Auditing Security Measures

An Overview of schemes for auditing security measures

September 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Dr. Marnix Dekker, Christoffer Karsberg, Matina Lakka, Dimitra Liveri.

Contact

For contacting the authors please use resilience@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

This work has been done in collaboration with Dr. Vasilis Tsoumas, Expert in Information Security Audits.

ISBN 978-92-9204-067-3

doi: 10.2824/23801

Executive summary

Across society there are now critical services which rely on computers, networks and servers. Protecting the security of this information infrastructure is not easy. Often the information infrastructure is run by several organisations and uses different types of information technology from different companies. This report deals with the issue of how to enforce an adequate level of security across a sector of service providers.

By way of response, we give an overview of 12 different audit frameworks or certification schemes for auditing security measures, used in different settings and sectors, which are aimed at ensuring that providers comply with certain security requirements.

In particular we look at the following audit frameworks and certification schemes:

- ISO 27001
- COBIT 5
- Federal Information Security Management Act (FISMA)
- NERC Reliability Standards
- ISPS Code
- HIPAA
- Sarbanes-Oxley (SOX)
- Trust Services
- PCI-DSS
- BASEL II
- BSI-IT Grundschutz
- CESG

For each scheme we describe the overall setup and we depict the different entities and their roles in assessing or certifying compliance to the security requirements. Some of these audit frameworks are sector-specific and backed by specific legislation. Some large well-known frameworks (ISO27001 for example) are not sector-specific and are adopted across sectors on a voluntary basis. In some settings the auditing is delegated to auditors, and sometimes these auditors have to be licensed by an authority. In other settings this delegation is absent or done by a governing authority overseeing the overall scheme. In this paper we also introduce a single model that captures the most common features.

We conclude with some general remarks about the listed audit frameworks:

- **Every scheme is different:** Perhaps what is most striking about the different schemes is the fact that they are all so different. In each scheme the actual auditing is delegated to third-party auditors, but the construction used is different every time. The optimal structure for this kind of delegation depends on many factors, on the size and maturity of the sector, the resources and skills of the government authority, whether or not there are well-functioning industry initiatives, and so on.
- **Assessing certification authorities:** The generic model in Section 4 shows the key processes the involved authorities are executing or delegating: 1) auditing (what security measures are checked and how), 2) licensing of auditors (what skills sets or exams are required), 3) validation of monitoring tools (which scans or features are required), and 4) certification on the security requirements (how audit reports and monitoring reports are assessed). A governing authority could evaluate an auditing/certification authority by looking at these 4 key processes.

- **Continuous monitoring vs point-in-time assessment:** Most of the frameworks are based around periodic, point-in-time assessment of a provider or a service. In the IT industry, with the rapid changes of technology and products, the effectiveness of a point-in-time assessment might be limited – especially when considering online or cloud services that change continuously.
- **Incident reporting:** Whatever structure is used in the auditing scheme, the governing body should have a way to make a cross-check to assess the overall effectiveness of the framework in place, including the quality of the certification authority and the quality of the auditors. An objective way of assessing the overall framework or any of the constituent parts, is by looking at incident reports and/or independent test results.
- **Preventive auditing vs. post-incident investigations:** In most certification and audit frameworks the focus is on preventive and periodic audits. The goal of a preventive audit is to check whether or not all the necessary security measures are in place. Post-incident investigation is even more important, because it helps to understand the root cause of the incident, what are the lessons learnt and what could have prevented the incident. This is important to improve security and possibly the audit scheme itself too.
- **Compliance burden and entry barriers:** The digital society is rapidly changing. New services (cloud e.g.), new products (smartphones e.g.), new usage scenarios (smart grids e.g.) are emerging continuously. An important goal of EU Member States and the European commission is to foster innovation. It is important to take into account the effect of a high compliance burden on smaller providers. Large (incumbent) providers have the resources and (arguably) the need to set up advanced and sophisticated governance processes. In general it is important to take into account the impact of legislation on innovation and competition, and be particularly careful when obliging providers across a sector to submit to a fixed set of audit requirements or partake in a specific audit framework.
- **Auditing vs certification:** the scope of this document is limited to auditing frameworks and the most common schemes that are used to conduct an audit against security measures. Some of the auditing frameworks we describe below, have become certification frameworks, meaning that the audit goes one step further and compliance can be certified. This is the only meaning of certification in the context of this document.

Table of Contents

1 Introduction

In a number of different sectors and settings in society, there is a need to enforce compliance to information security measures. For example, in the EU electronic communication providers must take appropriate security measures under Article 13a of the Framework directive, and in the US health care providers must take security measures under legislation called HIPAA (Health Insurance Portability and Accountability Act). In different settings different approaches are taken: In some settings compliance is mandated by law (for example, by national regulators under Article 13a), in some settings compliance is voluntary (for example, for datacentres, ISO 27001 is often a matter of choice), or mandated by an industry association (for example, the Payment Card Industry (PCI) demands all payment processors to comply). In some settings the auditors are explicitly certified to audit the security measures (for example, ISO 27001), while in other settings anyone can audit the security measures (for example, HIPAA). This is just a taste of the different variations. In this document we give an overview of different settings where there is a need to comply with security measures to show the differences and similarities. Target audience

This paper is intended to provide background material for regulatory authorities, government authorities, national ministries, and experts in the EU involved (in passive or active role) in enforcing compliance to security legislation/security measures across providers in a sector; i.e. national regulatory authorities that need to audit the security measures proposed under Article13a, governmental authorities that need to transpose into legislation these requirements et cetera.

Goal

There is a plethora of different frameworks and standards for IT security measures. We do not give an exhaustive overview in this paper of all these different schemes, but we focus on schemes with the following characteristics:

1. **Wide adoption, possibly across sectors:** We focus on security measures standard and auditing frameworks which are widely adopted.
2. **Related to critical sectors**: We focus on critical sectors such as energy, government, health care, finance, et cetera.
3. **Different sectors, different approaches:** The goal of this paper is to show different approaches across different sectors. We do not go into the details of an auditing scheme if similar to another scheme already discussed.

We stress that the goal of this paper is not to give an exhaustive overview of governance schemes. Schemes or settings not addressed here are by no means inferior or less interesting topics for discussion.

Structure of this document

The rest of this paper is structured as follows: In Section 2 we introduce the general problem these auditing frameworks or certification schemes are trying to address. In Section 3 we derive a single model with the entities and roles that are most common across the schemes. In the conclusions we draw conclusions about the auditing schemes discussed in this paper.

2 Information Security Governance

The need to enforce compliance to information security requirements across a group of providers (businesses, government organisations, et cetera) is evident throughout different sector in society. We gave examples in the introduction.

In this section we explain the general problem, by introducing a simple model in the diagram below (Fig. 1).

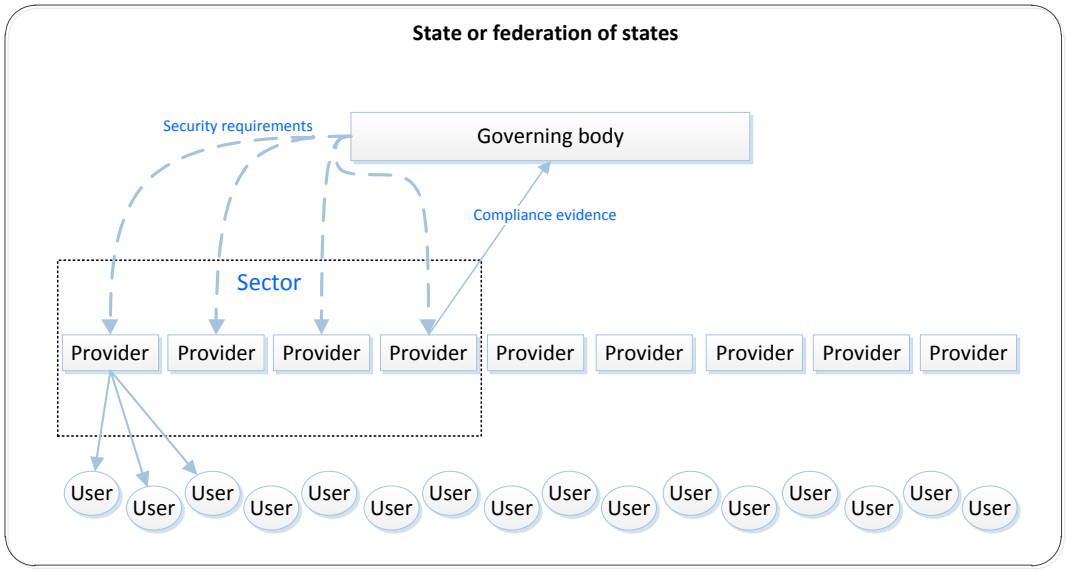

Figure 1 Abstract model depicting the issue of governance of information security requirements

The model has three types of entities (providers, users, government authority):

- Providers: Entities providing services to users (sometimes for a fee), ranging from equipment vendors, to online service providers, outsourcing firms, consultancy firms, and e-government, et cetera. Providers can be subdivided in sectors (see the dashed box). A sector is a subset of service providers which provide a specific set of services. For example, the energy sector is a group of service providers providing power (electricity, usually).
- Users: Entities consuming services provided by providers, including citizens, businesses, organisations, government organisations - in a role of consumer of services.
- Government authority: Entity set up or supported by law and/or with a legislative mandate to address security incidents with an impact on society or users, ranging from government bodies, governmental agencies, regulators, data-protection authorities, to non-governmental organizations, PPPs, or industry associations.

The government authority mandates (possibly sector-specific) security requirements which should be implemented by providers[1]. The authority normally seeks evidence of compliance – i.e. that security requirements are met. In practice the details of such a set-up are very different in different settings. In this document we examine different settings to show these differences.

[1] Users may still have further, stricter, requirements, which may be dealt with bilaterally in agreements between provider and user.

3 Audit Frameworks

In this section we give an overview of different auditing frameworks related to information security across different sectors. Some audit frameworks have a legal or regulatory backing. Some frameworks are voluntary, industry-led. Some audit frameworks are sector-specific, while others are not.

We discuss and summarize the following audit frameworks:

- ISO 27001
- COBIT
- Federal Information Security Management Act (FISMA)
- NERC Reliability Standards
- ISPS Code
- HIPAA
- Sarbanes-Oxley (SOX)
- Trust Services
- PCI-DSS
- BASEL II
- BSI-IT Grundschutz
- CESG

For each framework we provide a general introduction, we discuss the overall control and audit framework, the roles of the different actors involved, and the enforcement mechanisms.

We would like to remark that although there are several audit frameworks, the content of these frameworks is often similar. There have been initiatives to converge and align the different security standards and audit frameworks. UCF is an example[2].

3.1 ISO 27001

The ISO/IEC 27001:2005[3,4] is a well-known information security standard published by the International Organization for Standardization (ISO)[5] and the International Electro-technical Commission (IEC)[6]. ISO27001 is part of the ISO/IEC 27000 family of standards . Although ISO 27001 is not tied to a particular country's legislation, it is very popular among security practitioners worldwide, and a number of countries have adopted localized variants of the ISO 27001 standard as a primary source of recommended security controls (e.g. Revised Turnbull Guidelines on Internal Control Oct 2005[7], Australian/New Zealand Standard AS/NZS 4360:1999 Risk Management[8], etc.).

[2] Among others: Unified Compliance Framework, http://www.unifiedcompliance.com

[3] Full title is ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements.

