Penetration Tests; Architectural Review; Vulnerability Scans; and, Reviewing Documented Policies, Procedures, and Processes) ranks first also when it comes to cost-effectiveness. "Comb. 5" is ranked second (i.e., Vulnerability Scans; Architectural Review; Configuration Review; and, Penetration Tests). In the third position there is "Comb. 10" (i.e., Architectural Review; Configuration Review; Penetration Tests; and, Reviewing Documented Policies, Procedures, and Processes). The list of the top five highly ranked combinations of assurance techniques, with regards to cost-effectiveness, is completed with "Comb. 3" (i.e., Red Team Exercise; Penetration Tests; Reviewing Documented Policies, Procedures, and Processes; and, Vulnerability Scans) and "Comb. 11", which includes Threat Assessment; Architectural Review; Interviews; and, Reviewing Documented Policies, Procedures, and Processes.

Cost-Effectiveness of Assurance Techniques for Individual Competences

Figure 12 depicts the overall effectiveness of techniques to assure individual competence to conduct the other assurance techniques described above based on the values respondents provided for the on-line survey. For each technique to assure individual competence, Figure 12 also includes the number of people who provided their perception of how effective each technique was.

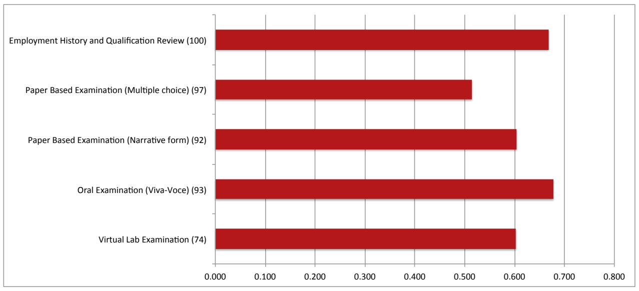


Figure 12: Perceived effectiveness of competence ATs

Oral Examination (Viva-Voce) was perceived to be the most effective one, closely followed by Employment History and Qualification Review. However, the differences of these two with respect to Paper Based Examination (Narrative form) and Virtual Lab Examination, though existing, were minimal. There was a more substantial difference with respect to Paper Based Examination (Multiple choice), which was clearly considered as the least effective technique to assure individual competence.

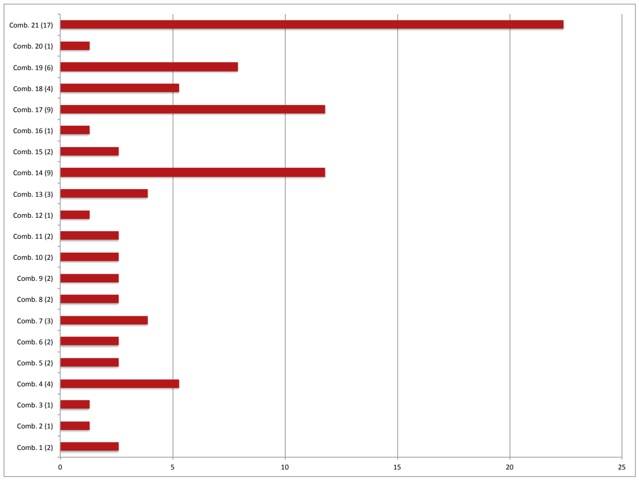


Figure 13: Perceived cost-effectiveness of competence ATs

As part of the on-line survey, another question was also asked, this time about what combination of techniques would be the most cost-effective in assessing individual competence. The results are reported in Figure 13 and Table 13 provides the mapping of each label in Figure 13 with the corresponding combination. Most respondents (76 out of 115) selected the combination of Oral Examination (Viva-Voce) and Employment History and Qualification Review, which actually consists of a combination of the top two highest rated techniques in Figure 12.

Special Scenario: ICS Case Study

This study examines the application of assurance techniques within Industrial Control System (ICS) environments. To contextualise the opportunities and challenges of applying such techniques, interviews with ICS security practitioners (including CESG, penetration testing providers, and a non-academic research institute) were conducted to discover how ICS operators address security risks in practice. A framework for future improvement in ICS security is outlined from this review's findings. Three phases of the ICS system development lifecycle are then examined (during product development; during procurement; once operational) to determine when and how the assurance techniques defined within this project can be applied, and what challenges are present in conducting such security assessments.

Critical infrastructure such as that of utility industries (e.g., oil and gas) is a frequently cited example of an ICSs, although their usage is considerably more diverse and widespread. Service industries (e.g., logistics), and manufacturing industries (e.g., aerospace) make heavy use of ICS technologies. The technologies that support ICSs are largely similar in concept, and in many cases, identical. The technological similarity can be further expanded to small-scale installation, such as Building Automation Systems, although they are not addressed here.

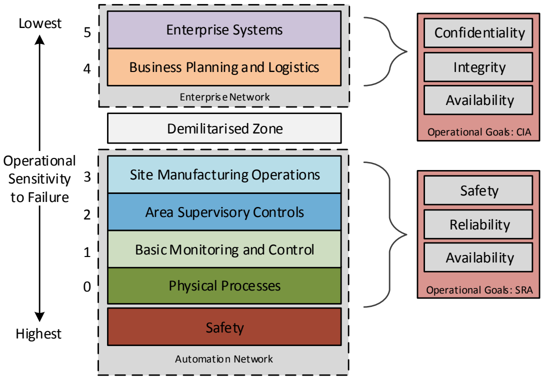


Figure 14: A Conceptual Model of an ICS: Safety and Security Goals (Adapted from [5, 13])

At a conceptual level, an ICS can be seen as a series of layers, split into two areas (Figure 14). Layers 0-3 constitute the "automation network". Present in layers 0-2 are safety systems, the sensors and actuators that monitor and manipulate physical processes, and the devices enforcing the intended logic of such processes. Multiple instances of layers 0-2 may exist, which may be geographically clustered or dispersed (e.g., a utility network may have many thousand "field sites"). In both cases, they have been conceptually labelled "Cell Zones". Layer 3 manages automation network wide functions. Layer 3 systems capture and archive cell zone process data, monitor these processes, and take managerial action as necessary. Layers 4-5 are known as the "enterprise network". Centralised IT services are found here (e.g., business-to-customer services). Both the automation network and enterprise network may be physically isolated from each other, in what is known as an "air gap" which can act as a security feature. However, these networks in contemporary ICSs are frequently interconnected, due to the potential to facilitate core business functions (e.g., to enable automation in a manufacturing system, through linking the consumer purchasing system to the production line).

Risk Management, Risk Perception and Standards for ICS Security

The use of appropriate assurance techniques within the risk management process is paramount, as it is the output of these techniques that influences the way that risk is perceived, assessed and treated in a cyclical fashion. Therefore, understanding the current practices and challenges of securing ICS environments must be contextualised, in order to understand the potential application for assurance techniques within ICS environments. Academic surveys of publications are available from alternative sources (e.g., [13]). Instead, this review intends to collate the perceptions and experiences about ICS security of those with experience of the realities of these environments.

Industry surveys such as that of ENISA [7] (EU-centric) and SANS [15] (US-centric), highlighted low utilisation of standards, with a greater preference for guidelines. Standards where used included: ISO/IEC 27002[3]; ISA/IEC 62443; and NERC CIP. In both surveys, fulfilment criteria is not qualified as to the extent to which it constitutes (e.g., how close to achieving certification). Despite this, positive respondent count remained low, with 10-20% current *implementation* or *utilisation* and 10-45% planned. Such findings raise question around security risk management practices; more so if non-response bias is considered.

Survey results represent a snapshot in time, and may not reflect the current status. This study does not purport to be a comprehensive or quantitative reflection of what is; however, interviewed practitioners, with experiences of assessing many environments, expressed views that largely paralleled the findings of surveys: strict conformance to standards within automation networks was scarce, with verified compliance or certification only where there was a mandatory requirement for it. Notably this was

[3] ISO/IEC 27002 here is notable, as it outlines controls, rather than ISO/IEC 27001 which focuses on managing security risk.

predominantly for NERC CIP requiring ICS operators.

Formal publication use focused on guidelines, with standards also acting in this fashion. "Awareness" of publications from NIST (notably 800-82 and the more general 800-53) and CPNI (the Good Practice Catalogue) was high within the critical infrastructure sectors, although the perception of the latter was that much was now outdated and needed replacement. These findings are in line with SANS survey [15], which listed NIST 800-82 as the most "utilised" ICS publication. Practitioners felt such publications were used in an "informative" manner, rather than strict conformance; however, this is unsurprising given Knowles et al's [13] findings that publication focus centred on security control recommendation rather than risk management (making any form of conformance challenging). Perceptions of standards use within enterprise networks was markedly different, with standardisation common where a business requirement existed for it (notably for ISO/IEC 27001 and PCI DSS). Despite this familiarity with security standardisation, it is clear that this process has not yet "hopped the gap" into automation networks. It should be noted, that as with the survey's non-response bias, these results potentially have their own dark figure of publication adoption. Interviewed practitioners largely experience environments with a requirement or interest in security (e.g., through procuring a security assessment); therefore, the true rate remains unknown.

Although standards adoption does not precede a strong security posture, it does provide some indicator of an industry's maturity. Strong risk management can exist without standardisation. Practitioners expressed views that there were many examples of such cases in ICS environments. The vast majority, however, fell short of this goal. Practitioners stated that in many cases formal processes for managing security risk did not exist, and was largely divorced from implementation, with security risk treated on an ad-hoc basis by a small number of active engineers that championed security. In the rare occurrence where processes did exist, practitioners referenced ISO/IEC 27005, with ISO/IEC 62443 in "some cases" but with its adoption hindered as it is still considered "drafty". Such findings conflict with others from surveys, such as those of a 2013 ENISA survey [8] on ICS security assessment frameworks, where ~78% respondents stated that a risk management system for ICS security had been implemented. This highlights two issues. First, that again, of non-response bias. Second, the importance of treating quantitative results with caution, as it says little of the depth and complexity of what constitutes a risk management system in practice. In the frequently cited situation of security champions, such a process may exist, but is it integrated into formalised decision making, and of influence to those outside the adopted security function? Both issues here can be extrapolated to raise questions about what the extent of the "awareness" or "adoption" of guidelines truly represents.

In 2010, Anderson and Fuloria [1] wrote of a "natural experiment" in ICS security, whereby the UK encourages industry, the US enforces standardisation in the energy sector, but not in others such as oil and gas, instead providing guidelines, and European countries have adopted a multitude of postures, including intervention. The perils of enforced standardisation, with respect to NERC CIP were also discussed; however, in the intermittent years since this publication, it would be difficult to argue that ICS operators have put forward a robust case for self-determination for ICS security. Indeed, many have; our findings suggest significantly more have not. In reading this study, the stimulus of negative feelings would not be unfounded. Security for many ICS operators, including within the critical infrastructure that supports our very society, has been deemed insufficient in many cases; however, practitioners were equally clear in their views: *security is improving*. The question that must be asked is whether this improvement is fast enough, and whether a resilient minimum can be achieved throughout the population of operators without enforced standardisation. Despite NERC CIP's faults, the US energy industry was widely considered to be leading the way in ICS security. Criticisms of enforced standardisation must be balanced against the counter argument of what operators would be doing if there was no requirement. Our findings provide some resource for this discussion. In such a scenario, one must postulate the merits of one of the core principles of standardisation: "do what you want, but you can't be worse than this".

The discussion has fallen so far upon the use of formal publications and extent of security risk management. It is in this latter category that we proceed, in order to explore the challenges to its practice. Practitioners perceived a slow but growing increase in managerial awareness and funding for ICS security; if such perceptions are a reality, why and where are many ICS operators failing in security risk management? Our findings fall into four categories.

No Safety and Security Process Integration. Security risk management, at least with respect to cyber security (rather than just physical security), unlike its safety counterpart, is a recent phenomenon in ICS environments. It has largely transferred from the enterprise domain and must adapt to its sub-ordination to ICS' core operational goals of Safety, Reliability, and Availability (Figure 14). Practices for achieving this are immature. A failure to employ security risk management processes could be attributed to its failure to integrate with those for safety. Practitioners perceived an almost wholly absent attempt to integrate such processes in modern environment, where they are instead treated in isolation. Furthermore, formal security publications do little to encourage this through largely neglecting safety [13]. Practitioner opinions on why this occurs were split around two themes. First, the engineering background of ICS practitioners, which emphasises safety leading to a lack of understanding about security requirements, treating Security as a "bolt-on".

Second, information requirements for risk management and the information asymmetry for safety and security. In part, this occurs due to the way data is computed. Safety is based on trusted data sets (e.g., of historical faults) and handles values in probabilistic ranges. Security, however, is event driven, and there is a lack of such datasets and reliable ICS security metrics [13]. Furthermore, practitioners believed most ICS operators lack the infrastructure to support security monitoring. Real-time process monitoring exists on a wider scale, but is seen to be inadequate for detecting most attack types. This was largely seen to be a resource challenge despite funding availability. Technology exists for passive network monitoring and intrusion detection, and academia has extensively examined real-time risk assessments [12]; however, any widespread implementation is hindered by three factors: the large financial and operational undertaking; the lack of security risk management processes to make a business case for such an implementation; the lack of trained staff to implement and monitor the implementation.

ICS Risks: Perception, Acceptability and Communication - Interviewed practitioners believed a consequence of the educational gap was a systematic underrating of security risks of individuals within many ICS environments (security champions excluded). The lack of ICS incidents was perceived to cause a lack of "dread" [16], which creates a mental gap with the unremitting cyber attacks of the enterprise network domain. Surveys have shown improved awareness of threats; however, our findings suggest non-response bias must be accounted for, while further questioning the extent of the penetration of awareness *within* ICS operators. In-depth risk perception studies are yet to be conducted in this context, although one study has examined ratings of Confidential, Integrity, and Availability at each layer of the conceptual ICS model [10]. The perception of the frequency of malicious compromise and incident is a larger issue: do these ICS attacks really not occur or are they simply not identified due to a lack of real-time monitoring and forensic capabilities (e.g., as *may* be suggested by the frequent attacks on ICS honeypots)? Risk perception can be modified through a process of risk communication. The increasing frequency of ICS security in the news and pop culture was seen to have had a positive effect on encouraging greater security efforts; however, practitioners identified areas of improvement for the security community: focus more on providing remediation than identifying vulnerabilities; improve communication of security risks with safety personnel and senior management (measured and relayed in terms each would understand) which is currently described as "ineffective"; and focus more on relatable threats rather than the sensationalist (e.g., Stuxnet).

Risk Management at Enterprise and Automation Network Boundaries - One symptom of the lack of security risk management processes was deemed to be the poor definition of roles and responsibilities for managing components at the boundary between automation and enterprise networks. Such components were deemed to often be inadequately maintained and secured due to conflicts over responsibilities. One practitioner argued that the boundary itself should not require special treatment; if you have a mature automation network and mature enterprise network, you should have a well managed, secure boundary. Unfortunately, one is usually weak, and that is the automation network. A secondary consequence of this poor boundary management is the use enterprise technologies in the automation network. This manifests itself in two ways. First, a direct use of the technologies with physical proximity (e.g., a human-machine interface on a tablet device). Second, when this is done remotely. Neither is inherently bad, but the way that it is realised in modern environments often can be; largely due to the rise of Bring-Your-Own-Device (BYOD) cultures, and the lack of security awareness and training. One practitioner stated that they had experienced the remote management of ICS infrastructure by individuals on tablet devices within coffee shops, and that the perception amongst individuals in these environments is largely that "if they have Citrix and two factor authentication they're secure".

