28

December 2014

testing experience

The Magazine for Professional Testers

The Three Pillars of Agile Quality and Testing

by Robert Galen

Testing the Internet of Things – The Future is Here

by Venkat Ramesh Atigadda

… and many more

printed in Germany

print version 8,00 €

free digital version

www.testingexperience.com

ISSN 1866-5705

By Klaus Haller

What Developers and Testers Need to Know about the ISO 27001 Information Security Standard

Late in 2013, the International Organization for Standardization released a new version of its ISO 27001 information security standard [1]. The standard covers requirements applying all organizations and ones relevant only for organizations with in-house software development and integration projects. They impact testers, developers, and release managers. This article summarizes the relevant facts and points out topics that testing and development teams have to work on.

Why Managers Like ISO 27001

Managers are held accountable for security incidents, even if they have no information security expertise. Gregg Steinhafel illustrated this involuntarily. He is a former CEO of Target, the second biggest discount retailer in the USA. Steinhafel was the first CEO of a major corporation to lose his job due to a data leak [2]. Thus, managers cannot rely simply on a statement from their Chief Information Officer – "Security? Everything is fine!" – without risking the company's and their personal future. Here, ISO 27001 comes into play. It brings together, first, a list of best practices for information security and, second, an auditing and certification industry. The best practices prevent basic mistakes or leaving security topics completely unaddressed. External auditors validate whether the best practices have been implemented. This external validation gives CEOs and stakeholders extra confidence.

Three Popular Misunderstandings about Information Security

Information security is a widely used term. Everybody has his own definition, which can differ from ISO 27001's understanding. The three most common misunderstandings are:

Misunderstanding 1: Information security focuses (mainly) on protecting sensitive data

Information security requires the protection of sensitive data. However, this is only one of the three aspects of the **CIA triangle** [3], a core concept in information security. The "C" represents confidentiality: protecting sensitive data against unauthorized access. The "I" stands for integrity: Information must not be changed inappropriately, either accidentally or intentionally. Finally, "A" stands for availability: Users must be able to retrieve information when needed; no data must get lost. ISO27001 covers all three aspects of the CIA triangle. Thus, organizations must address all of them for their certification.

Misunderstanding 2: Information security fights (mainly) hackers and malware coming from the outside

Outside hackers and malware pose a threat to every organization, but employees pose a risk as well. Humans make mistakes, even if they handle sensitive data. Worse, employees might engage into criminal actions. Snowden illustrated how one single person only can harm a large organization [4]. Thus, information security must also address risks from internal employees.

Misunderstanding 3: Information security looks (mainly) at production systems

Production systems store and process sensitive data, but sensitive data can also reside in development and test environments. This refers to the confidentiality aspect. When looking at availability, bad code and wrong configurations are risks as well. They can harm the stability of production systems. Thus, IT departments have to address the risk associated with their change and release process, too.

The ISO 27000 Standard Series

The information security standard consists of a broad document family (Figure 1). It is essential to understand the purpose of the various documents. First, ISO 27000 is the *vocabulary standard*. It provides a basic overview and defines the terminology. Second, there are *requirement standards*: ISO 27001 and ISO 27006. ISO 27006 applies to auditing organizations only. They are not in the scope of this article. ISO 27001, however, is the bible for any certification and lists all certification requirements. The current release dates from late 2013 and is referred to as ISO27001:2013 to distinguish it from the older version, ISO27001:2005. ISO 27001 has two parts: a main section and appendix A. The main section defines a general information security framework. Topics include top management involvement or the need for an incident management system. Appendix A lists concrete security topics ("controls") to be implemented.

This **ISO 27001** standard is the only **normative binding** document. In contrast, *guideline standards* offer best practices. ISO 27002 helps in setting up the controls of appendix A of ISO 27001. Other documents focus on aspects of the main section of 27001. ISO 27003, for example, looks at information security management systems, and ISO 27005 at risk management. Industry sector-specific best practices *(sector specific guideline standards)* are also available, e.g., for the financial services industry or for telecommunications. **Guideline** standards are **not mandatory**. Organizations must implement the ISO 27001 requirements but they are free to follow or not to follow the guideline standards.

