Cybersecurity Assurance and Certification for Systems

Daniel S Fowler
Secure Cyber Systems
Research Group (SCSRG)
WMG, University of Warwick
Coventry, UK, CV4 7AL
dan.fowler@warwick.ac.uk

Gregory Epiphaniou
Secure Cyber Systems
Research Group (SCSRG)
WMG, University of Warwick
Coventry, UK, CV4 7AL
gregory.epiphaniou@warwick.ac.uk

Carsten Maple
Secure Cyber Systems
Research Group (SCSRG)
WMG, University of Warwick
Coventry, UK, CV4 7AL
cm@warwick.ac.uk

***Abstract*— Society requires assurances that sufficient levels of cybersecurity exist to reduce cyber-attack risk. Achieving cybersecurity goals for components, sub-systems, and systems will require appropriate security-focused processes. Furthermore, organisations will need to operate with enhanced security when supplying government and military systems. Systems for highly classified use, e.g., SECRET or TOP SECRET, will require additional security controls applied to system designs. Additionally, customers for systems are likely to require proof of a security-focused supply chain throughout the system's life cycle. The engineering processes for systems should not introduce potential cybersecurity vulnerabilities and cater for ongoing or emerging security risks. Here, a holistic view of security certification is provided, allowing organisations, and others, to understand how certification can aid the provision of security assurance. Certification for an organisation against a security process standard, e.g., ISO/IEC 27001, contributes to security assurance. Likewise, security certification of components, sub-systems, or a system can adhere to an internationally recognised standard, e.g., Common Criteria, which is foundational to the new European cybersecurity certification scheme, for which a discussion is provided.**

1. Introduction

Despite decades of investment into cybersecurity, incidents of system security failure still occur with regularity [1]. It is impossible to guarantee that a system will not be subjected to a cybersecurity incident, indeed *"security breaches are inevitable"* [2]. Yet billions of us continue to use connected systems and the Internet successfully every day. Indeed, we trust the computer-controlled systems we interact with, whether websites, electronic payment systems, the vehicles we travel in, our smartphones, or the connected washing machine. It could be argued that despite all the cybersecurity issues and concerns, and seemingly piecemeal and incremental implementation of cybersecurity [3], we have successfully engineered a usable and useful supersystem-of-systems that is our digitally connected world. However, concerns around the trustworthiness of systems remain and people, organisations, and governments want evidence that cybersecurity is addressed. For example, since the mid-2010s [4], the UK Government and Ministry of Defence (MOD) have required supply chain organisations to be signed up to the UK's Cyber Essentials (CE) scheme, see Section 6, as a *minimum* requirement. Such *certification* schemes are designed to provide a level of *assurance* in the cybersecurity capabilities of people and processes. Yet, cybersecurity assurance and certification are large topics with few succinct summaries existing for new organisations, particularly those that wish to engage with governmental bodies. That issue is addressed in the following sections. Section 2 provides a definition for assurance, Section 3 discusses the various meanings of certification, Section 4 provide an overview of commonly used security standards and guidelines, Section 5 provides an interesting discussion on security gradations that are often used by governments and military organisations, Section 6 discusses supply chains and how suppliers need to demonstrate their cybersecurity capabilities, Section 7 provides an overview of Common Criteria and the European cybersecurity certification scheme (with supplementary information in the Appendix), and Section 8 concludes.

2. What is Security Assurance?

Security Assurance is a long-standing concept. It is defined in the 1991 *Information Technology Security Evaluation Criteria* (ITSEC) [5] as *"Assurance: the confidence that may be held in the security provided by a Target of Evaluation."* Generally, a Target of Evaluation (ToE) is any component, device, sub-system, or system. It is the item being evaluated for its security aspects. It applies to the system's hardware and software and all its constituent parts.

ITSEC is a forerunner of the *Common Criteria for Information Technology Security Evaluation* [6], [7], [8], [9], which is simply referred to as Common Criteria (CC), see Section 7. The International Organization for Standardization (ISO) publishes, in association with the International Electrotechnical Commission (IEC), the standard ISO/IEC 15408 [10] which is derived from CC.

3. What is Certification?

Certification is an assurance that a product, system, process, or person is meeting an expectation laid out in a series of rules. The types of rules can fall into different categories:

1. *Functional operation of a product, device, or software interface* - determining if components, sub-systems, and systems perform according to their design specifications, national and international engineering standards, interoperability requirements (e.g., physical connectors, wireless interfaces, protocols, APIs), and contractual requirements. For example, assessing a component against its operational parameters from datasheets or technical manuals. This is usually a point-in-time certification and is often subject to periodic recertification.
2. *Non-functional attributes of a product, device, or software* - determining if non-functional aspects meet the expectations of a guideline or standard. This can include hazard analysis, the styling of the human-machine interface, and security aspects.
3. *Procedural, process, or methodology* - determining if a system or service's operational and/or management aspects are maintained.
4. *A person's education, training, and skillset* - determining if a person has the correct knowledge, abilities, and experience to perform a role or task.