Supply Chain Assurance - Recent concern around supply chain assurance is not isolated to ICSs; however, practitioners perceived ICS operators to enforce minimal security requirements on the supply chain, despite the integral and integrated role it plays in their operation. Concerns fell into three themes. First, risks arising from the large number of contractors (e.g., from maintenance contracts, which may involve unsupervised access). Good security risk management practice dictates the definition and enforcement of policies and procedures for third party providers; however, beyond personnel checks which are conducted regularly (whose current practice one practitioner described as "security theatre") the perception and experience was that policies and procedures are rarely made available or enforced if they exist. Second, the procurement process for ICS components (both hardware and software). Many ICS have been demonstrated to have fundamental design flaws over the past five years, which creates challenges for securing them in operational environments. For example, because patch availability varies (in some cases due to inaction, but also through deliberate choice to prevent conflicts with legacy components), and the challenges of high-uptime patch management. Although component security was perceived to have improved, mostly as a result of industry and governmental pressure, most ICS vendors were still perceived to have insufficient security integration in their development lifecycle. Standards are under development for component development (e.g., IEC 62443-4-1); however, only time will indicate their real-world usage. Procurement in such an uncertain environment is challenging. Assessment before procurement is one option, but many ICS operators do not have the skills to assess products in-house, and there currently exists no certification framework to refer to for third party independent testing. Furthermore, components are typically closed-source and closed-hardware which limits the types of security assessments that can be conducted. The biggest problem, however, was deemed to be that security assessments are never conducted at all as operational teams had limited influence on procurement where decisions were largely based on costs. Risks arising from the current scenario for product procurement are shown in Figure 15; the alternative highlights the key role of security risk management from ICS operators in ensuring resilient and secure products through establishing a business requirement for change. Third, the process of information sharing with third parties to facilitate business operations in the up and downstream supply chain. One concerning trend for practitioners was the increasing outsourcing of ICS functions (in many cases outside national borders), without validating the security postures of these third parties. The enforcement of entry-level security certification on the supply chain is one potential route to address this, which is currently being trialled by the Nuclear Decommissioning Authority with Cyber Essentials for suppliers that handle sensitive data.

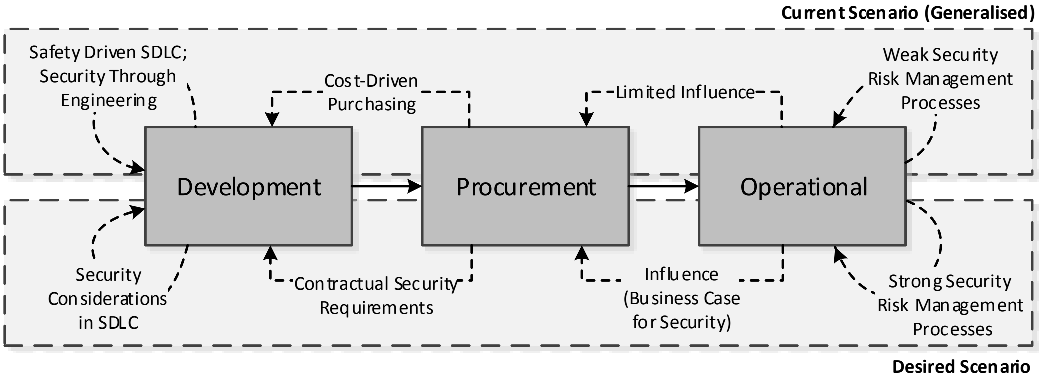

Current Scenario (Generalised)
Safety Driven SDLC; Security Through Engineering
Cost-Driven Purchasing
Limited Influence
Weak Security Risk Management Processes
Development
Procurement
Operational
Security Considerations in SDLC
Contractual Security Requirements
Influence (Business Case for Security)
Strong Security Risk Management Processes
Desired Scenario

Figure 15: The Security Risk Management of Operators and the Procurement Process

Assurance Techniques within ICS

In the midst of a largely immature environment for security risk management the appropriate, effective and economic application of assurance techniques becomes a challenge. This section examines the current approaches for assessing ICS environments. A set of principles is presented based upon the findings of practitioner interviews. These principles are then applied to the assurance techniques defined within this study to examine their use within three phases of the ICS system development lifecycle.

To what extent are ICS operators conducting security assessments? Results of a 2013 ENISA survey [8] show high variation: only 15% are ”always” testing, 30-35% ”often” and 60% ”sometimes”. The 2014 SANS survey [15] has similar findings, but refers to how many operators use broad techniques, and does not quantify their frequency. Neither quantifies the extent of use. With hesitance of repetition, non-response bias must again also be considered. More interesting, perhaps, is *who* is conducting these security assessments when there is third party involvement. Practitioners described heavy involvement of governments, primarily for critical infrastructure, which may come as no surprise; however, private sector involvement varied highly. Within the UK context, security assessments are predominantly government-led for critical infrastructure, either by CESG or government departments (in some cases, facilitated with CESG involvement). Commercial assessments of ICSs in the UK were described as significantly less prominent than in other countries; notably the US. As the UK ICS security industry matures, commercial involvement may increase, as it has the secondary benefit of reducing the burden on government assessments. Indeed, the UK government has initiated schemes for such a reason in the past: notably “IT Health Checks”[4] for public body systems. Furthermore, CREST (`http://www.crest-approved.org/`), the leading UK body for penetration testing, has recently announced the involvement of CESG and CPNI in the expansion of its STAR scheme which is targeted at critical infrastructure.

Practitioners were asked about their experiences of what types of assurance techniques are used within ICS security assessments. The perception was that for UK-based assessments of automation networks, assessments were in effect risk assessments that used the “big three” audit techniques: Review of Documented Policies, Procedures, and Processes; Observe; Interview. In-house technical security assessment were rare, as ICS operators do not yet have appropriately trained individuals to conduct such tasks. Commercial security assessments, such as penetration tests, were increasing for the critical infrastructure sectors, but infrequent, and highly rare for non-critical ICS environments. For enterprise networks, the frequency of security assessments was deemed to parallel those of non-ICS systems, although automation components within the enterprise network would often be out of scope. It was

[4] `http://www.cesg.gov.uk/servicecatalogue/service_assurance/IT-Health-Check/Pages/IT-Health-Check.aspx`

the general consensus of practitioners that current modes of assessing such environments were limited and greater effort needs to be placed on ensuring security controls are not only in place, but are effective in their objectives.

For automation networks, the lack of security assessments was suggested to lie with the lack of risk management processes or business requirement for such tests. A technical assessment would create a de-facto obligation to address issues found. Security assessments exist to push organisations to a higher level of security. Vulnerabilities in assessments of any infrastructure are frequently found; ICS are no exception, and arguably present greater opportunity for vulnerability. A security assessment in effect is the purchasing of a problem. For operators that have invested heavily in security risk management there is a benefit of such an assessment; however, without the basic organisational competency for assessing and managing security risk, any issues found will be challenging to address, which may act as a deterrent.

Commercial security assessment providers described methodologies for assessing the automation networks of *operational* systems. Such assessments unsurprisingly shied away from the active and found passive alternatives to what would be conducted in a typical engagement. Highly cited techniques included configuration reviews, architecture reviews (including passive network monitoring and mapping), physical inspections, and threat assessments. Supplementary test-bed assessment were sought allowing for greater active assessment, although few ICS operators were found to have this capability (either owned or shared with other operators), and many were not representative of live networks. Third party involvement in the assessment of security during procurement was rare, although one practitioner stated its popularity is slowly increasing, and that they encourage ICS operators to attempt to include security testing clauses within their procurement contracts. If the device fails a security assessments, a discount is received. Based upon the findings of practitioner interviews, five principles were derived for ICS security assessments of live environments: PASIV.

Proximity requirements.Assurance techniques should be used when the assessor is in physical proximity to the system under evaluation. Remote assessment should be avoided, but if a scenario necessitates this, it should only conducted with alternative personnel present on-site.

Accessibility limitations. Assessments should consider to what extent claims of assurance can be made and addressed due to the wide accessibility limitations that restrict assurance technique usage (e.g., proprietary, closed source systems create little opportunities for the use of some assurance techniques).

Safety requirements. Ensuring that the use of an assurance technique does not negatively impact human and environmental safety should be the primary goal of an assessment.

Impact of the assurance technique. Assurance techniques should not impact the core operational goals of the operator, nor cause faults in live environments.

Value generated by using an assurance technique. A cost-benefit trade-off must be considered in assurance technique use and its implications for aiding the management of organisational risk (e.g., considering the extent to which a system under evaluation represents the wider system due to the infeasibility of testing many thousands of field sites).

To illustrate the limitations placed upon assurance technique usage within ICSs, the application of assurance techniques defined within this study to three phases of the system development lifecycle is examined. The phases focus specifically on the role of assurance technique in product assurance within automation networks and excludes services. Phases were selected based upon pressing sources of risk identified in Section : assurance technique used during product development; during procurement; once operational. These phases were earlier illustrated in Figure 15 and are described below:

Development During the supplier's development process, what assurance techniques can *the supplier themselves* use to ensure that a product has been designed in a secure manner? To illustrate the wider range of potential assurance techniques that can be used in this scenario, the focus here is on applying assurance techniques within the product development process itself, rather than the organisational security that supports it. In practice, both are necessary to ensure resilient products (e.g., to mitigate against supply chain threats).

Procurement When a product is being procured, what assurance techniques can the procuring operator use to gain assurances of a product's security?

Operational Once a system is operational, what assurance techniques can be used in a security assessment? Operational is split into two parts: First, the assessment of products and the manner in which they are deployed within a testbed setting. Second, a broader review of how assurance techniques can be used within live environments, while also considering an organisation's wider security processes and controls.

The application of assurance techniques is described in Table 11. The mapping is based on a *typical scenario* for an ICS operator, and follows the principles of only mapping what is *feasible* and of *benefit* in such a case. Mapping uses three labels. "✓" indicates an assurance technique has widespread application, while "×" means it is unlikely for most cases. "P" indicates a possible application but is limited by certain factors, which are indicated by one of two suffixes. "(I)" when limited by concerns surrounding operational impact, and "(C)" when the application is case dependent (e.g., whether the operator has the resources to fund a testbed, or has bargaining power in the procurement process).

Assurance Technique	D	P	O(T)	O(W)
Review of Documented Policies, Procedures, and Processes	P(C)	×	×	✓
Review of Client-Completed Self-Assessment Form	P(C)	P(C)	×	✓
Threat Assessment	×	×	P(C)	✓
Architectural Review	P(C)	×	✓	✓
Configuration Review	✓	×	✓	✓
Source Code Review	✓	×	×	×
Observe	P(C)	×	×	✓
Interview	P(C)	P(C)	×	✓
Red Team Exercise	×	×	×	P(IC)
Penetration Testing	✓	P(C)	✓	P(IC)
Vulnerability Scan	✓	P(C)	✓	P(IC)
Social Engineering	×	×	×	✓
Static Analysis	✓	×	×	×
Dynamic Analysis	✓	×	×	×
Fuzzing	✓	P(C)	✓	P(IC)
Formal Verification	✓	×	×	×
Cryptographic Validation	✓	P(C)	✓	P(IC)
Emanation Security Analysis	P(C)	×	×	×
Witnessed Test	P(C)	P(C)	✓	✓
Public Review	×	×	×	×

Table 9: The Feasibility of Using Assurance Techniques for Three ICS Lifecycle Phases — D: Development, P:Procurement, O(T): Operational (Testbed), O(W): Operational (Whole inc. Organisation.

The mapping aids in illustrating the importance of a robust product development lifecycle as it at such a stage where there is greatest opportunity not only for remediating security faults, but also conducting in-depth assessments. Once operational the use of demonstrable assurance techniques, such as penetration testing, becomes limited and is marred by the PASIV principles imposed upon the process. Tesbed assessment aids somewhat in addressing this, but as discussed, representative testbeds are a rarity. One limitation of such a mapping is that it highlights only potential uses of assurance techniques, and the need for further review with respect to three factors. First, on *where* these assurance techniques are used. For example, as shown in Figure 14, operational sensitivity increases at lower layers of ICSs, and this mapping does not consider the opportunities for assessing ICS components that bridge the enterprise network boundary. Second, *how* they are used. The enforcement of PASIV principles requires assumptions not explicit in the mapping. A conspicuous example of this is for architecture review. Part of this process requires the mapping of current assets and communications channels. Active techniques that may be used in enterprise networks to facilitate this such as port scanning can not be used. In automation networks this mapping involves alternative approaches such as passive traffic analysis, which is supported by other assurance techniques (e.g., physical inspection, which is defined here as "Observe"). Due to these differences, caution should be expressed in extrapolating the cost-effectiveness of techniques outlined in this study. Third, on *what* assurance techniques are used. This report has defined commonly used assurance techniques. For automation network assessments, however, the inclusion of additional techniques may be required; notably in the areas of radio frequency analysis and hardware analysis.

Next Steps

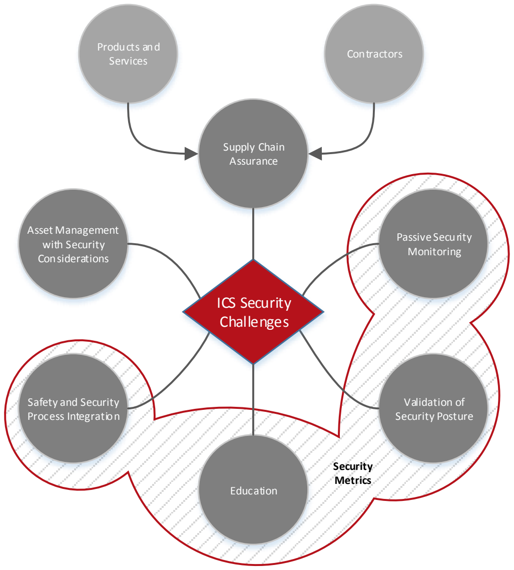

Products and Services
Contractors
Supply Chain Assurance
Asset Management with Security Considerations
Passive Security Monitoring
ICS Security Challenges
Safety and Security Process Integration
Validation of Security Posture
Security Metrics
Education

Figure 16: Future Areas of Research for ICS Security

Based on the findings above, a number of practical opportunities for future improvement were identified which can be seen visualised in Figure 16. In many respects, the challenges faced in securing ICS environments parallel those of SMEs, but with considerably greater stakes. The core area for improvement involves encouraging ICS operators to develop security risk management systems, and the areas outlined here can be seen to be a subset of that. Interviewed practitioners as part of this study described a scenario that does not call for highly advanced technical solutions to improving the security of ICSs in the majority of cases. Instead, greater focus is required on the "mundane" fundamentals, before the advanced can be practically contemplated and of real benefit. On the human side this involves addressing the education gap for security in a safety culture, and the importance of enforcing security requirements beyond organisational boundaries. On the technical side it involves establishing a greater understanding of the assets within these environments, and the attempt to provide greater validation that any implemented security controls had achieved the desired effect. Through this we can begin to understand cost-effective approaches to securing such environments in order to establish further managerial buy-in. The development of appropriate security metrics is integral to this process.

The Assurance Ecosystem: Economics and Incentives

This document also sought to report a more high level analysis of the economics of assurance schemes and incentives in the assurance scheme ecosystem, which could hamper/facilitate cost-effective assurance schemes and techniques. In particular, a study of assurance schemes was conducted in terms of the broad goals they aim to achieve and the incentives that are in place so that all involved stakeholders in the ecosystem work towards those goals. This study was conducted analysing data obtained from public sources and from the assurance schemes reviewed as well as through a number of targeted interviews. We particularly elaborate on two case studies: ISO/IEC 27001 and Cyber Essentials.

Seven main actors were identified to play a crucial role as part of the broader assurance ecosystem in most of the assurance schemes studied. These are:

Formal or de facto regulator(s) - Formal regulators are usually governments (e.g., the UK government) or supranational organisations (e.g., European Commission). De facto regulators include international organisations, such as VISA, MasterCard, etc.

Standards body(s) - Organisations whose primary activities entail the development and coordination of standards and guidelines. This includes international bodies like the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), but also national bodies that have a direct input into international bodies, e.g., the British Standards Institute contributes to international standards.

