Government and commercial organizations rely heavily on the use of information to conduct their business activities. Loss of confidentiality, integrity, availability, accountability, authenticity and reliability of information and services can have an adverse impact on organizations. Consequently, there is a critical need to protect information and to manage the security of IT systems within organizations. Alongside significant benefits, every new technology introduces new challenges for the protection of this information. The requirement to protect information is particularly important in today’s environment because many organizations are internally and externally connected by networks of IT systems.¹

IT systems are prone to failure and security violations due to errors and vulnerabilities. These errors and vulnerabilities can be caused by many factors, such as rapidly changing technology, human error, poor requirement specifications, poor development processes or underestimating the threat. In addition, system modifications, new flaws and new attacks are frequently introduced, which contributes to increased vulnerabilities, failures and security violations throughout the IT system life cycle.²

The industry came to the realization that it is almost impossible to guarantee an error-free, risk-free and secure IT system due to the imperfection of the opposing security mechanisms, human error or oversight, and component or equipment failure.³

Completely secure IT systems do not exist; only those in which the owners may have varying degrees of confidence that security needs of a system are satisfied do.⁴

In addition, many information systems have not been designed to be secure. The security that can be achieved through technical means is limited and should be supported by appropriate management and procedures.⁵

The task of IT security (ITS) engineering and management is to manage the security risk by mitigating the vulnerabilities and threats with technological and organizational security measures to achieve an IT system with acceptable assurance. ITS management has an additional task: establishing acceptable assurance and risk objectives. In this way, the stakeholders of an IT system will achieve reasonable confidence that the IT system performs in the way intended or claimed, with acceptable risk and within budget.⁶

ISO/IEC TR 15443 Information technology—Security techniques—A framework for IT security assurance is a multipart technical report intended to guide ITS professionals in the selection of an appropriate assurance method when specifying, selecting or deploying a security service, product or environmental factor (known as a “deliverable”).⁷ The objective of ISO/IEC TR 15443 is to present a variety of assurance methods and to guide the ITS professional in the selection of an appropriate assurance method (or combination of methods) to achieve confidence that a given IT system satisfies its stated ITS assurance requirements. ISO/IEC TR 15445 analyzes assurance methods that may not be unique to ITS; however, guidance given in the standard is limited to ITS requirements. This article introduces the fundamental concepts of ITS assurance based on ISO/IEC TR 15443.

ASSURANCE AND CONFIDENCE

It is important to emphasize that assurance and confidence are not identical and cannot be used in place of one another. Too often, these terms are used incorrectly because they are closely related.⁸

ISO/IEC TR 15443 defines these terms as follows: “Confidence, from the perspective of an individual, is related to the belief that one has in the assurance of an entity, whereas assurance is related to the demonstrated ability of an entity to perform its security objectives. Assurance is determined from the evidence produced by the assessment process of an entity.”⁹

For security engineering, “assurance” is defined as the degree of confidence that the security needs of a system are satisfied.¹⁰ Assurance does not add any additional controls...
to counter risks related to security, but it does provide confidence that the controls that have been implemented will reduce the anticipated risk. Assurance can also be viewed as the confidence that the safeguards will function as intended.\textsuperscript{11}

It is also important to understand that assurance does not automatically imply good security. Assurance implies only that an enterprise meets its security objectives. In other words, assurance provides confidence that the deliverable enforces its security objectives without examining whether the security objectives appropriately address risk and threats.\textsuperscript{12}

**ASSURANCE REQUIREMENTS**

In terms of ITS, adequate assurance signifies that specific, predefined security assurance requirements have been satisfied by performing appropriate assurance processes and activities.\textsuperscript{13}

Security assurance requirements are determined by “analyzing the security requirements of the IT system, influencers, policies, business drivers and the IT system’s target environment. Influencers are any considerations that need to be addressed as they may affect the IT system assurance requirements. The influence can have any origin and may include such intangibles as politics, culture, local laws and mandated requirements.”\textsuperscript{14}

Security is concerned with the protection of assets. “Assets” are entities upon which someone places value.\textsuperscript{15} Many assets are in the form of information that is stored, processed and transmitted by IT products to meet requirements laid down by owners of the information. Safeguarding assets of interest is the responsibility of the owners who place value on those assets. Actual or presumed threat agents may also place value on the assets and seek to abuse assets in a manner contrary to the interests of the owner.\textsuperscript{16}

A risk assessment is performed to provide an in-depth look at asset sensitivity, vulnerabilities and threats to determine the residual risk and recommendations for existing and proposed safeguards. The recommendations implemented are factored into the original security requirements to revise the security assurance requirements.