This work is not concerned with functional certification of

systems, i.e., point 1 above, but it does address how security assurance can be derived from points 3 to 4. Security assurance as a non-functional attribute (point 2 above) is concerned with demonstrating the acknowledgement and mitigation of existing and future security threats. Different techniques can be used to address potential threats to targets (products, devices, software, or systems). These threat targets can be assessed using threat modelling and/or Threat Analysis and Risk Assessment (TARA). This will identify security weaknesses and allow appropriate mitigation to be performed by the supplier or manufacturer, impacting the functional design.

A system that can be used across organisational and national boundaries, for example, a communications system, needs to ensure that security assurance assessments are comparable. Few methodologies address transnational security assurance, one widely used scheme is CC.

Procedural, process, or methodology security assurance (point 3 above) is concerned with adherence to a guideline or standard to ensure that the operational, management and life cycle aspects of a system meet the relevant level for certification. Security controls can be placed onto processes and/or risk assessments performed to increase security assurance. The widely used standard ISO/IEC 27001 [11] is for the *"...requirements for establishing, implementing, maintaining and continually improving an information security management system..."*.

ISO/IEC 27001 is used by organisations for guidance on an Information Security Management System (ISMS). The ISMS can be used to implement policies to improve the security of information assets and their processing systems. ISO/IEC 27001 is further discussed in Section 4. Certification for ISO/IEC 27001 can be achieved via an accredited organisation.

Alternatives to the ISO/IEC 27001 ISMS exist, these include the *CIS Controls* [12] from the Center for Internet Security and the US National Institute of Standards and Technology (NIST) *Security and Privacy Controls for Information Systems and Organizations* [13]. Organisations using these security controls are likely to require self-certification. Spreadsheets are available that can be used to guide self-certification.

The arrangement and the description of the security controls do differ between ISO/IEC 27001, NIST and CIS. However, there are similarities, and it is possible to perform mappings between them. For example, all three have controls over the management of accounts to access system resources. However, items may not exist across all three. For example, whilst all three cover employee security awareness training, NIST has a sub-control on training to recognise insider threats, which is not present in 27001 and CIS. Security control frameworks are unlikely to cover all eventualities for all organisations, and organisations should be aware of their specific requirements.

Security certification of people (point 4) is dominated by Information Technology (IT) enterprise requirements, and a variety of organisations offer training, exams, and knowledge to cater for enterprise requirements. There are many organisations offering certification exams. Examples include:

- Computing Technology Industry Association (CompTIA) certifications, e.g., Security+.
- $(ISC)^2$, formally International Information System Security Certification Consortium, e.g., Certified Information Systems Security Professional (CISSP)
- Information Systems Audit and Control Association (ISACA), e.g., Certified Information Systems Auditor (CISA)

4. STANDARDS FOR SYSTEMS SECURITY

There exists an extensive public body of work on the security of systems and information assurance certification. This means that organisations can use that existing knowledge to build up their cybersecurity capabilities and address their specific security challenges. However, smaller organisations engaging with larger bodies are likely to need to conform to documentation that is not in the public domain, e.g., classified government and military documents, and commercially sensitive documents.

Security Assurance for Service Provision

Many larger organisations will follow service management methodologies to help maintain service quality and formerly manage the service provision. Examples include:

- ITIL (Information Technology Infrastructure Library) for IT service management
- ISO/IEC 20000 IT service management

Similarly, to promote and improve security assurance within the organisation, a standard or guideline can provide a structure to ensure good practice is followed, as with the previously mentioned ISO/IEC 27001.

ISO/IEC 27001 for an Information Security Management System

Implementing an ISMS and conforming to ISO/IEC 27001 (and the corrigenda), provides a framework for an organisation to examine how information security is addressed systematically. ISO/IEC 27001 is not a single document but a family of documents that need to be assimilated and used for risk reduction to information technology assets. A useful summary tabulation of the ISO/IEC 27001 set of documents can be seen in [14]. Independent assessment against ISO/IEC 27001 provides an organisational security assurance indicator.

ISO/IEC 27001 certification can be a difficult task for new businesses and any organisation focused on commercial delivery. However, it can be viewed as embedding security awareness and processes into an organisation. ISO/IEC 27001 requires an organisation to provide leadership and implement policies to establish an ISMS proactively. This requires planning, supporting, operating (considering the full life cycle), evaluating, and improving information security. ISO/IEC 27002 [15] (and the corrigenda) provide information on the ISMS control points, their objectives, and guidance on implementation.

There is a high reliance on software-based systems in the running of organisations and the design, delivery, and operations of the mission. This makes application security a consideration. Therefore, it makes sense to operate a secure Systems Development Life Cycle (SDLC). In that regard, ISO/IEC have the seven-part standard ISO/IEC 27034 [16] to support an ISMS. Alternatively, the operation and management of a Secure Development Lifecycle (SDL) can use one of several available methodologies [17] if an SDL is not already in operation by project development teams.