Accreditation body(s) - Organisations who are usually appointed by regulators and whose main task is to assess the technical competence and integrity of certification bodies (detailed below) regarding how these certifications bodies conduct their evaluation services. Accreditations issued usually have limited lifetime and require to be reissued regularly (e.g. UKAS states that after an initial assessment visit; accreditation will be confirmed on an annual basis; and full reassessment is performed every four years[5]). Examples of accreditation bodies in the UK are the United Kingdom Accreditation Service (UKAS) for several standards including ISO/IEC 27001, and IASME, CREST, etc for Cyber Essentials Scheme. Based on the EU Regulation (EU) 765/2008, accreditation bodies for *internationally agreed* standards (like ISO/IEC 27001) should be restricted to one on a national level.

Certification body(s) - Organisations whose business is to check/evaluate businesses or companies' conformity and compliance with standards and guidelines. The main actors identified under this entity are mainly practitioners, which are able to work on the certification of individual businesses or companies. Nevertheless, another type of actor, i.e., a consultant, might appear in some cases. The main objective of a consultant is to provide consultant services to a business or company in order for the latter to meet certain requirements, and eventually help in getting certified after being assessed by the certification body. Depending on the standard, assessment and consultancy from the same certification body may be forbidden.

Organisation(s) - Organisations involved in the trade of services or goods to consumers or other organisations (e.g., supply-chain). These organisations procure the services of certification bodies to *get certified* according to standards or guidelines. Organisations might conduct self-assessments according to standards or guidelines. Obviously, this does not lead to any certification without a certification body reviewing self-assessment reports (e.g. Cyber Essentials Scheme). Furthermore, there might be cases where a set of internal auditing activities could occur. Such internal auditing might include supply-chain auditing, gap analysis, or audits for certification.

Collaborator(s) - Collaborators could be perceived as initiatives, forums, etc., which are able to influence the formation of standards. These are differentiated from business organisations since the latter in most cases produce a product or provide services.

Consumer(s), purchaser(s) - Consists of entities that are purchasing services for personal or not use.

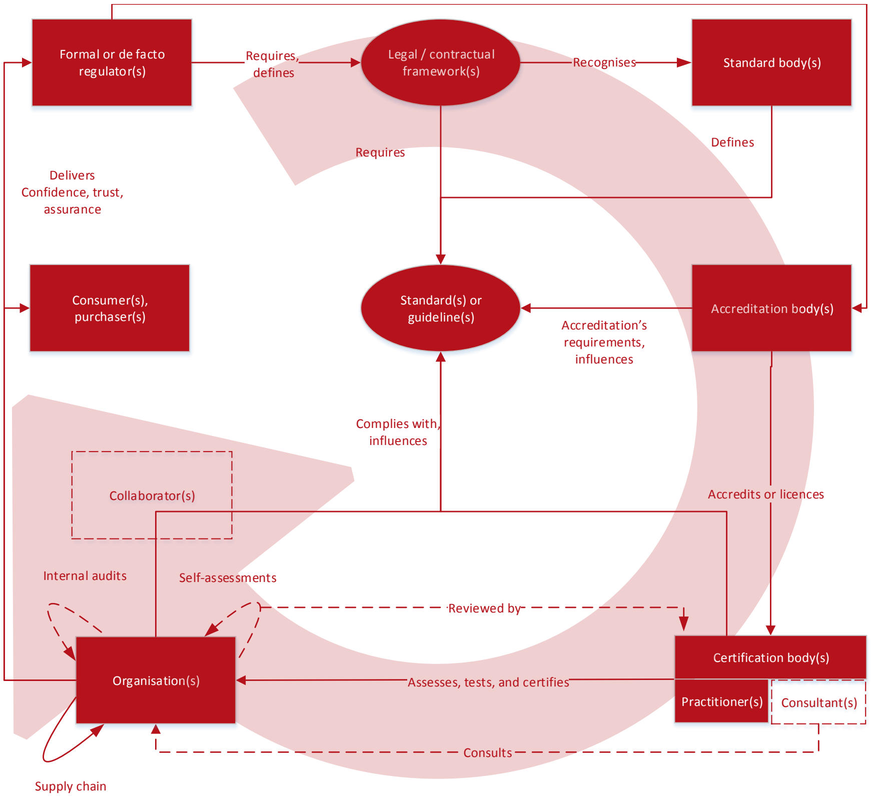
There are also a number of other entities that, even though they are not actors, play an important role in the ecosystem:

Legal/Contractual framework(s) - Refers to the various laws or contractual obligations set by regulators, which set the *rules* all other actors in the ecosystem must abide by.

Standard(s) or guideline(s) - A standard is an agreed way of doing something[6], and a guideline can be considered to be a statement by which to determine a course of action or a best practice.

[5] http://www.ukas.com/library/Tools/The%20Route%20to%20Accreditation.pdf

[6] http://www.bsigroup.com/en-GB/standards/Information-about-standards/what-is-a-standard/



Formal or de facto regulator(s)
Requires, defines
Legal / contractual framework(s)
Recognises
Standard body(s)
Requires
Defines
Delivers Confidence, trust, assurance
Consumer(s), purchaser(s)
Standard(s) or guideline(s)
Accreditation body(s)
Accreditation's requirements, influences
Complies with, influences
Collaborator(s)
Accredits or licences
Internal audits
Self-assessments
Reviewed by
Organisation(s)
Assesses, tests, and certifies
Certification body(s)
Practitioner(s)
Consultant(s)
Consults
Supply chain

Figure 17: Assurance ecosystem

Figure 17 depicts actors, entities and interactions amongst them. Dashed arrows or dashed rectangles indicate potential existence of them, because different procedures are followed in various assurance schemes. A potential chain of actions would include a regulator to require/define a legal or contractual framework and to recognise and work with standards bodies and other actors to create a standard or a set of guidelines to meet the legal/contractual framework. Furthermore, a regulator is usually in a position to appoint accreditation bodies that would set the accreditation requirements certification bodies need to comply with. Then, certification bodies would *certify* whether organisations comply with standards or guidelines. Note, however, that Figure 17 admits many interpretation variations in terms of the potential chain of actions. For instance, other possible chain of actions may include a standard that was created in the first instance by one or more standards bodies, and then regulators would set the legal/contractual framework afterwards based on the standards/guidelines. Another example is that certification bodies, or businesses in the large may also participate and influence in the development or refinement of standards, so they not only abide by them but actively influence them.

The ultimate collective aim of such assurance ecosystem is to deliver **confidence, trust, and assurance** to both regulators and consumers [9]. In other related security disciplines, it has been identified that, some times, even if a collective aim is clear, individual incentives may be misplaced, which can jeopardise the ultimate collective aim of information assurance [3].

In terms of **economic incentives**, profit would obviously be one such incentive as some of the actors in the ecosystem are indeed private and for-profit organisations. For instance, businesses and companies may want to get certified according to a particular standard if this opens up market opportunities for them. However, businesses may be deterred to get certified if they cannot afford the cost of doing so, or if this cost is too high when compared to the market opportunities the certification may open up for them. Furthermore, being certified provides a level of confidence in the supply-chain, and helps to avoid data breaches (for which they could be fined by law) and reputation damage.

A rather interesting topic is that of misaligned incentives. Misaligned incentives are usually in place when there is absence of proper rules that control the rewards or penalties for the participants in a particular ecosystem. Examples of misaligned incentives are liability and insurance. In the first case, liability is known to be assigned to the party that can manage best the risk; however in most cases allocation is done poorly. In turn, insurance may raise issues in cases where insurance parties cannot observe the behaviour of insured parties, and the latter behaves recklessly [2].

Accreditation bodies are an actor of vital importance in the assurance ecosystem. In all cases, its main goal should be to assure adherence with specific requirements set by standards, whether international or national standards. Regarding international standards, accreditation is permitted via only one national body (UKAS), so this might potentially lead to a monopoly. On the contrary, licensing for some national schemes like Cyber Essentials, can be provided by more that one accreditation bodies (APM Group, CREST, IASME, and QG Business Group). In this case, competition amongst various accreditation bodies may exist, and the cost of assessment and licensing might vary significantly amongst them. Variations in cost might also stem from the incentives placed by each accreditation body.

Certification bodies are usually for-profit, though there may be some certification bodies that are not. In any case, their revenue (and perhaps their economic survival) strongly depends on how many organisations they certify, as well as on the price they need to pay to get accredited by an accreditation body (to be able to certify organisations). The latter has obvious implications for organisations that would like to get certified in turn, as the price for certifications is likely to be affected by the costs set by the accreditation body.

Consultancy companies also play a crucial role in the ecosystem. Despite the fact that it is not explicitly required for an organisation to go through the process of consultancy, this might some times be a safer, faster and cheaper route for an organisation to finally achieve the desired certification. Some assurance schemes identify potential conflicts of interest between certification bodies and consultancy practices, so it appears that in most cases consultants are to be different from certification bodies for a particular organisation seeking certification.

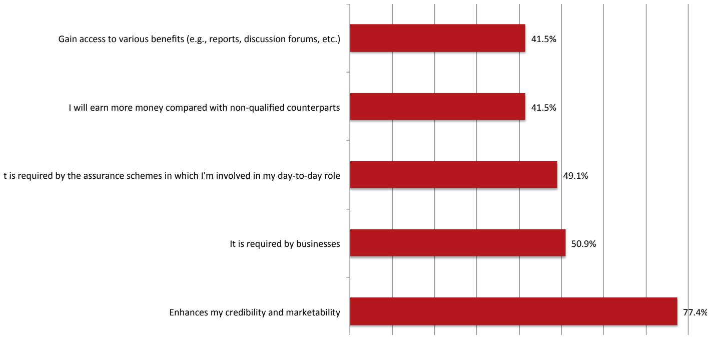


Figure 18: Incentives to get individual competence certification (X-axis percent of respondents, Y-axis reasons).

Finally, we also analysed the **incentives for getting individual competence certifications**. To this aim, we based on data gathered via the on-line survey. Figure 18 shows the results we obtained. In particular, 77.4% of respondents stated that they pursue a certification to enhance their credibility and marketability; 50.9% because such a certification is required by businesses; 49.1% indicated the it is required by the assurance schemes in which they are involved in their day-to-day role; 41.5% because they stated that they will earn more money compared with non-qualified counterparts; and 41.5% that will gain access to various benefits (e.g., reports, discussion forums, etc.).

ISO/IEC 27001 Case Study

The main objective of ISO/IEC 27001 is to *"... provide requirements for establishing, implementing, maintaining and continually improving an information security management system"*[7].To this aim, ISO/IEC 27001 defines the requirements for an Information Security Management System (ISMS), and it is designed in such a way to ensure the selection of adequate and proportionate security controls. Examining ISO/IEC 27001 in the context of the assurance ecosystem, we identified that standard bodies such as ISO and BSI are set responsible for its definition. More specifically, the latter is recognised as the UK National Standards Body by the UK Government[8]. It is also defined in the memorandum of understanding (MoU) between the UK Government and BSI[9] that standards published by BSI may have their origin in international standards developed by ISO and IEC. Therefore, it is clear that the legal framework for recognising a standards body for ISO/IEC 27001 in the UK, is in place. BSI's main responsibilities, including directions towards the development of British standards are further clarified in the MoU between the UK Government and BSI.

According to EU directives, a sole accreditation body is set on a national level in order to accredit certification bodies against internationally agreed standards, such as ISO/IEC 27001. The UK government appointed UKAS to be that sole national accreditation body.Therefore, UKAS is able to accredit or licence certification bodies, which in turn are in position to assess, test and certify organisations. An interesting topic of further clarification is that certification bodies, being accredited by UKAS, are not permitted to provide any consultancy services to organisation that will be assess. This is a requirement set by ISO/IEC 17021, which forbids consultancy from certification bodies. The main reason for that is to ensure that there will be no conflicts of interests between certifications bodies and organisations being certified. Yet, the provision of consultant services by other parties appears not to be forbidden. Figure 19 illustrates the different actors and relationships amongst them.

[7] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[8] http://www.bsigroup.com/en-GB/about-bsi/uk-national-standards-body/UK-National-Standards-Body/

[9] http://www.bsigroup.com/Documents/about-bsi/BSI-UK-NSB-Memorandum-of-Understanding-UK-EN.pdf

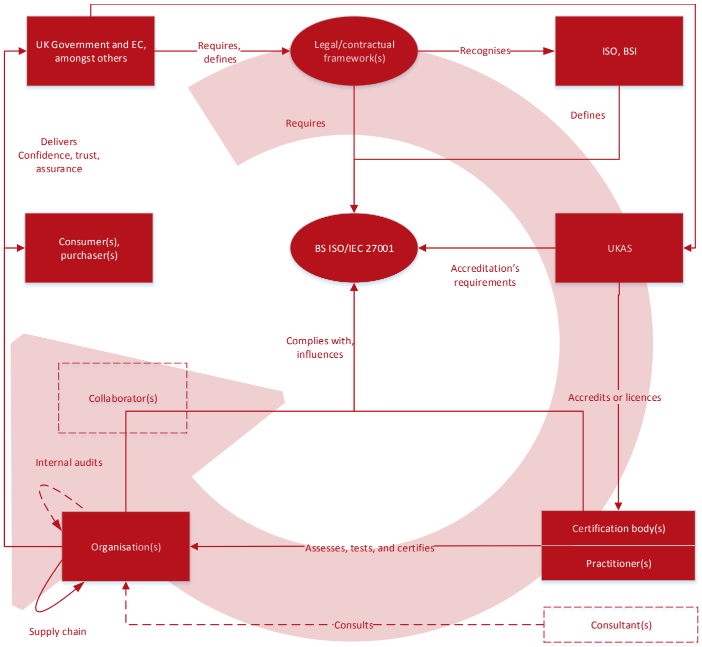

UK Government and EC, amongst others
Requires, defines
Legal/contractual framework(s)
Recognises
ISO, BSI
Requires
Defines
Delivers Confidence, trust, assurance
Consumer(s), purchaser(s)
BS ISO/IEC 27001
Accreditation's requirements
UKAS
Complies with, influences
Collaborator(s)
Accredits or licences
Internal audits
Organisation(s)
Assesses, tests, and certifies
Certification body(s)
Practitioner(s)
Supply chain
Consults
Consultant(s)

Figure 19: Assurance ecosystem in ISO/IEC 27001

Cost consists of an important factor for selecting the appropriate assurance scheme for an organisation. Regarding the certification process for ISO/IEC 27001, that includes a daily rate. Therefore, the cost of ISO/IEC 27001 is proportional to the size of the company. Based on our findings during the interview process, a small company (i.e., approximately 50 employees and one office) requires four days for the auditing process to complete. The daily cost for the certification is around £750. Yet, the final cost for being certified includes additional costs that refer mostly to the number of resources (e.g., number of consultants) and technologies used by the certification, and thus, raising the total cost for the examined study to approximately £6000. Hence, it appears that consultancy consists of another factor that affects the overall cost of the ISO/IEC 27001 certification is the use of third party consultants. As stated already, UKAS accredited certification bodies, are not permitted to offer any type of consultant services to organisation being certified by the same body. However, there is no restriction for an organisation to get consultancy by third party consultant companies. Such a process appear to add an overhead of £5000 + VAT in the total cost of the process for small companies (< 20 employees). In terms of duration, that would require approximately three months to complete[10].

Cyber Essentials Case Study

Cyber Essentials is a UK *"government-backed, industry supported scheme to help organisations protect themselves against common cyber attacks"*[11]. Specifically, the UK government operates as its main regulator. A set of various actors participated in the definition of the Cyber Essentials Scheme, including the BSI standards body, and organisations like the Information Assurance for Small and Medium Enterprises (IASME) consortium, and the Information Security Forum (ISF). The UK government appointed a set of accreditation bodies. These are currently the APM Group, CREST, IASME, and QG Business Group. It is noteworthy that the definition of more that one accreditation body is permitted due to the fact that the defined assurance scheme consists of a national, and not an international one (opposed to ISO/IEC 27001). In turn, Cyber Essentials certification bodies are able to provide appropriate certification to businesses and companies. Certification of companies can be done through a self-assessment process (i.e., a businesses or companies internal operation) that is further reviewed and assessed by the certification body. Such a procedure leads an organisation to be certified against "Cyber Essentials". A second stage requires the organisation to be certified by the independent Cyber Essentials certification body. The latter, if successful, will eventually provide the organisation with the certification of "Cyber Essentials Plus". Likewise ISO/IEC 27001, there is the potential for assessors of the Cyber Essentials PLUS level, to provide consultancy services, but if a certification body acts as a consultant it is forbidden in some cases to act as assessor, as well[12]. Figure 20 illustrates the different actors and relationships amongst them.