It is also important to note that “assurance requirements are unique to each environment due to the myriad business and security requirements of each environment. The same IT system may not be suitable to other environments without modifications because different assurance requirements will usually need to be satisfied.”\textsuperscript{17}

**ASSURANCE METHODS APPLICABLE TO ITS**

Application of appropriate assurance activities establishes confidence that the IT system satisfies its security objectives. Confidence is realized by reviewing the assurance evidence gained through assessment processes and activities during development, deployment and operation and through experience gained in using the IT system. Any activities that can reduce uncertainty by producing evidence attesting to the correctness, effectiveness and quality of the IT system’s attributes are useful in determining security assurance.\textsuperscript{18}

There are many existing assurance methods, but only a small number are specific to ITS. However, non-ITS assurance methods may also contain certain assurance properties that are relevant to ITS assurance.\textsuperscript{19} Due to the small number of available assurance methods specific to ITS, it is important to recognize the value of all assurance methods, since many nonsecurity-related assurance methods are used throughout the IT industry. Anything that can be used to construct an assurance argument and, thereby, reduce the uncertainty associated with a particular deliverable is of considerable importance.\textsuperscript{20}

**SELECTING SECURITY ASSURANCE**

Selecting a security assurance method and the appropriate amount of assurance should be based on the organizational security assurance policy, business requirements and type
of deliverable (i.e., product, process, environment, system, service or personnel). For example, some assurance methods are applicable only to processes (i.e., ISO/IEC 21827), others are applicable to products (i.e., ISO/IEC 15408 Information technology—Security techniques—Evaluation criteria for IT security) and others are applicable to security management (i.e., ISO/IEC 27001 Information technology—Security techniques—Information security management systems—Requirements). The following are brief descriptions of three commonly used models:

- Modern statistical process control suggests that higher-quality products can be produced more cost-effectively by emphasizing the quality of the processes that produce them and the maturity of the organizational practices inherent in those processes. More efficient processes are warranted, given the increasing cost and time required for the development of secure systems and trusted products. The operation and maintenance of secure systems rely on the processes that link people and technologies. These interdependencies can be managed more cost-effectively by emphasizing the quality of the processes being used and the maturity of the organizational practices inherent in the processes. ISO/IEC 21827 provides a process reference model that is focused on the requirements for implementing security in a system or series of related systems that are within the ITS domain. Within the ITS domain, ISO/IEC 21827 is focused on the processes used to achieve ITS, most specifically on the maturity of those processes.21

- Safeguarding assets of interest is the responsibility of the owners who place value on those assets. Owners of assets may be (held) responsible for those assets and, therefore, should be able to defend the decision to accept the risk of exposing the assets to the threats. Many owners of assets lack the knowledge, expertise or resources necessary to judge sufficiency and correctness of the countermeasures, and they may not wish to rely solely on the assertions of the developers of the countermeasures. These consumers may, therefore, choose to increase their confidence in the sufficiency and correctness of some or all of their countermeasures by ordering an evaluation of these countermeasures. ISO/IEC 15408 provides a common set of requirements for the security functionality of IT products and for assurance measures applied to those IT products during a security evaluation. The IT products may be implemented in hardware, firmware or software. The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers determine whether these IT products fulfill their security needs.22

- “Information security” is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.23 Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes. ISO/IEC 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system (ISMS) within the context of the organization's overall business risks. An ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. ISO/IEC 27001 can be used to assess conformance by interested internal and external parties.25

The assurance method selection must take into account available resources.

ASSURANCE APPROACHES

Assurance methods can be categorized into three high-level approaches:26

1. Assessment of the deliverable, i.e., through evaluation and testing
2. Assessment of the processes used to develop or produce the deliverable
3. Assessment of the environment, such as personnel and facilities

ISO/IEC TR 15443 defines these three high-level approaches as follows. Assessment of a deliverable involves an examination of the deliverable (e.g., product, system, service). In this case, these assurance methods examine the deliverable and its associated security design documentation independent of the development processes.

Assessment of a process involves an examination of the organizational processes used in the production and operation of the deliverable throughout its life cycle (i.e., development, delivery, operation). Assurance is gained through the inference that the processes implemented by people affect the quality of the development and implementation of the deliverable and, therefore, yield security assurance when applied to ITS deliverables.

