IT Security Audit Based on CISSP PMBOK Framework

Kheri Arionadi[1]., Suta Adya Dharma[2], Cok Gede Indra Partha[3]
[1][2]Department of Electrical and Computer Engineering, Post Graduate Program, Udayana University
Email: kherias@gmail.com
[3]Department of Electrical and Computer Engineering, Udayana University

Abstract - ***XYZ International School redesign their IT System and Infrastructure to meet their target in implementing ICT based learning process. The implementation of new system and infrastructure have good impact in speed and accuracy of learning process but not yet evaluate in term of security matters. IT security audit perform to fulfill the evaluation need for security implemented in XYZ International School. Audit perform based on CISSP common body of knowledge from (ISC)^2 and concentrate in Access Control area. Result show that security concern already implemented and have a good standard in certain area like identification, authentication, authorization and implementation, but still need improvement in accountability and monitoring area.***

Keywords - IT Security Audit, CISSP, CMMI, Access Control

I. INTRODUCTION

YZ International School (XYZ) located in Badung District Province of Bali serving more than 500 international students from Reception, Preschool, Primary, Secondary and iB. XYZ supported by 50 Expatriate Teacher, 50 Local Teacher and 60 Supporting Staff.

After big change in information technology infra-structure started on June 2015, all user has better experience in using service from ICT Department. To evaluate security compliance in new infrastructure, ICT Department agreed to audit their information technology operation based on domain from CISSP (certified information system security professional) CBK (common body of knowledge).

II. IT SECURITY AUDIT BASED ON CISSP CBK

A. IT Security Audit

IT auditing is a branch of general auditing concerned primarily with governance, risk, control and compliance in relation to IT, i.e. information and communications technologies. IT auditors are interested in how IT systems, networks and peripherals, plus the related procedures for designing, developing, testing, configuring, implementing, using, managing and maintaining them, handle risks to the organization. We spend the bulk of our audit time dealing with the people rather than the IT but being able competently to audit the IT is what sets us apart from the riff-raff and hoi-palloi. Like many IT professionals, we may at times appear to view people as peripheral devices responsible for generating inputs and consuming outputs, and as the principle generators of flaws, bugs and errors, but that’s a cynical perspective [1].

A security audit is a systematic evaluation of the security of a company's information system by measuring how well it conforms to a set of established criteria. A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes, and user practices. Security audits are often used to determine regulatory compliance, in the wake of legislation (such as FDIC, GLBA, HIPAA, HITECH, NCUA, OCC, PCI DSS, the Sarbanes-Oxley Act, and the California Security Breach Information Act) that specifies how organizations must deal with information.

B. (ISC)^2 CISSP

(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, programmatic approach to security. (ISC)² membership, over 123,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry.

(ISC)² develops and maintains the (ISC)² CBK, a compendium of information security topics. The CBK is a critical body of knowledge that defines global industry standards, serving as a common framework of terms and principles that our credentials are based upon and allows professionals worldwide to discuss, debate, and resolve matters pertaining to the field. Subject matter experts continually review and update the CBK.

C. CISSP CBK

The (ISC)² CBK is a taxonomy - a collection of topics relevant to information security professionals around the world. The (ISC)² CBK establishes a common framework of information security terms and principles which al-lows information security professionals worldwide to discuss, debate, and resolve matters pertaining to the profession with a common understanding.

(ISC)² was established in 1989, in part, to aggregate, standardize, and maintain the (ISC)² CBK for information security professionals worldwide.

Domains from the (ISC)² credentials are drawn from various topics within the (ISC)² CBK. (ISC)² uses the CBK domains to assess a candidate's level of mastery of the most critical domains of the practice of information security.

The (ISC)² CBK, from which the (ISC)² credentials are drawn, is updated annually by the (ISC)² CBK Commit-tee to reflect the most current and relevant topics required to practice the profession of information security.