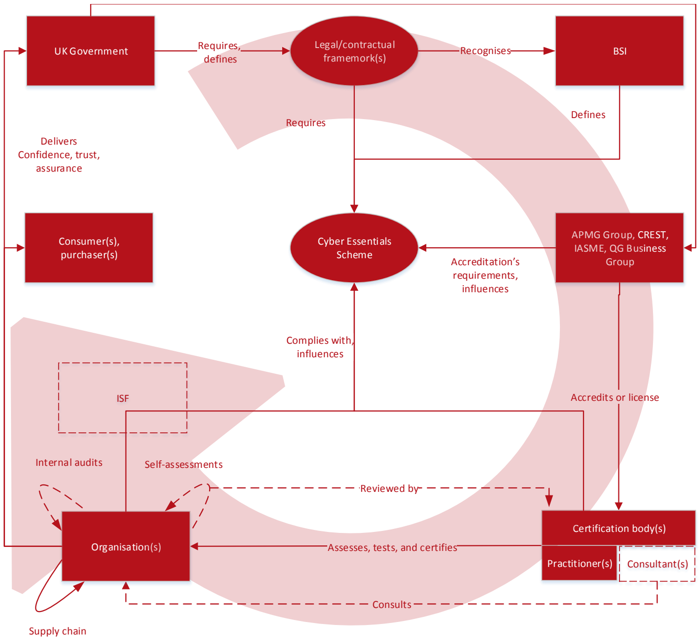

UK Government
Requires, defines
Legal/contractual framework(s)
Recognises
BSI
Requires
Defines
Delivers Confidence, trust, assurance
Consumer(s), purchaser(s)
Cyber Essentials Scheme
Accreditation's requirements, influences
APMG Group, CREST, IASME, QG Business Group
Complies with, influences
ISF
Accredits or license
Internal audits
Self-assessments
Reviewed by
Certification body(s)
Organisation(s)
Assesses, tests, and certifies
Practitioner(s)
Consultant(s)
Consults
Supply chain

Figure 20: Assurance ecosystem in Cyber Essentials Scheme

As already stated, Cyber Essentials provides two levels

[10] http://www.itgovernance.co.uk/shop/p-555-fasttrack-iso-27001-consultancy.aspx
[11] https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
[12] https://www.iasme.co.uk/index.php/cyberessentialsprofile/cyber-essentials-plus

of assurance, i.e., basic and PLUS. In respect to the Cyber Essentials basic level, there is usually a fixed cost of £300 (this amount has been identified for IASME[13], QG[14] and some CREST-accredited certification bodies like IT Governance[15]), and is independent of the size of the company. Note, CREST requires a vulnerability scan to be performed together with the review of client-completed self-assessment forms even for Cyber Essentials basics. Both assurance techniques have been identified in this report as being cheap and Vulnerability Scans was particularly considered one of the most cost-effective assurance techniques. With the costs stated above, Cyber Essentials can clearly be an affordable security solution for many businesses. Nevertheless, the cost may increase when there is a need for the PLUS level of assurance (e.g., for a SME with less than 16 IP addresses in one location, there are certification bodies that would charge around £1,650[16]), which may also add up to further need for consultancy services.

Having a closer look at the aforementioned case study, it appears that being certified against ISO/IEC 27001 is in general more expensive than Cyber Essentials (also when compared to Cyber Essentials Plus). Note that the first and most obvious reason is that ISO/IEC 27001 and Cyber Essentials are not directly comparable to each other. Just to give an example, they use different assurance techniques as stated in *Appendix A*. Another reason for this difference in price might also be related to the fact that for ISO/IEC 27001 the certification body must be accredited by the national accreditation body, i.e., UKAS. In particular, the accreditation process costs £1000 per day. Accreditation requires in overall 15 to 20 days, depending on the size of the certification body. Accreditations have to be revised on a yearly basis, requiring four to six days to complete, and certification bodies have to be fully accredited every four years[17]. Then, this cost may be proportionally transferred from certification bodies to organisations.

Finally, in terms of incentives, two main Cyber Essentials incentives are reported here. The first one is about liability or insurance. At least one of the accreditation bodies, namely IASME, provides a cyber liability insurance. Such an insurance cover, provides security or protection against a loss or other financial burden stemming from event management; data protection obligations; and liability[18] issues (with an indemnity limit of £25,000). This is definitely an important incentive that has been characterised in the literature as a "misaligned incentive" [2, 3] when it is not present. The second incentive is about *added* value that particular accreditation bodies may want to consider. An example of this is CREST, which also includes a Vulnerability Scan as part of the Cyber Essentials basics. Another example is IASME, which provides as well certification against the IASME standard when getting Cyber Essentials basic.

[13] https://www.iasme.co.uk/index.php/cyberessentialsprofile
[14] http://www.qgstandards.co.uk/cyber-essentials/
[15] http://www.itgovernance.co.uk/solutions-for-ces-certification.aspx
[16] https://www.xyonecybersecurity.co.uk/certification-pricing
[17] http://www.ukas.com/library/Tools/The%20Route%20to%20Accreditation.pdf
[18] https://www.iasme.co.uk/index.php/cyberessentialsprofile/automatic-insurance-cover

Recommendations

Based on the data gathered and the analysis conducted under the frame of this report, the following recommendations should be considered for current and future assurance schemes:

1. **Reconsider assurance techniques for individual competences**. The first important result of this report is that multiple-choice exams are used extensively, but it seems they are perceived by experts as the least effective to assure individual competences. The use of multiple-choice exams, specially when they are the only technique used to award a qualification, should be reconsidered in future schemes. Options may even include re-framing multiple-choice exams, e.g., APM Group seems to be using a qualitative rating of confidence to be entered for each multiple-choice answer within their CESG CCP assessments. Furthermore, according to the results obtained in the survey, Oral Examinations (Viva-Voce) and Employment history and Qualification Reviewed were perceived to be the most cost-effective combination to assess individual competences.

2. **Reconsider assurance techniques use based on their cost-effectiveness.** An analysis of survey data identified that the most cost-effective assurance techniques to assess security controls were architectural review, penetration testing, and vulnerability scans. Further analyses examined effective and cost-effective combinations of assurance techniques and found the highest combination in both analyses to be: penetration testing; architectural review; reviewing documented policies, procedures, and processes; and vulnerability scans. The datasets presented are expected to provide invaluable information in the development of future iterations of assurance schemes.

3. **Conduct a follow-up study to confirm the least cost-effective assurance techniques.** The least cost-effective assurance techniques were perceived to be public review, fuzzing, static and dynamic analysis, and emanation security analysis. It is worth noting that public review, static analysis, and dynamic analysis were not found to be currently used within the 17 assurance schemes reviewed, emanation security analysis was only used in one assurance scheme, and fuzzing was only used in two. It is also worth noting that these assurance techniques received less responses in the on-line survey. A follow-up and more in-depth study should be conducted focusing on these techniques to be able to decide whether their contribution to particular assurance schemes is (or could be) useful.

4. **Assurance schemes to make explicit which assurance techniques assess which security controls.** A limited number of assurance schemes (excluding those for assessing individual competencies) made explicit reference to the assurance techniques that should be used to assess conformance. Cyber Essentials was alone in having an explicit assessment criteria, while other schemes that mention assurance techniques, did so only for a subset of security controls (e.g., PCI DSS). Based on stakeholder interviews, it was determined that assessments primarily revolve around the “big three” audit techniques (review, interview, observe), with other assurance techniques being used as audit evidence at the discretion of the assessor, and if available. The initial mapping we have provided in Appendix B should aid in facilitating understanding of assurance technique use within schemes.

5. **Explore the use of assurance techniques in different life-cycle stages.** Most assurance techniques were reported to be used within assurance schemes only in the operational stage of a system’s life-cycle, with very few exceptions in some particular assurance schemes, in which assurance techniques may also be used at the pre-deployment stage. However, no mention was found in any of the assurance schemes or the interviews conducted about assurance techniques being used in other stages of the life-cycle, like acquisition or end-of-life. Therefore, an interesting issue to explore would be the potential and benefit of using assurance techniques in more stages of a system’s life-cycle than just the operational stage.

6. **Risk-based choice of the most suitable assurance techniques.** There is the notion of proportionality of security controls to be implemented relational to the risk in some assurance schemes (e.g. ISO/IEC 27001). However, this notion seems not to be considered in assurance schemes in order to decide the assurance techniques to be applied to test security controls. An extreme example, what is the point of conducting a very expensive assurance technique to test a particular security control (or families/sets of security controls) if the likelihood of getting these controls compromised (or having them not adequately configured) is very low and the anticipated impact in a company’s assets (e.g. in terms of revenue loss) should an attack exploit them is also very low?

7. **Consider special cyber security scenarios like ICS.** A review of ICS environments indicated an endemic lack of security risk management processes in ICS environments, with security assessments (where they occurred) often providing limited assurance about an environment’s security. In order to encourage the

development of ICS security risk management processes a series of practical “next steps” were identified, which involves encouraging: safety and security process integration; security awareness; asset management with security considerations; passive monitoring; validation of security postures; supply chain assurance for both products and services (including contractors).

8. **Reconsider Vulnerability Scans for Cyber Essentials Basic.** The flexibility, and diversity provided within the Cyber Essentials scheme was perceived to be very beneficial in encouraging innovation and facilitating the entry of the scheme into the mass market. However, as reported in the Cyber Essentials ecosystem case study, different accreditation bodies suggest different assurance techniques for Cyber Essentials in its basic form, i.e., some accreditation bodies would require only Review of Client-completed Self-assessment Forms while others would require Review of Client-completed Self-assessment Forms together with Vulnerability Scans. Based on the results from the on-line survey, both assurance techniques were perceived to be similar in terms of number of people, expertise, duration, and cost required to conduct the technique. However, Vulnerability Scans were perceived to be one of the most cost-effective assurance techniques, so including them if the added costs to get the certification are not significantly increased would seem, a priori, beneficial.

References

[1] Ross Anderson and Shailendra Fuloria. Security Economics and Critical National Infrastructure. In Tyler Moore, David Pym, and Christos Ioannidis, editors, *Economics of Information Security and Privacy*, chapter 4, pages 55–66. 2010.

[2] Ross Anderson and Tyler Moore. The economics of information security. *Science*, 314(5799):610–613, 2006.

[3] Ross Anderson, Tyler Moore, Shishir Nagaraja, and Andy Ozment. Incentives and information security. *Algorithmic Game Theory*, pages 633–649, 2007.

[4] Nooper Davis. Secure Software Development Life Cycle Processes. Technical report, Software Engineering Institute, 2013.

[5] Paul Didier. *Converged Plantwide Ethernet (CPwE) Design and Implementation Guide*. Cisco Systems and Rockwell Automation, 2011.

[6] Antonio Drommi, Dan Shoemaker, Jeff Ingalsbe, John Bailey, and Nancy Mead. Models for assessing the cost and value of software assurance. 2007.

[7] ENISA. Protecting Industrial Control Systems: Annex II. Survey and Interview Analysis, 2011.

[8] European Network and Information Security Agency (ENISA). Survey and interview analysis. For the Report :Good practices for an EU ICS testingcoordination capability. Technical report, 2013.

[9] Marion Frenz and Ray Lambert. The economics of accreditation. 2013.

[10] B Green, D Prince, U Roedig, J Busby, and D Hutchison. Socio-Technical Security Analysis of Industrial Control Systems (ICS). In *2nd International Symposium for ICS & SCADA Cyber Security Research 2014 (ICS-CSR 2014)*, pages 10–14, 2014.

[11] David Jackson and David Cooper. Where do Software Security Assurance Tools Add Value. In *Workshop on Software Security Assurance Tools, Techniques, and Metrics. SSATTM05*, pages 14–21, 2005.

[12] William Knowles, Daniel Prince, David Hutchinson, Jules Ferdinand Pagna Disso, and Kevin Jones. Towards Real-Time Assessment of Industrial Control Systems (ICSs): A Framework for Future Research. In *1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013)*, pages 106–109, 2013.

[13] William Knowles, Daniel Prince, David Hutchison, Jules Pagna Disso, and Kevin Jones. A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, 2015.

[14] NIST. Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations. Technical report, 2013.

[15] SANS. Breaches on the Rise in Control Systems: A SANS Survey. Technical report, 2014.

[16] P Slovic. Perception of Risk. *Science*, 236(4799):280–285, April 1987.

[17] Gregory Tassey. The economic impacts of inadequate infrastructure for software testing. *National Institute of Standards and Technology, RTI Project*, 7007(011), 2002.

[18] UK Cabinet Office. Government Security Classifications: April 2014. Technical report, 2013.

[19] DC Washington Navy Yard and Booz Allen Hamilton. Software security assessment tools review. *Mar*, 2:145, 2009.