ISO 27001 Implementation Responsibilities

As mentioned above, ISO27001 has a main section and an appendix A. The main section defines an information security framework and the Chief Security or Chief Compliance Officer has to work on these topics. In contrast, the IT department in general must implement the

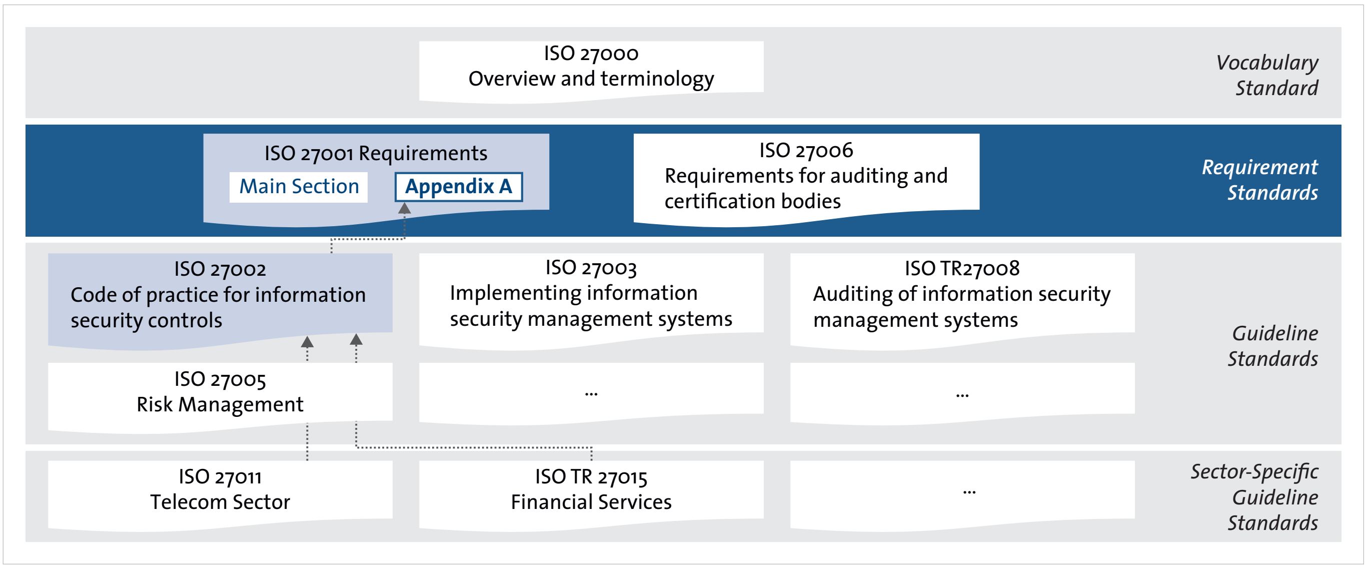

Figure 1. Overview of the 27000 Standard Series. This article mainly deals with ISO 27001 Appendix A with interpretations derived from ISO 27002.

majority of the 114 controls from Appendix A. Some of them are only relevant to developers, testers, and change managers. They have to provide solutions for the controls (see Figure 2), for which they can rely on the next sections.

		Does a control define an obligation for developers, testers, and change managers?	
		Yes	No
Does a company-wide solution exist?	Yes	✓ Developers/testers/release managers rely on company-wide solution from the IT department/IT Security/Legal & Compliance, etc.	✓ Nothing to be done by developers, testers, and change managers
	No	! Developers/testers/change managers must provide a solution (focus of this article)	

Figure 2. ISO27001 Appendix A Standards and the Need for Engineering, Testing and Change Teams to Come Up with a Solution on their Own.

Information Assets in Development and Testing

Information security starts with identifying the valuable information assets, and classifying and labeling them. The user groups with access have to be clarified. Data access and protection mechanisms must be defined (controls A.8.2.1-3).