Since April 15, 2015 CISSP Domains change from 10 domains into 8 domains [2]. The new domain of CISSP their sub domains are:

1. Security and Risk Management
   a. Confidentiality, integrity and availability concepts
   b. Security governance principles
   c. Compliance
   d. Legal and regulatory issues
   e. Professional ethic
   f. Security policies, standards, procedures and guidelines
2. Asset Security
   a. Information and asset classification
   b. Ownership (e.g. data owners, system owners)
   c. Protect privacy
   d. Appropriate retention
   e. Data security controls
   f. Handling requirements (e.g. markings, labels, storage)
3. Security Engineering
   a. Engineering processes using secure design principles
   b. Security model fundamental concepts
   c. Security evaluation models
   d. Security capabilities of information systems
   e. Security architectures, designs, and solution elements vulnerabilities
   f. Web-based systems vulnerabilities
   g. Mobile systems vulnerabilities
   h. Embedded devices and cyber-physical systems vulnerabilities
   i. Cryptography
   j. Site and facility design secure principles
   k. Physical security
4. Communications and Network Security
   a. Secure network architecture design (e.g. IP & non-IP protocols, segmentation)
   b. Secure network components
   c. Secure communication channels
   d. Network attacks
5. Identity and Access Management
   a. Physical and logical assets control
   b. Identification and authentication of people and devices
   c. Identity as a service (e.g. cloud identity)
   d. Third-party identity services (e.g. on premise)
   e. Access control attacks
   f. Identity and access provisioning lifecycle (e.g. provisioning review)
6. Security Assessment and Testing
   a. Assessment and test strategies
   b. Security process data (e.g. management and operational controls)
   c. Security control testing
   d. Test outputs (e.g. automated, manual)
   e. Security architectures vulnerabilities
7. Security Operations
   a. Investigations support and requirements
   b. Logging and monitoring activities
   c. Provisioning of resources
   d. Foundational security operations concept
   e. Resource protection techniques
   f. Incident management
   g. Preventative measures
   h. Patch and vulnerability management
   i. Change management processes
   j. Recovery strategies
   k. Disaster recovery processes and plans
   l. Business continuity planning and exercises
   m. Physical security
   n. Personnel safety concerns
8. Software Development Security
   a. Security in the software development lifecycle
   b. Development environment security controls
   c. Software security effectiveness
   d. Acquired software security impact

After evaluating the need of audit result, ICT Department agreed that item audit from CISSP variety to wide to evaluate. The agreed that the audit will only item related to access control, a part of Domain 5 CISSP: Identity and Access Management.

Audit team and ICT Department agreed that the item of access control to be audit are:

1. Identification
   a. User identification
   b. Program Identification
   c. Process identification
   d. Data Identification
2. Authentication
   a. Implement Something You know
   b. Implement Something You have
   c. Implement Something You are
   d. Implement Combination
3. Authorization
   a. Implement Access Criteria
   b. User Access Classification
   c. Asset Access Classification

   d. Resources Classification
   e. Single Sign on Environment

4. Accountability
   a. Access Control Accounting
   b. Access Control Audit

5. Access Control Implementation
   a. Access Control Model
   b. Access Control Technique
   c. Access Control Administration
   d. Access Control Administrative
   e. Access Control Physical
   f. Access Control Technical
   g. Access Control Functionality
   h. Access Control Practice
   i. Unauthorize disclosure information

6. Access Control Monitoring
   a. Host Based Intrusion
   b. Network Based Intrusions
   c. Intrusion Detection
   d. Intrusion Prevention
   e. Honeypots
   f. Network Sniffers

D. ICT Infrastructure XYZ IS

To support teaching process XYZ have 250 desktop computers, 150 Computing, 8 host for server virtualization, 40 wireless access point and 1100 BYOD (bring your own device) belong to student, teacher and staff. XYZ provide 100Mbps internet bandwidth with CIR 1:1 for all user in school.