Appendix A: Assurance Technique Characteristics per Assurance Scheme

Assurance Technique	Assurance Scheme	Intended Outcome	Stage Used	Qualifications and/or Certifications	Nature of input material	Extent of Contrib.
Review of Documented Policies, Procedures, and Processes	CPA	Evaluation of developer documentation to seek eveidence that various mitigations are present and to identify products with known issues	Operational	ISO 17025 (Evaluation team), ISO 27001 (Lead auditor), ISO/IEC 27000:2005, ISO/IEC 18028:2006 (Product developers, 3rd party suppliers)	OFFICIAL	Xsig
	CAS-T	Evidence is gathered and reviewed to ensure compliance with all relevant standards	Operational	ISO 17025 (General lab requirements), ISO 27001 (lead auditor), CLAS Consultant	OFFICIAL-COMMERCIAL	Xsig
	CAS-D	Obtaining an audit trail showing that data has been processed and sanitized appropriately	Operational	ISO 17025 (General lab requirements), ISO 27001 (lead auditor), CLAS Consultant	OFFICIAL-COMMERCIAL	Xsig
	CAS-SS	Ensure to HMG IA Standard No. 5 Sanitization Methodology is followed	Operational	ISO 17025 (General lab requirements), ISO 27001 (lead auditor), CLAS Consultant	SECRET, TOP SECRET	Xsig
	CTAS	Produce an assessment statement outlining risks and recommendations	Operational	ISO 17025 (General lab requirements), ISO 27001 (lead auditor), CHECK Green Light, CLAS Consultant	OFFICIAL-COMMERCIAL	Xsig
	CREST Member Company	Ensure that the company has a good standard of professionalism and capability in four areas that support penetration testing engagements: (1) Company operating procedures and standards; (2) Personnel security and evelopment; (3) Approach to testing; (4) Data security. Based on the assessment, the request for membership will pass or fail.	Operational	ISO/IEC 27001 and ISO 9001 are mentioned but not mandatory, just "evidence" of an ISMS and QMS.	OFFICIAL-COMMERCIAL	Xsig
	CHECK Approved Company	Ensure that the company has the necessary capabilities to conduct IT Health CHECKs over three areas: (1) company background (e.g., previous work); (2) practical assessments (e.g., methodology); (3) staff resources e.g., that there is enough staff members with CHECK qualifications to form a team). Based on the assessment, the request for accreditation will pass or fail	Operational	Appropriate CHECK qualifications and security clearances (SC) for the individuals that make up a CHECK team (minimum one CHECK Team Leader).	OFFICIAL-COMMERCIAL	Xsig
	PCI DSS	Review/Examine is mentioned in PCI DSS v3. These can be used to evaluate security procedures such as access control mechanisms being correctly implemented	Operational	QSA	OFFICIAL-COMMERCIAL	Xsig
	ISO/IEC 27001	Ensures that the organisatonal has appropriately implemented an ISMS. This technique generates audit evidence (facts relating to performance of the ISMS).	Operational	Audit type dependent. In some cases, no requirement (e.g., internal audits). For ISO/IEC 27001 qualifications, there are training course requirements. For example, an ISO/IEC 27001 Lead Auditor is required to undergo a five day training course, and pass a qualification exam. If an ISO/IEC 27001 audit is from an accreditation body they will ensure auditors are competent through validating qualifications and an appropriate level of professional experience.	OFFICIAL-COMMERCIAL	Xsig
	CC	Judge adequacy of documentation describing how the user can handle ToE. It provides increased assurance that the modelled security requirments are satisfied by the TOE.	Pre-deployment, Operational	ISO 17025, ISO 270001	OFFICIAL-COMMERCIAL	Xsig
Review of Client-completed Self-Assessment Forms	Cyber Essentials	Organisations wishing to achieve certification must complete a self-assessment form. This will be reviewed by the Certification Body through which they are undergoing assessment.	Operational	The review must be conducted by an approved Certification Body from one of the four accrediation bodies of the Cyber Essentials scheme.	OFFICIAL-COMMERCIAL	Xsig
	PCI DSS	Conduct self-assessment for some merchants	Operational	In some cases a QSA may be required; however, the self-assessment may determine that no QSA is required.	OFFICIAL-COMMERCIAL	Xop
Threat Assessment	CAS-T	Identification of possible threats which can affect the system	Operational	ISO 17025 (General lab requirements), ISO 27001 (lead auditor), CLAS Consultant	OFFICIAL-COMMERCIAL	Xmin
	CAS-D	Identification of possible threats which can affect the system	Operational	ISO 17025 (General lab requirements), ISO 27001 (lead auditor), CLAS Consultant	OFFICIAL-COMMERCIAL	Xmin
	CAS-SS	Identification of possible threats which can affect the system	Operational	ISO 17025 (General lab requirements), ISO 27001 (lead auditor), CLAS Consultant	OFFICIAL-COMMERCIAL	Xmin
	CTAS	Provide documented recommendations and evaluations of the system based on the Target of Evaluation (ToE)	Operational	ISO 17025 (General lab requirements), ISO 27001 (lead auditor), CHECK Green Light, CLAS Consultant	OFFICIAL-COMMERCIAL	Xsig
Architectural Review	CC	Provide additional assurance from the development of a formal security policy model of the TSF, and establishing a correspondence between the functional specification and this security policy model.	Pre-Deployment, Operational	ISO 17025, ISO 270001	OFFICIAL-COMMERCIAL	Xsig
Configuration Review	Cyber Essentials	The test scecification contains multiple requirements that fall under configuration, notably: (i) ingress filtering of binaries through email and web browsing, which if fails, a verification of the extent user access is blocked; (ii) an authenticated vulnerability scan of a system (e.g., to determine patch level and configuration risks).	Operational	The configuration review must be conducted by an approved Certification Body from one of the four accrediation bodies of the Cyber Essentials scheme.	OFFICIAL-PERSONAL	Xsig
Source Code Review	CTAS	Part of the Evaluation Work Program (EWP) which is aimed to clearly define the Target of Evaluation (ToE).	Operational	ISO 17025 (General lab requirements), ISO 27001 (lead auditor), CHECK Green Light, CLAS Consultant	OFFICIAL-COMMERCIAL	Xop
	CC	Determine the completeness and structure of the TOE implementation representation.	Pre-Deployment	ISO/IEC 15408-3	OFFICIAL-COMMERCIAL	Xsig
	CAPS	Evaluate products to discover flaws	Pre-Deployment	UK Government's List X scheme	SECRET, TOP-SECRET	Xsig
Observe	PCI DSS	The use of observation is explicitly referenced in PCI DSS v3 (e.g., "Observe an administrator log on to each system").	Operational	QSA	OFFICIAL-COMMERCIAL	Xmin

Continued from previous page

Assurance Technique	Assurance Scheme	Intended Outcome	Stage Used	Qualifications and/or Certifications	Nature of input material	Extent of Contrib.
	ISO/IEC 27001	Ensures that the organisatonal has appropriately implemented an ISMS. This technique generates audit evidence (facts relating to performance of the ISMS).	Operational	Audit type dependent. In some cases, no requirement (e.g., internal audits). For ISO/IEC 27001 qualifications, there are training course requirements. For example, an ISO/IEC 27001 Lead Auditor is required to undergo a five day training course, and pass a qualification exam. If an ISO/IEC 27001 audit is from an accreditation body they will ensure auditors are competent through validating qualifications and an appropriate level of professional experience.	OFFICIAL-COMMERCIAL	Xsig
	CAS-D	To ensure products are working in accordance with their certifications and reducing risk of unexpected disruptions to the service	Operational	Developed Vetting (DV) clearance for destruction of IL6 media, Security checks (SC) for IL5 and Baseline Personnel Security Standard (BPSS) for IL4 media	OFFICIAL-COMMERCIAL	Xsig
	CAS-SS	Ensure safe transport of equipment and correct use of sanitization equipment	Operational	DV clearance for Top Secret, SC for Secret and BPSS for Official Media	SECRET, TOP-SECRET	Xsig
Interview	CC	Check awareness of the application of defined standards and procedures	Operational	ISO 17025, ISO 270001	OFFICIAL-COMMERCIAL	Xop
	ISO/IEC 27001	Ensures that the organisatonal has appropriately implemented an ISMS. This technique generates audit evidence (facts relating to performance of the ISMS).	Operational	Audit type dependent. In some cases, no requirement (e.g., internal audits). For ISO/IEC 27001 qualifications, there are training course requirements. For example, an ISO/IEC 27001 Lead Auditor is required to undergo a five day training course, and pass a qualification exam. If an ISO/IEC 27001 audit is from an accreditation body they will ensure auditors are competent through validating qualifications and an appropriate level of professional experience.	OFFICIAL-COMMERCIAL	Xsig
	PCI DSS	To assess some security controls	Operational	QSA	OFFICIAL-COMMERCIAL	Xmin
Red Team Exercise	CBEST/STAR	A report that describes the findings of the security posture of an organisation. This assurance technique will provide evidence about the of the organisation to social and technical attacks. For CBEST engagement, this will be passed onto the UK Financial Authorities (i.e., the regulator). STAR report have no requirement for circulation.	Operational	CREST STAR Member Company and individuals with CREST STAR qualifications. A threat intelligence partner company is also needed.	OFFICIAL-COMMERCIAL	Xsig
Penetration Testing	CTAS	Documented answers and related observations and recommendations based on the evaluationsconducted by the CTAS company	Operational	Testing must meet the ITHSC requirements as defined for a CHECK evaluation	OFFICIAL-COMMERCIAL	Xsig
	CPA	Investigation and resolving of identified flaws; ensure the quality of the product.	Operational	ISO 17025 (Evaluation team), ISO 27001 (Lead auditor), ISO/IEC 27000:2005, ISO/IEC 18028:2006 (Product developers, 3rd party suppliers)	OFFICIAL	Xsig
	CC	Confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE.	Pre-Deployment, Operational	ISO/IEC 15408-3	OFFICIAL-COMMERCIAL	Xsig
	PCI DSS	This assurance technique generates a report which may be used as audit evidence (by a QSA).	Operational	None (note: vulnerability scans (a separate requirement) must be through an approved ASV).	OFFICIAL-COMMERCIAL	Xmin
	ISO/IEC 27001	Ensures that the organisatonal has appropriately implemented an ISMS. This assurance technique generates a report which may be used as audit evidence.	Operational	A penetration test is unlikely to be conducted by an auditor, with it instead, likely acting as client-generated audit evidence. No minimum qualification or certification requirements are mandated.	OFFICIAL-COMMERCIAL	Xop
	CAPS	Investigation and resolving of identified flaws	Operational	UK Government's List X scheme	SECRET, TOP SECRET	Xsig
Vulnerability Scan	Cyber Essentials	To check for signs of obvious and known vulnerabilities in a client's system, from both an internal and external vantage point.	Operational	The vulnerability scan must be conducted by an approved Certification Body from one of the four accrediation bodies of the Cyber Essentials scheme.	OFFICIAL-PERSONAL	Xsig
	ISO/IEC 27001	Ensures that the organisatonal has appropriately implemented an ISMS. This assurance technique generates a report which may be used as audit evidence.	Operational	A vulnerability scan is unlikely to be conducted by an auditor, with it instead, likely acting as client-generated audit evidence. No minimum qualification or certification requirements are mandated.	OFFICIAL-COMMERCIAL	Xop
	PCI DSS	This assurance technique generates a report which may be used as audit evidence (by a QSA).	Operational	ASV	OFFICIAL-COMMERCIAL	Xmin
	CPA	Investigation and resolving of identified flaws	Operational	ISO 17025 (Evaluation team), ISO 27001 (Lead auditor), ISO/IEC 27000:2005, ISO/IEC 18028:2006 (Product developers, 3rd party suppliers)	OFFICIAL	Xsig
	CTAS	Part of the Evaluation Work Program (EWP) which is aimed to clearly define the Target of Evaluation (ToE).	Operational	ISO 17025 (General lab requirements), ISO 27001 (lead auditor), CHECK Green Light, CLAS Consultant	OFFICIAL-COMMERCIAL	Xsig
	CC	Deals with the threat that an attacker will be able to discover flaws that will allow unauthorised to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.	Pre-deployment, Operational	ISO/IEC 15408-3	OFFICIAL-COMMERCIAL	Xsig
Social Engineering	CBEST/STAR	A report that describes the findings of the security posture of an organisation. This assurance technique will provide evidence about the susceptibility of some individuals in the organisation to social attacks. For CBEST engagement, this will be passed onto the UK Financial Authorities (i.e., the regulator). STAR report have no requirement for circulation.	Operational	CREST STAR Member Company and individuals with CREST STAR qualifications. A threat intelligence partner company is also needed.	OFFICIAL-COMMERCIAL	Xsig
Fuzzing	CPA	Check if robust or not	Operational	ISO 17025 (Evaluation team), ISO 27001 (Lead auditor), ISO/IEC 27000:2005, ISO/IEC 18028:2006 (Product developers, 3rd party suppliers)	OFFICIAL	Xsig
	CAPS	Check if robust or not	Pre-Deployment	UK Government's List X scheme	SECRET, TOP-SECRET	Xsig

Continued from previous page

Assurance Technique	Assurance Scheme	Intended Outcome	Stage Used	Qualifications and/or Certifications	Nature of input material	Extent of Contrib.
Formal Verification	CC	Provide supplement assurance by a (semi-)formal presentation of the requirements, functional specifications, high and low level design, depending on EAL level, to show correspondence.	Pre-Deployment	ISO/IEC 15408-3	OFFICIAL-COMMERCIAL	Xsig
Cryptographic Validation	CPA	Compliance with good commercial practice	Operational	FIPS-140/2, CAVP, CMVP, CESG/CAPS	OFFICIAL	Xmin
	CAS PKI CA	Compliance with CESG good practice guides and cryptographic policy	Operational	CAVP, CMVP FIPS, CPA	OFFICIAL-COMMERCIAL	Xsig
	CTAS	Part of the Evaluation Work Program (EWP) which is aimed to clearly define the Target of Evaluation (ToE).	Operational	ISO 17025 (General lab requirements), ISO 27001 (lead auditor), CHECK Green Light, CLAS Consultant	OFFICIAL-COMMERCIAL	Xop
	CC	Precludes the use of unvalidated cryptography for the cryptographic protection of sensitive or valuable data.	Pre-Deployment	FIPS-140/2	OFFICIAL-COMMERCIAL	Xsig
	CAPS	Compliance with in-house algorithms	Operational	UK Government's List X scheme	SECRET, TOP-SECRET	Xsig
Emanation Security Analysis	CAPS	Identify any leaking electromagnetic emanations	Pre-Deployment	UK Government's List X scheme	SECRET, TOP-SECRET	Xsig
Witnessed Test	CPA	Technical mitigations for the product to implement.	Operational	ISO 17025 (Evaluation team), ISO 27001 (Lead auditor), ISO/IEC 27000:2005, ISO/IEC 18028:2006 (Product developers, 3rd party suppliers)	OFFICIAL	Xmin
Virtual Lab Examination	CREST Practitioner (CPSA)	Successful candidates must score 60% of available marks in the written (54/90) and practical (90/150) comonents. The written component is multiple choice; answers for the practical assessment are also multiple choice.	N/A	None	OFFICIAL-PERSONAL	Xsig
	CREST Registered Tester (CRT)	Successful candidates must score 60% of available marks in the written (72/120) and practical (60/100) comonents. The written component is multiple choice; answers for the practical assessment are also multiple choice.	N/A	None for the candidate. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
	CREST Certified Tester (CCT INF and CCT APP)	Pass or fail. Three sections - candidates must score the minimum number of marks in each (fail in one section results in an overall fail): written component requiring 90/135 marks where 90 come from a multiple choice exam (1 mark each question), and 45 from a long-form exam (15 marks each question). The practical component requires 140/210 marks.	N/A	None for the candidate. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
	CREST STAR (CCSAS only; does not apply to CCSAM)	Pass or fail. Three sections - candidates must score the minimum number of marks in each (fail in one section results in an overall fail): written component requiring 90/135 marks where 90 come from a multiple choice exam (1 mark each question), and 45 from a long-form exam (15 marks each question). The practical component requires 140/210 marks. NOTE: The assessment for CCSAM does not include a virtual lab assessment, but instead an additional theory section.	N/A	CREST CCT	OFFICIAL-PERSONAL	Xsig
	Tiger Scheme QSTM	Pass of fail. Consists of multiple choice paper, long question, virtual lab, and viva interview. Pass/fail crtieria not stated.	N/A	None for the candidate. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
	Tiger Scheme SST	Pass or fail. Consists of multiple choice paper, long question, virtual lab, and viva interview. Pass/fail crtieria not stated.	N/A	Tiger Scheme QSTM. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
	Cyber Scheme Associate (CSTM)	Pass or fail (must pass all components w/ 60% or more, or all are failed): A 100-question one hour multiple choice exam. A one hour written paper which covers theoretical and practical aspects of the course content. A two hour practical assessment, which provides a full scenario for penetration testing. A 15 - 30-minute viva during which students will provide a synopsis of their findings from the practical assessment.	N/A	None for the candidate. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
	Cyber Scheme Team Leader (CSTL)	Pass or fail - unlike other Cyber Scheme qualifications, the CSTL is assessed through a one day practical virtual lab examination, and a viva interview from a CHECK Team Leader.	N/A	None for the candidate. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
Oral Examination (Viva Voce)	Tiger Scheme QSTM	Pass of fail. Consists of multiple choice paper, long question, virtual lab, and viva interview. Pass/fail crtieria not stated.	N/A	None for the candidate. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
	Tiger Scheme SST	Pass or fail. Consists of multiple choice paper, long question, virtual lab, and viva interview. Pass/fail crtieria not stated.	N/A	Tiger Scheme QSTM. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
	Cyber Scheme Associate (CSTM)	Pass or fail (must pass all components w/ 60% or more, or all are failed): A 100-question one hour multiple choice exam. A one hour written paper which covers theoretical and practical aspects of the course content. A two hour practical assessment, which provides a full scenario for penetration testing. A 15 - 30-minute viva during which students will provide a synopsis of their findings from the practical assessment.	N/A	None for the candidate. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
	Cyber Scheme Team Leader (CSTL)	Pass or fail - unlike other Cyber Scheme qualifications, the CSTL is assessed through a one day practical virtual lab examination, and a viva interview from a CHECK Team Leader.	N/A	None for the candidate. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
	CCP	Pass or fail - the candidate does or does not have the required level of experience and/or qualifications.	N/A	Each role is based upon industry experience. "Penetration Testing" is a unique role, as unlike the others it is aligned with industry qualifications. Candidate's must have these qualifications to obtain penetration testing roles.	OFFICIAL-PERSONAL	Xop