[4] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

[5] http://www.iso.org

[6] http://www.iec.ch

[7] http://www.frc.org.uk/documents/pagemanager/frc/Revised%20Turnbull%20Guidance%20October%202005.pdf

[8] http://www.standards.org.au

3.1.1 ISO 27001 Framework

ISO 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. The standard is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. It is accompanied by the ISO 27002 standard[9] [10], which establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. Security measures are called controls. The objectives of security measures are called control objectives. In a way, ISO 27001 is taxonomy of possible controls, whereas ISO 27002 provides recommended practices for the implementation of controls. While there is no formal requirement that the two aforementioned standards (ISO 27001 & ISO 27002, respectively) must be used in conjunction, they are usually used together. The ISO 27001 standard can be used in a formal certification against the control objectives described.

It should be mentioned that ISO 27001 gives auditors a certain degree of freedom, in order to ensure effective and efficient implementation of an ISMS according to the specific information security requirements of the organization under question. Below is depicted the overall set-up of ISO 27001 framework (Fig. 2).

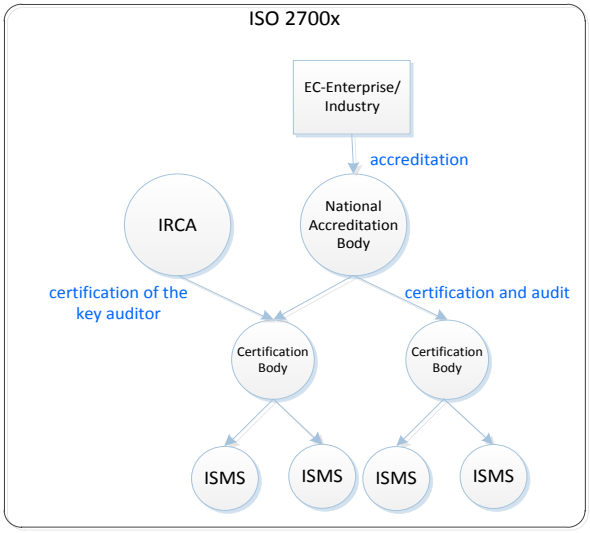

Figure 2 ISO 27001 audit framework

3.1.2 ISO 27001 Roles

In order to ensure equally high standards of certification across Europe, the European Commission for Enterprise and Industry set out a European-wide policy for accreditation[11]. This ensures consistency in the accreditation market and is designed to protect the consumer. Accordingly, it is mandatory for every European Member State to have a single National Accreditation Body (NAB). Outside of Europe, there is not a set regulation – e.g., in the USA there are multiple Accreditation

[9] Full name: Information technology -- Security techniques -- Code of practice for information security management

[10] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

[11] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:01:EN:HTML

Bodies (AB), whereas within Australasia there is the Joint Accreditation System of Australia and New Zealand[12]. For those countries without a designated National Accreditation Body, the International Accreditation Forum[13] lists member Accreditation Bodies that only accredit competent bodies, providing buyer confidence; certification against any of the recognized national variants of ISO/IEC 27001 (e.g. JIS Q 27001, the Japanese version) by an accredited Certification Body (CB) is functionally equivalent to certification against ISO/IEC 27001 itself.

An ISMS may be certified compliant with ISO 27001 by a number of Certification Bodies worldwide, which, in turn, must be accredited themselves by an International Accreditation Body for that scheme (e.g. UKAS in the United Kingdom[14]). The key personnel conducting the ISMS audit has also to be accredited as ISMS Lead Auditor(s) from a NAB-accredited Certification Body, or the International Register of Certificated Auditors (IRCA)[15].

The Accreditation Bodies accredit the competent Certification Bodies according to various scopes of ISMS accreditation[1617]; moreover, they perform periodic audits on Certification Bodies in order to ensure conformance with the accreditation standards (e.g. in the case of UKAS, the accreditation is confirmed on an annual basis by surveillance visits, with a full re-assessment every fourth year. In addition, the first surveillance visit takes place 6 months after the Grant of Accreditation). Sanctions to violators are immediately enforced[18]. More information about the accreditation process can be found on the UKAS site[19].

3.1.3 ISO 27001 Enforcement and Compliance

Certification Bodies with competent personnel re-assess the certified ISMS periodically, usually yearly. Certification Bodies, in turn, are subject to compliance audits from their respective Accreditation Bodies.

ISO 2700x is a horizontal, cross-sector family of information security standards and as such, they can be used in a variety of cases. It has to be noted that the ISO 27001 standard itself provides a structured way for auditing the implementation of the organization's information security, and lists an indicative pool of potential controls in a certain taxonomy (which may be extended by the implementer in an ad-hoc basis, according to the security needs of the organization); the responsibility of controls' selection and, more importantly, the intensity of the selected controls lies solely with the organization.

[12] http://www.jas-anz.com.au/

[13] http://www.iaf.nu/

[14] http://www.ukas.com/default.asp

[15] http://www.irca.org

[16] http://www.ukas.com/about-accreditation/accredited-bodies/certification-body-schedules-ISMS.asp

[17] http://www.ukas.com/about-accreditation/apply-for-accreditation/Extension_to_Scope.asp

[18] http://www.ukas.com/Technical-Information/Sanctions/suspended-withdrawn.asp

[19] http://www.ukas.com/library/About-Accreditation/Apply-for-Accreditation/The%20Route%20to%20Accreditation.pdf

3.2 COBIT 5

COBIT, originally 'Control Objectives for Information and related Technology' but used in acronym only since 2009, was first released in 1996 by ISACA. The current version, COBIT 5, was published in 2012. COBIT 5 helps enterprises create optimal value from information and related technology (IT) for their stakeholders by maintaining a balance between realizing benefits and optimizing risk levels and resource use. The framework addresses both business and IT functional areas across an enterprise and considers the IT-related interests of internal and external stakeholders. Enterprises of all sizes, whether commercial, not-for- profit or in the public sector, can benefit from COBIT 5.

3.2.1 COBIT Framework

COBIT is positioned as a high level framework, addressing the governance and management of enterprise information and related technology (GEIT) and has been aligned and harmonized with other, more detailed, IT standards and good practices such as COSO, TOGAF, ITIL, ISO 27000 series, PMBOK, etc. The framework is used as IT Governance best practice guidance in many cases, both at government and private sector[20].

COBIT 5 creates a single reference base for the governance and management of information and technology through its five principles. It establishes seven critical areas (enablers) that are relevant to all enterprises in the governance and management of information. Using COBIT helps enterprises to prepare for current and future compliance requirements.

Infotrmation security governance and management is a key aspet of GEIT – failure to adequately secure information and technology assets and resources destroys stakeholder value. To support information security professions in their use of COBIT 5, ISACA has published 'COBIT 5 for Information Security' [21]. This publication takes COBIT 5 as the base reference framework and provides guidance to help IT and security professionals understand, utilize, implement and direct important information security-related activities, and make more informed decisions while maintaining awareness about emerging technologies and the accompanying threats. An appendix relates the COBIT 5 for Information Security guidance to ISO/IEC 27001/2, ISF and NIST guidance.

Also in support of specific user aspects related to COBIT 5, other guide publications have been produced by ISACA, including:

- COBIT 5 Implementation[22]
- COBIT 5 for Assurance [23]
- COBIT 5 for Risk[24]
- COBIT 5: Enabling Processes[25]

[20] http://www.isaca.org/About-ISACA/Press-room/Pages/COBIT-Fact-Sheet.aspx
[21] http://www.isaca.org/COBIT/Pages/Information-Security-Product-Page.aspx
[22] http://www.isaca.org/COBIT/Pages/COBIT-5-Implementation-product-page.aspx
[23] http://www.isaca.org/COBIT/Pages/Assurance-product-page.aspx
[24] http://www.isaca.org/COBIT/Pages/Risk-product-page.aspx
[25] http://www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Processes-product-page.aspx

3.2.2 COBIT Enforcement and Compliance

COBIT 5 is an internationally accepted governance and management framework from ISACA[26], focussed on enterprise information and related technology assets and resources. COBIT 5 helps enterprises build bridges between stakeholder needs, business goals, IT related goals and enabler goals by providing a common non-technical base of reference for business and IT professionals to work with.

COBIT 5 focuses primarily on information and technology related business enablers thatupport the achievement of business goals through efficient and effective IT-related arrangements. Referring to Porter's Generic Business Model 27, core business activities (e.g., procurement, operations, marketing, sales) are discussed, as well as support activities (e.g., human resources, administration, information technology). As a consequence, COBIT adddreses the use of information and related technology across the whole enterprise, not only within the IT department.

3.3 Federal Information Security Management Act (FISMA)

In a report to the US congress[28], the government notes that for US federal agencies, on average, IT security spending amounts cover up to 16% of total IT spending. The same report notes that in 2010 US-CERT handled 107,439 incident reports, and that approximately 41,776 of those were incidents in federal agencies.

FISMA was passed as Title III of the E-Government Act (Public Law 107-347) in December 2002[29] and sets high level security requirements. FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Federal Information Processing Standards (FIPS) are developed by NIST and approved by the US Secretary of Commerce. Legislative basis for FIPS are the Information Technology Management Reform Act (Public Law 104-106) and the Federal Information Security Management Act (FISMA) of 2002 (Public Law 107-347). FIPS standards are also used by other organizations around the world[30], as a best practice for security requirements, especially in regulated industry sectors (such as financial and health-care institutions) that process Sensitive But *Unclassified* (*SBU*) information. FIPS does not apply to national security systems (as defined in Title III, Information Security, of FISMA).

Federal agencies must adhere to FIPS 200 which "specifies minimum security requirements for federal information and information systems and a risk-based process for selecting the security controls necessary to satisfy the minimum requirements." In essence, the high level security requirements mandated by FISMA are further specialized through FIPS and other more detailed standards, such as NIST SCAP. The interested reader can find a description of the FIPS framework in the appendix.

[26] www.isaca.org

[27] M. Porter, 1980, Competitive Strategy: Techniques for Analyzing Industries and Competitors

[28] *http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY10_FISMA.pdf*

[29] http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/content-detail.html

[30] Well-known example is HSMs (Hardware Security Modules) used by CAs and in other PKI infrastructures, which must be FIPS 140-2 certified.

3.3.1 FISMA Framework

National Institute of Standards and Technology (NIST) reviews[31] the security control requirements catalogue and in what is called the *Assessment and Update process*: FIPS 200[32] describes how security controls are assessed and (if needed) updated:

- "The security controls will be reviewed by NIST at least annually and, if necessary, revised and extended to reflect: (i) the experience gained from using the controls; (ii) the changing security requirements within federal agencies; and (iii) the new security technologies that may be available."
- "The minimum security controls defined in the low, moderate, and high security control baselines are also expected to change over time as well, as the level of security and due diligence for mitigating risks within federal agencies increases."
- All the modifications of the NIST catalogue go through "a rigorous, public review process to obtain government and private sector feedback and to build consensus for the changes".
- Change Management process: Upon modifications the Federal Agencies should: "up to one year from the date of final publication to fully comply with the changes but are encouraged to initiate compliance activities immediately."

In FISMA, organizations must:

a. periodically assess the security controls in organizational information systems to determine if the controls are effective in their application;
b. develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems;
c. authorize the operation of organizational information systems and any associated information system connections;
d. monitor information system security controls on an on-going basis to ensure the continued effectiveness of the controls.