Cryptographic Key Management

A section in ISO/IEC 27002 covers *Cryptography*, addressing *Cryptographic controls*. There is the *Policy on the use of cryptographic controls* and *Key management*. Cryptographic controls can be used to achieve different information security objectives such as confidentiality, integrity/authenticity, non-repudiation, and authentication. Systems already use cryptography, e.g., for encrypted communications, however, cryptography as a security assurance control is likely to be found deeper within systems as Zero Trust Architecture [18] increases in usage. A Zero Trust system assumes that anything inside and outside a system must be verified and authorised, increasing the importance of cryptographic controls and key management.

A policy on the use of cryptographic controls is needed to maximize the benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use. ISO/IEC 27002 guides the implementation of a cryptographic control policy:

- Deciding which information should be protected.
- A risk assessment identifies the required level of protection (i.e., the type, strength, and quality of the encryption algorithm).
- Deciding where to implement encryption on devices and/or across the communication lines.
- Deciding the roles and responsibilities of personnel for implementing the policy and key management.
- Adopting standards for effective implementation.
- Analysing the impact of using encrypted information on other controls (e.g., malware detection).

The control for key management is: *"A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle."*

This control includes generating, storing, archiving, retrieving, distributing, retiring, and destroying keys. The key management system should be developed with an agreement based on the following consideration [19]:

- Different keys should be generated for different cryptographic systems and different applications.
- Issuing and obtaining public key certificates.
- Distributing keys to the intended entities, including the procedure for activating keys.
- Key storage.
- Changing and updating keys.
- Dealing with compromised keys.
- Key revocation.
- Recovery of lost or corrupted keys.
- Key back up and archive.
- Destroying keys.
- Logging/auditing within the key management activities.

NIST has guidelines on cryptography due to it being mandated in several US laws and directives, thus, requiring US government agencies to have key management policies. A NIST Special Publication (SP) [20] summarises the US requirements within the US legislation on cryptography and key management, and it references several other US documents. In another SP [21] the benefits of standards are stated, confirming that a Federal Information Processing Standard (FIPS) is mandatory when implementing functionality covered by the FIPS in a federal organisation. However, a NIST SP is not mandatory unless specifically requested (and [20] includes where the law states the NIST SPs to use). Furthermore, the NIST guidelines are mandated for certain sensitive information. However, for SECRET or TOP SECRET information (see the next section), additional classified guidelines likely exist for key management in classified US systems.

The NIST cryptographic guidelines recognise the features required for a key management process (the framework) and the attributes that may need to be covered by the key management system (the profile). These two aspects of a Cryptographic Key Management System (CKMS) are discussed by two additional NIST SPs [22], [23]. The two documents address terminology, keys and their metadata, usability, accountability and responsibilities, key life cycle, auditing, testing, and assurance. The key life cycle aspects include generation, registration, activation, deactivation, revocation, suspension, destruction, backup, archive, establishment, transportation, restrictions, compromise, interoperability, controls, disaster recovery, and security assessments. The profile document is specifically concerned with the procurement aspects of a CKMS for use at a federal organisation.

The NIST and ISO/IEC family of information security standards, and most security standards and guidelines, are function-orientated, device, and technology agnostic, describing what systems, processes and components must handle, not technical implementation details or specific technology. They provide the high-level requirements for a CKMS. This is common to many standards where specific technology implementation detail is not present. Standards need to be agnostic due to technological progress. This prevents the standards from being tied to a specific engineer device and allows them to support broad applications. However, this may cause issues with standards interpretation if they are not written precisely enough.

5. SECURITY AND RISK GRADATION

Ensuring the confidentiality, integrity and availability of information requires the use of security mechanisms, e.g., data encryption. The assets that are storing or communicating the information need protection against unauthorised parties, i.e., the threat agents. The information can be graded to help determine the amount of security that needs to be applied to assets. The grading can help with balancing the cost of providing security against the cost of the information being exposed. No system can provide total security; however, security can be improved to reduce the risk of a security breach.

A universal consensus on security grading does not exist. Different personnel and organisations will define gradations differently. However, by describing a grading scheme, a general understanding of the level of importance of the information within a system can be defined. This then helps to determine the requirements for the security controls that need to be applied.

Different documents and organisations have defined different security grading classifications. The gradings can be related to informational or physical assets or both. Examples of security gradings are shown in Table 1. The more grades, the more likely that information in a system will be incorrectly graded and the more complex the systems that are required to handle multiple grades. A smaller number of grades allows for simpler classification of information and reduction in systems complexity. Table 1 shows that a minimum of three grades is common.