Continued from previous page

Assurance Technique	Assurance Scheme	Intended Outcome	Stage Used	Qualifications and/or Certifications	Nature of input material	Extent of Contrib.
Paper-Based Examination (Narrative Form)	CREST Certified Tester (CCT INF and CCT APP)	Pass or fail. Three sections - candidates must score the minimum number of marks in each (fail in one section results in an overall fail): written component requiring 90/135 marks where 90 come from a multiple choice exam (1 mark each question), and 45 from a long-form exam (15 marks each question). The practical component requires 140/210 marks.	N/A	None for the candidate. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
	CREST STAR (CCSAS and CCSAM)	Pass or fail. The assessment differs for CCSAS and CCSAS. CCSAM has a multiple choice, long-form and "scenario" (but still theory) component. CCSAS has a multiple choice, long-form, and virtual lab component. Candidates must pass all three sections to achieve the qualification.	N/A	CREST CCT	OFFICIAL-PERSONAL	Xsig
	Tiger Scheme QSTM	Pass of fail. Consists of multiple choice paper, long question, virtual lab, and viva interview. Pass/fail crtieria not stated.	N/A	None for the candidate. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
	Tiger Scheme SST	Pass of fail. Consists of multiple choice paper, long question, virtual lab, and viva interview. Pass/fail crtieria not stated.	N/A	Tiger Scheme QSTM. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
	Cyber Scheme Associate (CSTM)	Pass or fail (must pass all components w/ 60% or more, or all are failed): A 100-question one hour multiple choice exam. A one hour written paper which covers theoretical and practical aspects of the course content. A two hour practical assessment, which provides a full scenario for penetration testing. A 15 - 30-minute viva during which students will provide a synopsis of their findings from the practical assessment.	N/A	None for the candidate. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
Paper-Based Examination (Multiple-Choice)	CISSP	Pass or Fail depending on outcome of exam	N/A	For the candidate a minimum of five years experience in two of ten of CISSP's "domains" (topic themes).	OFFICIAL-PERSONAL	Xsig
	Certified Ethical Hacker (CEH)	Pass or fail - the candidate does or does not answer the appropriate number of questions correctly.	N/A	None	OFFICIAL-PERSONAL	Xsig
	CREST Practitioner (CPSA)	Successful candidates must score 60% of available marks in the written (54/90) and practical (90/150) comonents. The written component is multiple choice; answers for the practical assessment are also multiple choice.	N/A	None	OFFICIAL-PERSONAL	Xsig
	CREST Registered Tester (CRT)	Successful candidates must score 60% of available marks in the written (72/120) and practical (60/100) comonents. The written component is multiple choice; answers for the practical assessment are also multiple choice.	N/A	None for the candidate. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
	CREST Certified Tester (CCT INF and CCT APP)	Pass or fail. Three sections - candidates must score the minimum number of marks in each (fail in one section results in an overall fail): written component requiring 90/135 marks where 90 come from a multiple choice exam (1 mark each question), and 45 from a long-form exam (15 marks each question). The practical component requires 140/210 marks.	N/A	None for the candidate. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
	CREST STAR (CCSAS and CCSAM)	Pass or fail. The assessment differs for CCSAS and CCSAS. CCSAM has a multiple choice, long-form and "scenario" (but still theory) component. CCSAS has a multiple choice, long-form, and virtual lab component. Candidates must pass all three sections to achieve the qualification.	N/A	CREST CCT	OFFICIAL-PERSONAL	Xsig
	Tiger Scheme AST	Pass or fail. 80 multiple choice questions, with a 70% pass mark.	N/A	None	OFFICIAL-PERSONAL	Xsig
	Tiger Scheme QSTM	Pass of fail. Consists of multiple choice paper, long question, virtual lab, and viva interview. Pass/fail crtieria not stated.	N/A	None for the candidate. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
	Tiger Scheme SST	Pass of fail. Consists of multiple choice paper, long question, virtual lab, and viva interview. Pass/fail crtieria not stated.	N/A	Tiger Scheme QSTM. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
	Cyber Scheme Associate (CSA)	Pass or fail. Unknown number of multiple choice questions, with a 60% pass mark.	N/A	None	OFFICIAL-PERSONAL	Xsig
	Cyber Scheme Associate (CSTM)	Pass or fail (must pass all components w/ 60% or more, or all are failed): A 100-question one hour multiple choice exam. A one hour written paper which covers theoretical and practical aspects of the course content. A two hour practical assessment, which provides a full scenario for penetration testing. A 15 - 30-minute viva during which students will provide a synopsis of their findings from the practical assessment.	N/A	None for the candidate. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig
Employment History and Qualification Review	CISSP	Ensure that candidates with required work experience are able to appear for the exam	N/A	For the candidate a minimum of five years experience in two of ten of CISSP's "domains" (topic themes).	OFFICIAL-PERSONAL	Xsig
	CHECK Team Member	Pass or fail - the candidate does or does not have the required level of qualifications.	N/A	Requires a specific "Intermediate" level qualification (see Table) from one qualification body: CREST; Tiger Scheme; Cyber Scheme. Security Clearance (SC) is also required.	OFFICIAL-PERSONAL	Xsig
	CHECK Team Leader	Pass or fail - the candidate does or does not have the required level of qualifications.	N/A	Requires a specific "Advanced" level qualification (see Table) from one qualification body: CREST; Tiger Scheme; Cyber Scheme. Security Clearance (SC) is also required.	OFFICIAL-PERSONAL	Xsig

Continued from previous page

Assurance Technique	Assurance Scheme	Intended Outcome	Stage Used	Qualifications and/or Certifications	Nature of input material	Extent of Contrib.
	CCP	Pass or fail - the candidate does or does not have the required level of experience and/or qualifications.	N/A	Each role is based upon industry experience. "Penetration Testing" is a unique role, as unlike the others it is aligned with industry qualifications. Candidate's must have these qualifications to obtain penetration testing roles.	OFFICIAL-PERSONAL	Xsig
	CLAS	Pass or fail - the candidate does or does not have the required level of experience and/or qualifications.	N/A	"Any" level of CCP qualification is required. Also Security Clearance (SC).	OFFICIAL-PERSONAL	Xsig
	Tiger Scheme SST	Pass of fail. Consists of multiple choice paper, long question, virtual lab, and viva interview. Pass/fail crtieria not stated.	N/A	Tiger Scheme QSTM. For this qualification to qualify for the equivalent CHECK qualification, the exam must be invigilated by a CHECK Team Leader.	OFFICIAL-PERSONAL	Xsig

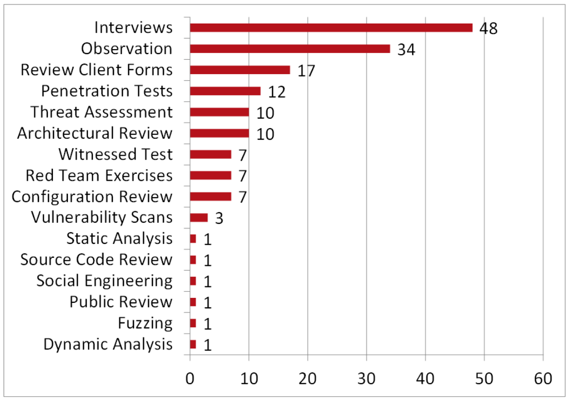
Appendix B: Mapping of Assurance Techniques to Assurance Controls

Security Clauses	Security Categories	Review of Documented Policies, Procedures, and Processes	Review of Client-Completed Self-Assessment Form	Threat Assessment	Architectural Review	Configuration Review	Source Code Review	Observe	Interview	Red Team Exercise	Penetration Testing	Vulnerability Scan	Social Engineering	Static Analysis	Dynamic Analysis	Fuzzing	Formal Verification	Cryptographic Validation	Emanation Security Analysis	Witnessed Test	Public Review
A.5 Information Security Policies	A.5.1 Management Direction for Information Security	Yes	Yes	No	No	No	No	Yes	Yes	No	No	No	No	No	No	No	No	No	No	Yes	No
A.6 Organisation of Information Security	A.6.1 Internal Organisation	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No	No	No	No	No	No	No	No	No	Yes	No
	A.6.2 Mobile Devices and Teleworking	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	Yes	No
A.7 Human Resource Security	A.7.1 Prior to Employment	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	No	Yes	No	No	No	No	No	No	Yes	No
	A.7.2 During Employment	Yes	Yes	No	No	No	No	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	Yes	No
	A.7.3 Termination and Change of Employment	Yes	Yes	No	No	No	No	Yes	Yes	No	No	No	No	No	No	No	No	No	No	Yes	No
A.8 Asset Management	A.8.1 Responsibility for Assets	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No	No	No	No	No	No	No	No	No	No	Yes	No
	A.8.2 Information Classification	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	Yes	No
	A.8.3 Media Handling	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	Yes	No
A.9 Access Control	A.9.1 Business Requirement of Access Control	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	Yes	No
	A.9.2 User Access Management	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	Yes	No
	A.9.3 User Responsibilities	Yes	Yes	No	No	No	No	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	Yes	No
	A.9.4 System and Application Access Control	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	Yes	No
A.10 Cryptography	A.10.1 Cryptographic Controls	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	No	No	No	No	No	Yes	No	Yes	No
A.11 Physical and Environmental Security	A.11.1 Secure Areas	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	Yes	No
	A.11.2 Equipment	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	Yes	No
A.12 Operations Security	A.12.1 Operational Procedures and Responsibilities	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	Yes	No
	A.12.2 Protection from Malware	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	Yes	No
	A.12.3 Backup	Yes	Yes	No	No	No	No	Yes	Yes	No	No	No	No	No	No	No	No	No	No	Yes	No
	A.12.4 Logging and Monitoring	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	No	No	No	No	No	No	No	No	No	Yes	No
	A.12.5 Control of Operational Software	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	Yes	No
	A.12.6 Technical Vulnerability Management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	A.12.7 Information Systems Audit Considerations	Yes	Yes	No	No	No	No	Yes	Yes	No	No	No	No	No	No	No	No	No	No	Yes	No
A.13 Communications Security	A.13.1 Network Security Management	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No
	A.13.2 Information Transfer	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	Yes	Yes	Yes	No
A.14 System Acquisition, Development, and Maintenance	A.14.1 Security Requirement of Information Systems	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No
	A.14.2 Security in Development and Support Processes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	A.14.3 Test Data	Yes	Yes	No	No	No	No	Yes	Yes	No	No	No	No	No	No	No	No	No	No	Yes	No
A.15 Supplier Relationships	A.15.1 Information Security in Supplier Relationships	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No	No	No	No	No	No	No	No	No	Yes	No
	A.15.2 Supplier Service Delivery Management	Yes	Yes	No	No	No	No	Yes	Yes	No	No	No	No	No	No	No	No	No	No	Yes	No
A.16 Information Security Incident Management	A.16.1 Management of Information Security Incidents and Improvements	Yes	Yes	No	No	No	No	Yes	Yes	No	No	No	No	No	No	No	No	No	No	Yes	No
A.17 Information Security Aspects of Business Continuity Management	A.17.1 Information Security Continuity	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No	No	No	No	No	No	No	No	No	Yes	No
	A.17.2 Redundancies	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No	No	No	No	No	No	No	No	No	Yes	No
A.18 Compliance	A.18.1 Compliance with Legal and Contractual Requirements	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	Yes	No	Yes	No
	A.18.2 Information Security Reviews	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

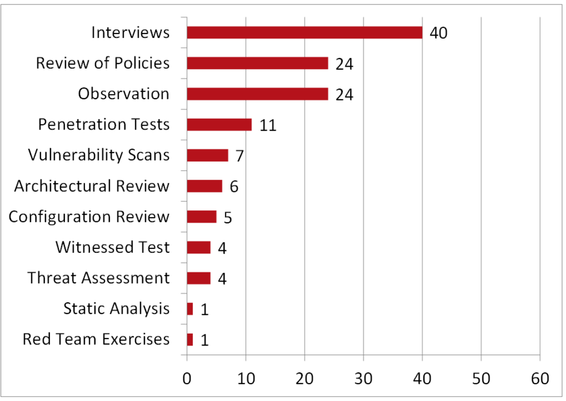
Control Families	Assurance Technique Count
A.5.1 Management Direction for Information Security	5
A.6.1 Internal Organisation	6
A.6.2 Mobile Devices and Teleworking	9
A.7.1 Prior to Employment	7
A.7.2 During Employment	8
A.7.3 Termination and Change of Employment	5
A.8.1 Responsibility for Assets	7
A.8.2 Information Classification	10
A.8.3 Media Handling	9
A.9.1 Business Requirement of Access Control	12
A.9.2 User Access Management	9
A.9.3 User Responsibilities	8
A.9.4 System and Application Access Control	10
A.10.1 Cryptographic Controls	10
A.11.1 Secure Areas	10
A.11.2 Equipment	10
A.12.1 Operational Procedures and Responsibilities	11
A.12.2 Protection from Malware	9
A.12.3 Backup	5
A.12.4 Logging and Monitoring	7
A.12.5 Control of Operational Software	9
A.12.6 Technical Vulnerability Management	20
A.12.7 Information Systems Audit Considerations	5
A.13.1 Network Security Management	14
A.13.2 Information Transfer	12
A.14.1 Security Requirement of Information Systems	13
A.14.2 Security in Development and Support Processes	19
A.14.3 Test Data	5
A.15.1 Information Security in Supplier Relationships	6
A.15.2 Supplier Service Delivery Management	5
A.16.1 Management of Information Security Incidents and Improvements	5
A.17.1 Information Security Continuity	6
A.17.2 Redundancies	6
A.18.1 Compliance with Legal and Contractual Requirements	10
A.18.2 Information Security Reviews	19

Table 11: The Number of Assurance Techniques for Each Security Control Family

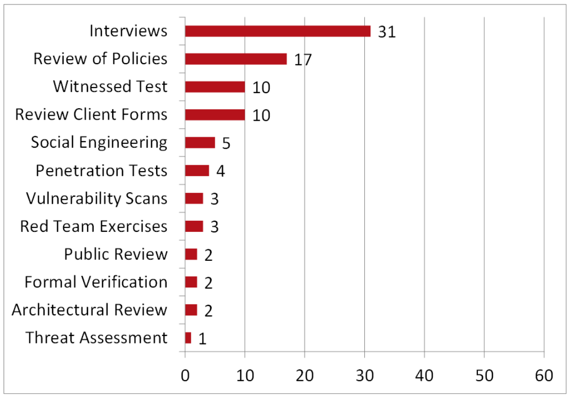
Appendix C: Complementary Assurance Techniques