Assessment of the environment involves an examination of the environmental factors that contribute to the quality of the processes and the production of the deliverable (it does not examine a deliverable or process directly). These factors include personnel and physical facilities (e.g., development, production, delivery, operation).

Assurance methods produce specific types of assurance depending on their technical and life-cycle focus. Some of the more widely known assurance methods for a given focus include:27

- **ISO/IEC 21827**—Assurance focus on quality and development process
- **Developer’s pedigree**—Assurance focus on branding; recognition that a company produces quality deliverables (based on historical relationship or data)
- **Warranty**—Assurance focus on insurance, supported by a manufacturer’s promise to correct a flaw in a deliverable
- **Supplier’s declaration**—Assurance focus on self-declaration
- **Professional certification and licensing**—Assurance focus on personnel expertise and knowledge
- **ISO/IEC 14598-1 Information technology—Software product evaluation—Part 1: General overview**—Assurance focus on direct assessment of deliverable
- **ISO/IEC 27001**—Assurance focus on security management

**CORRECTNESS AND EFFECTIVENESS PROPERTIES**

Assurance can be viewed as the confidence that safeguards will function as intended. This confidence derives from the properties of correctness and effectiveness.28

“Correctness assurance” refers to the assessment of the deliverable to verify the correct implementation according to the design. In contrast, “effectiveness assurance” refers to the suitability of the deliverable’s security functions to counter the perceived or identified threats.29

The concept can be illustrated with two examples from ISO/IEC TR 15443:30

- If the IT system’s security functionality addresses the potential threats, but the functionality has not been analyzed to establish its correct design and implementation, one cannot have confidence that the deliverable will withstand an attack. In this example, it is seen that the effectiveness assurance has been established, but the correctness assurance has not been established due to the lack of verified security functionality.
- Similarly, if analysis has found the design and implementation of the IT system’s security functionality to be correct, but the design does not contain the appropriate functionality to address the probable threats, one cannot have confidence that the deliverable will withstand an attack by those threats. In this example, although the correctness assurance is there, it lacks effectiveness assurance due to the implementation of ineffective security functionality against the probable threats.

To achieve comprehensive assurance, the IT system must be assessed to ensure the correct design, implementation and operation (correctness element) and the deliverable must provide the appropriate security functionality to counter the identified threats (effectiveness element).

**CONCLUSION**

Traditionally, assurance has been associated only with IT products and systems composed of hardware or software and referred to as “product assurance” or “system assurance.” It is now recognized that to address a wider range of risks, there is a need for assurance of other security objectives such as a security service, process, personnel, organization or other environmental factors.

Assurance may be sought by the stakeholders of IT systems who have assets at risk in IT systems. Therefore, the determination of an acceptable assurance method and
level of assurance may be required/and or influenced by the stakeholders.

Assurance does not add any safeguards or services to the deliverable. Thus, it is sometimes difficult for nonsecurity personnel to understand what benefit they are receiving from the investment of resources in assurance.

Direct qualification or valuation of the contribution of assurance or increased assurance to the organization is not easy to achieve. However, increased assurance of a security control reduces the uncertainty associated with the risk, specifically the vulnerability components of the risk that the control is implemented to address.

It is necessary to understand how each assurance method establishes assurance in order to decide whether a particular assurance method will satisfy the organization's assurance requirements.

ENDNOTES

3 Ibid.
4 Dražen, Dragicevic; Computer Crime and Information Systems, Informator Zagreb (in Croatian), 1999
6 Op cit, ISO/IEC TR 15443-1:2005
7 Ibid.
8 Ibid.
9 Ibid.
12 Op cit., ISO/IEC TR 15443-1:2005
13 Ibid.
14 Ibid.
16 Ibid.
17 Op cit, ISO/IEC TR 15443-1:2005
18 Ibid.
19 For example, while ISO 9000 Quality management systems is a quality assurance standard originally intended for manufacturing organizations, it also contains process assurance properties applicable to software and, as such, to ITS software products and systems.
20 Op cit, ISO/IEC TR 15443-1:2005
21 Op cit, ISO 2002
22 Op cit, ISO 2009
23 Op cit, ISO/IEC 27002:2005
24 Ibid.
26 Op cit, ISO/IEC TR 15443-1:2005
27 Ibid.
28 Op cit, ISO 2002
29 Op cit, ISO/IEC TR 15443-1:2005
30 Ibid.