Table 1. **Examples of Security Gradations**

Grades	Ref.	Comment
CONFIDENTIAL, SECRET, TOP SECRET	[24]	The US classifications of national security information. The base classifications are extended using Sensitive Compartmented Information (SCI) for additional need-to-know restrictions.
UNCLASSIFIED, CONFIDENTIAL, SECRET, TOP SECRET	[25]	Application of the previous classifications marks to documents and electronic communications when protection from unauthorised disclosure is required. The additional UNCLASSIFIED mark can be used for information that does not meet the criteria for classification and where additional controls may be required.
OFFICIAL, SECRET, TOP SECRET	[26]	Her Majesty's Government (HMG), i.e., the UK's, classification of information assets. Levels above and below the given grades can be applied where appropriate. Additional indicators can be applied to a classification for specific need-to-know precautions, e.g., OFFICIAL-SENSITIVE to protect procedures/personnel.
NATO UNCLASSIFIED, NATO RESTRICTED, NATO CONFIDENTIAL, NATO SECRET, COSMIC TOP SECRET	[27]	NATO classifications indicate the possible damage to security, and that of the member Nations, on the unauthorised disclosure of information. NATO UNCLASSIFIED is an addition for items outside of sensitive security information. Other supplementary markings to cover additional policies may apply, e.g., CRYPTO.
ESA RESTRICTED, ESA CONFIDENTIAL, ESA SECRET, ESA TOP SECRET	[28]	European Space Agency (ESA) levels of classification for information that requires protection, increasing levels signify the possible increasing harm and damage to ESA and its member states if the information is disclosed.
Functional, Revitalised Enhanced, High Grade	[26]	HMG encryption grades for electronic information at rest or in transit.
Not Applicable, Very Low, Low, Moderate, High	[29], [30]	Level of Risk, within the UK's Cyber Essentials scheme. A Cyber Risk Profile (CRP) is an outcome of a risk assessment, that affects the degree of the level of approval required for suppliers.
Low (limited impact), Moderate (serious impact), High (severe or catastrophic impact)	[31]	NIST levels of impact of unauthorised actions on information confidentiality, integrity, and availability.
Basic, Substantial, High	[32]	The European Union's (EU) Cybersecurity Act defines increasingly stringent security assurance compliance levels.
Level C, Level B, Level A	[33]	NATO TEMPEST (signal radiation) levels for devices processing classified information.
Zone 2, Zone 1, Zone 0	[34]	NATO zoning distances for installed devices for TEMPEST considerations.

UK Security Classifications for Information

The three basic classifications for UK Government information [26] are shown in Table 2, together with the expected encryption level for electronic data at rest or in transit.

The lowest classification, official, is for day-to-day operations, and the information does not need to be specifically marked. Official information is analogous to information that a commercial organisation would not want to make public. Information that is classified SECRET and TOP SECRET is marked as such and requires increasingly stringent controls and handling.

The classifications are the minimum starting point for protecting the different importance rankings of information. The security classifications of information and assets will impact real-world locations, for example, a commercial facility handling classified material under a government contract, e.g., List X status [35] for HM Government.

There is a recognition within classifications that additional controls may be required depending on the information and who needs to handle it. For example, in the UK, there is the OFFICIAL-SENSITIVE marker for a sub-set of day-to-day information that needs extra consideration due to the potential to damage individuals, organisations, and the government. Another example is for information sent overseas, it must be marked with a UK prefix, e.g., UK SECRET. Furthermore, it can be marked UK EYES ONLY if it should not be sent overseas (e.g., TOP SECRET - UK EYES ONLY). Thus, whilst three UK classifications of information are defined, it acknowledges it must work within the complex operations of local, national, and international requirements and procedures. These additional caveats are a consideration when designing a system that may span disparate procedural, local, national, and international boundaries, such as cross-border communication systems. However, it may be that such a system is only concerned with providing the capability to protect all levels of information. It is then the clients of the system that apply correct procedural controls. The specific controls required for a high classification system are unknown until a customer achieves security clearance and engagement.

The UK Government's security classification states that electronic information at rest and in transit is protected by en-

Table 2. UK Government Security Classifications

OFFICIAL	SECRET	TOP SECRET
"The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile."	"Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime."	"HMG's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations."
Foundation Grade encryption (commercially available encryption)	*Revitalised Enhanced Grade encryption* (classified meaning)	*High Grade encryption* (classified meaning)

cryption. At the lowest classification, commercially available encryption is used. At the higher classifications, the encryption used is government approved. Thus, a system used for SECRET and higher classified information will need to be assessed by a government body, for example, the National Cyber Security Centre (NCSC) for the UK.

6. Supply Chain Risks

Adherence to a guideline or standard to ensure suitable security controls are being used within an organisation is not the only aspect of security assurance. Organisations need to protect themselves from cybersecurity risks that could be introduced via suppliers. Cyber-attacks can be and have been perpetrated via suppliers [36], [37]. Furthermore, a supplier may need to demonstrate how they maintain a level of cybersecurity. Adherence to a security scheme is increasingly essential for business suppliers, and mandatory for contracts with many governments and organisations.