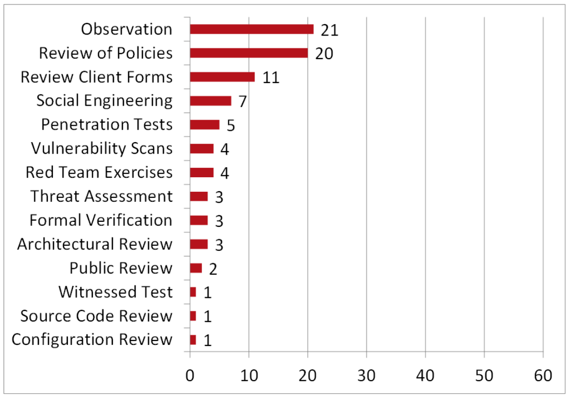
C1: Review of Policies



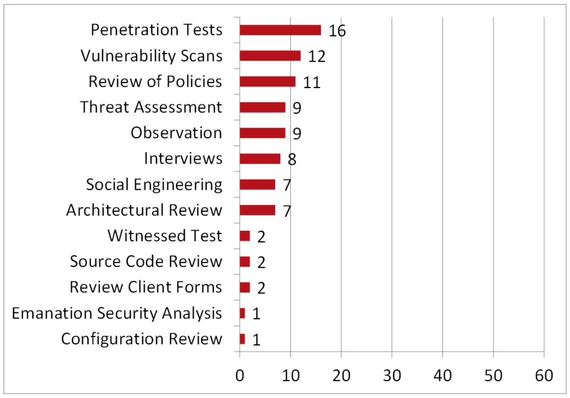
C2: Review of Client Forms



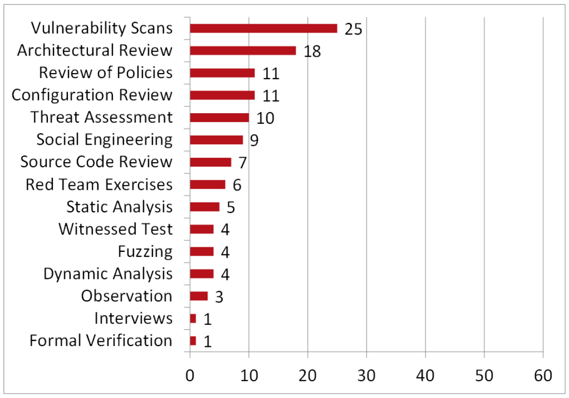
C3: Observation



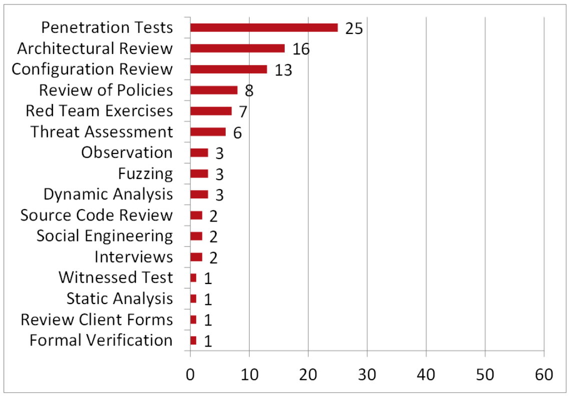
C4: Interviews



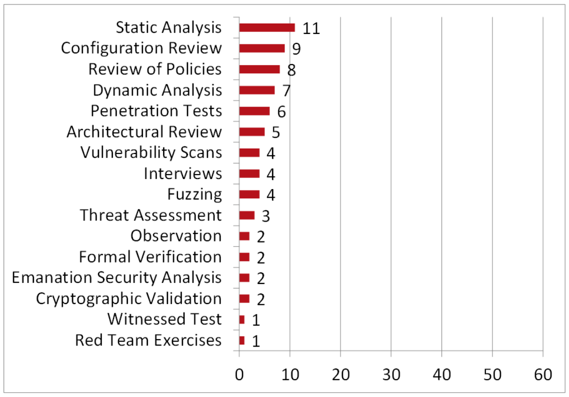
C5: Red Team Exercise



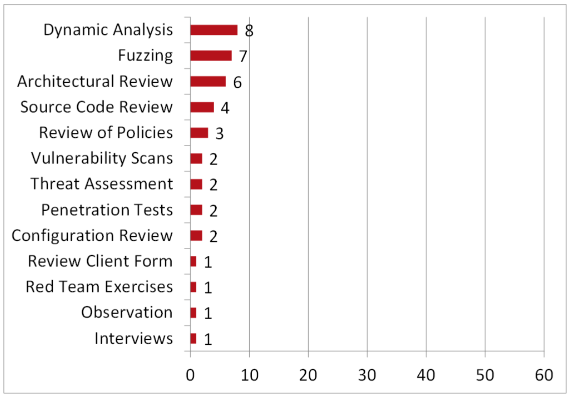
C6: Penetration Tests



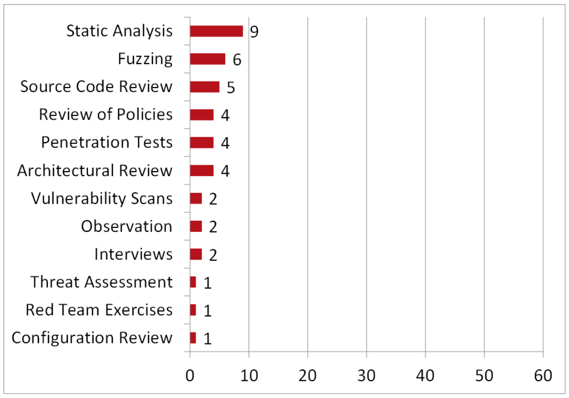
C7: Vulnerability Scans



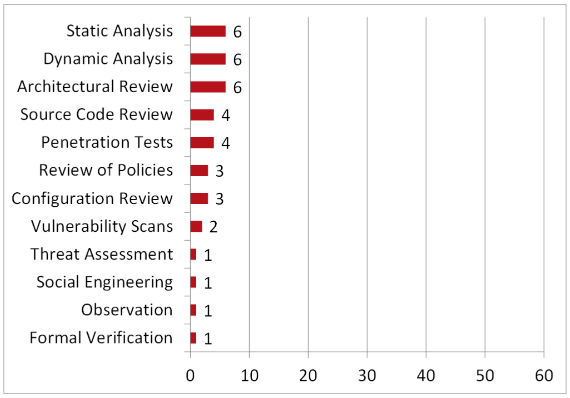
C8: Source Code Review



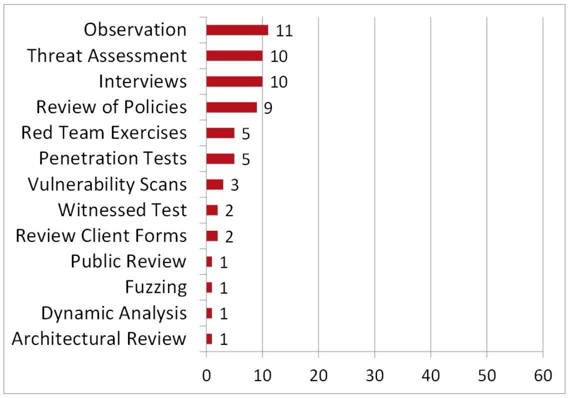
C9: Static Analysis



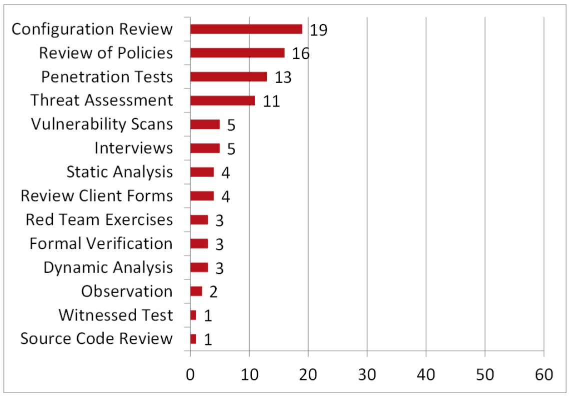
C10: Dynamic Analysis



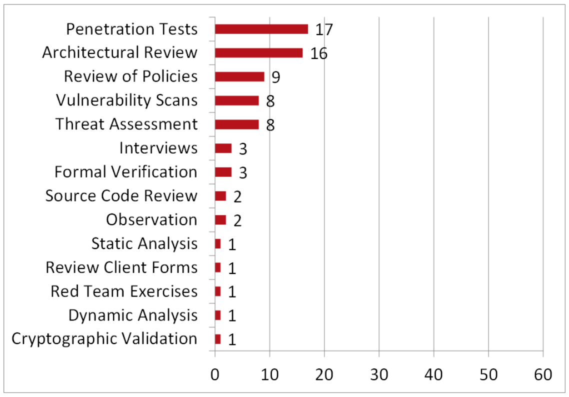
C11: Fuzzing



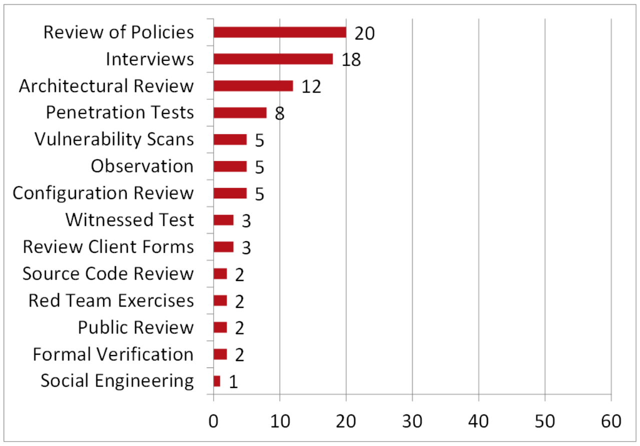
C12: Social Engineering



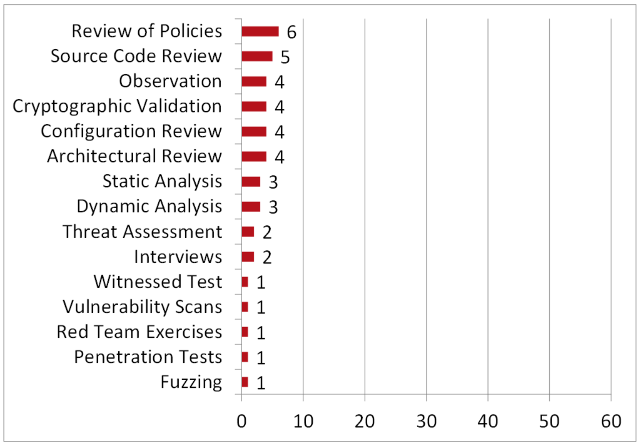
C13: Architectural Review



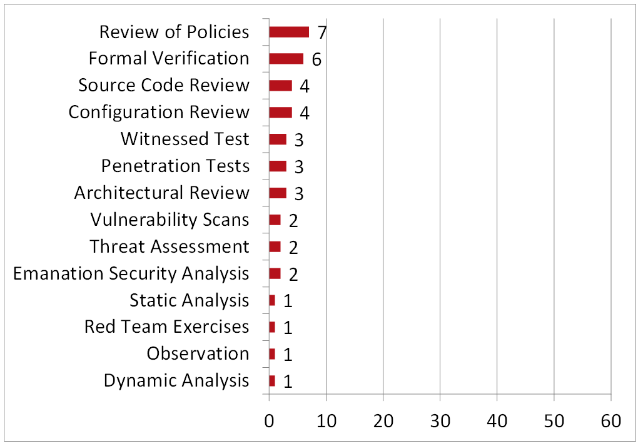
C14: Configuration Review



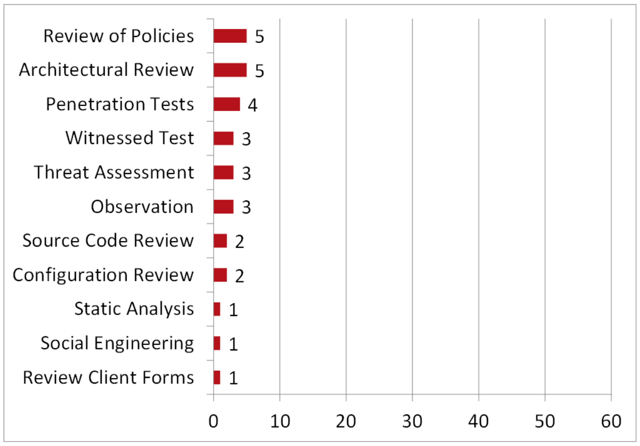
C15: Threat Assessment



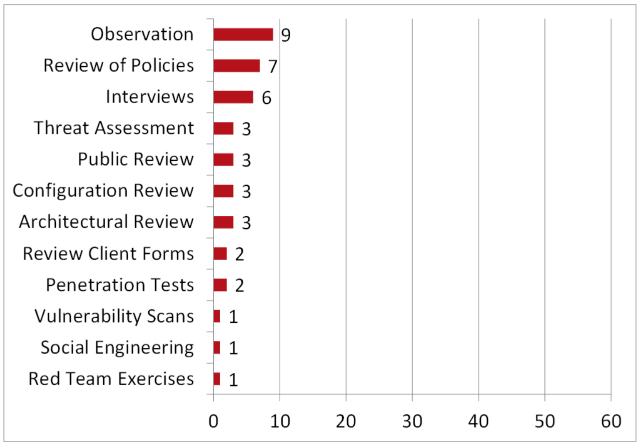
C16: Formal Verification



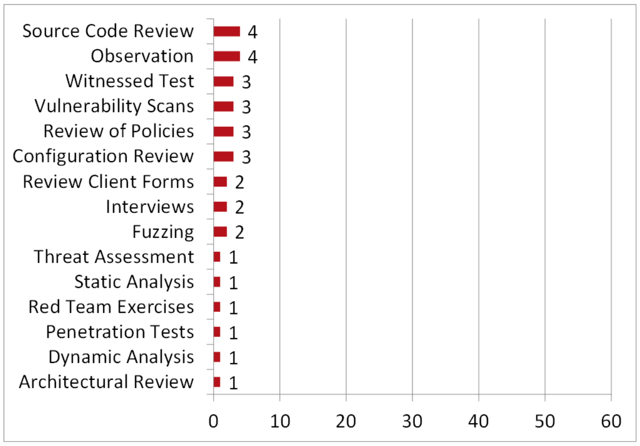
C17: Cryptographic Validation



C18: Emanation Security Analysis



C19: Witnessed Test



C20: Public Review

Appendix D: Combinations of Assurance Techniques

Label	**Combination of assurance techniques for Sec. Controls**
Comb. 1	Reviewing Documented Policies, Procedures, and Processes; Interviews; Observation; Reviewing Client-Completed Self-Assessment Form
Comb. 2	Observation; Interviews; Witnessed Test; Reviewing Documented Policies, Procedures, and Processes
Comb. 3	Red Team Exercise; Penetration Tests; Reviewing Documented Policies, Procedures, and Processes; Vulnerability Scans
Comb. 4	Penetration Test; Architectural Review; Vulnerability Scans; Reviewing Documented Policies, Procedures, and Processes
Comb. 5	Vulnerability Scans; Architectural Review; Configuration Review; Penetration Tests
Comb. 6	Source Code Review; Configuration Review; Static Analysis Reviewing Documented Policies, Procedures, and Processes
Comb. 7	Static Analysis; Architectural Review; Dynamic Analysis; Fuzzing
Comb. 8	Dynamic Analysis; Fuzzing; Source Code Review; Static Analysis
Comb. 9	Social Engineering; Interviews; Observation; Threat Assessment
Comb. 10	Architectural Review; Configuration Review; Penetration Tests; Reviewing Documented Policies, Procedures, and Processes
Comb. 11	Threat Assessment; Architectural Review; Interviews; Reviewing Documented Policies, Procedures, and Processes
Comb. 12	Formal Verification; Architectural Review; Social Engineering; Reviewing Documented Policies, Procedures, and Processes
Comb. 13	Cryptographic Validation; Configuration Review; Formal Verification; Reviewing Documented Policies, Procedures, and Processes
Comb. 14	Emanation Analysis; Architectural Review; Penetration Testing; Reviewing Documented Policies, Procedures, and Processes
Comb. 15	Witnessed Test; Interviews; Observations; Reviewing Documented Policies, Procedures, and Processes
Comb. 16	Public Reviews; Observations; Source Code Review; Vulnerability Scans