There are two types of information assets: production data and document assets, and engineering-owned assets. In the case of *production data and documents*, the business, the legal and compliance department, and risk management all work together. They classify the assets and define policies for handling them. Data privacy laws impact the policies, especially in Europe. The policies define, for example, whether customer data is sensitive, who can access it, etc. Testers and engineers are not involved in the classification, although the policies can impact them. They might forbid, e.g., the storage of credit card numbers of clients in test systems.

Engineering-owned assets have to be classified as well. Potentially, IT has to drive this. The main assets are source code and documentation, such as requirements, specifications of new product features, architectural documents, trading algorithms of hedge funds, etc., and they can be as critical as production data. ISO27001 does not declare any asset to be sensitive or not, it just demands clarification.

The policies for handling production data and engineering-owned assets impact tool decisions. In the last few years, outsourcing requirements and test or project management tools became popular. Software-as-a-service is thriving. With ISO 27001, organizations must ensure that projects store data in externally hosted systems only if this does not contradict information security policies.

ISO 27001 also demands **secure development environments** for the complete development cycle (control A.14.2.6). The need for confidentiality, availability, and integrity has a broad impact on access control mechanisms, the hiring and contracting of developers and testers, and backup strategies.

A highly critical asset in development and test environments is the **test data**. Many applications – especially business applications – incorporate databases. Testers need suitable data in the databases in test environments and ISO 27001 control A.14.3.1 demands that the test data is protected. When looking at the ISO 27002 guideline, it is clear that the standard reflects "old style" test data management. In other words, test data comes from production. The focus in ISO 27002 is to mitigate the risks associated with the use of production data, such as the ability to audit the copy process and strict access rules for test environments. The trend towards synthetic test data in Europe is not reflected (see [5] for an in-depth discussion on test data management). However, ISO 27002 is not normative. Organizations can implement ISO 27001 in their own way. Especially when organizations test with synthetic data, many ISO 27002 ideas are obsolete.

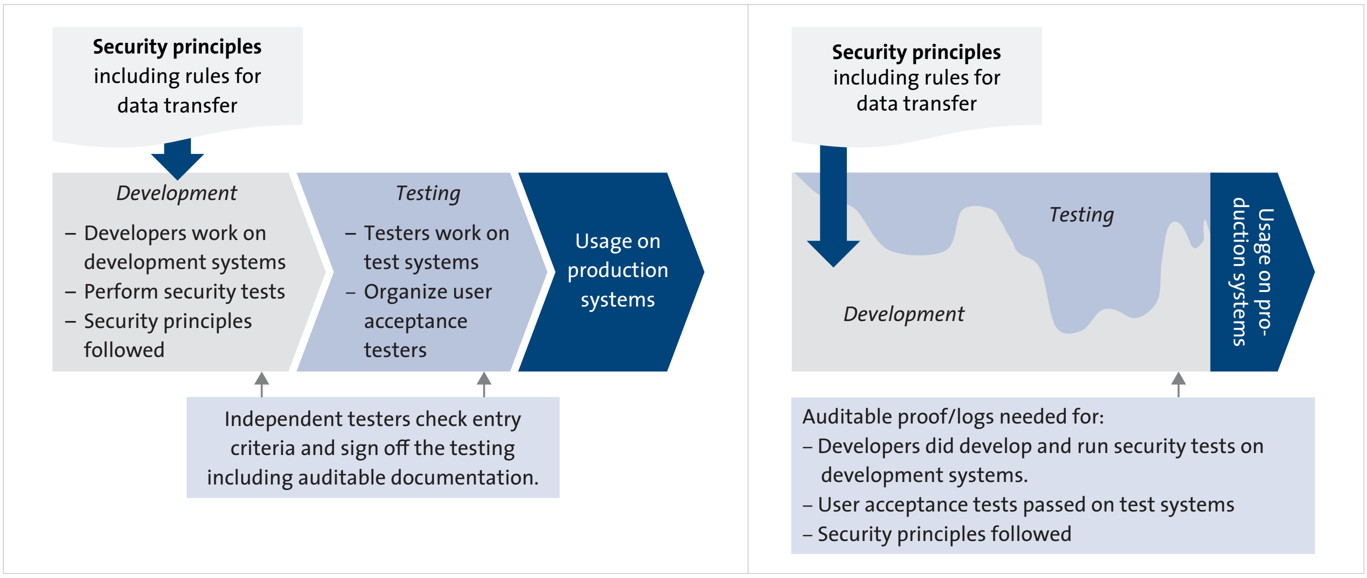
Security principles including rules for data transfer
Development
– Developers work on development systems
– Perform security tests
– Security principles followed
Testing
– Testers work on test systems
– Organize user acceptance testers
Usage on production systems
Independent testers check entry criteria and sign off the testing including auditable documentation.
Security principles including rules for data transfer
Testing
Development
Usage on production systems
Auditable proof/logs needed for:
– Developers did develop and run security tests on development systems.
– User acceptance tests passed on test systems
– Security principles followed