A model of FIPS framework is illustrated below (Fig. 3).

[31] Indicative documents: "FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems, 2006#", and "NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems#", as updated.
[32] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

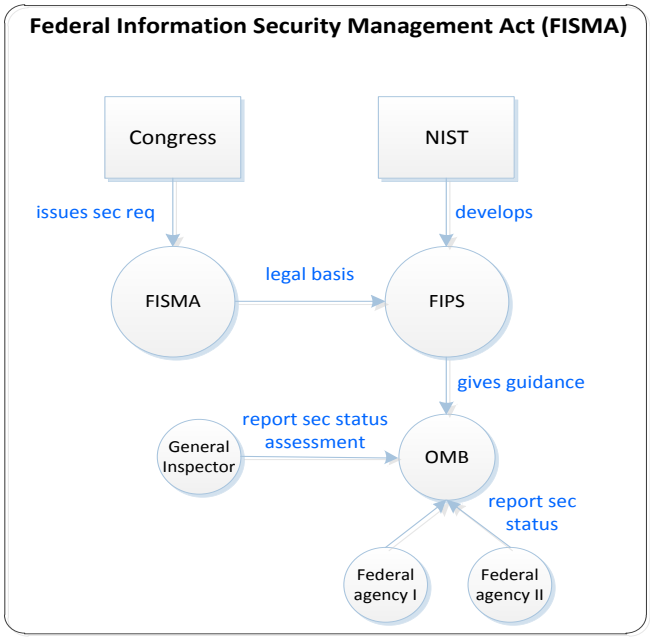

Figure 3 FISMA audit framework

3.3.2 FISMA Roles

The following organizations play a role in implementing FISMA.

- The USA Congress establishes top-level security requirements for federal agencies and support contractors in the FISMA legislation.
- NIST develops the security standards and guidelines (called FIPS) for FISMA implementation, including a risk-based approach for selecting, implementing, and assessing security controls for federal information systems and for determining risk to organizational operations and assets, individuals, other organizations, and the Nation.
- Agency heads, in coordination with their Chief Information Officers and Senior Agency Information Security Officers report the security status of their information systems to the Office of Management and Budget (OMB) in accordance with annual FISMA reporting guidance.
- Inspectors General provide an independent assessment of the security status of federal information systems, also reporting results to OMB annually.

3.3.3 FISMA Enforcement and Compliance

FISMA compliance is mandatory for federal agencies of the USA. To achieve compliance with the NIST Standards and Guidelines, the common practice is to base the detailed description of each system's technical configuration on the NIST derived, Security Content Automation Protocol (SCAP[33]) format[34]. Moreover, the OMB has required, in July 31st, 2007 memorandum to Federal CIOs[35], that "Information technology providers must use SCAP validated tools, as they become available, to certify their products do not alter these configurations, and agencies must use these *tools when*

[33] http://scap.nist.gov/
[34] The relevant specification ("The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2") is available at the NIST site
[35] http://www.cio.gov/documents/FDCC_memo.pdf

monitoring use of these configurations."[36]. SCAP deals mainly with the technical configurations of certain technologies (operating systems, databases and active network components), while the support for secure configuration at the application level is limited, due to the custom character of the applications themselves.

In the federal agencies of the USA there is a trend towards the automation of security requirements, and therefore promoting the standardization of technical configurations of the ICT systems[37]. Requirements to establish mandatory configuration settings derive from the FISMA as implemented by FIPS 200 and NIST Special Publication 800-53 (Security Control CM-6, Configuration Settings), and OMB [38] Policy. Federal CIOs must deploy appropriate configuration settings on commercial information technology products that compose their organizational information systems. These products include, for example, mainframe computers, workstations, portable and mobile devices, and network components.

3.3.4 FIPS 140

The FIPS 140 series establishes requirements and standards for cryptography modules that include both hardware and software components. The use of validated cryptographic modules is required by the United States Government for all unclassified uses of cryptography.

In order to use a cryptography module in a production environment, the module has to be accompanied by a validation certificate issued by an accredited laboratory through the Cryptographic Module Validation Program (CMVP), a joint effort by the NIST and the Communications Security Establishment Canada (CSEC). Moreover, as a prerequisite action the algorithms themselves are tested via the Cryptographic Algorithm Validation Program (CAVP), with the same setting and philosophy as in CMVP. All of the tests under the CAVP are handled by third-party laboratories that are accredited as Cryptographic and Security Testing (CST) Laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP). Vendors interested in validation testing of their algorithm implementation may select any of the accredited laboratories. A certificate is valid for the lifetime of that version of the product.

Vendors of cryptographic modules use independent, accredited Cryptographic and Security Testing (CST) laboratories to test their modules. The CST laboratories use the Derived Test Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules against the applicable standards. NIST's Computer Security Division (CSD) and CSEC jointly serve as the Validation Authorities for the program, validating the test results and issuing certificates.

Cryptographic modules that conform to FIPS 140 use approved security functions such as cryptographic algorithms, cryptographic key management techniques, and authentication techniques. Approved security functions include those that are either:

- specified in a Federal Information Processing Standard (FIPS),
- or adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS, or
- specified in the list of Approved security functions.

[36] http://nvd.nist.gov/scapproducts.cfm
[37] http://www.ca.com/~/media/Files/whitepapers/20-cscs-wp.pdf

[38] For a NASA-related audit report, refer here: http://oig.nasa.gov/NASA2010ManagementChallenges.pdf

The audit process of the FIPS 140 implementation on behalf of the accredited laboratories is defined in the "NIST Handbook 150-xx" standard series; numerous managerial, organizational, procedural and technical countermeasures are defined in the "NIST Handbook 150-xx" standard series (many of them with specific metrics, such as probabilities of false positives occurrence). The complementary NVLAP standard "NIST Handbook 150" provides detailed controls for ensuring the adequacy of a laboratory practices throughout its whole life cycle.

3.4 NERC Reliability standards

The North American Electric Reliability Corporation (NERC)[39] is an international, independent, not-for-profit, self-regulatory organization, that aims to ensure the reliability of the bulk power system in North America. In 2007, the U.S. Federal Energy Regulatory Commission (FERC)[40] granted NERC the legal authority to enforce reliability standards with all users, owners, and operators of the bulk power system in the United States, and made compliance with those standards mandatory and enforceable.

3.4.1 NERC Framework

Reliability standards are the planning and operating rules that electric utilities follow to ensure reliable systems. NERC's reliability standards development process has been accredited by the American National Standards Institute (ANSI).

The first set of enforceable standards was filed with FERC in 2006. In 2007, FERC approved 83 of the 102 proposed standards. Those 83 standards became mandatory and enforceable in the U.S. on June 18, 2007. The remaining standards are still being reviewed by FERC. The U.S. Department of Energy designated NERC as the electricity sector coordinator for critical infrastructure protection. NERC serves as the Information Sharing and Analysis Center for the electricity sector. The NERC's security initiatives are coordinated by the Critical Infrastructure Protection Committee (CIPC), which also works closely with the U.S. Department of Homeland Security and Public Safety and Emergency Preparedness Canada to ensure that the critical infrastructure protection functions so vital to the industry are fully integrated and coordinated with the governments of the Unites States and Canada.

Regarding the ICT security measures defined, there are multiple standards developed for US NERC ("Reliability Standards"), with a number of them addressing cyber security issues; complementary to this, specific and detailed audit programs have been developed with the aim of ensuring compliance with the aforesaid Reliability Standards (e.g. *"CIP-005-3a — Cyber Security — Electronic Security Perimeter(s)"*, *"COM-001-1.1 — Telecommunications"*, etc. These standards and their respective audit programs are in a process of continuous update, in cooperation with the DHS and FERC, among others. The focus is on security objectives and not on the actual implementations of specific technologies, but a FISMA-like approach may be adopted for specific technologies (i.e. checklists, tools, SCAP, etc.). The NERC control and audit framework is represented below (Fig 4).

[39] http://www.nerc.com

[40] FERC (http://www.ferc.gov/) is a federal agency that regulates the interstate transmission of electricity (as well as natural gas and oil). FERC oversees NERC in the U.S.

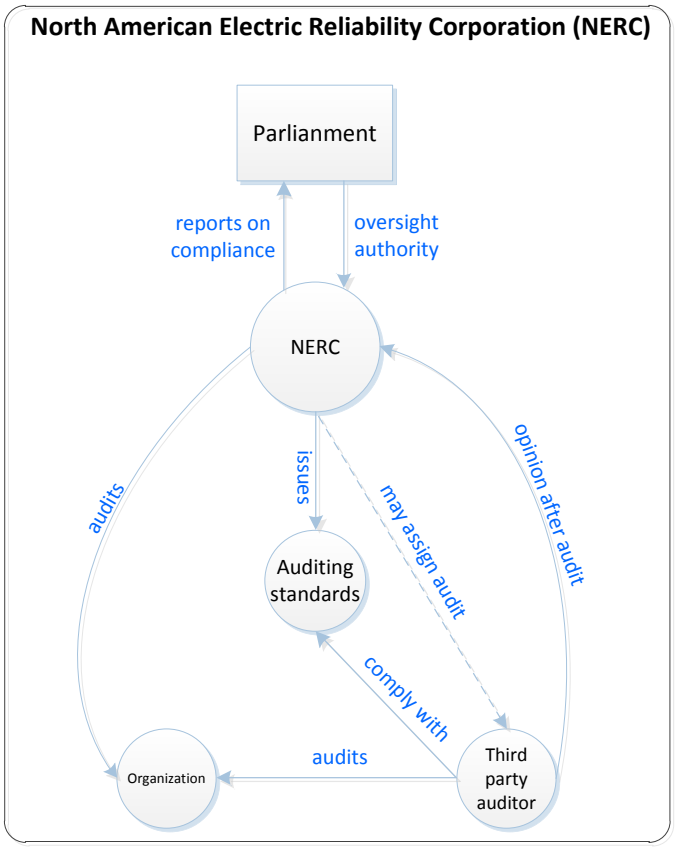

Figure 4 NERC audit framework

3.4.2 NERC Roles

All bulk power system owners, operators, and users must comply with approved NERC reliability standards. These entities are required to register with NERC through the appropriate regional entity. NERC's compliance efforts comprise three key activities:

1. Compliance monitoring is the process used to assess, investigate, evaluate, and audit in order to measure compliance with NERC standards;
2. Compliance enforcement is the process by which NERC issues sanctions and ensures mitigation of confirmed violations of mandatory NERC reliability standards;
3. Due Process provides registered entities the opportunity to contest any finding of a violation of a NERC reliability standard. The process allows for hearings at the regional entity and appeals before NERC.

NERC works with eight regional entities to improve the reliability of the bulk power system. These entities account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico[41].

Regional compliance implementation plans[42] are the strategic plans for the annual compliance monitoring and enforcement activities implemented by each to fulfil its responsibility to monitor compliance with NERC reliability standards as specified by each region's delegation agreements. All

[41] http://www.nerc.com/page.php?cid=1|9|119

[42] http://www.nerc.com/page.php?cid=3|23|209

regional entities submit their annual plans to NERC for consideration by November 1 every year, at which point NERC reviews and subsequently approves the regional annual implementation plan. As part of its oversight, NERC conducts periodic audits of each regional program. Reports generated from these activities can be found on the NERC site[43].