An example is the UK's Cyber Security Model (CSM) [30] that the UK's MOD requires for the protection of MOD Identifiable Information [38] (MODII) (i.e., information that could identify capability, activities, or personnel). The CSM requires all MOD suppliers, and their suppliers in the supply chain, to complete a risk assessment to enable the creation of a Cyber Risk Profile (CRP). The CRP is categorised as not applicable, very low, low, moderate, and high. The higher the CRP the greater the information cyber security controls that are required to be in place for suppliers to the MOD. The UK Government's Cyber Essentials (CE) scheme is the baseline requirement for MOD suppliers. As the CRP increases the required controls will increase. At the lowest level, CE is a self-assessment process, at the next level up, Cyber Essentials Plus is where an external body assesses certification. At a higher CRP, additional controls are required depending on the MOD contract in question. CE is an example of a guideline or standard being used to improve an organisation's cyber hygiene, increasing its ability to secure its information and other assets.

An example of a supply chain cybersecurity incident was the ransomware attack on the company Kaseya [37], a Managed Service Provider (MSP). Kaseya software manages IT assets for businesses. However, its systems were compromised and used to deliver and install ransomware. Kaseya, who holds ISO/IEC 27001 certification, proactively shut down their systems to halt the spread of ransomware. The number of their customers affected was around 50 out of 37000. This example demonstrates both the issues of supply chain cybersecurity risks and mitigating action to limit the damage.

Another consideration for systems suppliers is national laws on data privacy. Some nations do not allow personal data to leave national boundaries, or only under certain conditions, (e.g., restrictions under the General Data Protection Regulation [39] in Europe, and its UK equivalent). Furthermore, laws may restrict not only national boundaries but how personal data flows between organisations. Breaches of data privacy laws can lead to substantial fines for organisations and other penalties under a nation's laws.

7. Common Criteria

CC allows comparability between the results of independent security evaluations by providing common assurance measures. CC is a product security assurance scheme [40], namely: *"... IT Products and Protection Profiles which earn a Common Criteria Certificate, as per the requirements of the CC standard, can be procured or used without the need for further Evaluation."*

It is used for the security assurance of a product and/or software system (examples include silicon chips, operating systems, smartcards, cell phones, electronic signature devices, banking cards, databases, and software). The provision of a *Protection Profile* (PP) for a device or product (the entity) allows a common template to be used as the basis for the security assurance assessment, ensuring the security assurance process's consistency. PPs exist for many types of devices. The adoption of CC for an emerging technology domain would require the creation of PPs for entities, i.e., components, software, and systems used within a technology domain.

The use of defined Evaluation Assurance Levels (EALs) reduces the influence of subjectivity within the security assurance assessment. There are seven levels of EAL, from the lowest at EAL1 to the highest at EAL7. An example of EAL1 would be a manufacturer confirming that a device has been independently tested against its specification. An example of EAL7 would be a microcontroller or CPU used in a device that has been formally analysed to verify its operation.

Once a PP is developed, then CC compliance for the PP, for a given EAL, is awarded by an approved organisation. This enables the entity's independent assessment against the PP and enables the entity to achieve certification.

Under CC a *Security Target* (ST) is a description of the

elements required to validate the security assurance claims. Think of it as a container of everything required to provide security assurance. It includes descriptions of the ToE, the conformance claims made against the specific PPs, the security threats and objectives, and the security requirements and rationale. The ST is the wrapper for what is to be evaluated and what was evaluated. Thus, the ST documents the security assurance claims between the engineers and security assessors, and between the engineers and ToE users.

Limitations on Security Assurance

Once a product is CC certified, that certification is recognised by other CC bodies. However, *"It is likely that some sensitive government IT Systems will be procured, certified and Recognised according to specific user's requirements for their strategic need or separate bilateral or multilateral agreements."*

Therefore, it recognises that a CC certificate may still require additional security assurance controls for a particular application (e.g., a system for a government operating with SECRET or TOP SECRET information). Evaluations at EAL5 and above tend to involve the security requirements of the host nation's government. Furthermore, CC recognises that an evaluation is a point in time assessment [6]: *"... the fact that an IT product has been evaluated has meaning only in the context of the security properties that were evaluated and the evaluation methods that were used."*

This reinforces that security is not a one-time issue and needs life cycle management. This is to ensure that new vulnerabilities and possibly new assessment criteria that emerge are dealt with appropriately. This is reflected in the ST, which captures the point-in-time security claims. An updated ST and reassessment would capture updated security assurances.

Common Criteria and the EU Cybersecurity Act

The EU Regulation 2019/881 [32], a.k.a. the *EU Cybersecurity Act* of 2019, has enhanced the European Union Agency for Cybersecurity (ENISA né European Network and Information Security Agency). It has given ENISA the role of developing a CC-based European cybersecurity certification scheme (EUCC) [41]. The EUCC has embraced CC and the equivalent ISO/IEC standards as its basis, recognising that CC has been effective for the certification of devices and products. The Appendix provides an overview of CC and EUCC development.

