Risk-based information security audit applied research in the power industry

Gengshen Yu [1, a *],Qian Guo[2,b]

[1] State Grid Smart Grid Research Institute, Nanjing, China

[2] State Grid Smart Grid Research Institute, Nanjing, China

[a] yugengshen@epri.sgcc.com.cn, [b] guoqian@epri.sgcc.com.cn

Keywords: Information security audit; Information Security; electric power information security; risk.

Abstract. This paper analyzes the information security situation in the power industry,Combined with information security requirements of the power industry, From the information security audit objectives, audit evidence, information security control framework, information security and other aspects of the audit process is proposed for the power industry to establish risk-based information security audit systems and processes.

1 Introduction

After years of construction power information system, has been covering the generation, transmission, transformation, distribution, use, transfer these six areas, and have been the formation of functional complexity and diversity of management information systems, information systems widely used to bring electricity production convenience and efficiency, but also brings information security problems, in recent years the power industry through the "secondary power system security requirements", "SG186 project", "smart grid information security" and other measures to promote, strengthen the power of information systems safety and protection.

Electricity security of information systems related to national security and social stability, according to Information security technology Baseline for classified protection of information system(GBT 22239-2008), Power applications are mostly of level three&level four. Currently information security environment is complex and the means of attack update. How to find an effective information security risks, improving the status of information security to meet the electric power enterprises information systems security compliance requirements.The use of information security audit methodology can make power enterprises to master their information security satisfies security regulatory compliance requirements, but also can help organizations comprehensive understanding and mastering the effectiveness,adequacy and suitability of their information security controls.

2 INFORMATION SECURITY AUDIT STATUS

A. The development of foreign information security audit

2002 U.S. Enron and WorldCom financial fraud case after the outbreak, the United States enacted the Sarbanes-Oxley Act (SOX), given the "audit" a new meaning. "Sarbanes - Oxley Act (2002 Sarbanes-Oxley Act)" section 302 and 404, the emphasis on strengthening corporate governance through internal controls, including the strengthening of the financial statements related to the IT systems of internal control, including, IT systems internal control is a specific business-oriented, which is closely around the core of information security audit. "Information security audit" has become a corporate internal control, information systems management, security, risk control key means indispensable.

B. Domestic Information Security Audit

Compared with foreign countries, China's information system security audit started late, the relevant security audit information technology, information security audit specification and information security audit system and so needs to be further improved.

In 1999 the Ministry of Finance issued the "Independent Auditing Standards No. 20 - Computer Information Systems Environment audit" part refers to the overseas research results.

This is the first time clearly stated on computing information systems audit requirements.

In the same year "GB17859-1999 computer information system security classification criteria" publish, the implementation of an important foundation for security protection standards, which expressly requires a computer information systems to create and maintain access to objects protected audit trail, and to prevent unauthorized user access or destroy it. "

December 2005, the Ministry issued Decree No. 82, "Internet Security provides protection of technological measures", which explicitly requires "Internet service providers and enterprises to connect to the Internet on the unit must be recorded, tracking network running status, network security incidents and other safety record audit function, and kept for at least sixty days should have recorded backup function. "

June 2008, the Ministry of Finance, the Commission, the CBRC, CIRC and Audit Commission jointly issued the "basic norms of internal control" is a major country in the field of auditing reform initiatives, the specification will be implemented first in the listed companies.

3 ELECTRIC CORPORATION INFORMATION SECURITY AUDIT OBJECTIVES

In the electric power enterprises to implement information security audit, first we must determine the information security objectives of the audit.

Information security audit objectives can be divided into two kinds, Information security audit objectives can be divided into two kinds,

First, the overall audit objective, the overall audit objective information security audit objectives, based on electricity main business oriented.To confirm whether information systems and resources to ensure assets, data, applications, complete and reliable operation, whether the effective use of resources, information security control objectives are achieved, whether the operation for the power company, business, control objectives provide effective protection.

Second, the specific audit objectives, specific audit objective is to develop an auditing practice when the goal,Is a link for a particular project or pilot implementation of audit in the current risk-based audit approach, can be understood as how to find, validation, verification, information security risk assessment of its sphere of influence.

4 INFORMATION SECURITY AUDIT BASIS AND CONTENT

A. Audit evidence

Information Security Audit and information security management is closely related to.The main basis for information security audit of information security management standards such as: ISO 27001, COSO, COBIT, ITIL, NIST SP800 series, Baseline for classified protection of informationsystem .These standards are actually made for different point of the control system.Based on the control system can effectively control the information security risks.So as to achieve the purpose of information security audit and improve information systems security.Based on the basic situation of power enterprises, combining national information security regulations and requirements. With "GB/T22239 Baseline for classified protection of information system " as the basis, with "power enterprise Baseline for classified protection of information system (draft)", "secondary power system security protection requirements", "ISO / IEC 27001 (GB / T22080) information Security management System Requirements "and" COBIT 4.0 "and other standardsto establish information security control system.