Figure 3. How ISO 27001 Influences in the Software Development Processes – V-model (Left) and Scrum (Right)

Scrum, V-Model, Security Principles, and ISO 27001

ISO27001 defines three controls for the software development processes. First, **acceptance testing** against the requirements is mandatory (control A.14.2.9) – against functional and non-functional ones, the latter including the security requirements. Second, there must be **security tests** during the overall development process (control A.14.2.8). Third, development, test, and operational **environments** must be **separated** (control A.12.1.4).

These controls are compatible with many software development processes such as Scrum or the older V-model (Figure 3). However, Scrum requires more thoughts than the V-model. IT departments using the V-model often have a test center and quality gates. Quality gates define the criteria for when tests can start and when they succeed. One criterion before the test start can be that developers performed security tests. One exit criterion for testing can be that user acceptance tests in the test environment succeeded for functional and non-functional requirements. When testers work in a test center and are not part of a development team, development teams cannot put much pressure on them. Thus, testers can enforce the ISO 27001 requirements more easily for *all* projects, even delayed ones.

In the world of Scrum and Agile, there are often no test centers and no central governance. It might be questionable, but it is reality (see [6] for better options). Development and testing overlap time-wise. Roles overlap. In the development methodology, however, this is no excuse for missing documentation or non-implemented controls in an ISO 27001 audit. **All controls** mentioned above must exist **for *all* projects**, even delayed ones. This is the key challenge for agile projects in an ISO 27001 organization.

Besides the controls for the development process, the ISO standard formulates **controls for the software product** itself. It demands that the security needs in the engineering process are reflected by defining principles and they must be applied to all development projects (control A.14.2.5). First, the IT department has to write them down. Second, the IT department must enforce the principles in all projects.

As part of the requirements analysis for new software or new releases, information security requirements have to be collected and specified (control A.14.1.1). The standard requires clarification of the security needs of data transfers via public networks and electronic transactions (control A.14.1.2/A.14.1.3). Again, confidentiality alone is not sufficient. Integrity and availability have to be addressed, too.

ISO 27001 Controls for Release and Change Management

The ISO 27001 standard emphasizes availability controls, too, i.e., the "A" of the CIA triangle. The following controls help **to ensure stable production** systems:

- Formal change management for changes in IT and business (control A.12.1.2)
- Discouraging changes to vendor-provided software packages (A.14.2.4)
- Strict change control procedures even during development to prevent unwanted modifications (control A.14.2.2)
- Specific testing needs for operation system changes, which require business critical applications to be tested against a new platform (control A.14.2.3)
- Mandatory rules for software and operating system installation procedures, and who can do what (A.12.5.1)
- Preventing even "small" changes to circumvent testing or the change process by separating development, testing, and operational environments (control A.12.1.4), and by having access control on the source code (control A.9.4.5)

This is old-time check-box style release management. IT staff have a list of criteria they check. If all have been met, a change can go to production. This model fulfills today's needs of many organizations. Highly agile organizations, however, prefer continuous integration [7] and DevOps [8]. They invest in test automation to have quick feedback loops. There might be even no manual testing before deploying small changes into production, which raises the question as to whether this conforms to ISO 27001.