Bandwidth of 100Mbps supported from by 2 ISP with 50Mbps from each ISP. The connection to ISP using fiber optic and backup used wireless link. Each ISP have minimum 2 route to international internet backbone. Both link manage using load balancing to get maximum benefit from each other's. Average utilization at 60Mbps and peak utilization at 80Mbps and sometime reach 100Mbps.

After redesign of information technology infrastructure of XYZ international school, student increase their bandwidth allocation from 128Kbps to 2Mbps per user, Staff increase their bandwidth allocation from 384Kbps to 4Mbps per user and Teacher increase their bandwidth allocation from 384Kbps to 6Mbps per user.

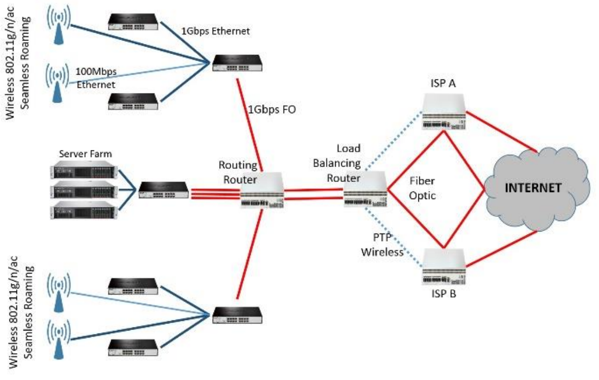

Fig. 1. New architecture of XYZ International School ICT System & Infrastructure after redesign.

WLAN (wireless local area network) using product from Ubiquity Unifi and implement seamless roaming between access point.

E. Audit Methods

Audit will be conduct based on self-assessment by the Manager of ICT Department from XYZ international school. Assessment will be follow the guidance form created by Audit team.

Each item will be quantified based on Capability Maturity Model Integration (CMMI) [3], [4]. The model involves five aspects:

1. **Maturity Levels**: a 5-level process maturity continuum - where the uppermost (5th) level is a notional ideal state where processes would be systematically managed by a combination of process optimization and continuous process improvement.

2. **Key Process Areas**: a Key Process Area identifies a cluster of related activities that, when performed together, achieve a set of goals considered important.

3. **Goals**: the goals of a key process area summarize the states that must exist for that key process area to have been implemented in an effective and lasting way. The extent to which the goals have been accomplished is an indicator of how much capability the organization has established at that maturity level. The goals signify the scope, boundaries, and intent of each key process area.

4. **Common Features**: common features include practices that implement and institutionalize a key process area. There are five types of common features: commitment to perform, ability to perform, activities performed, measurement and analysis, and verifying implementation.

5. **Key Practices**: The key practices describe the elements of infrastructure and practice that contribute most effectively to the implementation and institutionalization of the area.

Within each of these maturity levels are Key Process Areas which characterize that level, and for each such area there are five factors: goals, commitment, ability, measurement, and verification. These are not necessarily unique to CMM, representing as they do the stages that organizations must go through on the way to becoming mature.

The model provides a theoretical continuum along which process maturity can be developed incrementally from one level to the next. Skipping levels is not allowed/feasible.

1. **Level 1 - Initial (Chaotic).** It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending

to be driven in an ad hoc, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes.

2. **Level 2 – Repeatable.** It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.
3. **Level 3 – Defined.** It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place (i.e., they are the AS-IS processes) and used to establish consistency of process performance across the organization.
4. **Level 4 – Managed.** It is characteristic of processes at this level that, using process metrics, management can effectively control the AS-IS process (e.g., for software development). In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level.
5. **Level 5 – Optimizing.** It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes / improvements

III. AUDIT RESULT

After self-assessment filled in and calculated based on sub domain of Access Control, the result is showed in Table 1.