ENISA will provide a website to promote the EUCC scheme and information on issued certifications. Like the existing CC, the EUCC will be transnational, i.e., under the EUCC the certification of products from one European country will be valid in other EU countries.

ENISA being given the remit to implementing the EUCC provides an example of designing a CC-style certification scheme. Thus, it is possible to examine what was drafted for the EUCC scheme as a basis for a certification framework for a new technology domain, and the security assurance for the assets used within it.

Defining the Various Types of Assessment Information and Criteria Required (the Protection Profiles)

For a category of a product, service, or process, a PP or equivalent is constructed. In CC, assurance requirements are grouped into families consisting of assurance components. The components are described by elements, identified with a unique tag, and are the evaluation criteria. Assurance components are mapped to defined assurance levels (EALs for CC). For example, the vulnerability assessment family of assurance components have increasingly stringent requirements as the EAL level increases. At EAL 1 it is a *vulnerability survey*, tagged AVA_VAN.1. At EALs 2 and 3, it is a *vulnerability analysis*, tagged AVA_VAN.2. The defined assurance criteria can have dependencies upon other criteria if necessary.

A PP, or equivalent, will define the security functional and assurance requirements using assurance components, referring to the uniquely tagged criteria. Assurance assessment items to construct a PP under CC or a similar assessment definition are:

- A PP reference or identifier
- ToE type and overview
- Allowable strictness of conformance claims
- Security problem definition: Threats
- Security problem definition: Organisational Security Policy (OSP)
- Security problem definition: Assumptions
- Security objectives for conformance (for threats, OSPs, and assumptions)
- Handling extensions for undefined criteria, i.e., the extended components definition
- Security Functional Requirements (SFRs), i.e., ToE security behaviour within its environment
- Security Assurance Requirements (SARs), e.g., required EALs and their defined criteria
- Reusable packages of SFRs and SARs for ToE types
- Chaining assessment criteria
- Handling composition of ToEs

The Methodologies for Conformity Assessments at the Required Assurance Levels

According to the security risk level of the product to certify (e.g., obtained from threat modelling or a TARA methodology), a mapping to a required assurance level is made. In the EUCC, three assurance levels are defined compared to 7 EAL levels in CC. (The EUCC provides commentary on how the CC EALs map to EUCC assurance levels.) The three EUCC assurance levels are:

- **Basic** - Aimed at products with a low-risk level. The conformity assessment should demonstrate that known vulnerabilities are not there.
- **Substantial** - Aimed at products with a medium and high-risk level. The conformity assessment will include a demonstration of the existence of security functionalities (as defined in the PP) and a vulnerability assessment. A test plan is required for assessment. It includes the basic assurance conformity assessment.
- **High** - Aimed at products with a very high or critical risk level. The conformity assessments include a technical documentation review, testing the existence of security functionalities, and a penetration test. These are all referencing best practice codes and other guidelines and standards. It includes the substantial assurance conformity assessment.

The EUCC scheme is targeted at devices, software and systems that need to reach assurance levels of substantial or high. The basic level is documentation and self-assessment-based tasks to lower security risks. The substantial level requires assessment against skilled attacks. The high assurance level targets the need to protect against highly skilled and heavily resourced attacks.

8. IN CONCLUSION

This work provides concise information on the topics of cybersecurity assurance and certification and associated guidelines and standards. This is useful for individuals and organisations who need to understand the foundations of cybersecurity assurance and certification and what is available in the wider corpus. Organisations, particularly new ones, may not have considered security assurance as they concentrate on developing their business and bringing new products and services to market. Alternatively, they may have been put off by the costs involved in implementing adherence to the procedures and controls from cybersecurity guidelines, requirements, and standards. Those costs can include extra resources for product development and personnel training or recruitment of security specialists. Yet, the path to commercialising any system, especially for high-security classification applications, will require the commercial stakeholders to embrace the security assurance aspects. Cyber-attacks against many types of systems have happened before and will continue to happen. Hence the focus on cybersecurity by governments as society has become reliant upon computer-based systems.

Emerging systems innovators cannot ignore cybersecurity considerations. In that respect, following appropriate security standards does provide a structure to manage risks and ensure a degree of assurance for a delivered product or service. An organisation can use widely recognised certification frameworks (Common Criteria, ISO/IEC 27001) or follow some of the many other guidelines that exist. In doing so it will involve awareness, education, and training within the project, engineering, and management teams of organisations.

Acknowledgements—Funded by Grant EP/R026092/1 (FAIR-SPACE Hub) through UK Research and Innovation (UKRI) under the Industry Strategic Challenge Fund (ISCF) for Robotics and AI Hubs in Extreme and Hazardous Environments.