3.4.3 NERC Enforcement and Compliance

In the USA[44], NERC and the eight regional entities charged with compliance enforcement monitor compliance via a number of methods, including regular and scheduled compliance audits, random spot checks, and specific investigations as warranted by indications that a standard may have been violated. NERC and the Regional Entities work closely with each user, owner, or operator to review and monitor plans to resolve any reliability issues as quickly as possible.

As part of these efforts, NERC can also issue remedial action directives to immediately address and deter new or further violation(s), irrespective of the presence or status (i.e. confirmed or alleged) of a violation. Sanctioning of confirmed violations is determined pursuant to the NERC Sanction Guidelines and is based heavily upon the Violation Risk Factors and Violation Severity Levels of the standards requirements violated and the violations' duration. Entities found in violation of any standard must submit a mitigation plan for approval by NERC and, once approved, must execute this plan as submitted.

Especially for the audits relevant to cyber-security measures implementation, the regions have brought in cyber security experts in dedicated compliance enforcement roles for the additional workload brought about by CIP[45]. For 2012, 328 CIP audits are scheduled[46], whereas for the 2011 period 244 analogous audits were scheduled[47], which shows a raise of 34% regarding CIP audits activity.

In 2011 NERC published the first Compliance Analysis Report[48], in which it analyses the standards that have experienced a high frequency of violations since June 18, 2007, after the relevant audits. Among them, the CIP-004 (Personnel and Training), CIP-001 (Sabotage Reporting), CIP-006 (Physical Security of Critical Cyber Assets) and CIP-007 (Systems Security Management) are analysed.

An important concept is the inclusion of third-party independent organizations which act as auditors on behalf of the NERC; such an example exists for the Regional Entity "Midwest Reliability Organization (MRO)", for which the audit was performed by the private firm Crowe Horwath LLP[49]. For this specific audit, and with respect to the purely ICT security measures in place, only the Internal IT Security Policy and the Data Classification Procedure Manual of the organization were reviewed.

[43] http://www.nerc.com/page.php?cid=3|23|210

[44] Similar practices are followed in other North American countries where NERC operates.

[45] http://www.nerc.com/files/2010%20CMEP%20Annual%20Report_posted.pdf

[46] http://www.nerc.com/files/2012%20PUBLIC%20Audit%20Schedule.xls

[47] http://www.nerc.com/files/2011%20PUBLIC%20Audit%20Schedule%20POSTED%2009_28_11.xls

[48] http://www.nerc.com/files/Organization%20Certifications1.pdf

[49] http://www.nerc.com/files/MRO_AUP_Final_Report_20100408.pdf

3.5 International Ship and Port Facility Security (ISPS) Code

The International Ship and Port Facility Security (ISPS) Code[50] is an amendment to the Safety of Life at Sea (SOLAS) Convention (1974/1988)[51] mandating for minimum security arrangements for ships, ports and government agencies. ISPS is detailed in the Chapter XI-2 of the SOLAS ("Special measures to enhance maritime security") and has come into force in July 2004, signed by 108 Contracting Governments ("CGs"). Europe has adopted the International regulations with EC Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004, on enhancing ship and port facility security.

ISPS prescribes responsibilities to governments, shipping companies, shipboard personnel, and port/facility personnel to "*detect security threats and take preventative measures against security incidents affecting ships or port facilities used in international trade.*"[52]. In essence, the code takes the approach that ensuring the security of ships and port facilities is a risk management activity and that, to determine what security measures are appropriate, an assessment of the risks must be made in each particular case.

The purpose of the code is to provide a standardised, consistent framework for evaluating risk, enabling governments to offset changes in threat with changes in vulnerability for ships and port facilities through determination of appropriate security levels and corresponding security measures. The code (which does not refer to warships, naval auxiliaries or other ships owned or operated by a Contracting Government and used only on Government non-commercial service), has a serious impact on insurance rates.

3.5.1 ISPS Framework

The ISPS code is comprised of two parts: Part A is mandatory, describing minimum requirements for security of ships and ports, while Part B provides implementation guidelines. The ISPS Code applies to ships on international voyages (incl. passenger ships, cargo ships of 500 GT and upwards, and mobile offshore drilling units) and the port facilities serving such ships. The code gives flexibility to governments towards applying the code provisions even to port facilities that are used only occasionally for international voyages; moreover, the extent of code application to the selected ports lies solely with the governments. In a nutshell, the national governments are free to select the port facilities and the intensity of the applied measures according to a security assessment carried out as described in the code. Below is visualised the ISPS audit framework (Fig. 5).

[50] http://www.imo.org/blast/mainframe.asp?topic_id=583&doc_id=2689
[51] http://www.imo.org/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-%28SOLAS%29,-1974.aspx
[52] ISPS Code, Part A, 1.2.1

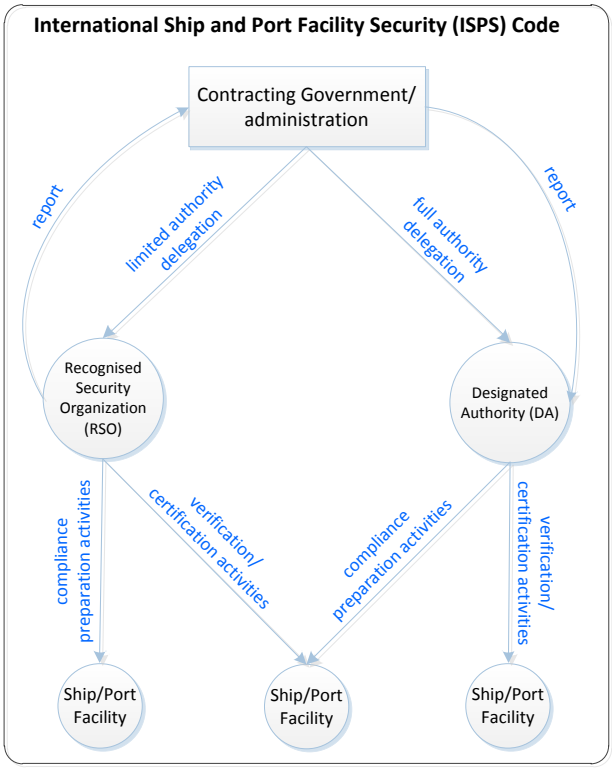

Figure 5 ISPS audit framework

Moreover, the code provides for three (3) security Levels, corresponding to a normal, heightened and exceptional threat situations enacted by the Contracting Governments as follows:

- Security level 1 means the level for which minimum appropriate protective security measures shall be maintained at all times.
- Security level 2 means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.
- Security level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

Because each ship (or class of ship) and each port facility present different risks, the method in which they will meet the specific requirements of this Code will be determined and eventually be approved by the Administration (i.e. flag state) or Contracting Government, as the case may be. In that respect, the measures are defined in a generic form of security requirements while their correct enforcement lies with the responsible party.

3.5.2 ISPS Roles

The ISPS Code is part of SOLAS, so compliance is mandatory for the 148 Contracting Parties to SOLAS. In terms of the ISPS Code, the Contracting Governments have various responsibilities, including:

- Setting the security level;
- Approving SSPs and any amendments to a previously approved plan;
- Verifying compliance of ships with the provisions of the regulation;

- Issuing the relevant International Ship Security Certificates (ISSC);
- Determining which port facilities located within their territory are required to designate and train a Port Facility Security Officer (PFSO);
- Ensuring completion and approval of the port facility security assessment (PFSA) and port facility security plan (PFSP) or any subsequent PFSP amendment;
- Issuing statements of compliance for port facilities;
- Exercising control and compliance measures over ships.

Regarding the responsibilities of the Company and the Ship, shipping companies are required to:

- Designate and train a CSO (at least one per company) and to have in place designated and trained SSOs for each of their ships;
- Approval of each SSP is normally by the administration (flag state). Thereafter, the SSP is used on board the ship with responsibility falling onto the SSO for successful implementation;
- While the setting of a security level is solely the responsibility of a contracting government, a Master or SSO can enhance the security measures that are in place on board the ship at any time (e.g. when the vessel is sailing through an area of increased vulnerability);
- The training of the ship's crew in terms of security practices linked to the SSP, as well for ensuring proper security-related records are maintained and that any security equipment used on board the ship is functioning properly;
- Ships after the issuance of the ISSC by their administration, must maintain documentary evidence of continued compliance with the legislation.

Finally, the responsibilities of the Port Facility are as follows:

- The PFSO prepares and implements a suitable PFSP, ensuring the port always operates at security level 1, and the additional measures / possible preparatory actions are in place to operate at security levels 2 and 3, if necessary.
- The PFSO is responsible for the training of port staff in terms of the PFSP procedures and the carrying out of regular security related drills and exercises, as well as for the proper security-related records and maintenance.

3.5.3 ISPS Enforcement and Compliance

Involved entities are bound to code provisions from July 1st, 2004. Towards ensuring the proper measures taken, the Contracting Government is responsible for communicating security-related information to the International Maritime Organization and to the shipping and port industries. In order to communicate the security threat to a port facility or a ship, the contracting government will firstly set the appropriate security level based on its assessment of all available current security intelligence. Whilst they can, if appropriate, designate or establish "Designated Authorities" ("DA") within government to undertake some of its' security duties and allow Recognised Security Organisations (RSOs)[53] to carry out certain aspects of this work[54], the final responsibility for the ISPS code remains with the CG.

The initial security assessments (SSAs, PFSAs) can be delegated to a DA or a RSO, while the final PFSA approval has to be approved by the contracting government or the designated authority concerned.

[53] Competent organizations to perform certain tasks of the regulation, according to section 4.5, pg. 36 of the Code.
[54] Important exceptions (including setting of the security level), are detailed in the section 4.3, pg.7 of the Code.

Port Facility Security Assessments are periodically reviewed. With respect to the effectiveness of the SSP / PFSP or the relevant amendments, these can, in the extent they consider appropriate, test the effectiveness of the SSP / PFSP or the relevant amendments.

Testing can be performed by the contracting government, a designated authority or a recognised security organisation. Finally, certain other tasks (such as assistance towards performing a PFSA, verification and certification of compliance of ships with the requirements of the code, etc.) can be assigned to an RSO. Typically, every contracting government creates a national recognised security organisation registry after a relevant bid; thereafter, the eligible RSOs may be assigned certain tasks, as prescribed by the code. Conflict of interest issues apply (e.g. an RSO should not be authorized to evaluate a PFSP which has been developed by this specific RSO).

3.6 Health Insurance Portability and Accountability Act (HIPAA)

The USA's Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, mandates the US Dept. of Health and Human Services (HHS) to adopt and enforce national standards for electronic health care transactions, health identifiers, security and privacy (Part 164).

The HIPAA evaluation standard (§ 164.308(a)(8)) also requires covered entities to perform a periodic (technical and non-technical) evaluation to assess if security policies and procedures meet the security requirements. This evaluation can be performed internally or by a third-party auditor.

3.6.1 HIPAA Framework

HIPAA defines security standards in the Subpart C, where privacy standards are defined in the Subpart E. Implementation specifications are "Required" (mandatory) or "Addressable" (optional) for "covered" (i.e. involved) entities. The HIPAA security and privacy provisions are expressed in a generic manner, independent of technology or specific implementations and cover managerial, policy, organizational, procedural and technical aspects[55]. The organisations that have to comply to HIPAA ('covered entities') are free to use whatever means they deem appropriate according to the nature of their business, e.g. organisational structures, technical checklists for hardening their IT systems, etc. The HIPPA overall set-up is shown in the following diagram (Fig. 6).