Table 12: Combinations of assurance techniques for security controls

Label	**Combination of assurance techniques for Ind. Competences**
Comb. 1	Virtual Lab Examination, Oral Examination (Viva-Voce) Paper Based Examination (Narrative form), Paper Based Examination (Multiple choice) Employment History and Qualification Review
Comb. 2	Virtual Lab Examination, Oral Examination (Viva-Voce) Paper Based Examination (Narrative form), Paper Based Examination (Multiple choice)
Comb. 3	Virtual Lab Examination, Oral Examination (Viva-Voce) Paper Based Examination (Narrative form), Employment History and Qualification Review
Comb. 4	Virtual Lab Examination, Oral Examination (Viva-Voce) Paper Based Examination (Narrative form)
Comb. 5	Virtual Lab Examination, Oral Examination (Viva-Voce) Paper Based Examination (Multiple choice), Employment History and Qualification Review
Comb. 6	Virtual Lab Examination, Oral Examination (Viva-Voce) Employment History and Qualification Review
Comb. 7	Virtual Lab Examination, Oral Examination (Viva-Voce)
Comb. 8	Virtual Lab Examination, Paper Based Examination (Narrative form) Employment History and Qualification Review
Comb. 9	Virtual Lab Examination, Paper Based Examination (Narrative form)
Comb. 10	Virtual Lab Examination, Paper Based Examination (Multiple choice) Employment History and Qualification Review
Comb. 11	Virtual Lab Examination, Paper Based Examination (Multiple choice)
Comb. 12	Virtual Lab Examination, Employment History and Qualification Review
Comb. 13	Paper Based Examination (Narrative form), Paper Based Examination (Multiple choice) Employment History and Qualification Review
Comb. 14	Paper Based Examination (Narrative form), Employment History and Qualification Review
Comb. 15	Oral Examination (Viva-Voce), Paper Based Examination (Narrative form) Paper Based Examination (Multiple choice), Employment History and Qualification Review
Comb. 16	Oral Examination (Viva-Voce), Paper Based Examination (Narrative form) Paper Based Examination (Multiple choice)
Comb. 17	Oral Examination (Viva-Voce), Paper Based Examination (Narrative form) Employment History and Qualification Review
Comb. 18	Oral Examination (Viva-Voce), Paper Based Examination (Narrative form)
Comb. 19	Oral Examination (Viva-Voce), Paper Based Examination (Multiple choice) Employment History and Qualification Review
Comb. 20	Oral Examination (Viva-Voce), Paper Based Examination (Multiple choice)
Comb. 21	Oral Examination (Viva-Voce), Employment History and Qualification Review

Table 13: Combinations of assurance techniques for Individual Competences

Appendix E: Cost-Effectiveness Calculations

Cost-effectiveness was defined in this study as a metric that expresses the relative cost and effectiveness of an assurance technique and depended on whether it was aiming to assure security controls and individual competences as follows:

- Assurance Techniques for *Security Controls*

  Data for the calculation of cost-effectiveness is based on information requested via the on-line survey, i.e., respondents' confidence in input (high, medium, low), and perceived effectiveness (excellent, very good, good, fair, poor) and cost (extremely expensive, very expensive, expensive, moderate, cheap) of the assurance technique. The mapping of qualitative values to quantitative ones is made using the following assignments:

  - Confidence = {(high = 1), (medium = 0.5), (low = 0.1)}
  - Effectiveness = {(excellent = 1), (very good = 0.8), (good = 0.6), (fair = 0.4), (poor = 0.2)}
  - Cost = {(extremely expensive = 1), (very expensive = 0.8), (expensive = 0.6), (moderate = 0.4), (cheap = 0.2)}

  Based on this, the following formula to calculate the cost-effectiveness of an assurance technique (AT) is:

  $\text{Cost-Effectiveness}_{AT} = \text{Overall\_Effectiveness}_{AT} \times (1 - \text{Overall\_Cost}_{AT})$

  In the above mentioned formula, for the calculation of the overall effectiveness, it is required to calculate the frequency of variables value, i.e., obtain counts on a single variable's values. This results in the calculation of percentage values for all single variable's values in the range of [0,1]. Since the cost for each assurance activity is considered to be inversely proportional to its overall effectiveness, we subtract cost from 1 (all values are expressed in [0,1]). With VP we refer to "Valid Percentage" that does not include missing cases, and is analysed as $VP_{value} = \frac{\text{Value Occurrences}}{\text{Total number of values}}, VP \in [0,1]$. In addition, we have that:

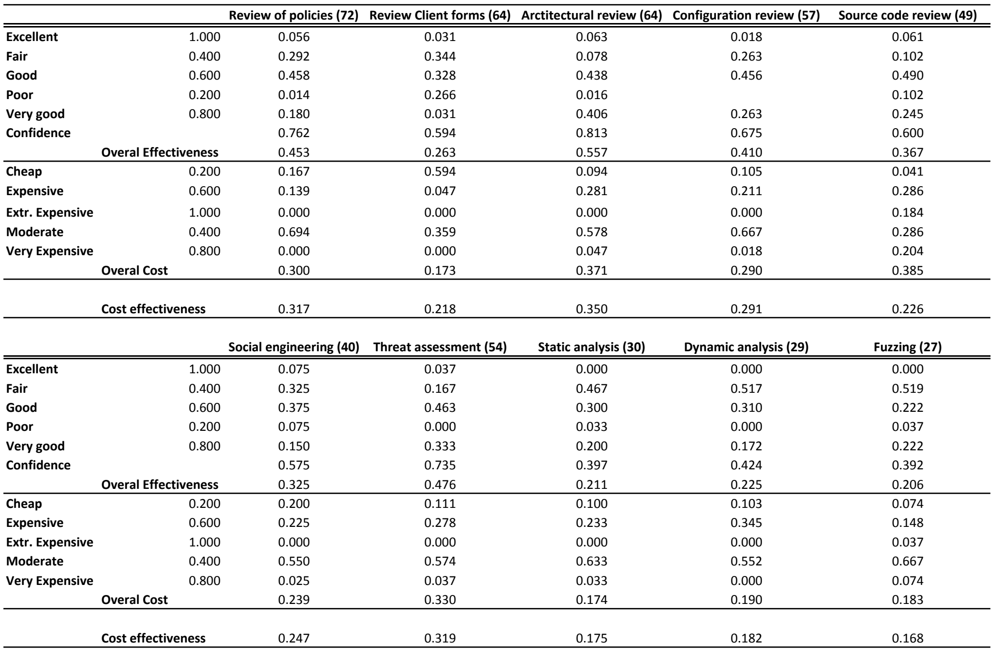
  $\text{Confidence}_{AT} = (1 \times VP_{high} + 0.5 \times VP_{medium} + 0.1 \times VP_{low})$

  $\text{Overall\_Effectiveness}_{AT} = \text{Confidence}_{AT} \times (1 \times VP_{excellent} + 0.8 \times VP_{very\ good} + 0.6 \times VP_{good} + 0.4 \times VP_{fair} + 0.2 \times VP_{poor})$

  , and,

  $\text{Overall\_Cost}_{AT} = \text{Confidence}_{AT} \times (1 \times VP_{extremely\ expensive} + 0.8 \times VP_{very\ expensive} + 0.6 \times VP_{expensive} + 0.4 \times VP_{moderate} + 0.2 \times VP_{cheap})$

  The following table provides detailed information on the calculated values of variables for all the examined assurance techniques for security controls:



		Review of policies (72)	Review Client forms (64)	Arctitectural review (64)	Configuration review (57)	Source code review (49)
Excellent	1.000	0.056	0.031	0.063	0.018	0.061
Fair	0.400	0.292	0.344	0.078	0.263	0.102
Good	0.600	0.458	0.328	0.438	0.456	0.490
Poor	0.200	0.014	0.266	0.016		0.102
Very good	0.800	0.180	0.031	0.406	0.263	0.245
Confidence		0.762	0.594	0.813	0.675	0.600
Overal Effectiveness		0.453	0.263	0.557	0.410	0.367
Cheap	0.200	0.167	0.594	0.094	0.105	0.041
Expensive	0.600	0.139	0.047	0.281	0.211	0.286
Extr. Expensive	1.000	0.000	0.000	0.000	0.000	0.184
Moderate	0.400	0.694	0.359	0.578	0.667	0.286
Very Expensive	0.800	0.000	0.000	0.047	0.018	0.204
Overal Cost		0.300	0.173	0.371	0.290	0.385
Cost effectiveness		0.317	0.218	0.350	0.291	0.226

		Social engineering (40)	Threat assessment (54)	Static analysis (30)	Dynamic analysis (29)	Fuzzing (27)
Excellent	1.000	0.075	0.037	0.000	0.000	0.000
Fair	0.400	0.325	0.167	0.467	0.517	0.519
Good	0.600	0.375	0.463	0.300	0.310	0.222
Poor	0.200	0.075	0.000	0.033	0.000	0.037
Very good	0.800	0.150	0.333	0.200	0.172	0.222
Confidence		0.575	0.735	0.397	0.424	0.392
Overal Effectiveness		0.325	0.476	0.211	0.225	0.206
Cheap	0.200	0.200	0.111	0.100	0.103	0.074
Expensive	0.600	0.225	0.278	0.233	0.345	0.148
Extr. Expensive	1.000	0.000	0.000	0.000	0.000	0.037
Moderate	0.400	0.550	0.574	0.633	0.552	0.667
Very Expensive	0.800	0.025	0.037	0.033	0.000	0.074
Overal Cost		0.239	0.330	0.174	0.190	0.183
Cost effectiveness		0.247	0.319	0.175	0.182	0.168

		Observation (41)	Interview (55)	Red team exercise (42)	Penetration testing (56)	Vulnerability scan (55)
Excellent	1.000	0.024	0.036	0.167	0.125	0.055
Fair	0.400	0.439	0.273	0.048	0.054	0.236
Good	0.600	0.317	0.327	0.381	0.321	0.345
Poor	0.200	0.000	0.055	0.048	0.000	0.036
Very good	0.800	0.220	0.309	0.357	0.500	0.327
Confidence		0.573	0.713	0.674	0.782	0.725
	Overal Effectiveness	0.324	0.427	0.479	0.578	0.453
Cheap	0.200	0.195	0.164	0.048	0.018	0.491
Expensive	0.600	0.171	0.255	0.524	0.518	0.200
Extr. Expensive	1.000	0.000	0.018	0.024	0.018	0.000
Moderate	0.400	0.634	0.545	0.238	0.339	0.291
Very Expensive	0.800	0.000	0.018	0.167	0.107	0.018
	Overal Cost	0.227	0.311	0.389	0.433	0.253
	Cost effectiveness	0.251	0.295	0.293	0.328	0.339

		Formal verification (32)	Cryptogtaphic validation (31)	Emanation security analysis (26)	Witnessed test (30)	Public review (26)
Excellent	1.000	0.000	0.065	0.000	0.033	0.038
Fair	0.400	0.281	0.226	0.385	0.267	0.385
Good	0.600	0.375	0.452	0.385	0.400	0.269
Poor	0.200	0.031	0.000	0.077	0.100	0.192
Very good	0.800	0.313	0.258	0.154	0.200	0.115
Confidence		0.594	0.510	0.419	0.594	0.354
	Overal Effectiveness	0.353	0.323	0.219	0.332	0.171
Cheap	0.200	0.000	0.065	0.077	0.133	0.423
Expensive	0.600	0.219	0.290	0.308	0.400	0.154
Extr. Expensive	1.000	0.219	0.129	0.038	0.000	0.038
Moderate	0.400	0.313	0.258	0.346	0.367	0.308
Very Expensive	0.800	0.250	0.258	0.231	0.100	0.077
	Overal Cost	0.401	0.319	0.235	0.293	0.142
	Cost effectiveness	0.211	0.220	0.168	0.235	0.147

The following tables provide detailed information on the calculated values of variables for all the identified combinations of assurance techniques (described in *Appendix D:Combinations of Assurance Techniques*):

			Comb. 1	Comb. 2	Comb. 3	Comb. 4	Comb. 5	Comb. 6	Comb. 7	Comb. 8
Cost effectiveness			0.317	0.251	0.293	0.328	0.339	0.226	0.175	0.182
	Effectiveness		0.453	0.324	0.479	0.578	0.453	0.367	0.211	0.225
			Reviewing Documented Policies, Procedures, and Processes	Observation	Red Team Exercise	Penetration Test	Vulnerability Scans	Source Code Review	Static Analysis	Dynamic Analysis
0.350	0.557	Architectural Review				**X**	**X**		**X**	
0.291	0.410	Configuration Review					**X**	**X**		
0.220	0.323	Cryptographic Validation								
0.182	0.225	Dynamic Analysis							**X**	
0.168	0.219	Emanation Analysis								
0.211	0.353	Formal Verification								
0.168	0.206	Fuzzing							**X**	**X**
0.295	0.427	Interviews	**X**	**X**						
0.251	0.324	Observation	**X**							
0.328	0.578	Penetration Tests			**X**		**X**			
0.147	0.171	Public Review								
0.293	0.479	Red Team Exercises								
0.218	0.263	Reviewing Client-Completed Self-Assessment Form	**X**							
0.317	0.453	Reviewing Documented Policies, Procedures, and Processes		**X**	**X**	**X**		**X**		
0.247	0.325	Social Engineering								
0.226	0.367	Source Code Review								**X**
0.175	0.211	Static Analysis						**X**		**X**
0.319	0.476	Threat Assessment								
0.339	0.453	Vulnerability Scans			**X**	**X**				
0.235	0.332	Witnessed Test		**X**						
Effectiness of combination			0.017	0.021	0.057	0.066	0.060	0.014	0.005	0.004
Cost effectiveness of combination			0.005	0.005	0.010	0.012	0.011	0.004	0.002	0.001

			Comb. 9	Comb. 10	Comb. 11	Comb. 12	Comb. 13	Comb. 14	Comb. 15	Comb. 16
Cost effectiveness			0.247	0.350	0.319	0.211	0.220	0.168	0.235	0.147
	Effectiveness		0.325	0.557	0.476	0.353	0.323	0.219	0.332	0.171
			Social Engineering	Architectural Review	Threat Assessment	Formal Verification	Cryptographic Validation	Emanation Analysis	Witnessed Test	Public Review
0.350	0.557	Architectural Review			X	X		X		
0.291	0.410	Configuration Review		X			X			
0.220	0.323	Cryptographic Validation								
0.182	0.225	Dynamic Analysis								
0.168	0.219	Emanation Analysis								
0.211	0.353	Formal Verification					X			
0.168	0.206	Fuzzing								
0.295	0.427	Interviews	X		X				X	
0.251	0.324	Observation	X						X	X
0.328	0.578	Penetration Tests		X				X		
0.147	0.171	Public Review								
0.293	0.479	Red Team Exercises								
0.218	0.263	Reviewing Client-Completed Self-Assessment Form								
0.317	0.453	Reviewing Documented Policies, Procedures, and Processes		X	X	X	X	X	X	
0.247	0.325	Social Engineering								
0.226	0.367	Source Code Review				X				X
0.175	0.211	Static Analysis								
0.319	0.476	Threat Assessment	X							
0.339	0.453	Vulnerability Scans								X
0.235	0.332	Witnessed Test								
Effectiness of combination			0.021	0.060	0.051	0.033	0.021	0.032	0.021	0.009
Cost effectiveness of combination			0.006	0.011	0.010	0.005	0.004	0.006	0.005	0.003

- Assurance Techniques for *Individual Competences*

  For the calculation of cost-effectiveness of individuals' competencies we use the following formula, which simply expresses that based on the perceived overall cost-effectiveness information provided by responders. Thus, we have that:

  $\text{Cost-Effectiveness}_{competency} = \text{Overal\_Cost-Effectiveness}_{expert\ knowledge}$

  Similarly to the calculation of assurance activities, we express the perceived cost-effectiveness as:

  $\text{CostEffectiveness}_{competency} = (1 \times VP_{excellent} + 0.8 \times VP_{very\ good} + 0.6 \times VP_{good} + 0.4 \times VP_{fair} + 0.2 \times VP_{poor})$

The following table provides detailed information on the calculated values of variables for all the examined assurance techniques for individual competences:

		Virtual Lab Examination (74)	Oral Examination (Viva-Voce) (93)	Paper Based Examination (Narrative form) (92)
Excellent	1.000	0.068	0.140	0.022
Fair	0.400	0.216	0.151	0.239
Good	0.600	0.378	0.323	0.359
Poor	0.200	0.081	0.043	0.054
Very good	0.800	0.257	0.344	0.326
Confidence		1.000	1.000	1.000
Cost effectiveness		0.603	0.678	0.605

		Paper Based Examination (Multiple choice) (97)	Employment History and Qualification Review (100)
Excellent	1.000	0.010	0.110
Fair	0.400	0.278	0.150
Good	0.600	0.381	0.290
Poor	0.200	0.165	0.060
Very good	0.800	0.165	0.390
Confidence		1.000	1.000
Cost effectiveness		0.515	0.668