APPENDIX - CC AND EUCC DEVELOPMENT

CC is developed and maintained by a variety of organisations from several different nations, see Table 3 for the Common Criteria Recognition Arrangement (CCRA) member nations.

Furthermore, CCRA has India, Italy, Malaysia, Norway, Singapore, and Turkey as *authorising* organisations, containing licensed laboratories for certification. The nations of Austria, Czech Republic, Denmark, Ethiopia, Finland, Greece, Hungary, Indonesia, Israel, Pakistan, Poland, Qatar, Slovak have CC *consuming* organisations. Thus, CC certification, licensing and recognition are transnational.

The UK was an original contributor to the CC, but the UK Government has reduced its role, concentrating on developing PPs of technologies of interest to the UK [42]. The UK's NCSC ceased to be a certificate producer; however, the UK is a Certificate Consuming Participant (CCP) and contributes to the international CC standards effort. In taking a step back from CC, the NCSC recognises that the security assurance of a product at a point in time is only one part of the overall security picture. However, the wide international use of CC (which includes the UK's continuing recognition), makes the CC a candidate for security assurance of system hardware.

There is some work to perform to implement CC for hardware entities (devices, components, software, or systems). The entities and/or their constituents will require the development of PPs. System stakeholders should consider collaboratively developing PPs, and if required, applying the CC process to any emerging technology domains (likely with the aid of security and CC experts). Commercial-of-the-shelf (COTS) components and devices that often appear in system designs would be candidates for PPs. If the development of PPs for systems is not performed, then some other audit mechanism for security assurance would be required. Alternatives include threat modelling or TARA processes, of which several flavours exist. However, if some form of recognised certificate is necessary then a method of independent assessment, like CC, would be required.

Table 3. Common Criteria National Development Organisations

Country	Common Criteria Authoring Organisation
Australia	The Australian Signals Directorate
Canada	Communications Security Establishment
France	Agence Nationale de la Sécurité des Systèmes d'Information
Germany	Bundesamt für Sicherheit in der Informationstechnik
Japan	Information Technology Promotion Agency
Netherlands	Netherlands National Communications Security Agency
New Zealand	Government Communications Security Bureau
Republic of Korea	National Security Research Institute
Spain	Ministerio de Administraciones Públicas and Centro Criptológico Nacional
Sweden	Swedish Defence Materiel Administration
United Kingdom	National Cyber Security Centre
United States	The National Security Agency and the National Institute of Standards and Technology

Under a CC (or EUCC) scheme, a certification can be released only by a Certification Body, and conformity assessment can be run only by a certification lab, i.e., an independent third-party assessment body and/or national authority. For the EUCC, ENISA is charged with oversight within the EU. Future European designed and manufactured COTS components used in systems may need to engage in the EUCC process to achieve assurance validation.

The documentation for the CC and EUCC style certification schemes provides the prerequisite knowledge for drafting a similar scheme for a new technology domain and includes:

- The CC documentation:
  - Part 1: Introduction and general model [6]
  - Part 2: Functional security components [7]
  - Part 3: Assurance security components [8]
  - Common Methodology for Information Technology Security Evaluation [9]

- The EUCC documentation:
  - Cybersecurity Certification [41]
  - Title III in EU Cybersecurity Act [32] for reference

It is a substantial task to design or define an operational cybersecurity certification framework for a technology domain or national, or international, body. Article 54 of the EU Cybersecurity Act lists the elements to consider for such a certification scheme. These elements were the basis for developing the candidate EUCC. Building a certification scheme for a new domain begins by similarly addressing those elements. If required, those elements are customised, giving a rationale for why and relating it to the CC, EUCC, or other security standards and guidelines. In brief, the elements relate to:

- Subject matter and scope (e.g., domain and its entities)
- Covered categories (products, services, processes)
- Scheme purpose and the security it addresses
- Intended users
- References to international/EU schemes or standards
- Assurance classes or levels
- Permitted conformity from self-assessment
- Evaluation standards, criteria (PPs), and methods
- Information to be supplied by an applicant
- Rules for marks, labels, and their conditions of use
- Content and format of certificates and reports
- Rules for issuing/renewing a certificate
- Rules for extending/reducing the scope of a certificate
- Rules for monitoring compliance
- Rules for non-conformity
- Rules relating to vulnerability management
- Retention period of information
- Correlation with other national/international schemes
- Rules for mutual recognition of other schemes
- Rules for scheme oversight and assessment bodies
- Rules for life cycle/user information and support

The above elements have to be defined in sufficient detail to enable a scheme to be functional and effective. This level of detail can take significant time and commitment.

REFERENCES

[1] P. Passeri, "Hackmegeddon Information Security Timelines and Statistics," 2022. [Online]. Available: https://www.hackmageddon.com/

[2] R. Bejtlich, *The Practice of Network Security Monitoring Understanding Incident Detection and Response*. No Starch Press, 2013.

[3] A. Odlyzko, "Cybersecurity is not very important," *Ubiquity*, vol. 2019, no. June, pp. 1–23, 2019.