[55] http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/index.html

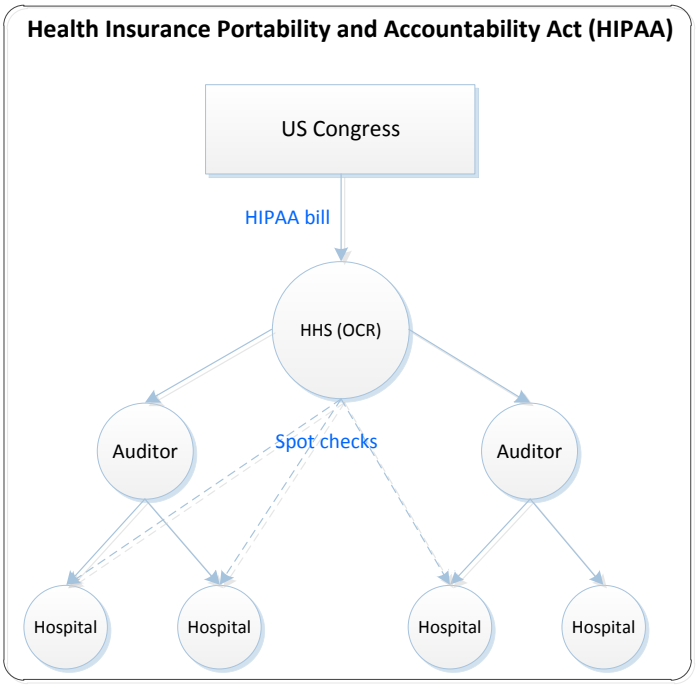

Figure 6 HIPAA audit framework

3.6.2 HIPAA Roles

HHS, and in particular the HHS's Office for Civil Rights (OCR), is responsible for the enforcement of HIPAA to the covered entities. HIPAA, with its (potentially) high penalties for non-compliance, has led to a niche market specialized in HIPAA readiness.

3.6.3 HIPAA Enforcement and Compliance

HHS enforces the HIPAA Privacy and Security Rules in several ways:

- by investigating complaints;
- by imposing financial sanctions;
- by conducting compliance reviews to determine if covered entities are in compliance; and
- by giving education to promote compliance with HIPAA

The American Recovery and Reinvestment Act[56] of 2009, in Section 13411 of the HITECH Act, requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification standards. To implement this mandate, Office of Civil Rights (OCR) is piloting a program to perform up to 150 audits of covered entities to assess privacy and security compliance.

Until recently HHS has limited its efforts to educating about HIPAA and dealing with complaints. To reassess HIPAA effectiveness and efficiency (and mandated by Section 13411 of the HITECH Act), an HHS audit program was started in late 2011 to asses compliance with the HIPAA Privacy and Security Rules and Breach Notification standards.

[56] http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf

3.7 Sarbanes-Oxley (SOX)

The USA Sarbanes Oxley Act (SOX)[57] was adopted in 2002 to protect investors from fraudulent accounting activities by businesses. SOX mandates strict reforms to improve financial disclosures from corporations and prevent accounting fraud. SOX was adopted in response to the accounting scandals in the early 2000s at Enron, Tyco, and WorldCom, to name a few. All public companies listed in New York Security Exchange (NY SEC) are bound to SOX Act[58].

The key provisions of the SOX Act are:

1. Section 302: requires management to certify the accuracy of the reported financial statement;
2. Section 404: requires that management and auditors establish internal controls and reporting methods on the adequacy of those controls. Section 404 had very costly implications for publicly traded companies as it is expensive to establish and maintain the internal controls.

SOX 404 describes in a generic manner the recommended security measures, and focuses on the desired outcome of the security measures. This approach aims to give flexibility to organisations to implement appropriate security measures but it also left room for interpretation by auditors which led to excessive compliance costs for organisations especially during the early years of the SOX introduction. Often the security measures are a subset of COBIT and ISO 27002, with customized security measures for this setting.

3.7.1 SOX Framework

Compliance to SOX is checked by the Public Company Accounting Oversight Board (PCAOB)[59], which is a non-profit organisation established by the US Congress for this purpose. The NY SEC has oversight authority over the PCAOB.

The role of PCAOB is twofold:

1. PCAOB sets the general framework for accounting/audit firms ("registered firms") who can perform SOX 404 audits.
2. PCAOB audits in a periodic, risk-based manner the registered firms for proper practices.

The SOX control and audit framework is depicted below (Fig. 7).

[57] *http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.htm*
[58] *http://pcaobus.org/Information/Pages/PublicCompanies.aspx*

[59] http://pcaobus.org/About/Pages/default.aspx

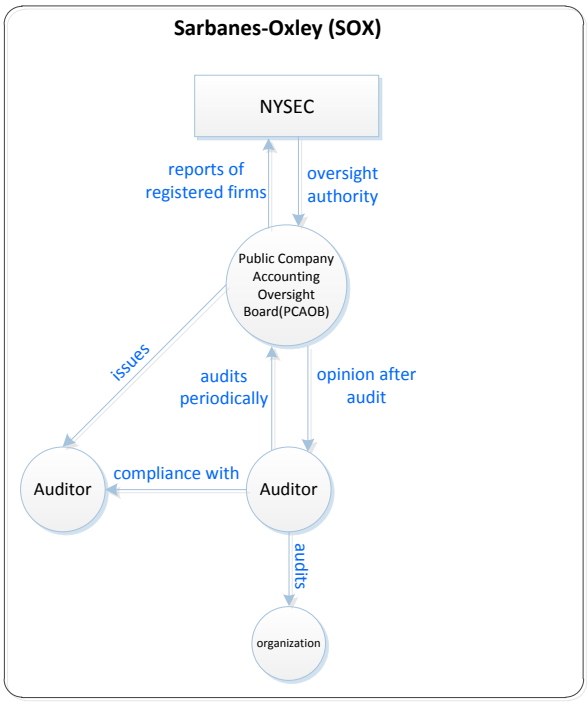

Figure 7 SOX audit framework

3.7.2 SOX Roles

There are three parties involved in checking compliance to SOX:

- An accounting/audit firm (a 'registered firm') audits an organisation and issues an opinion about the compliance of the organisation to SOX (usually through an integrated audit). This opinion is then disclosed to the PCAOB and the SEC.
- The PCAOB audits the effectiveness (primarily) and efficiency (secondary) of the implementation of SOX, by checking organisations that have to comply to SOX and firms that can perform SOX audits. PCAOB reports to the SEC and to certain state regulatory authorities.
- The SEC has oversight authority over the PCAOB, including the approval of PCAOB's rules, standards, and budget.

3.7.3 SOX Enforcement and Compliance

SOX 404 enforcement is split into the following parts:

- Accounting/audit firms perform SOX 404 audits (usually as part of an integrated audit, i.e. in conjunction with a financial statements audit).
- The PCAOB inspects accounting/audit firms ('registered firms') for the purpose of assessing compliance with laws, rules, and professional standards on auditing. PCAOB conducts regular, periodic inspections of hundreds of firms[60] PCAOB can impose severe sanctions to both registered firms and individuals in case of SOX violations. SOX requires the PCAOB to adopt a risk-based approach (annual inspections for firms audit reports for more than 100

[60] http://pcaobus.org/Inspections/Pages/InspectedFirms.aspx

businesses, and at least triennially for smaller firms). In 2011, 10 registered firms were audited annually.

- PCAOB reports about these audits to the SEC and to certain state regulatory authorities. PCAOB makes only portions of these reports available to the public[61].

3.8 Trust Services

Trust Services is a framework of assurance and audit services, to address security and privacy risks – mainly focussed on online service providers. The criteria and principles underlying Trust Services are set by AICPA[62]. These criteria are used by auditors providing attestation services on systems in the subject matters of security, availability, processing integrity, privacy, confidentiality, and certification authorities[63]. The current version of Trust Services reflects application in the USA as reflected by the references to the AICPA's attestation section AT 101, I (AICPA, Professional Standards, vol. 1). For international issuers of WebTrust and SysTrust reports, practitioners may also refer to international or domestic professional standards that are equivalent to AT 101.

SysTrust and WebTrust require accountants to conduct an independent examination that carries the professional equivalency of a financial statement audit; the attestation and advisory services based on Trust Services are discussed in the next section.

3.8.1 Trust Services Framework

The Trust Services framework has three types of assurances: examination, review, and agreed-upon procedures engagements. In examination and review engagements, the auditor expresses an opinion, for example, about whether there is the controls of a system were operating effectively to meet the criteria for systems reliability. In an agreed-upon procedures engagement, the practitioner does not express an opinion but rather performs an audit following agreed-up-on procedures, and reports the findings. Attestation services are developed in accordance with AT section 101, Attest Engagements (AICPA, Professional Standards, vol. 1)[64]. The following diagram shows the Trust Service audit model (Fig. 8).

[61] Note that in the latest (Jan. 2012) submission of the PCAOB performance review to the US SEC ("Review of the Public Company Accounting Oversight Board's Enforcement and Investigations Program") reported that "... the most significant issue facing the board's enforcement program and its ability to effectively protect investors was the statute-mandated non-public nature of disciplinary proceedings."

[62] American Institute of Certified Public Accountants (http://www.aicpa.org)

[63] The latest version can be found at http://www.webtrust.org/item27806.doc.

[64] Trust Services Principles, criteria, and illustrations (2009)

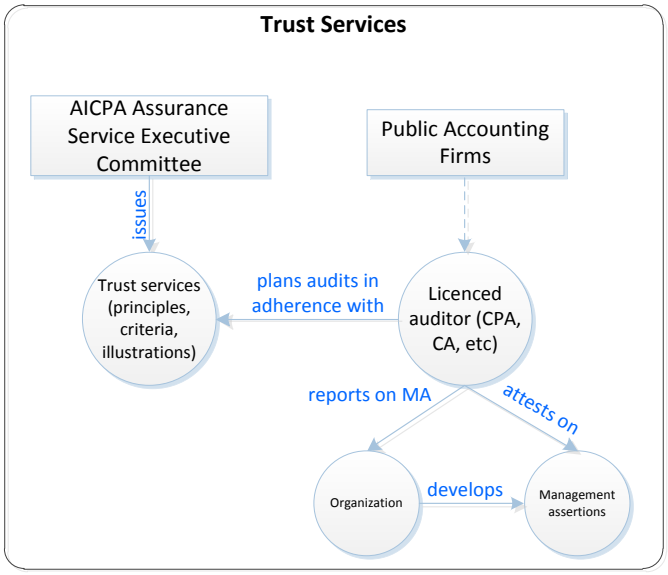

Figure 8 Trust Services audit framework

The guidance on Trust Services sets out principles, which are broad statements of objectives, and specific criteria that should be achieved to meet each principle. The Trust Services principles and criteria are supported by a list of illustrative controls that, if operating effectively, enable a system to meet the criteria. These illustrations are not intended to be all-inclusive and are presented as examples only. The practitioner should identify and assess the relevant controls that the client has in place.

3.8.2 Trust Services Roles

AICPA, the American Institute of Certified Public Accountants, is responsible for review, assessment and approval of the Trust Services on a periodic basis (the latest version is that of 2009. Audits against the Trust Services criteria can only be done by licensed auditors (Certified Public Accountants/CPAs, Chartered Accountants/CAs, or equivalent accounting professionals). Auditors licensed[65] to perform SysTrust and WebTrust services provide a report that gives assurance attesting to an entity's compliance with the Trust Services Principles and Criteria. In case of a WebTrust attestation, licensed auditors can provide a WebTrust seal that can be displayed on the client's web site.