B. Information security controls, and information security audit

First, to establish information security control system before implementation of information security audit.The content of information security control system can include: compliance control, risk control, process control, personnel security management, its control framework as shown:.

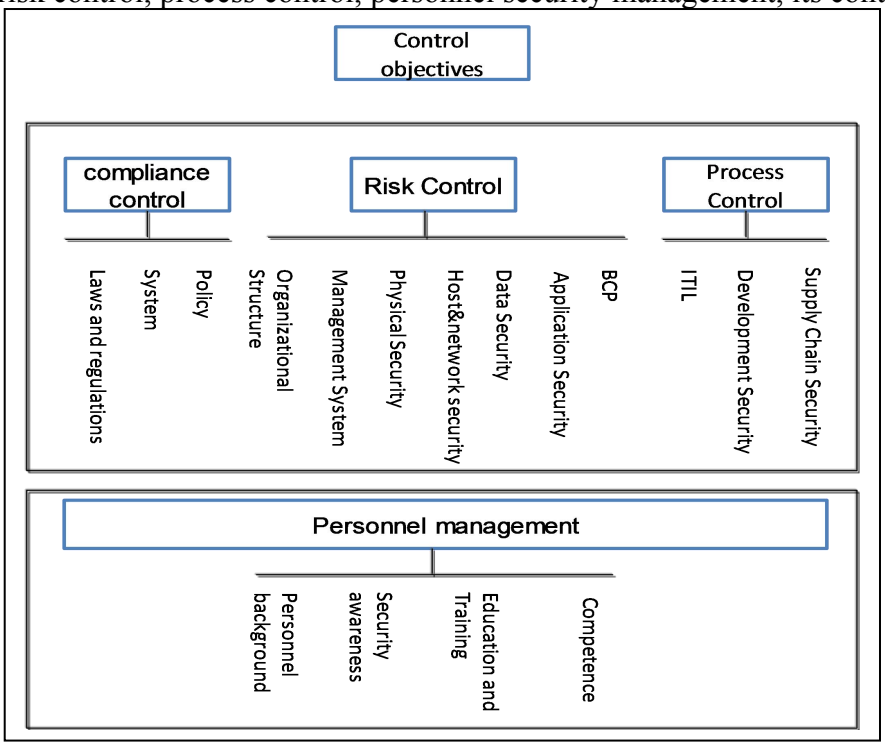

Fig. 1. control framework

C. Information security audit content

Information security audit may include the following main contents

Table 1. INFORMATION SECURITY AUDIT MAIN CONTENT

Level	Content
Information Security Organization	Organization of information security, information security leader, information security responsibilities
Information Security Management System	Information Security Management System Safety management system construction, operation and results of the records, security segregation of duties, assessment and accountability mechanisms
Physical Security	Engine room, office, spare parts warehouse, logistics, security, etc.
Application Security	Under construction, commissioning, operation, downline system life cycle Security
Device Security	Host, network equipment, risk assessment, safety measures, attack, etc.
IT Services and Management	IT operation and maintenance Security
Data Security	Database systems, data security, medium security
Business continuity and emergency response	Emergency response plan, emergency response plan, emergency drills, business continuity plans
Development Security	Code security, security development framework, developers of safety education
Supply Chain Security	Supply chain structures, processes, and business features, design supply chain security management systems
IT Outsourcing	Outsourcing process specifications, supplier visits, outsourced staff

Security	visits
Classified information	Information classification and control
Personnel security management	Personnel background, Security awareness, education and training, competence, etc.

5 INFORMATION SECURITY AUDIT ORGANIZATION AND IMPLEMENTATION OF ELECTRICITY

A. Set up an internal information security audit team

We should set up an internal information security audit team who is independent, responsible directly to superiors when the implementation of information security audit. This group consists of person who is able to represent the various relevant units and departments, Each of the person is responsible for related information security audit of the department, and be able to discuss some problems. The team need to specify a leader able to take responsibility, responsible for the overall coordination of assessment matters. Groups need to specify a leader able to take responsibility, responsible for the overall coordination of assessment matters.

B. Information security audit programs and plans

In the beginning of the information security audit, the group must first clear objectives and scope, describe the system environment, determine the evaluation index, clear the responsibility, carry out the necessary training, provide the necessary tables, questionnaires and the other materials, make project plan.

C. Implementation of information security audit

- Scope of the audit: Determining the specific system, functions or units which your organization want to check is a comprehensive audit or special audits;
- Data collection: Access to specific people, collect the relevant policies, standards, department, records and other information, Check the organizational structure, procedures, documentation, etc., observe the flow of information security, observe and record their performance;
- Risk identification: Risk identification includes asset identification, vulnerability identification, threat identification. Asset identification main evaluation critical information assets; Vulnerabilities identify main identified various weaknesses (including existing control deficiencies), to measure the severity of weakness;
- Assessment Test: In the phase of assessment test, we should assess the risk and control, describe risk scenarios and assess risk, divide risk level. Test the implementation of control and reliability through compliance testing, determine the results of compliance tests through substantive tests.

