




2007

Education Organization Baseline Control Protection and Trusted Level Security

Wasim A. Al-Hamdani

Information Security Lab, Division of Computer and Technical Sciences

Follow this and additional works at: <https://commons.erau.edu/jdfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Recommended Citation

Al-Hamdani, Wasim A. (2007) "Education Organization Baseline Control Protection and Trusted Level Security," *Journal of Digital Forensics, Security and Law*. Vol. 2 : No. 4 , Article 2.

DOI: <https://doi.org/10.15394/jdfsl.2007.1030>

Available at: <https://commons.erau.edu/jdfsl/vol2/iss4/2>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.



(c)ADFSL



Education Organization Baseline Control Protection and Trusted Level Security

Wasim A. Al-Hamdani, PhD

Information Security Lab

Division of Computer and Technical Sciences

Kentucky State University, Frankfort, KY 40601

Phone: (502)597-6728, Fax (502)597-5763

wasim.al-hamdani@kysu.edu

ABSTRACT

Many education organizations have adopted for security the enterprise best practices for implementation on their campuses, while others focus on ISO Standard (or/and) the National Institution of Standards and Technology.

All these adoptions are dependent on IT personal and their experiences or knowledge of the standard. On top of this is the size of the education organizations. The larger the population in an education organization, the more the problem of information and security become very clear. Thus, they have been obliged to comply with information security issues and adopt the national or international standard. The case is quite different when the population size of the education organization is smaller. In such education organizations, they use social security numbers as student ID, and issue administrative rights to faculty and lab managers – or they are not aware of the Family Educational Rights and Privacy Act (FERPA) – and release some personal information.

The problem of education organization security is widely open and depends on the IT staff and their information security knowledge in addition to the education culture (education, scholarships and services) has very special characteristics other than an enterprise or comparative organization

This paper is part of a research to develop an “*Education Organization Baseline Control Protection and Trusted Level Security.*” The research has three parts: **Adopting** (standards), **Testing** and **Modifying** (if needed).

The baseline control criteria covers the following topics: **management control, operational control, logic control, physical control and development and maintenance control.** This paper is concerned with the first two controls.

Definition: for the purpose of this research, the following definition will be used: **Education organization:** a university campus, technical colleges, and high school; include several education units (department, college), with four different personals: faculty, staff, student and administration.

EOBC stands for Education Organization Baseline Control.

Keywords: Information security, information security control, information security baseline, security trusted level, education organization, education environment, campus information security, information security education , information security infrastructure.

1. INTRODUCTION AND PROBLEM STATEMENT

The final version of national strategy encourages colleges and universities “to secure their cyberspace by establishing some or all of the following approaches” pp. 25, 41 (The National strategy secure cyberspace 2003)

- One or more information sharing and analysis centers deal with cyber attacks and vulnerabilities;
- An on-call point-of-contact to Internet service providers and law enforcement officials in the event that the school’s IT systems are discovered to be launching cyberattacks;
- Model guidelines empowering chief information officer (CIOs) to address cybersecurity;
- One or more sets of best practices for IT security; and
- Model user awareness programs and materials.

The report specifies the following: “Top university presidents have adopted a five-point Framework for Action that commits them to giving IT security high priority and to adopting the policies and measures necessary to realize greater system security,” these are:

- (1) Make IT security a priority in higher education;
- (2) Revise institutional security policy and improve the use of existing security tools;
- (3) Improve security for future research and education networks;
- (4) Improve collaboration between higher education, industry, and government; and
- (5) Integrate work in higher education with the national effort to strengthen critical infrastructure.

An education culture (education, scholarships and services) (Luker & Petersen 2003) has very special characteristics other than an enterprise or comparative organization. Education culture normally has in common : Free organization, focusing on learning, scholarship, services, large turnover in numbers (semester/year period), one semester as a major period, age of the participants in the organization, learning in group or individual settings, include non-academic and extracurricular services.

With all these factors, a major question arises: “How to protect assets?” and

furthermore, “What are the assets?” In an education organization, information assets could be defined as: student grades, research reports, exam papers, student/staff/faculty personal information, library (e-library), administration reports and process, personnel evaluations, accountancy department assets, student records, student registration, network infrastructure, lab resources, and others.

Compliance issues to the above assets are policies, procedures, guidelines, data backup and retention, data privacy, transferring and downloading data, communications, firewalls and external connectivity, intrusion detection systems, intrusive computer software, disaster controls, physical and logical access controls, device and media controls, and procedural controls.

How to protect these assets? The answer depends on the size of the education organization. The other side of the problem is the level of IT department expertise and knowledge in the field of information security. A normal solution is to adopt security best practices and standards.