3.8.3 Trust Services Enforcement and Compliance

Trust Services attestation is professionally equivalent with a financial statement audit attestation. Commercial agreements and partnerships often require a Trust Services attestation from an independent auditor. For example, the inclusion of a vendor's digital certificates in the Mozilla project Root CA store[66] and Microsoft Windows Root Certificate Program[67], requires the vendor to undergo some kind of audit: WebTrust for CAs, WebTrust EV are common options. Another common option is an ETSI compliance report.

[65] http://www.webtrust.org/homepage-documents/item27834.aspx

[66] http://www.mozilla.org/projects/security/certs/included/

[67] http://social.technet.microsoft.com/wiki/contents/articles/1760.aspx

3.9 Payment Card Industry Data Security Standard (PCI-DSS)

The Payment Card Industry Data Security Standard (PCI-DSS)[68], is a security standard for the payment card industry. PCI DSS is developed and management by the PCI Security Standards Council (PCI SSC) This council was set up by a number of large payment card brands (American Express, Discover Financial Services, JCB International, MasterCard, Visa) to strengthen security controls around cardholder data towards reducing credit card fraud, and, finally, enhance trust on electronic payments.

PCI DSS contains technical and operational requirements ('control objectives') set by the PCI Security Standards Council (PCI SSC) to protect 'cardholder data'. The PCI-DSS standard itself is comprised of 12 generic information security principles and it covers technical and operational system components used for the processing of cardholder data. The PCI DSS standard includes security measures which are technology-independent. PCI DSS also provides references to state-of-the-art technologies and best practices used in the payment industry.

3.9.1 PCI-DSS Framework

PCI-DSS applies to all organisations that store, process or transmit cardholder data. PCI DSS gives guidance to software developers and manufacturers of applications and devices used in payment transactions. The overall process is overseen by the PCI Council. Especially regarding the operational aspect, the Council manages programs that will help facilitate the assessment of compliance with PCI DSS. They certify auditors, called Qualified Security Assessors (QSA) and vendors, called Approved Scanning Vendor (ASV). Normally assessed entities have to provide annually two formally structured documents: a) a Report On Compliance (ROC[69]) and b) an Attestation of Compliance for Service Providers or Merchants[70], both according to each payment brand's respective reporting requirements to ensure each payment brand acknowledges the entity's compliance status. The ROC guidance in the PCI DSS provides for a general template structure of the report document, regarding content and format; certain reporting requirements may be imposed by the specific programmes of payment brands[71]. Below we depict the PCI-DSS framework (Fig. 9).

[68] https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0

[69] Please refer to the VISA Levels/Tiers of merchants and the VISA requirements for reporting here: http://usa.visa.com/merchants/risk_management/cisp_merchants.html where ROC is mandatory for VISA Level 1 merchants

[70] See http://usa.visa.com/merchants/risk_management/cisp_service_providers.html for the VISA case

[71] See "Requirements and Security Assessment Procedures Version 2.0 October 2010", section "Instructions and Content for Report on Compliance", pg. 14.

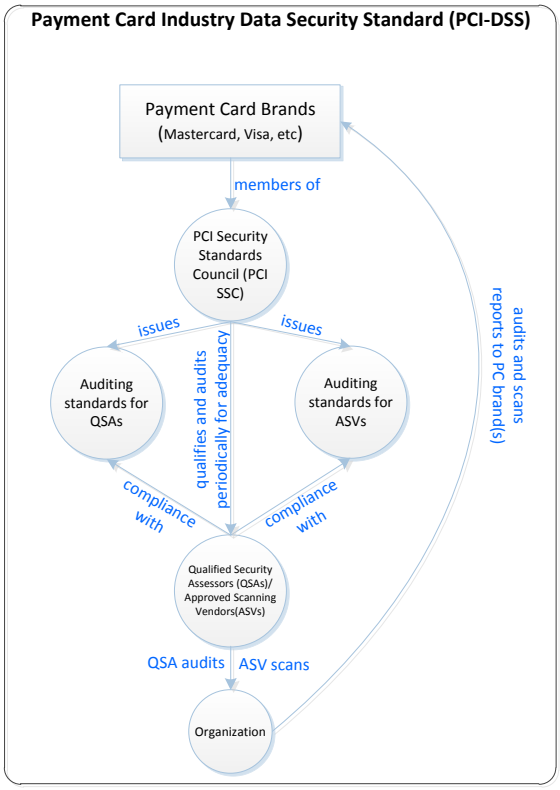

Figure 9 PCI-DSS audit framework

3.9.2 PCI-DSS Roles

- Each payment card brand has its own program for compliance with PCI DSS. Merchants and service providers must prove compliance and report their compliance status annually to the payment card brand they work with. So while the PCI Security Standards Council sets the standards, merchants and service providers participating in certain payment schemes have to comply with the requirements of their partners.
- The PCI Security Standards Council is responsible for managing the security standards lifecycle (including the amending process, member consultation, setup of working groups etc), while compliance with the PCI set of standards is enforced by the founding members of the Council. QSAs are approved by the PCI Security Standards Council to assess compliance with PCI DSS. QSA's have unlimited liability, as imposed an agreement between the PCI Security Standards Council and the prospective QSAs, and this has led to a number of organisations abandoning their nomination as QSAs, to avoid the high risks related to indemnifications in case of a damage or loss incurred during or after security assessment. The process of becoming (and be maintained as) a qualified approved security company (QSA, ASV, etc) is rigorous, towards ensuring the quality of the security checks at the highest level possible[72] and the PCI Security Standards Council mandates annual reassessment.
- ASVs are approved by the PCI Security Standards council to perform vulnerability scans of Internet-facing systems of merchants and service providers.

[72] https://www.pcisecuritystandards.org/security_standards/documents.php?category=validation

Finally, for smaller companies in the payment card industry that fall under PCI DSS mandate there is a Self-Assessment Questionnaire (PCI DSS SAQ), which can be used by merchants and service providers that are not required to undergo an on-site assessment per the PCI DSS Security Assessment Procedures. Banks who do transaction with these smaller companies may ask the company to share the results of the PCI DSS self-assessment[73] .

3.9.3 PCI-DSS Enforcement and Compliance

Enforcement of compliance with the PCI DSS and determination of any non-compliance penalties are carried out by the individual payment card brands and not by the PCI Security Standards council. Operational issues regarding compliance by involved entities are directed to the payment brands themselves.

Every assessed entity has to submit to payment card brands the details about annual assessments by a QSA, and details about the quarterly security scans carried out by an ASV. Assessment reports are considered non-compliant if these reports contains "open items", or items that will be finished at a future date. The merchant/service provider must address these items before being able to complete validation. After open items are addressed by the merchant/service provider, the assessor will then reassess to validate that the remediation occurred and that all requirements are satisfied. After revalidation, the assessor will issue a new Report on Compliance, verifying that the cardholder data environment is fully compliant, and submit it consistent with instructions. The complete procedure and supporting material is available on the PCI SSC website (www.pcisecuritystandards.org).

Regarding the eligibility of approved security companies[74] to provide PCI-DSS compliance audits, their nomination may be redrawn, even immediately, in case of failure to meet the PCI SSC requirements. In case of an incident to an assessed entity, the relevant procedures of individual payment brands are applied. For example the procedures used by VISA[75] [76]) contain detailed instructions and strict deadlines about alerts of involved parties, reports of compromise, independent forensic investigations, and so on.

3.10 Basel Accords (BASEL) II

Basel II is the second of the Basel Capital Accords[77], (now extended and effectively superseded by Basel III), which are recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision[78] ("Committee"). BASEL II builds on an evolving framework for managing risk in financial services transactions. In contrast to the First Capital Accord of 1988, information risk and information technology (IT) have become decisive factors in shaping modern business, and many financial services organizations have undergone a fundamental transformation in terms of IT infrastructures, applications and IT-related internal controls[79].

[73] https://www.pcisecuritystandards.org/merchants/self_assessment_form.php

[74] https://www.pcisecuritystandards.org/approved_companies_providers/

[75] http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf

[76] http://usa.visa.com/download/merchants/cisp_responding_to_a_data_breach.pdf

[77] http://en.wikipedia.org/wiki/Basel_Accords

[78] http://www.bis.org/bcbs/about.htm?ql=1

[79] ITGI, 2007, IT Control Objectives for Basel II, the Importance of Governance and Risk Management for Compliance

While the committee is not a legal entity and BASEL II is not a regulation per se, they heavily influence the financial organizations around the globe; BASEL II has been transposed (in various forms and degrees of compliance, either as a national law or secondary legislation issued by a national bank.

Basel II uses a "three pillars" concept, as follows:

1. Minimum Capital Requirements (addressing risk),
2. Supervisory Review and
3. Market Discipline.

Of particular interest is the operational risk (Pillar 2), which is defined as "the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events"[80] and it is closely relates with ICT-security controls implementation. Below we focus on how BASEL II manages operational risks.

3.10.1 BASEL II Framework

In BASEL II operational risks are calculated and dealt with using customized methods, specific for financial institutions[81], but the overall approach is similar to IT risk management frameworks. Measures to mitigate risks are technology-dependent, meaning that the financial institution has the freedom to implement controls objectives in a suitable way. The usual approach is to adopt a structured approach such as ISO 27001/2 or COBIT.

BIS (Bank for International Settlements (among other organizations) has issued a number of guidance documents such as the "Operational Risk Consultative Document" (2001), "Implementation of Basel II: Practical Considerations" (2004)[82], "Enhancing corporate governance for banking organisations" (2006)[83], etc. It is important to note that only control requirements are discussed, while no focus on specific technologies or implementations is given. The BASEL II audit framework is shown below (Fig. 10).

[80] BIS, 2001, Operational Risk Consultative Document, available at http://www.bis.org/publ/bcbsca07.pdf
[81] BIS, 2001, Operational Risk Consultative Document, available at http://www.bis.org/publ/bcbsca07.pdf
[82] http://www.bis.org/publ/bcbs109.htm
[83] http://www.bis.org/publ/bcbs122.pdf

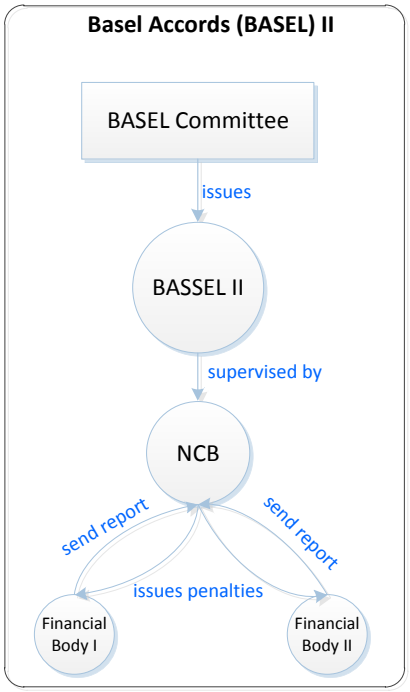

Figure 10 BASEL II audit framework

3.10.2 BASEL II Roles

The supervision of BASEL II is carried out by the national financial sector supervisor, typically National Central Banks (NCBs). The supervised entities (financial institutions) are required to report to national supervisors periodically. Article 156 of the EU Directive on Capital Requirements requires the European Commission to periodically monitor whether the directive has significant effects on the economic cycle. In the light of the examination, the Commission has to submit a bi-annual report together with any appropriate remedial measures to the European Parliament and to the European Council. National reporting to the Commission is the responsibility of the national supervisor. The first report has been issued in 2010[84].