D. The audit communication

In the implementation of information security audit, auditors need to communicate orally or in writing timely with the audit department managers and related person, in order to be able to effectively convey a clear audit purposes, evaluations, conclusions, recommendations, etc.; Communication contains the contents, process, results and other information of the audit. Audit staff should tell the problems of the information security audit to the audited entity or department managers. Submit information security audit results to the higher authorities after reaching agreement on the audit findings and proposing corrective action plan.

Communicate through the audit: One, the information security audit obtain the support and understanding of leadership. Second, get the support and cooperation of the audited departments or personnel, promote coordination, reduce conflict, improve relations with the audited units or departments. Third, share information between members, improve audit efficiency and avoid detours.

E. Information security audit report

The audit report of information security is the end and main results of audit work, information security audit report shall contain problems and disposal plan founded during the information security

audit at least. Meanwhile, the audit report is not just the negative description of the problem during the audit, should also be a positive description, including the effective control already exists, improve processes and control aspects of the constructive recommendations.

F. Audit tracking

A complete information security audits can be said that this audit activity is invalid if it ends when submits the audit report. Auditors need to confirm whether managers take appropriate measures to address the risks identified in audits, also need to confirm whether the corrective measures are implemented and achieved the desired effect.

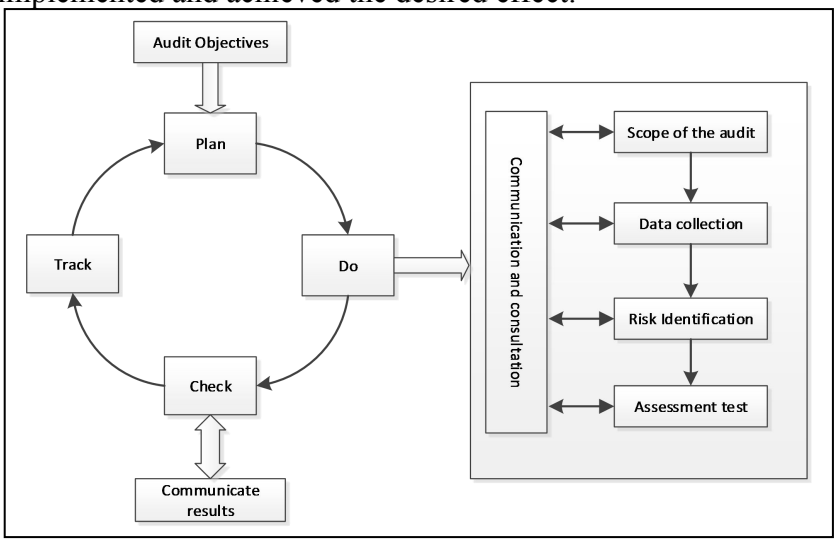

Fig. 2. Information Security Audit Process

6 CONCLUSION

Information security audit is an important and effective way of security information. Through the implementation of information security audit can make electric power enterprise master effects of information security work, understand whether the information security is full and appropriate, understand significance for safeguarding the sustained and stable operation of power business. After a recent practice, information security audit has been more widely used in the banking, securities, aviation and other industries, these industries have the traditional information security audit methodology digestion and absorption, the formation of the industry with its own characteristics, suitable to the industry structure audit approach. The implementation of information security audit in the electric power enterprise still lack practical basis, the information security audit theory and method of electric power industry also requires long-term practice to summarize formed.

Please keep a second copy of your manuscript in your office. When receiving the paper, we assume that the corresponding authors grant us the copyright to use the paper for the book or journal in question. Should authors use tables or figures from other Publications, they must ask the corresponding publishers to grant them the right to publish this material in their paper.

Use *italic* for emphasizing a word or phrase. Do not use boldface typing or capital letters except for section headings (cf. remarks on section headings, below).

References

[1] Li Xuehui, "Civil Aviation Security Audit System of Enterprise Information", "China Civil Aviation" Jun. 2007, pp53-54.

[2] Information Systems Audit and Control Association. IS Auditing Standards, Guidelines and Procedures. 2006.

[3] Zhao Yaxin, "Internal auditing information security controls Exploration", "Chongqing Electric Power College" 2011 Volume 16 No. 05, pp51, 52,59.

[4] ISO/IEC 27001 (GB/T22080) Information technology--Security techniques Information security management systems –Requirements.

[5] Du Ningning Zhaoqing Liang, "On the information security audit practice in the financial industry," "Chinese Internal Audit" Apr. 2012, pp66-68.

[6] Yang Jie, "Information security audit applied research", "Computer Security" Oct. 2010,pp18-21.

[7] HU Jie Lu Feng Ferring goods "Information security auditing technology in financial industry applications," "Computer Engineering and Design" 2007,Volume 21,PP5314-5316.