There are many information security standards and guidelines to be followed, such as:

- The free online National Institution of Standards and Technology. (National Institution of Standard and Technology 2007);
- Request for comments such as:(RFC 2196 site handbook or RFC 2504 user security handbook (Request for comments 2004);
- The international standards like ISO 19977 (INCITS/ISO/IEC 17799-2005 2005);
- IT Governance: A Manager's Guide to Data Security and BS 7799/ISO 17799 (Calder and Watkins 2005);
- American National Standard Institute (Code of practice for information security management publications standard and the guidance document Contracting for Information Security in Commercial Transactions: An Introductory Guide) (ANSI American National Standard Institute 2008).

Some universities do understand the problem and have organized their assets to standard policies, procedures and guidelines, such as:

- University of California (University of California 2007);
- University of Iowa (University of Iowa 2004);
- University of Colorado at Boulder (University of Colorado at Boulder 2007);
- University of Utah, (University of Utah 2006);
- University of Purdue (University of Purdue 2006).

The problem is cited in small population education organizations where the

enterprise best practices implementation is very costly and the edges between secure and insecure organizations are not clear. In addition, there is a lack of security expertise in the small institution in IT department. The case is quite different in large education organizations where information security is on the front burner to be a critical factor and to be attended. Theoretically speaking, the size of the population should not affect the information security practices – that is, disclosure of personal information is simply releasing personal information. The problem is there are no baselines, no trusted level and secure level in which one can say, “X or Y education organizations or campus is in a state of compliance with the security level required”? More specifically, there is no existing standard, best practices, standard policy level, guidelines in academic and education organizations that IT could follow up with. Total success is dependent upon the IT personnel – expertise, knowledge and so on. Even with this knowledge, creating or adapting standard or best practices is not an easy issue because IT has to select the most suitable for their campuses (quite possibly after some trial). Looking at a large population education organization, we can see their adaptation coming from IOS or the NIST standards or from error and trials.

Academic and education organizations have very special characteristics and features that distinguish them from any other enterprise or national agencies. Such organizations have features such as free organization, focuses on learning, large number of turnover (semester/year period), one semester is a major period, age of the participant in the organization, learning in group or individual, include non-academic and extracurricular services.

The need for information security base standards and trusted levels or even minimum levels of trust for an education institution is very essential, as some educational organizations are still using practices that are classified as security breaches for personnel and the organization; for example, using social security numbers for student ID numbers, no security policies, no network password policy, no secure managements, no information and data risk analysis, no backup policy, all faculty have level of administrative right, no access control policy, no physical security, no configuration managements, no change control managements.

The problem becomes more critical if we look at the research level where copyright (intellectual property) issues or grading systems are considered. The problem is very clear with cyber courses and e-classes where student assessment is based on open recourses (many instructors fall into cyber-cheating without being aware of it, such as blackboard cheating (Al-Hamdani, 2008). Hence, the need for standards to be developed and tested is very critical for small- and medium-sized education organizations (the case could be very critical for large populated campuses as well). The need for detailed standards and checklists, as well as a baseline security matrix could be automated to

deliver the best security practices needed. The matrix could also evaluate any education organization to decide the security level and then indicate where weaknesses and measures are needed to improve the level of security.

The need for standards in an education organization should take into account the education organization, culture properties, and culture behaviors, and focus on educational best practices for security control, legislation, architecture, and continuity of operations.

2. BASELINE SECURITY INFRASTRUCTURE

As the education campus population increases, the security issue starts to be a problem for IT personnel, and many depend on IT expertise, skill and knowledge for information security. The authentic need for security normally drives IT personnel to find the best solutions for their security problem. Basically, there are four solutions that IT would approach. These are:

NIST free publications as a guideline (National Institution of Standard and Technology 2007) using documents, such as:

- SP 800-12 An Introduction to Computer Security;
- SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems;
- SP 800-16 Information Technology Security Training Requirements
- SP 800-27 Engineering Principles for IT Security;
- SP 800-18 Guide for Developing Security Plans for Federal Information Systems;
- SP 800-26 Self-Assessment Guide for Information Technology Systems;
- SP 800-27 Engineering Principles for Information Technology Security (A Baseline for Achieving Security) ;
- SP800-53 Recommended Security Controls for Federal Information Systems.

ISO (IT Governance: A Manager's Guide to Data Security and BS 7799/ISO 17799; INCITS/ISO/IEC 17799-2005 2005) such as: ISO 17799 Information Technology Code of Practice for Information Security Management

Federal Information Processing Standards Publications (FIPS publications) (Federal Information Processing Standards Publications 2007), using documents such as:

- PS PUB 1999 Standards for Security Categorization of Federal Information and Information Systems, 2004 February;
- FIPS 200 Minimum Security Requirements for Federal Information and Information Systems.

Industry best practices issues, which normally comes with software and

hardware purchases.