3.10.3 BASEL II Enforcement and Compliance

In each country where BASEL II is used, the national supervisor has the right to impose on supervised entities appropriate administrative penalties, as provided for by the applicable legislation on credit institutions, in case of violation of legal and regulatory provisions concerning the conduct of their activities or the obstruction of supervisory control. These penalties may be imposed in conjunction with other administrative penalties and corrective measures, pursuant to applicable laws.

As discussed above, BASEL II is adopted by the major financial institutions around the world. For the EU the European Banking Association site[85] gives an overview of related laws, regulations, and administrative rules and provides guidance on regulation and supervision.

[84] http://ec.europa.eu/internal_market/bank/docs/regcapital/monitoring/23062010_report_en.pdf
[85] http://www.eba.europa.eu/Supervisory-Disclosure.aspx

3.11 Bundesamtes für Sicherheit in der Informationstechnik (BSI) - Federal Office for Information Security

The Bundesamtes für Sicherheit in der Informationstechnik (BSI) focuses on information security in public authorities. The BSI Standards contain recommendations by BSI on methods, processes, procedures, approaches and measures relating to information security. The BSI certifies information domains[86].

3.11.1 BSI Framework

The IT-Grundschutz standard is the BSI's best known publication on information security. It was published in 1994 and updated in 2005. IT-Grundschutz is a standard for establishing and maintaining an appropriate level of protection for all information assets in an organisation, and provides a methodology for management of information security.

The BSI certification involves auditing of the information security management system as well as auditing of the specific information security measures on the basis of IT-Grundschutz. The BSI certification always includes an official ISO certification in accordance with ISO 27001 but, due to the additionally audited technical aspects, is more comprehensive than only ISO certification.

The aim of IT-Grundschutz is to achieve an appropriate level of security for all types of information of an organization. IT-Grundschutz focuses on the protection of business-related information, which has normal security requirements. IT-Grundschutz may be useful also for IT systems and applications with high security requirements. We explain the different IT Grundschutz standards in more detail in an annex to this section.

3.11.2 BSI Roles

The BSI framework and the different roles are depicted below (Fig. 11). BSI defines standards, accredits certification authorities for the issuance of certificates, and licenses auditors. Licensed auditors can perform an audit, and the audit report is used by a certification authority to issue a certificate of compliance. The certificate can be used by the provider to show customers that it implements security measures according to BSI's IT Grundschutz standards.

To become a licensed auditor, auditors have to prove they have the appropriate technical background and expertise by providing evidence of more than two years of professional experience in the area of IT security and experience in three projects relating to IT-Grundschutz. Candidates must attend a training course and an exam to obtain a license. The licence is valid for a period of five years. During this period BSI organizes events for the exchange of experiences between auditors so as to ensure the uniformity of audits and improve the overall scheme. The license of an auditor can be revoked if the auditor fails to participate in these events or if an auditor negligently contravenes the framework.

[86] Information domains are defined as "the interaction between infrastructural, organisational, personnel and technical components that enable business processes and tasks to be performed"

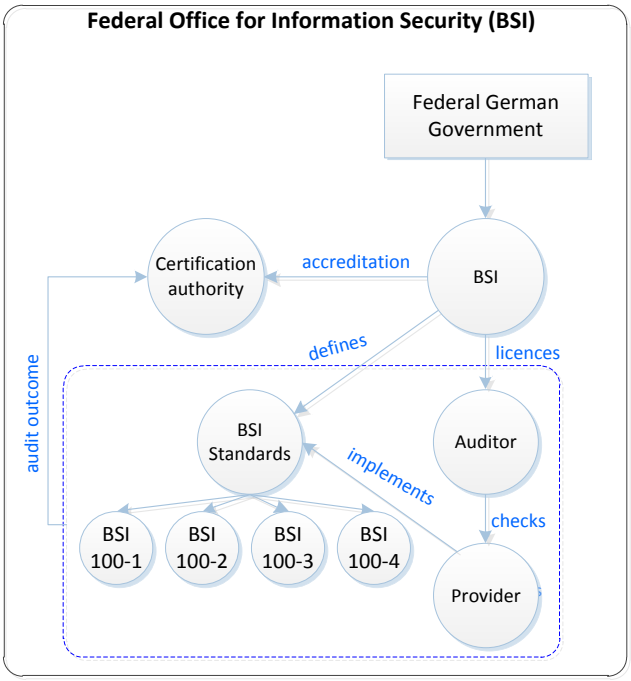

Figure 11 BSI-IT Grundschutz audit framework

3.11.3 BSI Enforcement and Compliance

The BSI standards recommend a standardised set of security measures for IT systems. The purpose of these standards is to achieve a baseline of security which is reasonable and adequate to satisfy basic security requirements. The standards could also be used for IT assets with higher security requirements.

The BSI is implemented mostly on a voluntary basis. Compliance with the IT-Grundschutz standards is optional. BSI also provides a subscription service, which provides registered users with news and updates about IT-Grundschutz and IT security topics. Registered users also participate in user surveys which are used by BSI to improve the methodology and standards. Numerous companies and public agencies use IT-Grundschutz Catalogues as the basis for their security measures.

3.11.4 BSI Standards

The BSI IT Grundschutz standard consists of 5 parts.

- BSI Standard 100-1 Information Security Management Systems (ISMS)
- BSI-Standard 100-2: IT-Grundschutz Methodology
- BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz
- BSI-Standard 100-4: Business Continuity Management
- IT-Grundschutz Catalogues

In this part we go over them in more detail.

- **BSI Standard 100-1 Information Security Management Systems (ISMS):** The BSI standard 100-1 Information Security Management Systems defines the general requirements of an ISMS and describes how an ISMS could be implemented. It is based on the ISO 27001 and 27002 standards. The BSI Standard 100-1 provides readers with an easy to understand and

systematic instruction manual, providing a brief and clear overview of the most important tasks of security management. The standard can be used irrespective of the precise ISMS an organization wants to use to implement.

- **BSI Standard 100-2 IT-Grundschutz Methodology:** The IT-Grundschutz Methodology (BSI standard 100-2) shows how a management system for information security can be developed and operated in practice. The IT-Grundschutz Methodology explains in detail how a policy for information security can be developed, which information security measures can be selected and what are pitfalls when implementing the information security policies.
- **BSI Standard 100-3 Risk Analysis based on IT-Grundschutz:** The BSI standard "Risk Analysis based on IT-Grundschutz" (BSI standard 100-3) outlines a methodology for determining assets that should be protected and how to perform a risk assessment. The standard uses the threats specified in the IT-Grundschutz Catalogue. It presents a method for performing a risk analysis that is optimised for use with the IT-Grundschutz methodology. The BSI has worked out a methodology for risk analysis on the basis of IT-Grundschutz. This approach can be used when companies or public agencies are already working successfully with IT-Grundschutz and would like to add an additional security analysis to the IT-Grundschutz analysis as seamlessly as possible.
- **BSI-Standard 100-4: Business Continuity Management:** The BSI Standard 100-4 explains a method for establishing and maintaining business continuity processes. The focus is on threats which could severely impact an organization (natural disasters for example) and on security measures to protect from those threats. The standard can be used by any organization (large or small). It is based on the previously mentioned BSI standards but it can also be used stand-alone.
- **IT-Grundschutz Catalogues:** Since 2005 the IT-Grundschutz Manual is called IT-Grundschutz Catalogues. The IT Grundschutz catalogue provides an overview and a categorization of different threats. The IT-Grundschutz Catalogues describe the standard security measures in detail, including:
    - Standard security measures for typical IT systems with "normal" protection requirements
    - A description of the threat scenario which is globally assumed
    - Detailed descriptions of measures to assist with their implementation
    - A description of the process involved in attaining and maintaining an appropriate level of IT security
    - A simple methodology for ascertaining the level of IT security attained by comparing the target with the actual system status.

3.12 CESG: Communications Electronics Security Group

CESG is the UK's national technical authority for information assurance (IA). Information Assurance is defined (by CESG) as obtaining confidence that information systems will protect the information they process, that they function as they need to, and when they need to, under control by legitimate users.

CESG aims to protect the vital interests of the UK by providing advice and assistance on the security of communications and electronic data. CESG focusses on training people, such as auditors and professionals managing/implementing information systems. CESG's primary customers are civil departments, government agencies and the military, industries forming part of critical national infrastructure (such as power supply and water supply). CESG also works with organisations in the wider public sector and with the private sector, including local government, health sector and law

enforcement. CESG offers a range of products and services including technical consultancy and advice, policy documentation, product evaluation and training.

3.12.1 CESG Framework

CESG provides:

- IA Products and Services (CAS, CAPS, CAS-T, CLAS, etc.)
- IA Policy and Guidance
- IA Awareness and Training

CESG has developed a framework for certifying IA professionals who meet competency and skill requirements for IA related roles and responsibilities. The CESG framework is consistent with ISO 17024 and has been developed in consultation with government departments, academia, industry, certification bodies, and members of the CESG listed advisor scheme (CLAS) which is a partnership with private sector consultants.

3.12.2 CESG Roles

The CESG framework includes a set of IA role definitions and a certification process. The different roles and process are depicted below (Fig. 12).

The IA roles are defined using 3 different levels. The skills and responsibilities per role are defined in the Skills Framework for the Information Age (SFIA). The skills are based on the set of skills defined by the Institute of Information Security Professionals (IISP). The CESG framework supplements the IISP2 skills with definitions to aid assessments of skills.

The certification process has been defined in detail and is operated by three Certification Bodies (CBs) appointed by CESG (APM Group, BCS, the Chartered Institute for IT Professionals, and IISP (a RHUL and CREST consortium). The process assesses applicants against the requirements of the role definitions and issues certificates endorsed by CESG stating the IA role and responsibility level at which the applicant has been assessed.