A clever strategy for dealing with ISO 27001 can help. Discussing whether ISO 27001 is outdated and Scrum, DevOps, etc. are state of the art will result in frustration. ISO 27001 is a top management decision that overrules any development or test process. Developers and testers should invest their time into explaining *how* they conform to ISO 27001, even if there is no or minimal human involvement between coding and deployment production. Written operational procedures, archived audit logs, etc. help to tell one story: All ISO 27001 controls are in place, some with manual check lists, others relying on automated, auditable processes.

Controls for Outsourcing

Outsourcing and offshoring are common in software development and testing, but pose two information security risks. First, the sourcing partners obtain sensitive data they should not have. Second, their software development and testing processes might not address the information security needs properly. ISO 27001 addresses the latter aspect with control A.14.2.7. It requires the supervision of outsourced development and testing. The work can be outsourced but the responsibility stays with the organization. In general, ISO 27001 requires suppliers also to be managed with regard to information security (control A.15). Any supplier management can enforce this. The controls are not specific to software development and testing, though the checks might differ slightly.

Two Main Conclusions on ISO 27001, and Development and Testing

Conclusion 1: Development, testing, and change management require clear written information security policies.

ISO 27001 does not require specific organizational forms or software processes. ISO 27001 emphasizes clear rules and policies for the handling of information assets and the engineering process. First, they must clarify what data is sensitive and how to handle it. Second, they must explain how the organization engineers secure software in a secure development area. Third, they must state how to get software into production without any risk for production stability.

Conclusion 2: The organization must enforce the policies in all projects and have evidence.

ISO 27001 expects policies to be enforced consistently and to have auditable evidence. In other words, there must be a process organization and all employees must be continuously educated and motivated to act accordingly. Chaotic geniuses or non-genius chaotic persons must be embedded into teams that ensure ISO 27001 conformity.

Not every developer and tester might appreciate the changes the ISO 27001 standard brings. Thus, we dedicate one Doug Larson quote to all who preferred working in IT in the times before standards such as ISO 27001: "Nostalgia is a file that removes the rough edges from the good old days." ■

References

[1] *ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements*, ISO, Geneva, Switzerland, 2013

[2] The Associated Press: *Target CEO Gregg Steinhafel resigns following last year's security breach,* 5.5.2014

[3] Wikipedia: *Information security*, *http://en.wikipedia.org/wiki/Information_security*, last retrieved July 5, 2014

[4] K. Dilanian: *A spy world reshaped by Edward Snowden*, Los Angeles Times, 22.12.20123

[5] K. Haller: *Test Data Management in Practice*, Software Quality Days 2013, Vienna, Austria, 2013

[6] K. Haller: *How Scrum Changes Test Centers*, Agile Records, August 2013

[7] M. Fowler, M. Foemmel: *Continuous integration* *http://ww.dccia.ua.es/dccia/inf/asignaturas/MADS/2013-14/lecturas/10_Fowler_Continuous_Integration.pdf*, 2006, last retrieved July 5, 2014

[8] J. Turnbull: *What DevOps means to me…*, *http://www.kartar.net/2010/02/what-devops-means-to-me/*, last retrieved July 5, 2014

> about the author

Klaus Haller has worked in IT consulting for more than nine years, primarily in the banking sector. His main topics are IT risk and compliance, data loss prevention, test center organization, and testing of information systems landscapes. He publishes regularly on testing and is a frequent speaker at conferences. He has been with Swisscom since 2006 and is based in Zurich.

Website: *www.klaushaller.net*

LinkedIn: *www.linkedin.com/pub/klaus-haller/48/a2b/798*