These guidelines (and others -see Appendix 1) can be classified as:

Information Security Management

- ISO/IEC 17799:2005 and ISO/IEC 27001:2005 (INCITS/ISO/IEC 17799-2005 2005; Calder and Watkins 2005) ;
- RFC 2196 (The Internet Engineering Task Force (IETF)) ;
- IT Baseline Protection Manual (Germany) (Sicheres E-Government 2008) ;
- OECD Guidelines for the Security of Information Systems (OECD Guidelines for the Security of Information Systems 2005).

Evaluation

- ISO 15408 ("Common Criteria") (ISO 15408. Common Criteria for Information Technology Security Evaluation, V3.1 2006) ;
- Perhaps the most important of these books is the Trusted Computer System Evaluation Criteria (TCSEC, or Orange Book) (Rainbow Series 2006) ;
- Information Technology Security Evaluation Criteria ("ITSEC") (UK) (Information Technology Security Evaluation Criteria (ITSEC) 1991).
- Gateway Certification Guide and DSD EPL (Australia/New Zealand) (Defence Signals Directorate 2007).

Development

- Capability Maturity Model (CMM) (Chrissis et al 2003) ;
- Capability Maturity Model (SSE-CMM) (System Security Engineering Capability Maturity Model (SSE-CMM) 2008).

Risk

- Acquisition Risk Management (US) (Risk Management Guide for DoD Acquisition 2003) ;
- AS/NZS 4360 ("Risk Management") (Australia/New Zealand) (Standards Australia Online Catalogue 2008).

Authentication

- ISO 11131 ("Banking and Related Financial Services; Sign-on Authentication") (Standards Australia Online Catalogue 2008) ;
- ISO 11131:1992 Banking and Related Financial Services; Sign-on Authentication (Standards Australia Online Catalogue 2008).

All these documents and their adaptations depend on:

- Level of security required
- IT personnel

- The management's support
- Cost efficiency for the campus
- Real threats (real case)

Normally, a large campus has more efficient security measures and this is reflected in their policies, standards, procedures and best practices. A campus with more than 33,000 students (not counting faculty and staff) must have reasonable information security practices and policies. Information security policies cover many issues, such as:

- Security Breach of Personal Information;
- Electronic Distribution of University Information via the Internet;
- Information Security ;
- Protection of Confidential Electronic Information ;
- Copyrighted Material.

Comparing the large campus security measures with a small campus and education organization of 3,000 to 5,000, we could find a single-page information security policy and other basic policies (such as a password policy or a firewall policy), which are normally software or hardware driven.

Even with advanced security issues having been taken care of, things happen in open organizations (Hacker News, 2006), such as universities when two students “have been accused of hacking into a professor's computer, giving grades to nearly 300 students and sending pizza, magazine subscriptions and CDs to the professor's home” . What about an education campus where the information security has one page and they use social security numbers as student/faculty and staff accounts numbers and the first password (for system login) is a home phone number? Especially the student level of knowledge in information technology has become higher in the last few years as a result of cheap hardware and open resource software.

The significant goals for this research are:

- Adopt national and international baseline security issues;
- Examine a number of large education campus security principles and baselines;
- Examine a number of small education campuses' security issues;
- Find the security connection (statistically) between the two types of education organizations;
- Build a trusted level of baseline security (standard);
- Develop a checklist;
- Deliver an information security matrix.

One of the most important objectives is the evolution, and this will be achieved by:

- Measuring the control trusted level on the two types of campuses (large and small);
- Using a feedback function to enhance the weakness in the developed baseline;
- Measuring again the changes in the trusted level;
- Developing an automated system to help the checklist and to deliver benchmarks.

3. THE SUGGESTED BASELINE

3.1 Basic Baseline Control

The level of baseline security is achieved by implementing a minimum set of controls to protect information against the most common threats. An early step in the baseline approach may be a *gap analysis* (Information Security Guideline for NSW Government 1997). The risk in the baseline approach is that there may be an unidentified 'non-standard' threat or vulnerability that is missed by gap analysis and/or baseline controls. For information assets assessed as high risk, IT department may be necessary to conduct a detailed risk analysis. Although this type of analysis normally requires considerable time, effort and expertise, the selection of controls should always include a balance of non-technical and technical safeguards. Non-technical controls are of a general nature and include those that provide physical, personnel, and administrative security. Technical controls relate specifically to the information system considered.

3.2 Baseline Control Classifications

Controls could be classified (Information Security Guideline for NSW Government 1997) as:

- Management and overall organization baseline control;
- Operation baseline control;
- Technical baseline control;
- physical baseline control;
- Development and maintenance baseline control.

These classifications are used to assist in identifying non-technical and technical controls, there are 10 classes of control (ISO/IEC 17799:2000) (International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management 2002):

- Security policy;
- Security organization;
- Asset classification and control;
- Personnel security;
- Physical and organizational security;

- Communications and operations management;
- Access control;
- System development and maintenance;
- Business continuity management;
- Compliance.