[4] Crown Commercial Service, "Procurement Policy Note – Cyber Essentials Scheme," HM Government, Liverpool, Tech. Rep., 2016.

[5] European Communities, "Information Technology Security Evaluation Criteria (ITSEC) Provisional Harmonised Criteria," Luxembourg, 1991.

[6] CCRA Members, "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1 Revision 5," Common Criteria Recognition Arrangement, Tech. Rep., 2017.

[7] ——, "Common Criteria for Information Technology Security Evaluation, Part 2: Functional security components, Version 3.1 Revision 5," Common Criteria Recognition Arrangement, Tech. Rep., 2017.

[8] ——, "Common Criteria for Information Technology Security Evaluation, Part 3: Assurance security components, Version 3.1 Revision 5," Common Criteria Recognition Arrangement, Tech. Rep., 2017.

[9] ——, "Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5," Common Criteria Recognition Arrangement, Tech. Rep., 2017.

[10] ISO, "ISO/IEC 15408-1:2009(E) Information technology - Security techniques - Evaluation criteria for IT Security," Geneva, 2014.

[11] International Organization for Standardization, "Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013)," Geneva, 2013.

[12] Center for Internet Security, "CIS Critical Security Controls - Version 7.1," East Greenbush, 2019.

[13] National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations," Gaithersburg, 2020.

[14] M. Szmit and A. Szmit, "Risk Management in NIST and ISO/IEC 27K Information Security Management Standards' Family - a Brief Analysis," *Mechanics Transport Communications, Academic journal*, vol. 13, no. 2015/3, 2015.

[15] International Organization for Standardization, "Information technology - Security techniques - Information security management systems - Code of practice for information security controls (ISO/IEC 27002:2013)," Geneva, 2013.

[16] ISO/IEC, "ISO/IEC 27034 Information Security - Security techniques - Application Security," 2011.

[17] A. Ramirez, A. Aiello, and S. J. Lincke, "A survey and comparison of secure software development standards," in *2020 13th CMI Conference on Cybersecurity and Privacy (CMI) - Digital Transformation - Potentials and Challenges(51275)*, 11 2020.

[18] National Institute of Standards and Technology, "Zero Trust Architecture," Gaithersburg, 2020.

[19] ISO/IEC, "ISO/IEC 11770-1:2010 Information Security - Security techniques - Key management," 2010.

[20] National Institute of Standards and Technology, "Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies," Gaithersburg, 2016.

[21] ——, "Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms," Gaithersburg, 2020.

[22] ——, "A Framework for Designing Cryptographic Key Management Systems," Gaithersburg, 2015.

[23] ——, "A Profile for U.S. Federal Cryptographic Key Management Systems," Gaithersburg, 2013.

[24] Executive Office of the President of the United States, "Executive Order 13526 - Classified National Security Information," Washington, 2009.

[25] Office of the Director of National Intelligence, "Intelligence Community Directive 710, Classification Management and Control Markings System," Washington, 2013.

[26] Cabinet Office, "Government Security Classifications Version 1.1," London, 2018.

[27] North Atlantic Treaty Organization, "Security within the North Atlantic Treaty Organisation," Brussels, 2020.

[28] European Space Agency, "ESA Security Regulations," Paris, 2015.

[29] Ministry of Defence, "Defence Standard 05-138 Issue 2, Cyber Security for Defence Suppliers," London, 2017.

[30] ——, "Defence Cyber Protection Partnership Cyber Security Model Industry Buyer and Supplier Guide," London, 2018.

[31] National Institute of Standards and Technology, "FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems," Gaithersburg, 2004.

[32] European Union, "Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)," Luxembourg, 2019.

[33] North Atlantic Treaty Organization, "NATO TEMPEST requirements and Evaluation procedures," Brussels, 2016.

[34] ——, "NATO Zoning Procedures," Brussels, 2005.

[35] Cabinet Office, "Security Requirements for List X Contractors," London, 2014.

[36] S. Peisert, B. Schneier, H. Okhravi, F. Massacci, T. Benzel, C. Landwehr, M. Mannan, J. Mirkovic, A. Prakash, and J. B. Michael, "Perspectives on the solarwinds incident," *IEEE Security & Privacy*, vol. 19, no. 2, pp. 7–13, 2021.

[37] M. Nevins, "How To Survive A Cybersecurity Attack," 2021. [Online]. Available: https://www.forbes.com/sites/hillennevins/2021/07/26/how-to-survive-a-cybersecurity-attack/

[38] Ministry of Defence, "Industry Security Notice Number 2016/05 Definition of MOD Identifiable Information," London, 2016.

[39] European Union, "General Data Protection Regulation," Brussels, 2016.

[40] Common Criteria, "Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security," 2014.

[41] ENISA, "Cybersecurity Certification, V1.1.1," Athens, 2021.

[42] National Cyber Security Centre, "Common Criteria," London, 2019.