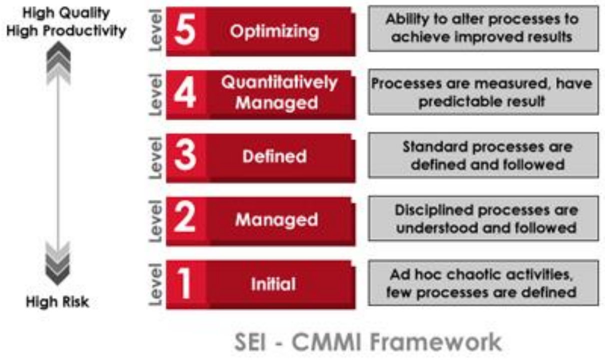
High Quality
High Productivity
Level 5 Optimizing
Ability to alter processes to achieve improved results
Level 4 Quantitatively Managed
Processes are measured, have predictable result
Level 3 Defined
Standard processes are defined and followed
Level 2 Managed
Disciplined processes are understood and followed
Level 1 Initial
Ad hoc chaotic activities, few processes are defined
High Risk
SEI - CMMI Framework

Fig. 2. CMMI Framework used for XYZ International School IT Security audit.

From the result, we found that XYZ IS, already implement access control and have good result in identification, authentication, authorization and implementation. Two sub subs domain have lower value are accountability and monitoring.

TABLE 1.
XYZ INTERNATIONAL SCHOOL AUDIT RESULT

No	Sub Sub Domain	Result
A	Access Control Identification	2.75
B	Access Control Authentication	3.50
C	Access Control Authorization	3.00
D	Access Control Accountability	1.50
E	Access Control Implementation	2.78
F	Access Control Monitoring	1.83
Audit Result Value Average		**2.56**

In identification, all user, process and program already identified, implemented and used for username based on their related information. Person identified based on first letter of their first name and concatenate with their last name.

Authentication implemented using password (what you know) to access network resources environment and manage by windows AD (active directory). Password synchronized with WLAN infrastructure using radius service. Email password still separated due to different provider. Email provider using google cloud and integrated with all service within google apps for education.

Biometric (who you are) used for time attendance and gate access to enter school area in elementary and secondary school.

Smart card (what you have) used to provide access for multifunction machine. Only person with a valid smart card can used the machine for copying, printing, scanning and faxing. Smartcard itself integrated with AD.

Two factor authentication already implement to get internet access using WLAN, user have to register their MAC address and provide access password from AD.

Access to internet monitored for every user by AD login. Access to network file sharing and application also monitored. But in some case log report should be processed before can be submitted as a report activity monitoring to school management.

Access to internet already recorded to provide report for most usage bandwidth, most time spent, most accessed website, and most downloaded website. From these report, management can decide policy for internet access management.

IV. CONCLUSION

IT security audit for XYZ international school has succeed to provide the image of security concern from the school. Audit target has been adapted to fulfill the expectation of the school about security system.

Eight domain of CISSP common body of knowledge can implemented as an item to be audited based on agreement between audit team and audited team.

Result of the audit used as baseline to performed improvement for next year target of IT service continuous improvement.

V. ACKNOWLEDGMENT

The authors wish to thank to I Made Sudarma the Lecturer of IT Audit subject in the Department of Electrical and

Computer Engineering, Post graduate program, Udayana University.

VI. REFERENCES

[1] "Computer Audit FAQ." [Online]. Available: http://www.isect.com/html/ca_faq.html.

[2] "CISSP - Certified Information Systems Security Professional | (ISC)2." [Online]. Available: https://www.isc2.org/cissp/default.aspx.

[3] "CMMI Maturity Levels." [Online]. Available: http://www.tutorialspoint.com/cmmi/cmmi-maturity-levels.htm..

[4] O. Matrane, A. Talea, C. Okar, and M. Talea, "Towards A New Maturity Model for Information System," International Journal of Computer Science Issues (IJCSI), vol. 12, no. 3, p. 268, 2015.