Others classifications covers administrative, technical and physical (Harris, S 2005)

Controls may perform one of the following functions:

- Deter: Avoid or prevent the occurrence of an undesirable event;
- Protect: Safeguard the information assets from adverse events;
- Detect: Identify the occurrence of an undesirable event;
- Respond: React to or counter the adverse event;
- Recover: Restore the integrity, availability and confidentiality of information assets to their expected state.

3.3 Broad Baseline

The following questions should be considered when applying baseline security:

- Which parts of the education organization or education organization systems can be protected by the same baseline?
- Should the same baseline be applied throughout the whole education organization?
- What security level should the baseline education organization aim at?
- How will the controls forming the baseline(s) be determined?

The use of one baseline level will reduce the cost of implementing controls considerably, and everyone within. In doing so, a security professional in an education organization is usually advisable to aim at the highest security level of the information and information systems to be protected by the baseline controls since such implementation is normally not very expensive and provides adequate security for all information assets. A careful consideration of all information assets is necessary to make the final decision on which information assets should be protected by the same baseline.

4. MANAGEMENT AND OVER ALL ORGANIZATION BASELINE CONTROL

This control dealing with the management of information security, planning, assignment of responsibilities, and all other relevant activities, controls of the following activities:

4.1 Information Security Policy

Such as e-mail policy, e-mail retention policy, acceptable user policies, Application polices, Ethic policy, Password Protection Policy , Personal

Communication Device, Remote Access Policy, Mobile Computing and Storage Devices, Router Security Policy, The Third Party Network Connection Agreement, Student network access policy, student wireless policy and other policies as the education organization required.

EOBC 1.1: A POLICY DOCUMENT *should be approved by management, published, and communicated, as appropriate, to all faculty, staff and student.*

- *The policy should be reviewed regularly, in case of influencing changes, to ensure it remains appropriate.*
- *The implementation of the information security policy should be reviewed independently.*

4.2 Information Security Infrastructure

Information security should be managed within the education organization structure that appropriate to its size (space/population/ratio of faculty-staff-student). The education organization unit should identify resource requirements and assign the appropriate roles and responsibilities to allow the effective management of the information security policy from within the unit. This may involve the utilization of specialist resources.

EOBC 1.2: A MANAGEMENT COMMITTEE *to ensure that there is clear direction and visible management support for security.*

- *Where appropriate to the size of the education organization, a cross-functional committee of management representatives from relevant parts of the organization should be used to coordinate the implementation of information security controls.*
- *Responsibilities for the protection of individual assets and for carrying out specific security processes should be clearly defined.*
- *Contact with external information security specialists should be developed to ensure that the education organization kept to best practices and identified security vulnerabilities.*
- *Appropriate contacts with law enforcement authorities, regulatory bodies, should be maintained.*
- *Advice on information security provided by in-house or specialist advisers should be sought and communicated throughout the organization.*

4.3 Information Security Awareness and Training

Training of all personnel (faculty, staff, student and administrators) is critical to the effective implementation of information security baseline control. Security awareness and training activities should be ongoing to further demonstrate management's commitment to information security. Personnel should be made aware of the importance of the information processes, the

associated threats, vulnerabilities, risks and understand why baseline controls are needed.

EOBC 1.3: AWARENESS AND TRAINING *to all employees of the educational organization (and third party if they exist) should receive appropriate training and regular updates in policies and procedures.*

4.4 Third Party Access Control

The education organization should control access to information processing facilities by third party organizations and access should be assigned based on the assessment of the risk of granting such access. Third parties include:

- Hardware and software staff of service providers located off-site;
- Trading partners or joint ventures;
- On-site contractors for hardware and software maintenance and support;
- Cleaning, catering, security guards and other outsourced support services;
- Student placement;
- Casual short-term appointments;
- Consultants.

EOBC 1.4: THIRD PARTY ACCESS CONTROL, *any arrangements involving third-party access to education information processing facilities should be based on a formal contract containing all necessary security requirements, such as:*

- *The risks associated with access to education information processing facilities by third parties should be assessed and appropriate security controls implemented.*
- *If confidentiality of information is an issue (student information, student medical information, faculty personal information, and other assets), third parties should be required to sign a non-disclosure agreement.*

4.5 Mobile Computing control

Policies and procedures should be established for the use of mobile computing facilities (laptops, notebooks, palmtops and mobile phones).

EOBC 1.5: MOBILE COMPUTING CONTROL: *A formal policy and appropriate baseline controls should be in place with proper adaptation to protect against the risks of working with mobile computing facilities. Mobile computing security includes (but not limited):*

- *Security management policies (for example, handheld devices).*
- *Physical security.*

- *Labeling (GPS tracking system if needed).*
- *Access controls (Identification card, biometrics, etc.) and remote access.*
- *Virus protection.*
- *Encryption of data and passwords.*
- *Backups procedures.*
- *Sanitization, declassification and destruction of equipment.*

4.6 Asset Classification and Assets Control

In order to assess information security risks, the education organization needs to identify all major assets that require protection and assign an asset. The owner who has primary responsibility for the protection of this asset, and should be able to establish the relative importance and value of the asset to the education management.

EOBC 1.6: ASSET CLASSIFICATION AND ASSETS CONTROL: *Any means of asset classification and asset control should be used.*

- *An inventory of all important assets should be identified and maintained.*
- *Classifications and associated protective controls for information should be suitable to day-to-day needs for sharing or restricting information and their impacts associated with such needs.*
- *A set of procedures should be defined for information labeling and handling in accordance with the classification scheme adopted by the education organization*

4.7 Personnel Control Practices

Personnel cover not only permanent and part-time employees of the education organization but extend to contractors, consultants and other individuals working on the education organization premises or using the education organization information and information processing assets. A personal control practice covers all (depends on the education organization book definitions):

- *Job description, Duties, Recruitments, Monitoring of personal,*
- *Termination and job changes.*

EOBC 1.7: PERSONNEL CONTROL PRACTICES *to support full-time, part-time, contractors and consultant employees:*

- *Security roles and responsibilities as laid down in the education information security policy should be documented in job definitions where appropriate.*
- *Duties and areas of responsibility should be segregated in order to reduce opportunities for unauthorized modification or misuse of information or services.*

- *Verification checks on permanent staff should be carried out at the time of job applications.*
- *Employees should sign a confidentiality agreement as part of their initial terms and conditions of employment.*
- *The terms and conditions of employment should state the employee's responsibility for information security.*

4.8 Compliance with Legal and Regulatory Requirements

Information security officer should consider all relevant statutory, regulatory and contractual requirements to ensure compliance. Advice on specific legal requirements should be obtained from the education organization's legal counsel.

EOBC 1.8: COMPLIANCE WITH LEGAL AND REGULATORY REQUIREMENTS

All relevant statutory, regulatory and contractual requirements should be explicitly defined and documented for each information system and process.

- *Appropriate procedures should be implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights, and on the use of proprietary software products.*
- *Important records of the education organization must be protected from loss, destruction and falsification.*
- *Controls should be applied to protect personal information in accordance with relevant legislation.*
- *Education organization management authorizes the use of information processing facilities and controls should be applied to prevent the misuse of such facilities.*
- *Where action against a person or organization involves the law, either civil or criminal, the evidence presented must conform to the rules for evidence laid down in the relevant law or in the rules of the specific court in which the case will be heard. This should include compliance with any published standard or code of practice for the production of admissible evidence.*
- *Education organization management should ensure that all security procedures within their area of responsibility are carried out correctly and all areas within the education organization should be subject to regular review to ensure compliance with security policies and standards.*
- *Information systems should be regularly checked for compliance with security implementation standards.*

4.9 Security Incident Handling

Incident handling is an important aspect of managing information security risk. A security incident may occur from failures of hardware, infrastructure or

software; inadequate operational procedures; malicious code; hacking; and/or human errors.

EOBC1.9: SECURITY INCIDENT HANDLING *of the education organization must have a clear definition of “security incident” and where to report an incident.*

- *Security incidents should be reported through appropriate channels as soon after the incident is discovered as possible.*
- *Users of information services are required to report any observed or suspected security weaknesses in or threats to systems or services.*
- *Procedures must be established and followed for reporting software malfunctions.*
- *Incident responsibilities and procedures should be established to ensure a quick, effective and orderly response to security incidents.*

4.10 Educational Business Continuity Plan

Business continuity plans may be developed in case of any disaster.

EOBC1.10: EDUCATIONAL BUSINESS CONTINUITY PLAN

- *There should be a process in place for developing and maintaining education business continuity throughout the education organization.*
- *There should be a managed process in place for developing and maintaining education business continuity throughout the education organization.*
- *Plans should be developed to maintain or restore education business operations in a timely manner following interruption to, or failure of, critical processes.*
- *Business continuity plans should be tested regularly and maintained by regular reviews to ensure that they are up to date and effective.*
- *Single framework of education business continuity plans should be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance.*
- *Backup copies of essential education organization information and software should be taken regularly.*

4.11 System Audits

To monitoring user behavior and system activity, audits are a key element in managing vulnerabilities.

EOBC1.11: SYSTEM AUDITS

- *Audits of operational systems should be planned and agreed such as to minimize the risk of disruptions to business.*
- *Access to systems audit tools should be protected to prevent possible misuse or compromise.*

5. OPERATION BASELINE CONTROL

The controls relating to the secure, correct and reliable functioning of the education organization, operational controls can be implemented by education organization procedures.

5.1 Documentation

Documented operating procedures should be maintained for all normal operating and kept under configuration control. The security policy – where all the security procedures are documented – and the business continuity plan should be maintained and kept up-to-date.

EOBC2.1: DOCUMENTATION: *The operating procedures identified in the security policy should be documented and maintained.*

5.2 Configuration Management

Software, hardware and documentation changes to the information process facilities must be controlled. Configuration management is the process of controlling and tracking changes to all items, software, hardware or documentation to ensure that they are authorized and can be reversed if required. Configuration management requires the establishment of baselines against which all changes are tracked.

EOBC2.2: CONFIGURATION MANAGEMENT

- *Changes to information processing facilities and all education organization systems should be controlled.*
- *New applications systems should be reviewed and tested before and through changes occur.*

5.3 Incident Management

Procedures should be developed, documented, and updated to record any security breach, and action taken to correct the breach and any recommendation to prevent such a breach. Whenever a security breach occurs, the incident should be logged, assigned for follow-up, and analyzed.

EOBC2.3: INCIDENT MANAGEMENT: *Incident management responsibilities and procedures should be established to ensure a quick, effective and orderly response to security incidents.*

5.4 Software Development

Software development, testing and operational environments should exist separately.

EOBC 2.4: SOFTWARE DEVELOPMENT

- *All required action should be documented for separation of duties to reduce unauthorized modification or misuse of information or services.*
- *Development and testing facilities (if they exist) should be separated from operational facilities.*
- *Strict control should be maintained over access to program source code libraries.*
- *The implementation of changes should be strictly controlled by the use of formal change control procedures.*

5.5 External Facilities

External facilities can introduce potential security exposures, such as the unauthorized access, damage or loss of data at the outsourced facility. The same could be applied for lease facilities and equipment.

EOBC 2.5: EXTERNAL FACILITIES: *External facilities management services will minimize security breaches.*

- *Security checks should be performed before and after using external facilities or equipments (computers) with appropriate policies and procedures.*
- *Data sanitization should be applied with leased computer and memory systems (to ensure that personal data, grades are not left in memories).*

5.6 Data Backup

Backup and restore procedures should be documented and tested on a regular basis. Backup procedures will be tested every time a backup is made, but only by performing a successful restore can the validity of the backup/restore procedure and the reliability of the media be verified.

EOBC 2.6: DATA BACKUP

- *Backup policies should be in place for all components of an education organization (centralize and decentralize depend on the organization).*
- *Backup copies of essential education organization information process and software should be taken regularly.*
- *Original software copies should be backed up and safely stored.*
- *Backup should be performed on all network components.*

5.7 Protection against Malicious Code

Viruses, Trojan horses, worms and logic bombs are all examples of malicious code. Controls need to be in place to prevent, detect, and correct the effects of malicious code.

EOBC 2.7: PROTECTION AGAINST MALICIOUS CODE: *Detection and prevention controls to protect against malicious software and appropriate user awareness procedures should be implemented. Controls over malicious code include (but are not limited to):*

- *All systems should be protected by the latest version of antivirus software, and an education organization must keep their antivirus software up to date.*
- *Not to install unauthorized software (widely) onto the education organization computers (clear system policies should be in place).*
- *Not to download software from the Internet (widely) onto the education organization computers.*
- *Clear firewall policies for all components (and sub-components, for all networks and subnets) of an education organization.*
- *The education organization should have administration management labs policies (faculty, staff and students).*

5.8 Logging

Operator logs and network logs should be maintained that report all the activities performed by different computers and the network activities. A complete log should be in place in teaching labs. These logs should detail:

- Who and what applications were running?
- What actions were initiated by the operator?

EOBC 2.8: LOGGING: *All log activities should be clearly specified by the education organization procedures.*

- *The education organization should be very clear in their policies and awareness program that the active log is recorded (could be through network login banner).*
- *Staff, faculty and student policy valuation should be reported.*
- *Operational staff should maintain a log of their operational activities.*
- *Faults should be reported and corrective action taken.*

5.9 Information and Data Exchange

Exchanges of data should be subject to a written agreement between education organizations. The security implications associated with electronic data interchange, electronic commerce and electronic mail need to be considered. When reviewing such agreements, security conditions should be considered, such as management responsibilities, notification of the sender retransmission, dispatch and receipt, identification of couriers, responsibility and liability for data loss, technical standards for packaging, transmission, recording and reading information and software.

EOBC 2.9: DATA EXCHANGE: *Exchanges of data between education*

organizations should be controlled and comply with relevant legislation.

- *Agreements, some of which will be formal, should be established for the electronic or manual exchange of information and software between organizations.*
- *Data and information being transported should be protected from unauthorized access, misuse or corruption.*
- *Electronic commerce (for registration and transaction) should be protected against fraudulent activity, contract dispute and disclosure or modification of information.*
- *Policies should be sited for electronic commerce use and registration.*

5.10 Electronic Office System

Electronic office systems include computers, laptops, PDAs, mail, voicemail, fax, multimedia and postal services. These systems provide for speedier distribution of information. Policies need to be implemented to control what is distributed. Use of mobile phones could lead to confidential information being overheard in public places.

EOBC 2.10: ELECTRONIC OFFICE AND E-CLASSES: *Policies and guidelines should be prepared and implemented to control the organization and security risks associated with electronic office system and e-classes and virtual classes.*

- *Procedures and controls should be in place to protect the exchange of information through the use of voice, facsimile and video communications facilities.*
- *Policies should be prepared for electronic classes and virtual classes.*
- *There should be a formal authorization process before information is made publicly available and the integrity of such information should be protected to prevent unauthorized modification.*
- *Policy and procedural control should be in place for intellectual properties (copyright issues) when dealing with virtual classes.*
- *A control procedure should be in place for electronic cheating.*

5.11 Operational Media

Accountability for media should be clearly defined, particularly in respect to easily removed media, such as floppy disks, backup tapes and paper. Policies and procedures should be developed and published that specifies the storage standards and environment for media storage, the process for logging movement of media, the access control standards and the guidelines for the proper disposal of media by the education environment.

EOBC 2.11 OPERATION MEDIA: *Policy and procedures should be developed and published that specify the storage standards and environment for media storage, the process for logging movement of media, the access control*

standards and the guidelines for the proper disposal of media by the education environment .

- *The management of removable computer media such as tapes, disks, cassettes and printed reports should be controlled.*
- *Media should be disposed of securely and safely when no longer required.*
- *Procedures for the handling and storage of information should be established in order to protect such information from unauthorized disclosure or misuse.*
- *Systems documentation should be protected from unauthorized people.*

6. OTHER CONTROLS

The other controls are technical controls, physical control and maintenance controls.

The TECHNICAL CONTROL will cover the following:

- Identification and Authentication
- Logical Access
- Access rights
- Network Management (user access path, network planning, network configuration, monitoring, Internet connection policies, virtual private network, etc.)
- Operating System Access Control (work stations, login procedures, systems utilities, time access and restrictions)
- Application Access Control
- Audit Trails and Logs

The PHYSICAL CONTROL will cover:

- Secure areas
- Equipment security
- Clear desk and screen policy
- Removal of property

The DEVELOPMENT AND MAINTENANCE CONTROL will cover:

- Software modifications
- Cryptography
- Application security
- Maintains security

7. SUMMARY AND CONCLUSION

This paper is part of a research to adopt and develop “education organization

baseline security control.” The research covers mainly three parts: Adaptation and development, testing, and evaluation. The controls adopted are:

- Management and overall organization baseline control;
- Operation baseline control;
- Technical baseline control;
- Physical baseline control; and
- Development and maintenance baseline control.

This paper is concerned with first two in particular.

8. REFERENCES

Al-Hamdani, Wasim (2008). “*Blackboard Cheating Prevention*” (Unpublished article)

ANSI American National Standard Institute, (2008) Retrieved 2008, from http://webstore.ansi.org/packages/it_security.aspx

Calder, A. and Watkins, S. *IT Governance: A Manager's Guide to Data Security and BS 7799/ISO 17799*. Kogan Page; (January 2005)

Chrissis, M. B.; Konrad, M., & Shrum, S. (2003). *CMMI : Guidelines for Process Integration and Product Improvement*. Addison-Wesley Professional.

Defence Signals Directorate (DSD) (2007). Retrieved 2007, from <http://www.dsd.gov.au/library/infosec/>

Federal Information Processing Standards Publications (2007) Retrieved 2008, from <http://csrc.nist.gov/publications/PubsFIPS.html>

Hacker News Posted by Freaky on 27 Jul 2006 - 08:09 6 comments
<http://www.hackwire.com/comments.php?id=192&catid=3>

Harris, S. (2005) *CISSP All-in-One Exam Guide*, Third Edition
McGraw-Hill Osborne Media; 3 edition

INCITS/ISO/IEC 17799-2005. (2005). Retrieved 2007, from Information technology -Security techniques - Code of practice for information: <http://webstore.ansi.org/default.aspx>

Information Technology Security Evaluation Criteria (ITSEC). (1991). Retrieved 2007 from http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf

Information Security Guideline for NSW Government.Part 1,2 and 3. (1997)
Retrieved 2005,from <http://oict.nsw.gov.au/docs/>

International Standard ISO/IEC 17799:2000 Code of Practicefor

Information Security Management. (2002). Retrieved 2007 from Frequently Asked Questions.

<http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf>

ISO 15408. Common Criteria for Information Technology Security Evaluation, V3.1 (2006). Retrieved 2007, from <http://www.iso15408.net/>

Luker, M., & Petersen, R., (ed). (2003). *Computer and Network Security in Higher education*. Jossey-Bass. ISBN: 0-7879-6666-5

National Institution of Standard and Technology (2007). Retrieved 2008, from <http://csrc.nist.gov/publications>

OECD Guidelines for the Security of Information Systems (2005). Retrieved 2007, from <http://www.oecd.org/document/>

Rainbow Series (1988). Retrieved 2008, from <http://www.fas.org/irp/nsa/rainbow.htm>

Request for Comments (2004). Retrieved (2008) from <http://www.rfc-editor.org/rfc.html>

Risk Management Guide for DoD Acquisition (2003) (Fifth Edition, Version 2.0) Retrieved 2008 from http://www.dau.mil/pubs/gdbks/risk_management.asp

Sicheres E-Government. Retrieved 2008, from <http://www.bsi.bund.de/gshb/english/etc/menue.html>

Standards Australia Online Catalogue. Retrieved 2008, from <http://www.saiglobal.com/shop/Script/search.asp>

System Security Engineering Capability Maturity Model (SSE-CMM). Retrieved 2008, from <http://www.sse-cmm.org/index.html>

The Internet Engineering Task Force (IETF). Retrieved 2006, from <http://www.ietf.org/rfc/rfc2196.txt>

The National strategy secure cyberspace. (2003). Retrieved from The white house: <http://www.whitehouzse.gov/pcipb/>

University of Iowa, Network Citizenship Policy (2004) . Retrieved 2008, from <http://cio.uiowa.edu/policy/NetworkCitizenshipV2.shtml>

University of California, Business and Finance Bulletin, Electronic Information Security. (2007). Retrieved 2008, from <http://www.ucop.edu/ucophome/policies/bfb/is3.pdf>

University of Utah. (2006). Retrieved 2008, from <http://www.it.utah.edu/leadership/policies>

University of Colorado at Boulder, IT Policies and Guidelines.(2007) Retrieved 2008 from: <http://www.colorado.edu/its/policies/index.html>

University of Purdue. (2006) from Department of Botany and plant pathology/ baseline security policy, Retrieved 2008,

<http://www.btny.purdue.edu/Pubs/DeptBaselineSecurityPolicy.pdf>

APPENDIX 1

Information Security Management

- ISO/IEC 17799:2005
- ISO/IEC 27001:2005
A widely accepted standard, the British Standard BS 7799 has been updated and published as the international standard ISO/IEC 27001. It was developed by the British Standards Institute) and is sometimes referred to as BS ISO/IEC 27001:2005.
- RFC 2196
The Internet Engineering Task Force (IETF) has produced *RFC2196 Site Security Handbook*, which provides practical guidance to administrators trying to secure their information and services. IT Baseline Protection Manual (Germany)
The Federal Agency for Security in Information Technology in Germany has produced the IT Baseline Protection Manual. This document presents a set of recommended standard security measures or "safeguards", as they are referred to in the manual, for typical IT systems. The most recent version is dated October 2000.
- OECD Guidelines for the Security of Information Systems are available at ACSI33 (Australia/New Zealand). The Defense Signals Directorate has produced the *Australian Communications Security Instruction Number 33 (ACSI33) Security Guidelines for Australian Government IT Systems* document.

Evaluation

- ISO 15408 ("Common Criteria") The International Organization for Standardization (ISO) has produced ISO standard IS 15408. This standard, *The Common Criteria for Information Technology Security Evaluation v2.1 (ISO IS 15408)* is effectively an evolutionary blending of *ITSEC* (see below), the Canadian criteria, and the *U.S. Federal Criteria*. Available from.
- Rainbow Series ("Orange Book") (Rainbow Series, 1988). An important series of documents are the Rainbow Series, which outline a number of security standards developed in the United States. Perhaps the most important of these books is the *Trusted Computer System Evaluation Criteria (TCSEC, or Orange Book)*. While this standard has effectively been superseded by other standards outlined above (it is dated 1985); it is, nevertheless, a useful document. A further document, the *U.S. Federal Criteria*, was drafted but not adopted in the early 1990s.
- Information Technology Security Evaluation Criteria ("ITSEC") (UK)
The United Kingdom produced the *Information Technology Security*

Evaluation Criteria (ITSEC) in 1991, and this is another important historical evaluation scheme/standard. It builds on the *Orange Book* scheme to some extent, with greater granularity.

- Gateway Certification Guide and DSD EPL (Australia/New Zealand)
The Defense Signals Directorate has also produced the *Gateway Certification Guide*, which provides guidelines for independent assessment of an agency gateway.
- The Defense Signals Directorate administers the Australian government's *Evaluated Products List*.

Development

- Capability Maturity Model (CMM).
The Software Engineering Institute pioneered the development of the *Capability Maturity Model*, which is method for process maturity assurance.
- System Security Engineering Capability Maturity Model (SSE-CMM).

Risk

- Acquisition Risk Management (US).
- AS/NZS 4360 ("Risk Management") (Australia/New Zealand)

Authentication

- ISO 11131 ("Banking and Related Financial Services; Sign-on Authentication")
ISO 11131:1992 Banking and Related Financial Services; Sign-on Authentication is