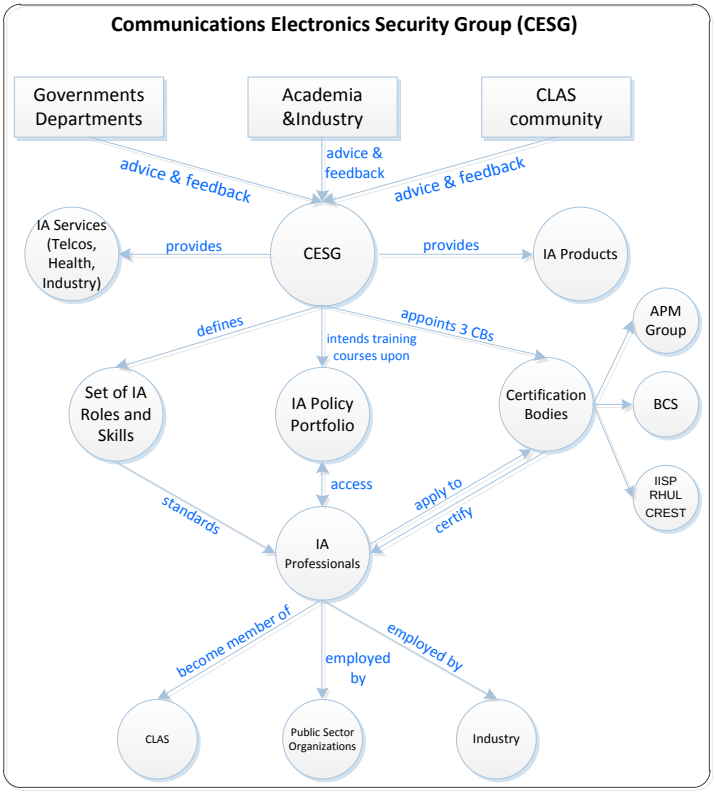

Figure 12 CESG certification framework

There are six IA roles in the CESG framework:

- **Accreditor:** To act as an impartial assessor of the risks that an information system may be exposed to in the course of meeting the business requirement and to formally accredit that system on behalf of the Board of Directors.
- **IA Auditor:** To assess compliance with security objectives, policies, standards and processes.
- Communications Security Officer / Crypto Custodian and deputy/alternate custodian: To manage cryptographic systems as detailed in HMG IA Standard No 4 (reference [i]) and in relevant product specific security procedures.
- **IT Security Officer/ Information Security System Manager/ Information Security System Officer:** To provide governance, management and control of IT security.
- **Security & Information Risk Advisor:** To provide business driven advice on the management of security and information risk consistent with HMG IA policy, standards and guidance.
- **IA Architect:** To drive beneficial security change into the business through the development or review of architectures so that they:
    - fit business requirements for security
    - mitigate the risks and conform to the relevant security policies
    - balance information risk against cost of countermeasures

3.12.3 CESG Enforcement and Compliance

The CESG framework is implemented mostly on a voluntary basis by helping to increase the level of Information Assurance awareness and professionalism across the public sector and its supply chains, which will lead to improved management of information risk and strong cyber defence. Through the collaboration with a range of stakeholders including other government departments, professional

bodies, academia and industry, CESG intends to create an environment in which public sector employees and suppliers have access to the appropriate IA professionalism, knowledge and skills to do their job.

Certification Bodies (CBs) assess competence of professionals depending on the skills needed for a role. The assessment process will typically include review of written evidence, knowledge testing, input from referees, an interview, recommendation from assessors, and a final decision by a ratifying panel. For roles that are more senior, the assessment is more extensive. CESG has appointed three CBs who will assess IA Professionals against the requirements of the role definitions. IA Professionals can use their certificates as evidence to prospective employers, clients or promotion panels of their competence to perform the defined role at the level to which they have been certified. CBs will charge IA Professionals for their certification.

3.12.4 CAS(T) - CESG

An example of one of the services that CESG offers, is the certification scheme for telecommunications services, called CAS(T). The CAS(T) framework is a set of processes set up by CESG specifically for electronic communications providers and services. The CAS(TP) model is illustrated in Figure 13.

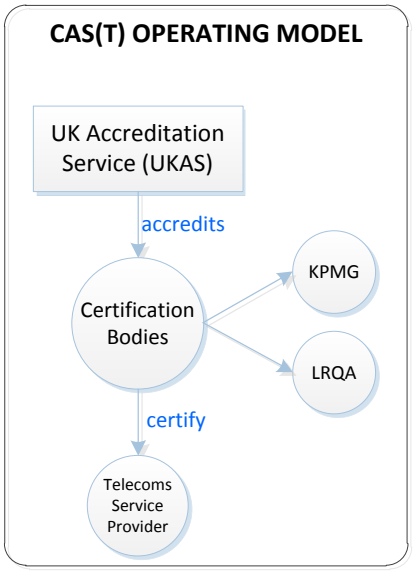

Figure 13 CAS (T)-CESG Certification Scheme for Telecommunications Services

4 Analysis

In this paper, we gave an overview of different auditing and certification frameworks, all focussed at governing information security measures, in various sectors, ranging from energy, health, finance et cetera.

In the diagram below we present a single model of the entities and roles that recur in most of the schemes we surveyed in the previous section. In individual schemes one or more roles are sometimes combined, or sometimes the roles are split. For example, there may be a different entity responsible for licensing auditors, or this might be done by the governing body.

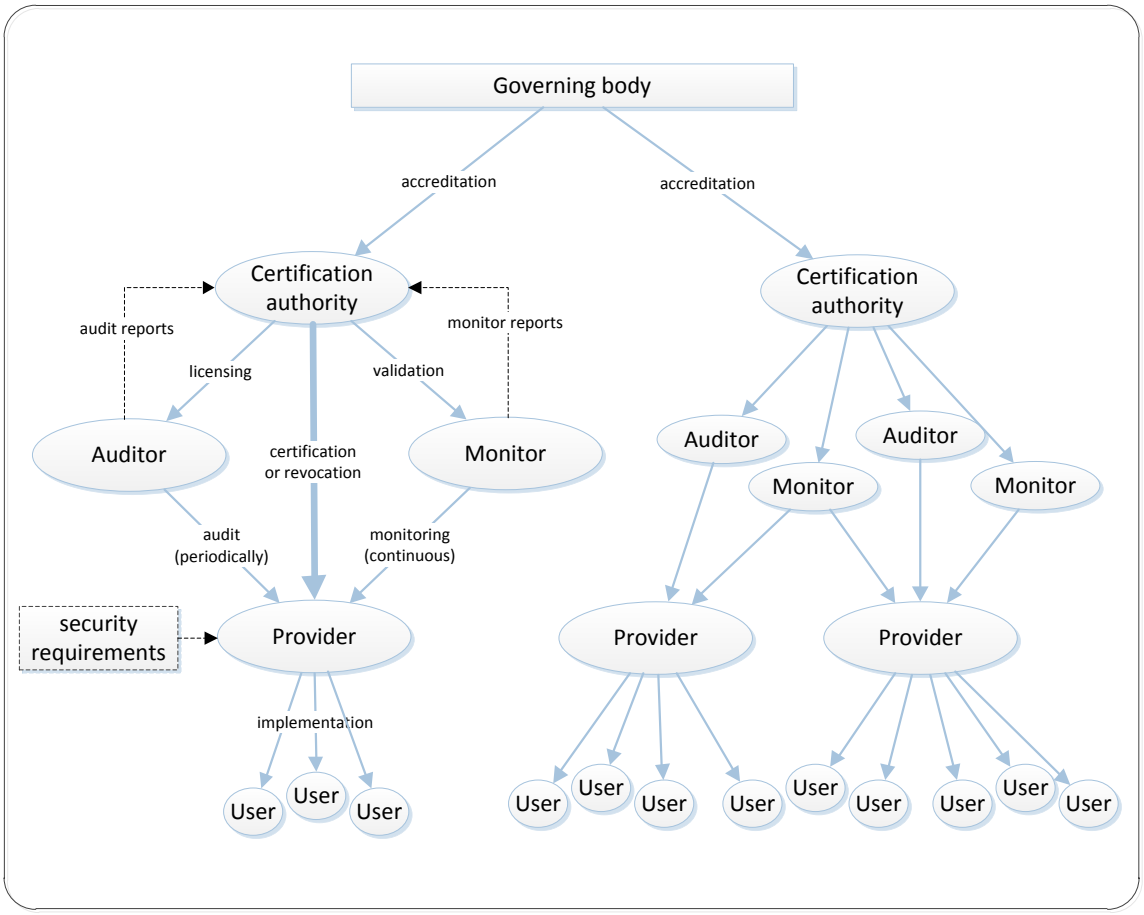

Figure 14 Single auditing model

The following explains the diagram in detail, starting from the core process – the delivery of the service to the end-user.

- Implementation: The provider, when providing the service, implements the security requirements
- Audit: The auditor audits the service or the provider to see that the requirements are met.
- Monitoring: A monitoring system monitors the service to see that the requirements are met.
- Certification: The certification authority certifies the service or the provider, based on audit reports and monitoring reports, from licenses auditors and validated monitoring tools.

- Licensing: The certification authority licenses auditors, for example by requiring them to take exams to assess their expertise and knowledge. Audit reports from licensed auditors can be used to obtain certification from a certification authority. Sometimes licensing is done by an
- Validation: The certification authority validates monitoring tools, for example by requiring specific measurements or scans as a baseline.
- Accreditation: The governing authority accredits certification authorities, basically asserting that the processes for licensing auditors, validating monitoring tools, certification of service or providers, are implemented in a sound way. The governing authority can accredit one or more certification authorities.

5 Conclusions

In this paper we gave an overview of different certification schemes and audit frameworks, and we derived a single model that covers most of the different schemes.

Every scheme is different: Perhaps what is most striking about the different certification and audit schemes is the fact that they are all so different. In each scheme the actual auditing is delegated to third-party auditors, but the construction used is different every time. Sometimes the third party is governmental – for example a ministry delegating to an agency. Sometimes the third party is non-governmental – for example an agency delegating to an audit firm. Sometimes auditing is delegated to an accreditation body, who accredits auditors, who in turn audit providers. In each of these cases the work of auditing providers is (structurally or on an ad-hoc basis) outsourced. The optimal structure for this kind of delegation depends on many factors, on the size and maturity of the sector, the resources and skills of the government authority, whether or not there are well-functioning industry initiatives, and so on.

Assessing certification authorities: The generic model in Section 4 shows the key processes certification authorities are executing or delegating: 1) auditing (what security measures are checked, how), 2) licensing of auditors (what skills sets or exams are required), 3) validation of monitoring tools (which scans or features are required), and 4) certification (how audit reports and monitoring reports are assessed). A governing authority could evaluate a certification authority by looking at these 4 processes.

Continuous monitoring vs point-in-time assessment: Most of the frameworks are based around periodic, point-in-time assessment of a provider or a service. Such an approach might be adequate in a situation where technology is fairly static (children seats for cars for example), but in the IT industry, with the rapid changes of technology and products, the effectiveness of a one-off certification is limited – especially when considering online or cloud services.

Incident reporting: Whatever structure is used in the certification or auditing scheme, the governing body should have a way to make a cross-check to assess the overall effectiveness of the framework in place, or the quality of the certification authority, or the quality of the auditors. An objective way of assessing the overall framework or any of the parts, is by looking at incident reports and/or independent test results.

Preventive auditing vs. post-incident investigations: In most certification and audit frameworks the focus is on preventive and periodic audits. The goal of a preventive audit is to check whether or not all the necessary security measures are in place. Post-incident investigation is even more important, because it helps to understand the root cause of the incident, what are the lessons learnt and what could have prevented the incident. This is important to improve security and possibly the audit scheme itself too.

Compliance burden and entry barriers: The digital society is rapidly changing. New services (cloud e.g.), new products (smartphones e.g.), new usage scenarios (smart grids e.g.) are emerging continuously. An important goal of EU Member States and the European commission is to foster innovation. It is important to take into account the effect of a high compliance burden on smaller providers. Large (incumbent) providers have the resources and (arguably) the need to set up advanced and sophisticated governance processes. For these incumbents it is relatively easy to partake in one or more elaborate audit frameworks. But for a smaller provider to even a single audit could be already be prohibitively costly. In any sector or market it is important to take into account also the smaller providers where less is at stake. In general it is important to take into account the impact of legislation on innovation and competition, and be particularly careful when obliging

providers across a sector to submit to a fixed set of audit requirements or partake in a specific audit framework.

TP-03-13-551-EN-N

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

doi: 10.2824/23801

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu