IT SECURITY FRAMEWORK FOR COMPUTER BASED EXAMINATIONS – A BLUEPRINT

BY

DR. ANTRIKSH JOHRI
COLLEGE OF ENGINEERING STUDIES
(CENTRE FOR INFORMATION TECHNOLOGY)

Submitted

IN PARTIAL FULFILLMENT OF THE REQUIREMENT OF THE HIGHER DOCTORAL DEGREE (D.SC.)

TO

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
DEHRADUN
September, 2017

Under the Guidance of

PROF (DR.) PARAG DIWAN
FORMER VICE CHANCELLOR
UPES

Dedicated to my all-time inspirations, torch bearers, philosophers, guides and

beloved parents

Smt Sheela Johri and Late Shri V.B.S. Johri

&

my most respected grandparents…

Late Shri L.B. Johri Ji

Late Smt Shyam Johri Ji

Late Shri P.M. Saxena Ji

Late Smt Dropdi Saxena Ji

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
DEHRADUN, UTTARAKHAND

CERTIFICATE

This is to certify that the thesis titled ***"IT Security Framework for Computer Based Examinations – A Blueprint",*** which is being submitted by Dr. Antriksh Johri for the award of Higher Doctoral Degree (Doctor of Science) in Computer Science to the University of Petroleum and Energy Studies, Dehradun, Uttarakhand is a record of bonafide research work. He has worked for approximately five years under my mentorship.

The thesis has reached the standard, fulfilling the requirements of regulations relating to the degree. The results obtained in this thesis have not been submitted to any other University or Institute for the award of any degree or diploma.

Prof (Dr.) Parag Diwan
Mentor
Former Vice Chancellor
University of Petroleum and Energy Studies
Dehradun, India

DECLARATION

I, Antriksh Johri, hereby declare that the thesis entitled ***"IT Security Framework for Computer Based Examinations – A Blueprint"*** which is being submitted by me to the University of Petroleum and Energy Studies, Dehradun, Uttarakhand is in fulfillment of the requirement for the degree of Higher Doctoral Degree (Doctor of Science) in Computer Science and has not previously formed the basis for award of any degree, diploma, associateship, fellowship or any other similar title or recognition.

(Dr. Antriksh Johri)

ACKNOWLEDGEMENTS

This research would not have been possible without the guidance and the help of few important people. These people stood by my side and gave me constant encouragement and made me believe in myself.

My first and foremost thanks goes to my learned mentor **Prof (Dr.) Parag Diwan** under whose directions the research work was completed and the thesis written. He not only served as my mentor but also encouraged and challenged me throughout my research program. He patiently guided me through the research process, never accepting less than my best efforts because of his work ethic, high standards and his passion for cutting-edge research. It was a great privilege for me to do this research under his learned guidance. During the research tenure he extended personal, professional and moral support to me.

I am immensely grateful to Ms Rakhi Ruhal, Research Co-Ordinator, UPES who has been driving me constantly to complete my work in time. I am also grateful to Shri S S Farmer, Asst. Registrar, UPES, other learned faculty members and non-teaching staff of UPES, Dehradun, Uttarakhand for their support.

Finally, I will never find words enough to express the gratitude that I owe to my most affectionate parents **Late Shri V B S Johri** & **Smt. Sheela Rani Johri** and my philosopher guide elder sister **Dr Aradhana** who have always worked as catalyst in keeping my morale high during my entire educational journey.

I have no words to express my thanks to my outstanding and genius daughter **Ms Jhanak,** who despite her awfully busy schedule worked day and night and helped me in organizing, formatting and proof reading of thesis. I am also short of words in expressing my thanks to my IT wizard and genius son **Mr Ayushman**, who also despite his busy schedule helped me a lot in implementing various logical checks in thesis. Besides these two wonder kids, I cannot forget the contribution of my wife **Mrs Anita Bharati** who always energized me with her inspiring thoughts throughout my work.

Besides them, I am also thankful to my other family members viz. **Mr Sanjay, Mrs Amita & Mr Sanjiv, Mrs Anuja & Mr Vinay, Mrs Gauri & Mr Ankur, Pratishtha, Shivam, Abhilasha, Sakshi, Gopala, Alokik, Kanha and Kuin** who had been source of energy, inspiration and moral support throughout this research work. Throughout the period all my family members were extremely co-operative and patient with my off-working hours and mood swings.

The lender love and affection of all of my family members has always been the cementing force for building the blocks of my academic career. The all-round support rendered by them provided the much needed stimulant to sail through the phases of stress and strain.

Last but not the least I would like to express my special thanks to my most trusted lieutenants **Mr Prashant Kumar, Mrs Bhawana, Mrs Sabika and Mr Avdhesh** who had been always with me during my all difficult days, supported and helped me a lot.

Needless to add any errors and omissions found in the thesis are entirely my responsibility and I will be extremely grateful if they were pointed out to me. To all of you, thank you very much.

Dr Antriksh Johri

CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Information Technology (IT) security, once an issue of interest for Intelligence Agencies of various countries, has gained importance in almost all sectors of life wherever the new technology based advancements have taken place around the globe. Governments, universities, business houses- all have become vulnerable in one way or another in today's cyber era where terrorism, with respect to violence as well as economic terrorism, has also become a prime issue of concern. The gravity of the threat has been well realized by all and great efforts are being put in the developing methodologies and framework so that IT security threats may be addressed effectively in the area of examination, particularly competitive examinations where every mark counts for selection of a candidate. This work also includes contribution from my twenty-six years of experience in planning and conduct of examination in addition to my core function of result compilation. This thesis presents the ongoing efforts and development of framework pertaining to various IT security protocols for safe and secure conduct of examination in particular Computer Based Examinations.

IT Security is defined as the prevention of damage to IT application, unauthorized use of IT application, exploitation of IT application, and, if needed, restoration of electronic information and communication systems and the information they contain, in order to ensure the confidentiality, integrity and availability of these systems.

IT security provides protection against all forms of IT security breach. Cyber-attacks have the potential of causing devastating disruption to critical national infrastructures, economies and even national security. Virus, worms, spam, publishing and other fraudulent schemes, as well as identity theft, also come under cyber-attacks. As the tools and technologies to bring about the intrusions are more freely available to the people who are very capable and smart but have a mind-set of causing havoc or disruption, the cyber world becomes more vulnerable as the time goes on.

To make significant progress in the magnitude of cyber, security must be built into systems from step one. New architectures containing new hardware, designed to include embedded cyber security monitoring and processing capabilities (e.g. on board or peripheral cyber security processing, virtualizes architectures) and even especially designed to accommodate new cyber security analysis (e.g. processes designed for ultra-fast data comparison and analysis encompassing searches, sorts, merges, joins, and pattern reorganization) as well as new encryption and decryption techniques are needed.

At present, the cyber security comes up as a reaction to an attack and it is generally achieved manually. Threats and vulnerabilities are defined and addressed only after they appear, then identified, analyzed and distilled into well-defined behaviors and even digital signatures. Definitely, today, sophisticated and intelligent systems are required which can detect and protect from threats based upon more than just tabulated data, using sophisticated, predictive mathematical models to “stay ahead of the curve”.

Software with good security features is efficient enough to repel most kinds of attacks, tolerate the maximum number of attacks which it cannot repel, and is also able to recover quickly, with minimum damage caused, from the attacks it cannot tolerate. Development of high assurance security software requires knowledge and techniques which are not usually known or used in practice by most software developers.

Usually, in a customary Software Development Life Cycle (SDLC), security is taken up as the last issue to be covered and all its scenarios like probabilities, estimation and solution are resolved at the very end after the software has been developed. Vulnerabilities are an emergent property of software which appears throughout the development phases.

Whenever the security aspect is considered during the system life cycle, they are in general: features like password protections, firewalls, virus detection tools and so on. These are, in fact, not security requirements at all but rather implementation mechanisms that are intended to satisfy unstated requirements, such as authenticated access. Thus, system specific security requirements which provide protection to essential services and assets are often overlooked. Even the view point of attackers is not calculated. So, the net result is that the security features, even which are present, are inadequate. Thus, a scientific approach dealing with the security requirements, step by step, will help to avoid the problem of generic lists of features and to take into account the attacker's perspective.

Including security at the beginning of the SDLC is often considered the most cost-effective approach for two reasons, (1) it is usually more difficult to add functionality into a system after it has been built, and (2) it is frequently less expensive to include the preventive measures to deal with the cost of a security incident.

Chapter 1, *"Public Examinations Going Online: A Paradigm Shift",* of this thesis talks about a paradigm shift in the examination system from traditional pen-and-paper mode to online or computer based mode. This is happening primarily due to various issues pertaining to sanctity of traditional system of examination with challenges of integrity and effectiveness.

Chapter 2, *"Challenges Of Offline Examinations And Need For Computer Based Examinations"*, talks in detail about various challeneges of offline examinations including unfair means used by students, less number of students being qualified, dissimilarities in handling the transcripts, leakage of question papers, evaluation being delayed, process/declaration of result being delayed, marks being manipulated, improper conduct of re-evaluations etc.

Chapter 3, *"Standard Operating Procedures for Computer Based Examinations"*, is a prescriptive and thorough guide for all examining bodies which are planning to introduce computer based examinations in place of traditional pen-and-paper and OMR based examinations. There are enormous number of stages for the conduct of such examinations and all such stages are highly sensitive. If these stages are not taken care of properly it may lead to a great disaster. In this chapter, an effort has been made to suggest a way ahead for tactfully and effectively executing all stages of the examination with complete IT security.

Chapter 4, *"Prescriptive Framework to Develop a Secure Cyber Application"*, has been purposely taken from my earlier research. This chapter emphasises a suggestive, secure framework to develop an online application, nearly a hundred per cent free from vulnerabilities. This is because for all the computer examinations, both at pre-stage and conduct stage, there is a huge role of the cyber application developed for this purpose. In this chapter, a Secure Software Development Life Cycle (SSDLC) has been introduced. The complete road map for web application security has been proposed. Besides this, a secure Software Development Model has been designed. A general SDLC is discussed that includes the following phases: initiation phase, acquisition / development phase, implementation phase, operations / maintenance and disposition phase. In addition to above, a complete IT security in the Software Development Life Cycle has been put forward. Finally, a complete Application Security Lifecycle model has been proposed.

Chapter 5, *"Infrastructure, Process and Security Audit for Computer Based Examinations"*, of this thesis is about another extremely crucial activity to be undertaken before the conduct of computer based examinations. A third party specialised audit is suggested. This audit is to be carried out by certain empaneled agencies or any other specialised IT audit agencies to ensure plugging-in of any possible loopholes in the system of computer based examinations. It is highlighted that the auditing of infrastructure for conduct, the process involved and software to be used are essential. The third-arty audit team should thoroughly conduct security auditing of examination software application, encryption process, physical and environment security, network security and process audit.

Chapter 6, *"Significance of IT Security in Public Examinations (Computer Based Examinations)"*, talks about various security issues in public examinations, such as confidentiality, integrity, availability, user authenticity, fairness of conduct etc. This chapter details out control for mitigation of risks from various threats. The assurance measures, both for offline examinations and computer based examinations have been given in detail. This chapter also proposes possible practices for safe and secure computer based examinations.

Chapter 7, *"Proposed Security Processes and Protocols in Digital Assessment"*, thrusts upon comprehensive security framework encompassing various domains of security, such as data security, physical security, application security and network security. It also takes care of various possible breaches in data centre security and suggests hardening measures for firewall, intrusion prevention system (IPS), server-hardening and other security controls. Besides this, this chapter talks about log correlation to trace any possible security incident. Emphasis on encryption and decryption techniques as well as algorithms for QP bundle, result data and report data has been given.

Chapter 8, *"Recommended Information Security Policies"*, speaks about most critical vulnerabilities such as injection flaws, cross-site scripting (XSS), broken-authentication session management, insecure direct object reference, cross-site request forgery, security misconfiguration, insecure cryptographic storage, failure to restrict URL access, insufficient transport layer protection, unvalidated redirects and forwards, malicious file upload and execution, denial of services, no lockout policy, enabled auto-fill feature, enabled password auto-complete feature and no audit trail report for administrative user. In this chapter, the impact of these breaches has been explained and remedial actions have been suggested. This chapter holds prime significance as it gives a comprehensive picture of suggested security protocols, including password policy, database server security, network security and other miscellaneous security. It is a holistic chapter which presents impact of IT security breach at every stage and recommends remedial measures to tackle all possible attacks and breaches.

Chapter 9, *"IT Security for Examination Conducting Body"*, gives a complete protocol of IT security for an exam conducting body, as it will not suffice alone if the process of examination is secure. The examination body conducting computer based examination and/or otherwise should also be secure from IT perspective in all stages and in all departments involved, from planning and conducting of the examinations to the declaration of result. Many hats and hands are involved in planning and conduct of an examination, so they all need to be sensitised for all possible security breaches and threats, and actions to be taken by them, both for prevention and cure, need to be known.

At the end, various valuable references have been given.

CHAPTER 1

PUBLIC EXAMINATIONS GOING ONLINE: A PARADIGM SHIFT

1.1 EXAMINATIONS – WHAT EXACTLY ARE THEY?

In the simplest terms, an examination is an evaluation or a fact-finding exercise. In terms of education, attributes being evaluated are functional skills, knowledge, aptitude, attitudinal skills, IQ, EQ, general awareness, etc. This is accomplished by asking the examinees specific questions, to which the correct answers or responses are already known (except those cases which aim at inquiring the person's opinions on a debatable subject).

1.2 PURPOSE OF EXAMINATIONS

Examinations in secondary schools serve THREE main purposes:

1. First one is the **SELECTION** function, which entails controlling access to secondary schools, courses within the schools and entry to higher educational institutions.

2. Next is the **CERTIFICATION** function, which helps in finding out and reporting what a student has achieved, what he knows, what he is capable of doing and whether he has graduated or not.

3. In addition to these, organizations/institutions often make use of examination results for **ACCOUNTABILITY** purposes, and in particular for evaluating the effectiveness of instruction, for motivating students and teachers to perform well, and for reviewing the efficiency of schools.

1.3 REVIEWING EFFECTIVENESS OF THE EXAMINATION SYSTEMS – THE FACTORS

The following guiding questions are intended to assist planners and managers in reviewing their examination system(s). The questions are based on the key areas for improvement, which have been identified in the preceding section.

*Note**:** The term 'authority' is used to refer to the organization responsible for examinations.*

1.3.1 ASSURING INTEGRITY OF ASSESSMENTS

1. Has a risk assessment of examination security and supervision been carried out? Have areas of vulnerability been identified and action taken to minimize those risks?
2. Does the authority have the backing of relevant regulations, legislation and law enforcement bodies to enable prompt action in cases of suspected malpractice; are there appropriate penalties for offenders?
3. Does the authority have access to high-level, independent legal advice and assistance in handling complaints and dealing with the cases of malpractice?

1.3.2 REDUCING EXAMINATION PRESSURES

1. Is there a scope for eliminating high-stakes examinations at the end of primary school and for providing greater access to upper secondary and higher education?

2. Is there a scope for incorporating school-based assessments into the examination process and for allowing them to contribute to a significant proportion of final assessments?

3. Are there second-chance opportunities and alternative routes for students to gain entry into higher education?

1.3.3 CATERING FOR AN EXPANDING AND MORE DIVERSE STUDENT CANDIDATURE

1. Do the standards allow majority of the students, who are diligent in their studies, to achieve a ‘passing’ grade, while providing the highest level of challenge to the most abled?

2. Are there rigorous processes for maintaining standards over time?

3. Does the authority use a combination of both norm-referenced and standards-referenced approaches for reporting results?

4. Are examinations offered for a range of subjects, including applied and vocationally oriented subjects?

5. Is there a qualification framework that confers status to applied and vocationally oriented subjects and provides pathways to work and further study?

1.3.4 ASSESSING A WIDER RANGE OF CURRICULAR OBJECTIVES

1. Is there a close alignment between the curriculum and the examinations?

2. Is there a systematic attempt to assess important outcomes that cannot readily be assessed in written examinations, including use of new information technologies?
3. Are effective moderation procedures in place to enable assessment of these outcomes to contribute significantly to overall examination results?

1.3.5 ASSURING QUALITY AND GAINING PUBLIC CONFIDENCE

1. Is adequate attention given to the recruitment and training of all examination personnel, especially part-time staff and teachers in schools who are assigned examination duties?
2. Is there a culture in which all assume responsibility for identifying weaknesses and improving quality of examinations?
3. Is the system of audit and internal controls efficient in execution?
4. Have examination processes been automated to improve efficiency and to eliminate human error?
5. Are there fair and transparent appeal processes in place to handle complaints and to compensate for those whose performance has been adversely affected through no fault of their own?

1.4 THE DRIVERS BEHIND THE GLOBAL MOVE TOWARDS ONLINE EXAMINATIONS

Based on the questions identified in the last section, here is a factor-by-factor comparative analysis of online and offline examination systems, and it establishes an understanding of the reason for the move towards online examination systems, as evident worldwide today.

Table 1.1: Factor Analysis in Offline and Online Examinations

Sr. No.	Factor	Offline vs. Online Examination
1.	Risk assessment, Vulnerabilities identification Taking actions to mitigate identified risks	Simpler to undertake for online examination than offline.
2.	Ability for prompt action in cases of suspected malpractice	Malpractice vectors are reduced and detection is much easier in online examinations.
3.	Scope for incorporating school-based assessments to contribute to a significant proportion in the final examinations	Easier to implement school based evaluation when an online universal exam exists to automatically calibrate and normalize the results of school based evaluations.
4.	Second-chance opportunities and alternative routes for students to gain entry into higher education	Provision of second (and potentially, subsequent) attempt(s) is much speedier and more cost effective to implement if the examination is automated.
5.	Processes for maintaining standards over time	Easier to implement for an online system (due to capability for centralized control).
6.	Use of both norm-referenced and standards-referenced approaches for reporting results	Result reporting is completely flexible and may be adapted even to vigorously evolving norms and standards in case of online system.

Sr. No.	Factor	Offline vs. Online Examination
7.	Important assessment outcomes that cannot readily be assessed in written examinations, including the use of new information technologies	While online or written examinations can generally not be used to assess practical skills and aptitude, but this is possible to some extent through simulation in case of online examinations.
8.	Effective moderation procedures to enable assessment of these outcomes to contribute significantly to overall examination results	Much more effectively implemented when the system is online (and therefore, automated and with capability for centralized control)
9.	Attention towards the recruitment and training of all examination personnel, especially part-time staff and teachers in schools assigned examination duties	Becomes a critical requirement where the examination is going to be online.
10.	Culture of collective responsibility for identifying weaknesses and improving quality	Automation of a system with appropriate logging eliminates the requirement for people to voluntarily accept responsibility, by making specific responsibility and ownership assignments, and making detailed evidences available.
11.	Effective audit system Internal controls	Becomes an essential requirement if any major examination system is automated and online.
12.	Improving efficiency and eliminating human error	Automation is the need of the hour.

Sr. No.	Factor	Offline vs. Online Examination
13.	Fair and transparent appeal processes to handle complaints and to compensate for those whose performance has been adversely affected through no fault of their own	Like in the case of provision of second attempt, this is more cost-effectively implemented where the examination system is automated and centralized.

CHAPTER 2

CHALLENGES OF OFFLINE EXAMINATIONS AND NEED FOR COMPUTER BASED EXAMINATIONS

Over the past few years, the advent of new technology and yet more discoveries in medical sciences has not only increased the level of the average age of an Indian, but has also been successful in creating a phenomenon, what we call as ‘population explosion’ in our country. It has thus evidently become important for the government to ensure quality education for the citizens, and to educate as many as possible.

Which technique for educating a populous country as India herself is *correct?* What procedures in the education system are *right* for India? Answers to these questions may be different for different people, but what is best *suited* for India has to be implied. It has been a debatable topic for years for the authorities, public, as well as the media in its various forms, and still remains. Definitely, the method agreed upon will not be flawless, and it is here that the required security related precautions and solutions come into play.

Quality of education system does not only depend on the curriculum being followed, and with what efficiency is it being taught, but also on making sure that the students are grasping all the teachings accurately, and in time. Examinations conducted serve this purpose. Examinations having such an important role in building an excellent work force for the nation, it is necessary that their conduct is carried flawlessly for them to be called *successful.*

2.1 CHALLENGES FACED DURING THE CONDUCT OF EXAMINATIONS (OFFLINE)

- Unfair means used by students
- Less number of students being qualified
- Dissimilarities in handling the transcripts
- Leakage of question papers
- Evaluation being delayed
- Process/declaration of result being delayed
- Marks being manipulated
- Improper conduct of re-evaluations

2.2 SUMMARY FINDINGS

2.2.1 GROWING GLOBAL PUBLIC EXAM MARKET FACES MANY CHALLENGES

New public examinations are coming up very swiftly across the globe. It has been estimated that over a billion exams in number are conducted for courses under higher studies, management of which is a crucial aspect in the functioning of an educational system. Undoubtedly, the system faces many challenges for the same. These challenges have been briefly discussed below:

1. **Administrative Challenges**

- **Registration:** The universities/colleges need to distribute the application forms as well as the prospectuses/information brochures to numerous different locations, and that too within a limited time period. Also, at the time of entrance, generation of hall tickets and then further ensuring that each candidate who has to appear for the examination must have received his/her hall ticket, is another challenge constrained by time.
- **Security:** One of the most crucial tasks of the administration is to make sure that the question papers and other confidential documents related to the

examination process are well-secured. Other aspects on which there is a need to keep an eye are the unfair means, such as impersonation, cheating by the examinee, involvement of examiners in such malpractices, paper leakages, etc.

- **Valuation and Scoring:** It is important that the process of evaluation goes unhindered and without any mistake, as the future of thousands of students may depend on the result of the examination which they had taken. This task includes careful handling of the answer sheets, sending them across different places to be checked by different examiners and simultaneously ensuring that no answer sheet is lost or misplaced. Once they have been received by the examiners, they must make sure that they check these very carefully and in a fair manner. Only then will the evaluation be called successful.
- **Declaration of Results:** The results which are published need to be accurate and should be out soon after the examination. This task is very tedious as all the institutes try their best to declare the result of numerous students as soon as possible. After all, delay of results may cause further delays in the schedule of functioning of the institutes as well as cause problems even for the students. It is also needed to be checked that there are no manipulations made to the final result, intentionally or unintentionally.
- **Exam Logistics:** During the conduct of examinations, especially for small universities/colleges, management of all the examination venues and the staff there is a difficult task. Hence, often, many errors and confusions get created for individual students.

2. Exam Design Challenges

- **Level of Difficulty:** For all those students who take the examinations related to the same course for the same semester/year, the level of difficulty of the examination paper provided to all of them should be uniform, so that the judgement made about these students on the basis of these examinations is fair and just. Many times, different codes of paper are given to the students for the same examination and then complaints emerge, stating that some question papers were easier than the other ones. This needs to be eliminated by making the faculty, which designs the question paper, choose very wisely the questions of the same level for all the codes of paper.

- **Importance of Internal and Informal Testing**

One thing that the teachers should remember is that the in-course examinations are as important as the final examinations, because they help assessing the student from time to time and are the only means of improving them. Even though these examinations do not count for the final scores, but they are very important for the development of the students. Hence the teachers should be meticulous in testing the students through the internal examinations and should be as serious about them as they are for the final ones.

- **Designing for Mass Testing**

Most of the times, the questions included in the entrance exams are objective type, which fail to test the ability of the candidates to write well and fail to check how creative they are. This is because a lot of time will be required for evaluation and processing of examinations including subjective type answers. Hence, this challenge seems to be unavoidable, keeping in mind the limitation of the time period.

3. Resource Allocation Challenges

- **Budgetary Constraints**

Those universities which are funded publicly often have hard times financially. The examination fees is usually largely subsidised, and hence the universities are not left with much money to maintain the process of examination. Hence, it also becomes difficult to improve on any technique or upgrade some system, as it would require quite an amount of money.

- **Availability of Qualified Examiners**

It is important for the universities to have not only a large number of examiners, but they should also be well qualified. If there are limited number of examiners, then the answer papers will take a lot of time to get corrected and since the burden of correcting so many exam papers will fall on a few number of examiners, then it might also deteriorate the efficiency with which the answers will get corrected. Hence the final result may not be accurate.

2.2.2 ONLINE EXAMINATIONS

E-Assessment, or as we call it, online assessment, is believed to be a technique of a quicker, safer and more transparent assessment. With the evolution of education system, the method of assessment also needs to develop with it. Use of technology, hence, seems to be a probable solution for this problem.

- **Better Progress in Evaluation through the Use of Technology-** E-Assessment has improved with the access to Internet and technology, which are used for process of the same. Also, with further improvement in various online applications and software, the procedure of assessment will be able to get completed more efficiently.
- **Various Uses of E-Assessments-** Many online quizzes, discussion forums etc. are assessed online by many institutes and organisations. This method is yet to be adopted by many more. Distance and open education is an applicable field for online assessment. Summative online assessment is taking some time to be accepted by various examination conducting boards due to problems of authenticity, accessibility and security of the answer sheets. But a new system, called the Online Screen Marking, has made this problem diminish. In this system, the answer sheets of the students are scanned and made anonymous to the evaluators. These evaluators, situated at different locations, are able to check the answers online, and the final score is summed up by the computer.
- **Helps in Dealing with Disruptions –**The on-going curriculum schedule of a university may get interfered due to some problems in the exam processes, and hence some procedures, processes or classes may get delayed. This can be minimised by bringing automation in the exam procedure. This will thereby reduce the involvement of the administrative staff, and the tasks can be carried out according to the schedule.

2.2.3 TECHNOLOGY IN EXAMS

According to recent reports, majority of current universities and institutions in India believe that the role of IT plays an important role in the conduct of examination, by benefitting in various ways such as reducing geographical constraints for any file/document transfer, eliminating human error as much as possible etc. This topic hence covers how technology is advantageous for Indian education system.

Many potential rewards for Indian educational institutions

Following are some benefits that technology provides for exam management:

- **Quicker Processes and Better Assessments**

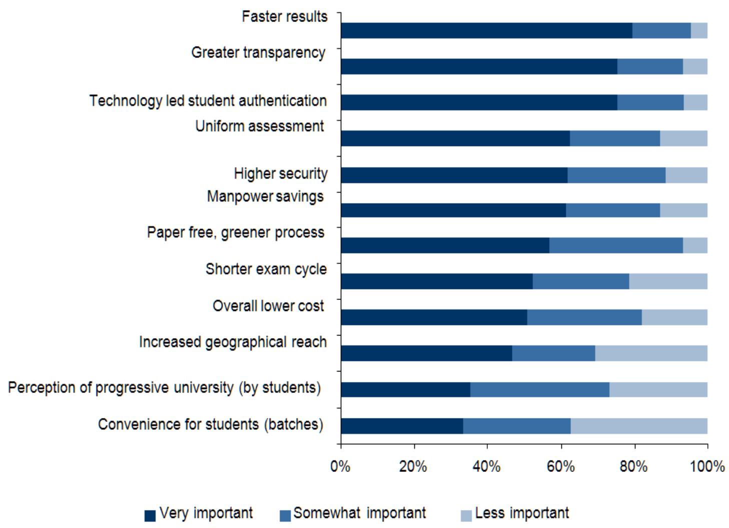
Use of technology by the institutions makes the ongoing processes to get completed at a faster rate, as majority of operations are carried out on machines. This definitely leads to better as well as more accurate results of the examinations.

- **Efficient Transparency is introduced**

With the use of online attendance or biometric attendance for examinations, greater transparency is created in the system amongst all the different institutes/boards/organisations as well as the students who are involved in the process. This helps in increasing students' confidence and satisfaction in the system.

- **Costs are Reduced**

Since use of IT in the examination process leads to reduction in the workforce, reduced use of papers, faster procedures etc., quite an amount of money is saved. Savings of money may not be a necessity for many universities, but the money saved here can be used in other fields, where it is probably needed more.



Source: ValueNotes Research

Fig 2.1: Online Examinations – Many Potential Rewards

- **Strengthened Security of Examinations**

Fear of malpractices during the examinations by the examinees/examiners/ invigilators is always present in the examination conducting body. A better check can be kept for this only through the use of technology, such as CCTV surveillance, biometrics etc.

- **Tasks Made Automatic**

Use of machines makes quite a number of tasks during the conduct of an examination automatic, hence resulting in reduced manual labour as well as cost. This also reduces the pressure on universities/colleges/schools for carrying out various tasks, and hence there remains no need for a large skilled staff to carry out all the operations.

- **Widened Reach**

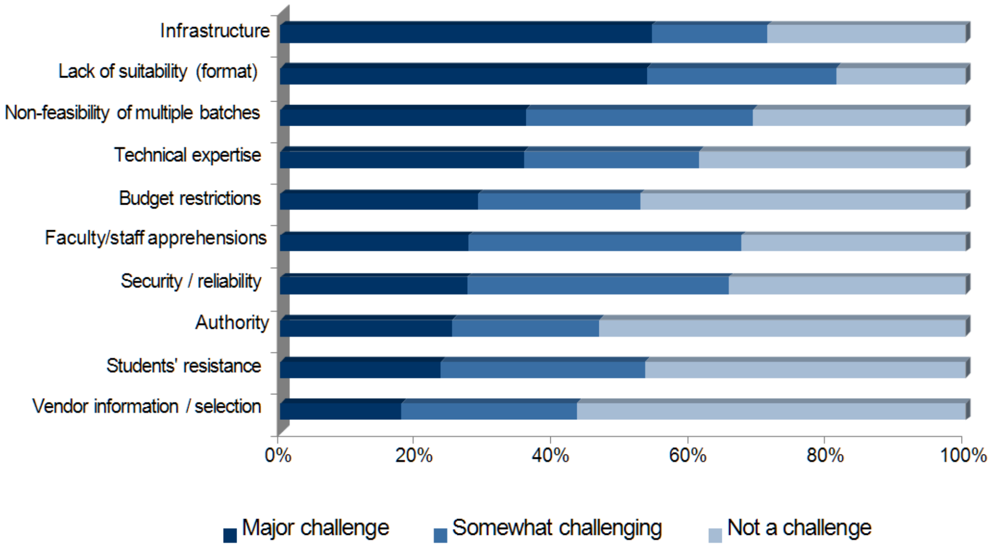
Using online procedures, different educational bodies are able to reach out to various students across a wide geographical area, and hence a lot of students are able to get involved in the courses/examinations of far-off universities. This especially comes in handy for the students pursuing distance education.

- **Saving Time**

Making admission forms or examinations available online also saves students' time as they don't need to go to various locations, wasting time in travelling or stand in long queues.

Infrastructure: the main challenge for Indian Higher Education System

Many challenges are faced by the Indian education system, solutions to which are needed to be sought. These challenges not only are related to the infrastructure and the training skills that will be required, but are also caused by the resistance to the acceptance of use of IT by the universities, institutes, students and staff:



Source: ValueNotes Research

Fig 2.2: Challenges to Online Exams

- **More Trust on Conventional Methods**

Many students and teachers experience resistance as a challenge and that since their current processes are working fine, they would prefer to retain that system. Since not much is known about creation of online exams, format and adaptability also came up as concerns. Majority of the respondents express the opinion that the current format of exams gives them more choices and they did not believe that online assessment would be able to handle it.

- **Lack of Infrastructure**

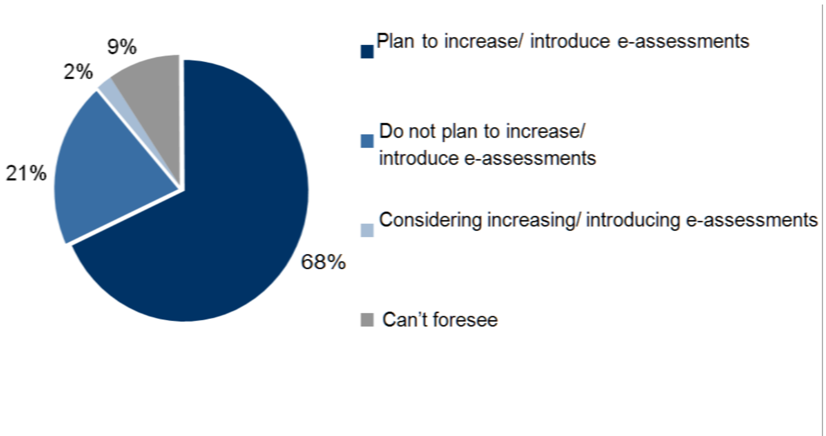
Making assessment online would require quite a number of computers and a reliable source of internet connection to be installed in the institutions. India is yet to develop to that extent to be able to afford this to happen for the conduct of all exams. In remote and rural areas, people are not yet aware of such a possibility.

- **Lack of Knowledge**

Not everyone would be aware of how to carry out online assessment, and hence the staff will have to be trained so as to ensure that no technical failure occurs during the assessment.

Online exams in India - future plans

More than fifty percent institutes believe that use of technology in universities and institutions can not only ease the procedure of conduct of examinations, but also make the process more efficient. This would, although, mean that they would have to invest in proper infrastructure and carry out experiments, mock runs and proper training of the staff to get well acquainted with this type of procedure. But the results of this investment would outdo the cost of it.

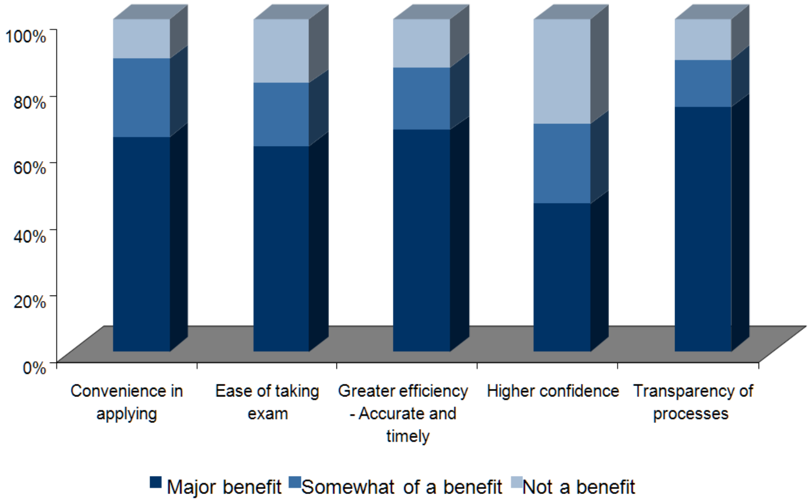


Source: ValueNotes Research

Fig 2.3: Online Exams as a part of Indian Higher Education's Plan

Perceived/expected benefits and issues

Even though a small proportion of the students are not aware of the method of online examinations and their further assessment, but studies have shown that such students have faith in the fact that automation of tasks in the examination procedure would result in more benefits to both students and institutions than the difficulties it would cause.



Source: ValueNotes Research

Fig 2.4: Perceived/ Expected Benefits of Online Exams

From the graph, it is clear that the major benefit, as felt by the most people, is transparency of processes, which is succeeded by greater efficiency. For online application/registration, the convenience acquired is about 32% more. But it can’t be neglected that the students have more confidence in conventional method of examinations as compared to the online system, because most of the students are attending various coaching centres for preparation for competitive examinations, which usually sell fear about computer based examinations. They generally prepare students based on the traditional OMR based examination system.

2.3 IMPORTANCE OF ASSESSMENT IN EXAM MANAGEMENT

2.3.1 INTRODUCTION

Educational institutions have a variety of functions, ranging from teaching, research, cultivating minds to enhancing social development. Hence, it is very important for the administration to be very strong and well disciplined. With the inclusion of various colleges, departments and communities, the administrative tasks of the universities become very challenging. Hence, they need to be carried out with extensive care for the institute to operate properly.

Out of various activities such as policy making, forming a suitable curriculum or provision of a uniform course, exam management is one of the crucial tasks of any educational body. The procedure of an examination includes:

- Registration of candidates
- Exam fee management
- Hall ticket generation
- Question bank management
- Question paper generation
- Evaluation
- Processing and publication of results
- Re-evaluation
- Re-tests

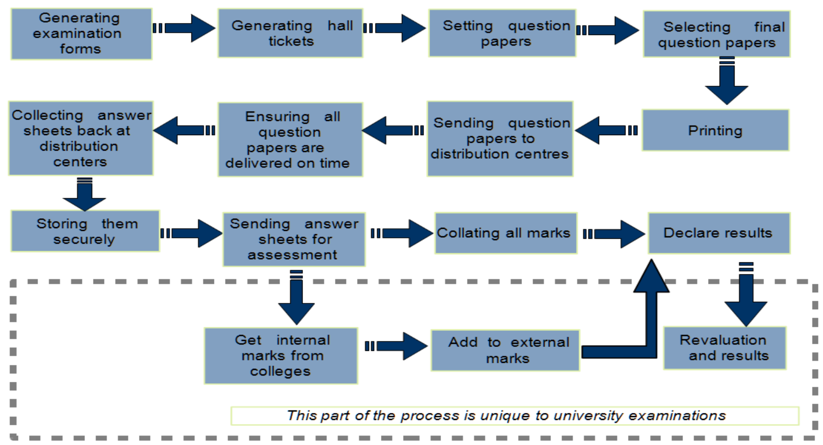
To carry out these processes, the administration takes care of:

- Conducting the examinations
- Keeping an account of examination expenditures
- Tracking academic calendars
- Scheduling examinations
- Managing a medium of communication among different departments, colleges and even the students.

Some universities conduct entrance examinations exclusively for entry in their courses, while some take students on the basis of their performance in some centralised examination (state/national/international level).

2.3.2 TYPICAL EXAM PROCESS

Conduction of an examination is a lengthy and tedious process, which includes a lot of administrative tasks at each tier. All the schools, colleges and universities have their own steps of procedure of an exam as per their convenience and necessity. The result of the conduct of the exam depends on how adequately and carefully the process was managed by the administrative authorities of the institutes. Hence, it is not just the procedure but also the way in which it was managed decides how fruitful the outcome would be of any task carried out, in this case the task being of conducting examinations at all levels. Following is a chart which depicts a typical exam process, which is broadly followed by almost all the universities and colleges:


Generating examination forms
Generating hall tickets
Setting question papers
Selecting final question papers
Printing
Sending question papers to distribution centres
Ensuring all question papers are delivered on time
Collecting answer sheets back at distribution centers
Storing them securely
Sending answer sheets for assessment
Collating all marks
Declare results
Get internal marks from colleges
Add to external marks
Revaluation and results
This part of the process is unique to university examinations

Source: ValueNotes Research

Fig 2.5: Typical Exam Process

It is pretty obvious from the chart that the process of an examination is very time consuming. Even though some experts feel that some steps of this process can be replaced by some shortcuts or eliminated, there will be more harm than good to the system by doing so. Also, it can be easily analysed that the real assessment constitutes about 20 per cent of the procedure.

2.3.3 TYPES OF EXAMS AND ASSESSMENT TOOLS

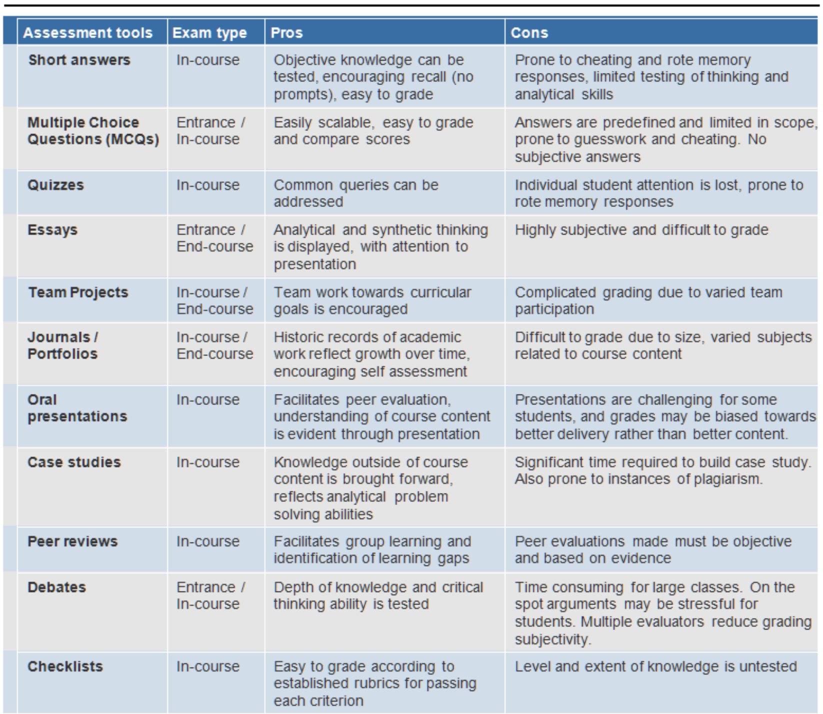
Various ways of assessment are used by the institutes, which in turn include a lot of steps. This assessment, is based on a number of types of examinations, and this helps in grading or ranking the students. These types of examinations are listed below:

1. **Entrance Exams:** Test the capability and potential of the students on the required standards for getting admitted into the institutions/courses for which the candidates are applying. These are either conducted by the institutions themselves, or by a national/state examination board.

2. **Internal Exams (or In-course Exams):** Help in keeping a regular check on the knowledge of the students, and give them scope for further improvement. Such exams may consist of case studies, presentations, tests with short answers, classroom quizzes, etc.

3. **Final Exams (or End-course Exams):** Act as final conclusion, judging what the student has finally learnt from the course(s) opted. These exams are taken by the students at the end of the semester/year.

The type of assessment tools used over the globe are tabulated as following:



Assessment tools	Exam type	Pros	Cons
Short answers	In-course	Objective knowledge can be tested, encouraging recall (no prompts), easy to grade	Prone to cheating and rote memory responses, limited testing of thinking and analytical skills
Multiple Choice Questions (MCQs)	Entrance / In-course	Easily scalable, easy to grade and compare scores	Answers are predefined and limited in scope, prone to guesswork and cheating. No subjective answers
Quizzes	In-course	Common queries can be addressed	Individual student attention is lost, prone to rote memory responses
Essays	Entrance / End-course	Analytical and synthetic thinking is displayed, with attention to presentation	Highly subjective and difficult to grade
Team Projects	In-course / End-course	Team work towards curricular goals is encouraged	Complicated grading due to varied team participation
Journals / Portfolios	In-course / End-course	Historic records of academic work reflect growth over time, encouraging self assessment	Difficult to grade due to size, varied subjects related to course content
Oral presentations	In-course	Facilitates peer evaluation, understanding of course content is evident through presentation	Presentations are challenging for some students, and grades may be biased towards better delivery rather than better content.
Case studies	In-course	Knowledge outside of course content is brought forward, reflects analytical problem solving abilities	Significant time required to build case study. Also prone to instances of plagiarism.
Peer reviews	In-course	Facilitates group learning and identification of learning gaps	Peer evaluations made must be objective and based on evidence
Debates	Entrance / In-course	Depth of knowledge and critical thinking ability is tested	Time consuming for large classes. On the spot arguments may be stressful for students. Multiple evaluators reduce grading subjectivity.
Checklists	In-course	Easy to grade according to established rubrics for passing each criterion	Level and extent of knowledge is untested

Source: ValueNotes Research

Fig 2.6: Types of Assessment Tools

Over the past few years, new means of assessments have been added in the curriculum for various courses, which include one-word answers, fill in the blanks, matching lists, multiple choice questions (MCQs), and like. It became a matter of concern for some that the process of learning for the students is now becoming less of comprehensive type. But the new innovations, such as projects, field works, self-assessments, peer assessments, portfolio, etc., have rather proved to embellish the learning process.

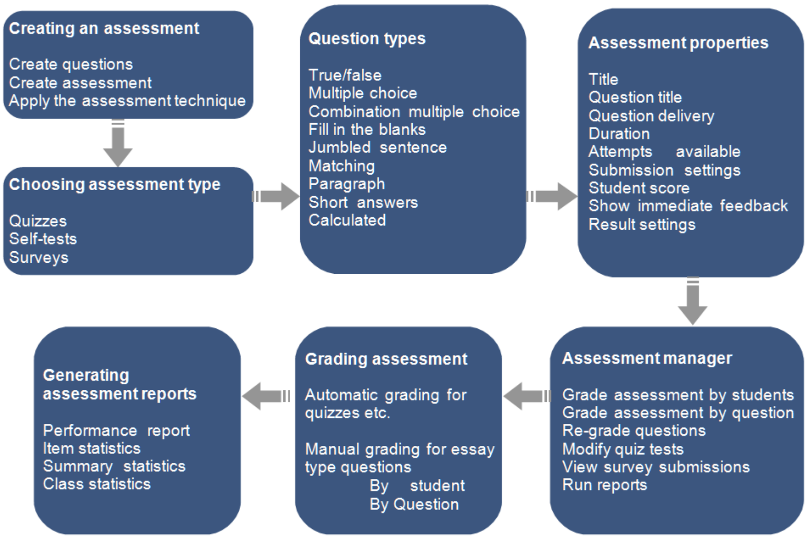
2.4. GLOBAL TRENDS IN ONLINE ASSESSMENT

The world today has been revolutionised with advent of the Internet. And it is a well-established fact that the Internet has emerged as an important source of learning for both students and teachers. People have now become more aware about various subjects, and hence the willingness to experiment and explore has also enhanced. In fact, now, even the social networking sites have emerged as tools for teaching people, as they act as a common platform for the people across the globe to share the ideas and facts they know with others. According to estimation on an average, users spend around 26.5 hours per week on the internet, and it has been proved how convenient it is to carry out some procedures online. This is the reason why some universities prefer to do their assessment online.

2.4.1 ONLINE ASSESSMENT: INCREASING SCOPE

Gone are those days when assessment was meant to check what a person had learnt from the pursued course. Assessing a child now means not only testing his memory, but also his application of knowledge, thought process, innovative bent of mind, ability to process any information and other aspects such as creativity, team work, spirit to take a challenge and ability to work even in stressful situations. Assessment, in itself, is a teaching process as it makes the child realise where he was wrong, and what skills/qualities he lacks. Once the flaws in a child are known, more attention is paid towards the required areas of teaching for that child.

A typical assessment process in the form of a flow-chart is given below:



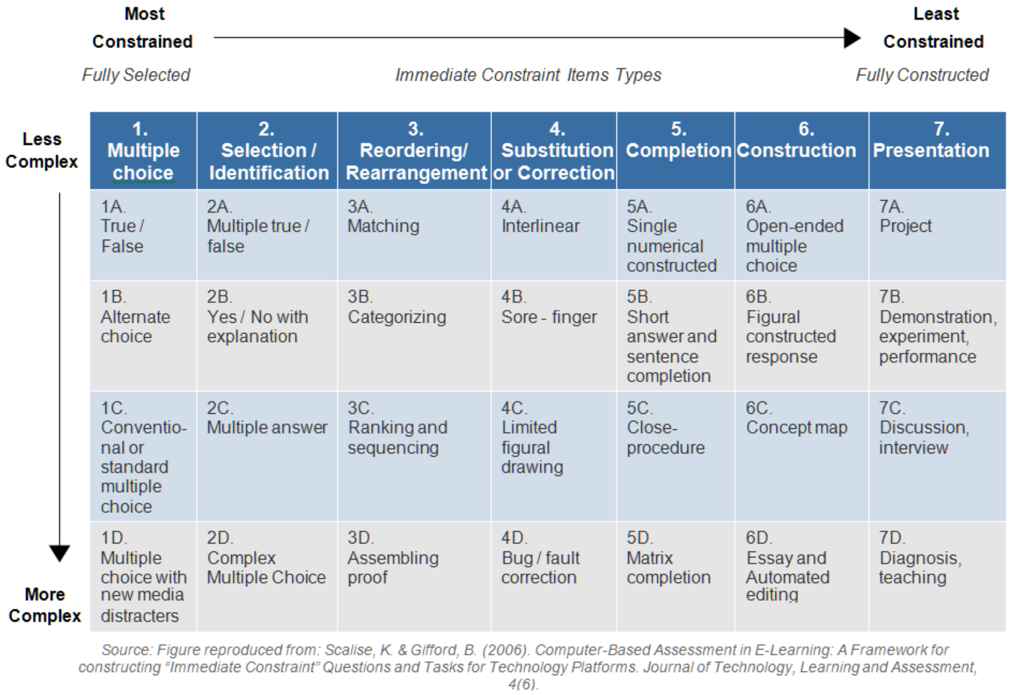
Source: Figure constructed with data from Macquarie University website

Fig 2.7: Online Assessment Process

2.4.2 ONLINE ASSESSMENT: INCREASING ACCEPTANCE

Online examinations include various types of tests, such as MCQs, true or false, matching the columns, fill in the blanks, and now new additions, such as rearrangement of statements or pictures, labelling the diagrams, drag and drop questions and even essay writing, have been made to them. It has been seen that such mechanisms are not only more effective in the learning process but are also easy to adopt. Such an interaction of students with computers for assessment also improves their readiness and willingness to appear for a test. There may occur some problems while teaching the students how to go about such assessment, but once learnt by them, online assessment can prove to be fruitful for both students as well as the universities.

Following is a table which concludes different types of tasks that are generally included in an online exam, and it highlights their level of constraints and complexity.



Most Constrained → Least Constrained

Fully Selected | *Immediate Constraint Items Types* | *Fully Constructed*

Less Complex ↓ More Complex

1. Multiple choice	2. Selection / Identification	3. Reordering/ Rearrangement	4. Substitution or Correction	5. Completion	6. Construction	7. Presentation
1A. True / False	2A. Multiple true / false	3A. Matching	4A. Interlinear	5A. Single numerical constructed	6A. Open-ended multiple choice	7A. Project
1B. Alternate choice	2B. Yes / No with explanation	3B. Categorizing	4B. Sore - finger	5B. Short answer and sentence completion	6B. Figural constructed response	7B. Demonstration, experiment, performance
1C. Conventio-nal or standard multiple choice	2C. Multiple answer	3C. Ranking and sequencing	4C. Limited figural drawing	5C. Close-procedure	6C. Concept map	7C. Discussion, interview
1D. Multiple choice with new media distracters	2D. Complex Multiple Choice	3D. Assembling proof	4D. Bug / fault correction	5D. Matrix completion	6D. Essay and Automated editing	7D. Diagnosis, teaching

Source: Figure reproduced from: Scalise, K. & Gifford, B. (2006). Computer-Based Assessment in E-Learning: A Framework for constructing "Immediate Constraint" Questions and Tasks for Technology Platforms. Journal of Technology, Learning and Assessment, 4(6).

Fig 2.8: Online Assessment – Questions and Tasks

2.4.3 DIVERSE APPLICATIONS OF ONLINE ASSESSMENT

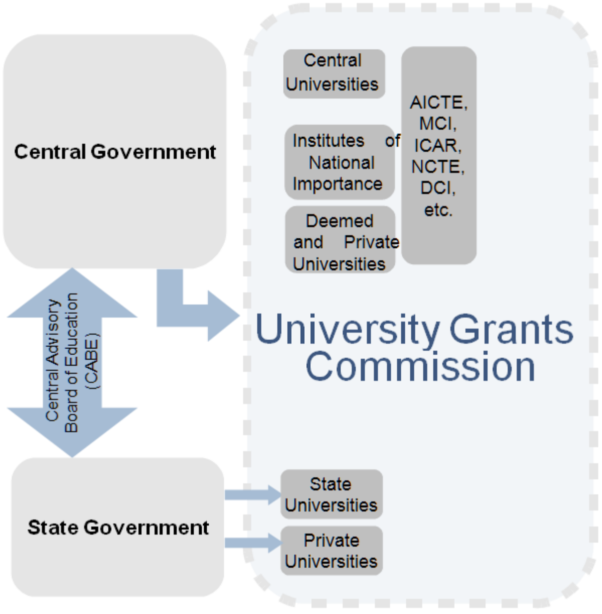
- Online assessments usually include questions in the form of quizzes or discussion forums. Storing all the questions online will make the quiz-making software choose randomly a number of questions and prepare them in the form of a test. This will eliminate the need of the faculty to select various questions and make a test out of them, and hence a lot of time can be saved.
- The online assessment of end-course examinations, which are generally summative in nature, is very slowly being adopted by the universities, as there are risks related to security, authentication and access. But many institutes are adopting the acceptance of online submission of assignments by the students. Almost 50% of the assessment process includes administrative tasks, and with the penetration of machines and IT in the examination system, the workload over the administrators will reduce immensely.
- Distance learning and open learning are now globally being aided by IT, as the online courses and examinations provide the 'anytime, anywhere' benefit to the students.

2.5. INDIAN HIGHER EDUCATION: AN OVERVIEW

2.5.1 INDIAN HIGHER EDUCATION: A SNAPSHOT

There are definitely numerous suggestions for bringing changes in the current Indian higher education. With the pressure from the side of the general public as well as the media, this education system is bound to get amended at various levels.

Our current Indian education system stands at the third position for the largest education systems in the world. It has been depicted in the following chart in a summarised way:



Central Government
Central Advisory Board of Education (CABE)
State Government
Central Universities
Institutes of National Importance
Deemed and Private Universities
AICTE, MCI, ICAR, NCTE, DCI, etc.
University Grants Commission
State Universities
Private Universities

Source: Department of Higher Education, Government of India

Fig 2.9: Structure and Size – Indian Higher Education

2.5.2 TACKLING EXAM CHALLENGES THROUGH TECHNOLOGY

India being such a diverse nation, having students as well as examiners from so many regions, does have a major challenge of acquiring adequate amount of skilled and qualified examiners. Although our developing nation has infrastructure and technology issues, but penetration of IT in assessment, as believed, can definitely help a lot in the examination process. From the past five years, universities such as BITS and Manipal University in India have been conducting exams online and, hence, prove what a success online assessment can be. There are many other universities and boards which have started adopting the e-assessment methodology.

Increase in experiments to increase assessment effectiveness

- **Making amends in assessment procedures**

All the examination conducting bodies, whether at central, state or university level, never cease to devise the best method of assessment possible and suitable for the students of a nation. Hence, it was seen that over the years, assessment of a student has transformed to a core subjective type to a practical, analytical and subjective type.

- **Online and Offline together**

It is not necessary for an institution to conduct purely online or purely offline examinations. Depending on the type of assessment, appropriate format, i.e., online or offline, can be chosen. Sometimes, options are also offered to the students, whether they would like to take one particular examination in a pen-and-paper mode or an online mode.

Managing with less resources

- **Tasks and procedures being distributed**

Some bodies are trying to distribute the various steps of assessment amongst different tiers. This helps in easing of the exam procedure for all. Hence, not the same examination body conducts examination at all the levels.

- **Less burden on the Administration**

As has been discussed before, use of IT in the assessment process reduces a lot of pressure on the administrators. Since many tasks are then carried out by the machines, workload, manual labour and other costs are also reduced.

Rising importance to security and controlling malpractices

- **Technology strengthens security**

Using various technical measures such as bar-coding, assessing answers through optical mark readers etc., security has been intensified for the examination procedure. This reduces the ability of the children to cheat or perform any other unfair practice.

CHAPTER 3

STANDARD OPERATING PROCEDURES FOR COMPUTER BASED EXAMINATIONS

3.1 LIST OF ABBREVIATIONS

BCP	Business Continuity Plan
CBE	Computer Based Examination
DHCP	Dynamic Host Configuration Protocol
DR	Disaster Recovery
DC	Data Centre
EC	Exam Centre
RC	Registration Centre
SP	Service Provider
IPS	Intrusion Prevention System
LAN	Local Area Network
OTBS	Online Test Booking System
PEB	Public Examination Body
RTO	Recovery Time Objective
RPO	Recovery Point Objective (RPO)
SME	Subject Matter Expert
SOP	Standard Operating Procedures

3.2 INTRODUCTION

A CBE Service Provider facilitates Public Examination Body in conducting CBE. The main stakeholders would involve:

- The Public Examination Body
- CBE Service Provider
- Registered Candidates

The end to end process can be divided into:

- Pre-examination Planning
- Examination Delivery
- Post-Examination

3.3 ONLINE (CBE) SCHEDULE DETAILS

The following needs to be planned carefully

- **Date –** The examination dates are to be planned well in advance
- **Location**
- **Session Type**
- **Session Timing**
- **Examination Duration**
- **Examination Format**
- **Medium used for examination**
- **Internet Connectivity** - Required only by the server for starting the drive and uploading of results. During Computer Based Examinations, candidates will connect to the server which is connected through a LAN.

3.4 ASSUMPTIONS

The PEB will own the following activities:

- Communicate the name and contact details of Point of Contact to CBE-SP
- To provide guidelines for the conduct of CBE
- Finalization of Test Schedule
- Candidate Registration (at the time of submission of application)
- To provide the list of applicants in the required data template
- Admit card generation
- Creation of Question Paper(s) in a secured environment
- Defining the scoring pattern
    - marks for each response
    - negative markings (if any)
- Provide the list of observers
- Define the guidelines for observers

3.5 THE CBE OPERATING PROCEDURE FRAMEWORK

The framework is defined below:

Table 3.1: Application Security Life Cycle

Pre-Examination Planning	**Examination Day**	**Post Examination**
Project Kick Off Meeting	Test Centre Readiness	Handover score in agreed format
Finalization of Test Centres	Candidate Registration – On the Day of Test	Share Feedback
Test Centre Staff - Identification & Management	Conduct Examination	Upload CBE Question Paper in Website
Test Centre Readiness – Planning		
Upload Candidate Data in the system		
Helpdesk Support Activation		
Defining the Rule Engine and creation of Question Bank.		
Upload Question Paper in a secured environment		

3.6 PRE-EXAMINATION PLANNING

3.6.1 PROJECT KICK-OFF MEETING

Purpose

To initiate the planning session for conduct of Online Examination /CBE.

Scope

This procedure will be followed to initiate and conduct a Project Kick-Off Meeting.

Responsibilities

Activity	**Responsibility**
• Identify all the relevant stakeholders	CBE-SP
• Schedule a Project Kick-Off Meeting	CBE-SP
• Communicate the list of deliverables to all the stakeholders	CBE-SP
• Identify the associated risks and arrive at the Risk Management Plan	CBE-SP
• Identify the support required from external/third parties (if any)	CBE-SP

Input

Award of contract to the Service Provider by the Public Examination Body.

Procedure

- The Service Provider will:
  - ➢ Identify all the relevant stakeholders who need to be involved in the successful completion of Online Examination/CBE.

- ➢ Schedule a Project Kick-off meeting and communicate to the corresponding representative from each stakeholder group.
- ➢ Communicate the following during the Kick-off meeting
    - ▪ Scope of the Engagement
    - ▪ Project Plan
    - ▪ Key Deliverables
    - ▪ Governance Model
    - ▪ Communication & Escalation Mechanism
- ➢ Discuss with the Stakeholder representatives and understand the various risks involved in every stage of the project.
- ➢ Arrive at the Risk Management Plan with descriptive Mitigation & Contingency Plans
- ➢ Identify the support required from external/third parties (if any)

Output

- Project Charter detailing Project Scope, Timelines, Expected Deliverables
- Project Governance Model
- Project Communication & Escalation Plan
- Project Risk Management Plan

3.6.2 FINALISATION OF TEST CENTRES

Purpose

To finalize and publish the list of test centres which can host the Online examination/CBE.

Scope

This procedure will be followed to scrutinize, finalize and publish the test centres which will host the Online examination/CBE.

Responsibilities

Activity: Responsibility

- Arrive at a list of potential centres (within the specified cities) which can host the Online examination: CBE-SP
- Visit the facility and conduct a high-level audit of the facilities available: CBE-SP
- Use the Test Centre Checklist in updating the details at each test centre: CBE-SP
- Perform LANSCAPing (Capacity Estimation) at the Shortlisted Test Centres: CBE-SP
- Certify the desktops that are eligible to host online examination: CBE-SP
- Certify the centre to host online examination: CBE-SP
- Share the list of certified centres with PEB: CBE-SP
- Publish the final list of test centres which will host online examination: PEB

Input

Decision to conduct the Online examination/CBE within specified cities, with the finalized number of candidates in each of the cities.

Procedure

- Service Provider team will
  - arrive at the list of potential centres (within the specified cities) which can host online examination,
  - arrive at the list of potential desktops that can be used for online examination within those centres,
  - include 20% above threshold value in the required number of desktops in addition to the number of registered candidates within that city,
  - visit the facility and conduct a high-level audit of the facilities available,
  - conduct LANscape test to ascertain the suitability of the potential desktops,
  - certify the desktops that are eligible in each centre to host online examination,
  - certify the centre to host online examination,
  - sign an agreement with the test centre (infrastructure provider) for conducting the online examination as per the stipulated time, and
  - share the list of certified centres with the Examining Body along with the desktop capacity.

- Examining Body team
  - in consultation with the Service Provider, will then finalize the list of test centres which will host online examination, and
  - will publish the above details on the website.

Output

- Finalized List of test centres (along with the desktop capacity) which will host the Online examination.

3.6.3 TEST CENTRE STAFF - IDENTIFICATION & MANAGEMENT

Purpose

To identify the Test Centre staff who will be involved in conducting the Online examination and communicate the corresponding roles, responsibilities and guidelines related to every stakeholder.

Scope

This procedure will be followed to identify and manage Test Centre Staff, who will be involved in conducting the Online Examination.

Responsibilities

Activity	**Responsibility**
• Identify relevant Test Centre Staff	CBE-SP
• Define and communicate the roles & responsibilities	CBE-SP
• Share guidelines with stakeholders	CBE-SP

• Share the list of stakeholders with Examining Body	CBE-SP
• Print ID cards for the identified stakeholders	CBE-SP
• Distribution of ID cards for the identified stakeholders	CBE-SP
• Impart training for the identified stakeholders	CBE-SP

Input

Finalization of Online Examination Schedule and the test centres.

Procedure

- The Service Provider will
    - Identify the relevant test centre staff:
        - Centre Head
        - Invigilators
        - IT Managers
        - Volunteers
        - Security Guards
        - LISP Resource
    - Share the relevant guidelines with the identified test centre staff.
    - Impart training to the above identified stakeholders.
    - Distribute the ID cards for the above identified test centre staff.
- The Examining Body team will
    - Identify the observers
    - Disseminate guidelines to observers
    - Share the List of Observers and their contact details with the Service Provider
    - Distribute the ID Cards for observers

Output

- All relevant stakeholders identified.

- Guidelines shared with the relevant test centre staff.

- Training imparted to relevant test centre staff.

3.6.4 TEST CENTRE READINESS – PLANNING

Purpose

To ensure and verify the readiness of the Test Centre to conduct the Online examination.

Scope

This procedure will be followed 2 - 5 days prior to the online examination, to verify and ensure that the finalized Test Centre meets all the specified requirements.

Responsibilities

Activity:

Responsibility

- Visit the finalized Test Centre to ensure the required facilities are available: CBE-SP
- Confirm the Infrastructure availability-

- Conduct LANscape:

  CBE-SP
- Share LANscape report:

  CBE-SP

Input

Finalization of Examination Schedule & Test Centres.

Procedure

- The Service Provider will check the following:
  - Seating arrangement
  - LAN Verification to ensure that the LAN
    - does not break during the test.
    - does not have any IP Traffic Managing Software installed that might interrupt the response of the candidate’s system.
  - Hoardings, Wall hangers and Signboards to be in place informing the candidates of various places like Rest Rooms, Locker Rooms, Registration Desk, Emergency Exits, etc.
  - Security Arrangements:
    - Availability of Physical Security to man the test centres.
    - Availability of Electronic Surveillance.
  - To be equipped with some of the Emergency needs like Fire Fighting Equipment at all the centres and First Aid Medicines to tackle minor injuries or infections.

- The Service Provider will conduct repeat LANscape on all the identified desktops which will be used to take up the online examination.
- The Service Provider will review the repeat LANscape report and share a sign off on the finalized desktops.
- The Service Provider will issue a sign off on the Test Centre

Output

- Sign off on the individual Test Centres confirming their availability for the online examination.

3.6.5 UPLOAD CANDIDATE DATA IN THE SYSTEM

Purpose

To load the details of the candidates who are registered for the Online Examination.

Scope

This procedure will be followed to update the details of all those candidates who have registered for the Online examination.

Responsibilities

Activity

Responsibility

- Meeting to understand the required fields in the application form

  PEB/CBE-SP
- Share Data template with Examining Body

  CBE-SP
- Data Conversion as per the Template

  PEB
- Share Specific Validation

  CBE-SP
- Share the list of test centres

  CBE-SP
- Provide the mapping of candidates and centres

  PEB
- Upload the data into the system

  CBE-SP
- Verify the finalized data in Online Examination System

  PEB

Input

Details of the candidates who have registered for the Online examination.

Procedure

- Public Examination Body and Service Provider will have a detailed meeting to

  - understand the design of the application form,
  - understand the required fields in capturing personal, qualification, address, payment and other details.
- CBE-SP will create a data template and share with PEB.
- PEB will capture all the applicant’s details as per the template and share it with CBE-SP.
- CBE-SP will provide the list of the finalized test centres in all the cities where online examination is to be conducted.
- PEB will also share with CBE-SP:
  - Any specific validation required for the captured data.
  - Mapping of candidates and the corresponding test centres.
- CBE-SP will then have all these details configured in the system.

Output

- System configured with the details of the finalized list of candidates appearing for the online examination along with their assigned test centre details.

3.6.6 HELPDESK SUPPORT ACTIVATION

Purpose

To activate a Helpdesk Support structure to provide timely and appropriate responses to all stakeholders and users of the online examination solution with specific focus on the *First Call Resolution.*

Scope

This procedure will be followed to activate a Helpdesk Support team to address the queries and clarifications raised by all the relevant stakeholders of online examination.

Responsibilities

Activity

Responsibility

- Arrive at the Helpdesk Support team size

  CBE-SP

- Publish to PEB the helpdesk communication channel

  CBE-SP

- Develop training material for helpdesk team

  CBE-SP

- Develop Exam specific FAQs, and Exception handling scenarios

  CBE-SP

- Publish select FAQs (in any of the formats of document, pdf, video, audio) on the PEB website

  CBE-SP

- Train the support team

  CBE-SP

- Set call handling flow, and process including recording of issues

  CBE-SP

Input

Decision to conduct the Online examination.

Procedure

- CBE-SP will
  - Understand the details of the test cities/centres/finalized number of candidates appearing from each test centre.
  - Identify the various stakeholders who will be involved– PEB/Candidates/IT Managers/Proctors/Test Centre Managers/ CBE-SP.
  - Arrive at the required helpdesk support team size required to support the stakeholders.
  - List the various modes (phone, mail, etc.) by which the helpdesk team can be contacted (various ways in which all the stakeholders can reach out to the helpdesk.
  - Arrive at the common queries that may be raised by each stakeholder and have the same updated in the database.
  - Adequately train the helpdesk support team.

Output

- Availability of trained helpdesk support team to handle all the queries/ clarifications raised by various stakeholders involved in the online examination.

3.6.7 UPLOAD QUESTION PAPER IN A SECURED ENVIRONMENT

Purpose

To create and seal the question/question paper template/question paper in a secured environment which would be later rendered for online examination.

Scope

This procedure will be followed to create the online examination question paper in a secured environment.

Responsibilities

Activity	**Responsibility**
• Impart training to concerned Director (Special Exams)/ SMEs/Agencies Personnel on question paper creation	CBE-SP
• Set up a secured VPN tunnel to ensure security	CBE-SP
• Decision to use question paper or question paper template	PEB
• Prepare the question paper in the CBE-SP provided format	PEB
• Seal question/question paper template/question paper	PEB
• Encrypt the question paper and images at PEB premise	PEB
• Upload the encrypted question paper and images to CBE-SP data centre	PEB/CBE-SP
• Provide the name of the question paper for further configuration	PEB

Input

Question base content is available with PEB to start the question creation process.

Procedure

- CBE-SP will impart training to concerned officials/Subject Matter Expert (SME) /Agencies Personnel on question paper creation.
- CBE-SP to set up the secured environment with the help of the VPN tunnel.
- PEB Team will
  - prepare the question paper in the format as requested by CBE-SP.
  - review the question paper with the images.
  - seal the question paper.
- CBE-SP will issue a new executable file to encrypt the question paper and images at PEB premises.
- The encryption of the question paper and the images can be done at the PEB premises, by the PEB technical team.
- On the day of the examination, PEB team will upload the Encrypted Excel Sheet (Question Paper) and Images folder to the CBE-SP Data Centre through a secure VPN tunnel, by a mutually agreed timeline.
- The name of the question paper will be disclosed to CBE-SP once the uploading activity to the Data Centre has been completed.
- CBE-SP will map the corresponding sealed question paper/question paper template for online examination.

- However, the key for the encrypted file can be given 60 minutes before the examination.

Output

Sealed Question Paper/Question Paper Template is available in the Data Centre and mapped to online examination drives.

3.7 ASSESSMENT DELIVERY

3.7.1 TEST CENTRE READINESS

Purpose

To ensure that the test centre is well managed on the day of the online examination.

Scope

This procedure will be followed at every finalized test centre where the examination is conducted as per the online examination schedule.

Responsibilities

Activity	**Responsibility**
• Open the centre	Centre Head
• Confirm the infrastructure availability	
o Physical arrangements	Centre Head

Input

- Test Schedule

- Agreement between CBE-SP and Test Centre team (infrastructure provider) or written communication from Test Centre team (infrastructure provider) confirming the availability of Test Centre to conduct online examination.

Procedure

- ➢ Centre Head along with the Centre Head (CBE-SP Resource) will ensure that the Test Centre is opened up at least 3 hours in advance of the online examination.
- ➢ Centre Head/Centre Head (CBE-SP Resource) will check the following:
    - o Seating arrangement
    - o Hoardings, wall hangers and signboards to be in place informing the candidates of various places like rest rooms, registration desk, emergency exits etc.
    - o Security arrangements
        - – Availability of Physical Security to man the test centres
        - – Availability of Electronic Surveillance and Surveillance room with the necessary arrangements
    - o Centres to be equipped with some of the emergency needs like firefighting equipment at each centre and first aid medicines to tackle minor injuries and infections.

Output

Test Centre marked ready to start the examination, as per the schedule.

3.7.2 CANDIDATE REGISTRATION AND VERIFICATION AT THE TEST CENTRE

Purpose

To ensure that only the registered candidates take up the online examination and a seat is allocated to the candidate to take up the assessment.

Scope

This procedure will be followed at every test centre to verify the identity of the registered candidate, capture their biometric information and photograph to avoid any impersonation. The registration procedure will also randomly allocate candidates their unique exam seats in their designated exam room for the online examination.

Responsibilities

Activity	**Responsibility**
• Start the exam drive to download the candidate details	CBE-SP
• Setup of registration desk in every exam room within the test centre	CBE-SP
• Availability of invigilators in every exam room within the test centre	CBE-SP
• Registration of candidates	CBE-SP
• Verification of candidates	CBE-SP
• Exception Handling at the registration desk	CBE-SP&PEB

Input

Test Centre and candidates ready on the day of the online examination.

Procedure

- Duties of the IT Manager:
  - To connect the Exam Centre Server to the Data Centre.
  - To download the question paper on the Exam Centre Server.
- CBE-SP will ensure that:
  - the registration desk is setup at least 2.5 hours in advance of the commencement of the online examination,
  - the list of registered candidates is available with the registration desk, and
  - the list of candidates and the corresponding exam room is displayed within the test centre.
- Candidates will
  - be allowed to enter the test centre only if a valid admit card is available. The admit card will be checked for the centre name and other details.
  - NOT be allowed to enter in case if he/she has come to a wrong centre.
  - enter the premises and look for details (posted on notice boards) of the allocated exam rooms for the online examination.

  - leave their belongings outside the exam room; however, PEB will not be responsible for any loss/damage/theft of the candidate’s belongings.
  - report at the registration desk at their corresponding exam room.
  - carry a valid photo identity card, including school/college identity card, driver’s license, voter’s identity, passport, pan card, employer ID card or a notarized affidavit having his photo, date of birth and residential address.
- Volunteers will assist the candidates in finding the allocated exam room.
- Invigilators at each exam room will
  - Verify the candidates for a valid admit card and photo identity proof.
  - Verify the candidates for their photo or biometric thumb impression and allow the candidates to enter the examination hall.
  - Capture the candidate’s signature once registration is completed.
  - Ensure that candidates do not carry any additional material which is not allowed in the exam room as per the guidelines for the candidates.
  - Issue required papers for rough work to each candidate.
  - Randomly allot exam seats to the candidates for the online examination session.
  - Ensure that no candidate changes the allotted seat, by matching the photograph affixed in the admit card with the photograph displayed on his/her terminal.

- Candidates will then
    - Sign the attendance sheet,
    - Occupy their allocated seat in the exam room.

Output

- Candidates enter the exam room at the stipulated time defined.
- Candidates will be allotted the exam seat for the online examination session.

3.7.3 CONDUCTING THE TEST

Purpose

To ensure that the online examination is conducted as per the schedule.

Scope

This procedure will be followed to conduct the online examination on the scheduled date and time.

Responsibilities

Activity	**Responsibility**
• Briefing to candidates	Invigilator
• Initiation of test	IT Manager
• Recording of responses	Candidates
• Video capture at each centre	CBE-SP
• Provide feedback on the test experience	Candidates
• End the test	IT Manager

• End the slot	IT Manager
• End the drive	IT Manager
• Upload of results from exam centre server to data centre	IT Manager

Input

Registered candidates ready to take the test online.

Procedure

- Roles of the invigilator:
  - To ensure that nodes are allocated to the candidates with their user ID and password.
  - To verify if the candidates are sitting in their allocated seats by verifying their admit cards, and comparing their photos available physically with the photos present in the system.
  - To instruct the candidates on
    - how to start the online examination,
    - how to record their responses,
    - what to do if the system or test hangs in between,
    - general rules and regulations, and
    - evacuation procedures, in case of any emergency.
- Candidates then login to the system with their credentials provided to them at the registration desk.

- Candidates start the exam and record their responses.

- In case of any system failure, the invigilator in each exam room verifies and unlocks the candidate’s account and the timer starts from the same point where the candidate had left.

- The candidate can submit his responses by clicking on the SUBMIT button. In case of timeout, the test automatically gets submitted and all his responses will be considered for evaluation.

- Candidates provide feedback on their experience of the test.

- At the end of the test, the IT manager

    - Ends the test, after which no candidate can attempt the test.

    - Ends the slot, once all the candidates have left the room.

    - Ends the drive, once all the slots have been completed.

    - Connects the Exam Centre Server to the Data Centre and uploads the candidates’ responses from each test centre.

    - The PEB observer at each centre would be responsible to ensure that the result file has been uploaded successfully.

- All the activities at the examination centre will be captured using a video camera. The list of sensitive cities/centres will be provided by PEB to CBE-SP. In these cities/centres, the recording of the examination, from the registration to the result upload, will be done. The candidates’ movements in the exam hall will also be captured. The final CD/DVD of the centres will be handed over to PEB as agreed.

Output

- Online Examination completed and the encrypted result files are uploaded.
- CD/DVD of the video captured at the test centres.

3.8 POST EXAMINATION

3.8.1 PROVIDING THE CANDIDATES' RESPONSES

Purpose

To ensure that the raw candidates' responses are available with PEB at the end of each exam day.

Scope

The encrypted candidates' responses after each exam day to be transferred to PEB system via VPN tunnel.

Responsibilities

Activity	**Responsibility**
• Consolidation of reports	CBE-SP
• Set up of the VPN unnel	CBE-SP

• Transfer of centre wise encrypted candidate response file to PEB	PEB

Input

Raw candidate response from CBE-SP data centre transferred to PEB system.

Procedure

- CBE-SP will perform the following:
  - Consolidation of all the results
  - Transfer the centre wise files to PEB
- PEB will perform the following:
  - Receive the files at PEB

3.8.2 COMPILATION AND PUBLICATION OF RESULTS

Purpose

To compile the results of the online examination.

Scope

This procedure will be followed to compile the results of the online examination.

Responsibilities

Activity	**Responsibility**
• Consolidation of Reports	CBE-SP

• Providing the correct answer key	PEB
• Generation of Reporting Dashboard	CBE-SP
• Sharing of audit trails with PEB	CBE-SP
• Generation of scores	PEB
• Publishing of results	PEB

Input

Candidates’ responses from all the test centres uploaded to the Data Centre.

Procedure

- ➢ CBE-SP will perform the following:
  - o Consolidation of all the results
  - o Generation of the reporting dashboard
  - o Sharing of the final report with PEB
- ➢ PEB will perform the following
  - o Provide the correct answer key to CBE-SP
  - o Cross check the result provided by CBE-SP
  - o Generate the rank list
  - o Publish the results

Output

Results of the online examination published.

3.8.3 FEEDBACK ANALYSIS

Purpose

To analyze the feedback shared on the online examination.

Scope

This procedure will be followed to analyze the feedback shared by the candidates post-exam completion, and by the PEB team on the overall examination experience.

Responsibilities

Activity	**Responsibility**
• Develop candidate feedback report	CBE-SP
• Share the feedback analytics with PEB	CBE-SP
• Share and collect the Engagement Feedback form from PEB	CBE-SP
• Analyze the feedback received from PEB	CBE-SP

Input

- Feedback shared by students in the system after the completion of online examination
- Feedback shared by PEB post conducting the online examination

Procedure

- CBE-SP will generate feedback report on the captured feedback and share it with PEB.
- CBE-SP will share Engagement Feedback form with PEB.
- PEB will share the completed feedback form with CBE-SP.

- CBE-SP will analyze the feedback and arrive at recommendations for improvement.

Output

- Feedback (shared by the candidates) Analysis Dashboard
- PEB feedback to CBE-SP on the overall process of conducting the examination.

3.9 IT DISASTER RECOVERY

IT disaster recovery is essential element of business resiliency and has a common objective to manage risks that disrupt business.

CBE-SP should have robust Disaster Recovery Plan (DRP) framework to ensure that operations continue in an emergency and quickly recover from the disaster with minimum impact to the business.

These ensure:

- Prevention of interruption in the online examination.
- Effective restoration of data with no/minimal loss when there is an unforeseen incident which occurs during the online examination.

Data Centre

Primary and backup should be located at two geographically spread locations.

Server in the Test Centre

Primary and backup servers should be functional in every test centre.

Candidate desktop within Exam Room in a Test Centre

Alternate desktop to be provided to the candidate by the invigilator in case of any failure.

3.10 EXCEPTION HANDLING PROCESS

3.10.1 INFRASTRUCTURE RELATED

What if power failure happens?

- UPS should take over the system if it is short power failure.
- Gen Set should take over the system if it is short power failure.
- Log the details in an incident register about power failure incident.

What if access to the Internet is not available in the test centre?

- Use data card to connect to the Internet.
- Use offline mode to start the examination on time.

What if LAN connection in the test centre breaks down?

- Inform the centre head about this and ask Controller of the Examination for extension of the exam time or get approval for changing the exam centre/ rescheduling the exam.
- Log the details in incident register about LAN connection break down.

What if the primary server goes down?

- Inform all the participants to logout and login with backup server URL and start accessing the test.

- Log the details in incident register about primary server going down.

What if the secondary server goes down?

- Inform the CBE-SP activation lead about this and ask Controller of the Examination for extension of the exam time or get approval for changing the exam centre/rescheduling the exam.

- Log the details in incident register about secondary server going down.

What if a candidate's machine can't connect to the server?

- Assign a new machine to the candidate and use the same login credentials.

- Log the details in incident register about the candidate shifting to another machine.

What if a candidate's machine gets locked?

- Assign a new machine to the candidate and use the same login credentials.

- Log the details in incident register about the machine crash and about the candidate shifting to another machine.

What if IP obtained by the server changes frequently?

- Disable DHCP service running into LAN.

- Ensure that there are no IP Traffic controllers installed in the LAN.

- Log the details in incident register about IP frequently changing

What if the biometric device doesn't work?

- Use backup Biometric to resume the registration process.

- Log the details in incident register about primary biometric failure.

What if the back-up biometric also doesn’t work?

- Use another registration desk, if available, for registration and divert candidates to other registration desks.

- Use ink based thumb impression capture to resume registration if there are no other registration desks available.

- Log the details in incident register about back-up biometric device failure.

What if the webcam doesn’t work?

- Use backup webcam to resume the registration process.

- Log the details in incident register about the primary webcam failure.

What if the back-up webcam also doesn’t work?

- Use another registration desk, if available, for registration and divert candidates to other registration desks.

- Log the details in incident register about back-up webcam failure.

What if inventory is out of stock/ inventory is broken/some of the items are mal-functioning?

- Inform the Centre Head to replace/add inventory.

What if the surveillance systems are not functioning at the test centre?

- Inform Infrastructure Provider to repair the system.

- If it is not reparable, then arrange for any local vendor for the video.

- Log into incident register on non-working of the surveillance system.

3.10.2 CANDIDATE RELATED

What if a candidate unknowingly logs out the exam?

- Ask the candidate to re-login and the exam will start from the time where he had stopped.

- Log the details in incident register about the candidate logout.

What if a student is found to have a cut in his/her thumb during the biometric capture?

- Any other finger impression can be taken for the same. The same needs to be mentioned in the system.

What if the photograph of the student taken is appearing dark and the face is not clear?

- That photograph will be discarded and a new photograph will have to be taken. In case the result is the same, adjust the web cam for a better quality.

What if any student gets his mobile phone inside and claims he brought it in unknowingly on being caught?

- Confiscate the mobile phone, record the incident and allow the candidate to answer the exam.

What if the student's mobile phone rings during the exam?

- Confiscate the mobile phone, switch it off, record the incident and allow the candidate to answer the exam.

What if a student tries to enter the exam hall after the start of the exam?

- No student will be allowed to walk in to the exam hall once the exam starts.

- Report the incident to the PEB observer.

What if a student's machine gets locked in the middle of the exam?

- Refer to the exigency plan sheet.

What if a student falls ill during the exam?

- Immediately call the volunteers to take the candidate for immediate treatment outside the room.

What if a student asks for a bio break?

- No student will be allowed to walk out of the room under any circumstances. In case of an emergency, the incident will be recorded and allowed in a controlled manner. However, the exam timer will not stop during this period.

What if a student is caught talking to another student? If there is any punishment, will it be for both the students or only for the person caught talking?

- Student(s) will be given two warnings, and thereafter will be restricted from continuing the exam. An incident will also be logged in the incident register for the same.

What if the student damages the infrastructure hardware before leaving the room?

- An incident will also be logged in the incident register for the same and the details of the student who had occupied the desk will be written in the record.

3.10.3 INVIGILATOR RELATED

What if a confirmed invigilator does not report at the test centre at the stipulated time on the day of the examination?

- Back-up invigilators would be asked to take charge instead of the confirmed invigilator.

What if the invigilator forgets to bring the photo identity proof required for the invigilator ID card?

- Invigilator ID card will not be issued without the proper photo identity card.
- Ensure that back up invigilator(s) is one of the volunteers. She/he will be asked to invigilate the exam

What if the invigilator is not able to make it on the previous day but confirms he will come on the day of the exam?

- The invigilator will be discarded and replaced with the backup invigilator.

3.10.4 GENERAL

What if a medical emergency/an examination disruption attempt/a natural disaster arises?

- Inform the Centre Head about the incident and seek for the next steps on rescheduling/cancellation/change of the test centre of the examination. Log in the incident register on this emergency incident.

CHAPTER 4

PRESCRIPTIVE FRAMEWORK TO DEVELOP A SECURE CYBER APPLICATION

4.1 INTRODUCTION

A secure cyberspace is critically important to any nation's safety, but today's cyber environment is anything but secure. There is an increase in the successful attacks on any nation's institutions and people's identities online in cyberspace by individuals, organizations and states at a rate which is very alarming.

The dependency of developed world on IT will only grow and grow. The optimal utilization of IT will be there only when these systems are secure, but the rate at which the volume of threat is increasing, whether associated with loss or damage, type of attack or presence of vulnerability (leak of confidential information like nation's security related, research related etc.), indicates that the problem is worsening. And also, the actual spread of the threat is unknown as some attacks are considered important or are not reported and noted down.

The possible penalty incurred as a result of security not up to the mark, can be put into the following categories:

- *Threat of Catastrophe* - a cyberattack, especially in conjunction with a physical attack- could result in losses of thousands of deaths and billions of dollars in a short time (e.g. intrusion into command and can be of nuclear devices, missiles etc.).

- *Frictional Drag* - Frictional drag takes away productivity and performance in important economic and security related processes. At present, an insecurity in cyberspace system and networks gives an opportunity to the opponents/adversaries to extract billions of dollars in fraud and extortion (e.g. some hackers blackmailed some banks for publishing certain auditing report) – and force businesses to expand additional resources to defend themselves against these threats. If cyberspace does not become more secure, the citizens, businesses and governments of tomorrow will continue to face similar pressures and on a larger scale.

- *Lost Opportunities* - Concerns about inadequate cyber security may inhibit development and deployment of IT in the future, thereby minimizing the benefits that IT brings, benefits that will be needed to enhance any nation's global competitiveness as well as national and homeland security.

Cybersecurity is defined as the prevention of damage to, unauthorized use of, exploitation of and, if needed, the restoration of electronic information and communication systems and the information they contain, in order to ensure confidentiality, integrity and availability of these systems.

Cybersecurity protects the virtual world against all forms of cyberattacks. Cyberattacks have the potential of causing devastating disruption to critical national infrastructures, economies or national security. For example, viruses, worms, spam, publishing and other fraudulent schemes, as well as identity theft also come under cyberattacks. As the tools and technologies to bring about the intrusions is more freely available to the people who are very capable and smart but having a mindset of causing havoc or disruption, the cyber world is more vulnerable as the time goes on.

To make significant progress in the magnitude of cyber, security must be built into systems from step one. New architectures containing new hardware, designed to include embedded cyber security monitoring and processing capabilities (e.g. on board or peripheral cyber security processing, virtualizes architectures) and even especially designed to accommodate new cyber security analysis (e.g. processes designed for ultra-fast data comparison and analysis encompassing searches, sorts, merges, joins, and pattern reorganization) and new encryption and decryption techniques are needed.

At present, the cyber security comes up as a reaction to an attack and mostly it is achieved manually. Threats and vulnerabilities are defined and addressed only after they appear, are then identified, analyzed and distilled into well-defined behaviors and even digital signatures. Definitely, today, sophisticated and intelligent systems are required which can detect and provide protection from threats based upon more than just tabulated data, using sophisticated, predictive mathematical models to “stay ahead of the curve”.

Software with good security features is efficient enough to repel most attacks, tolerate the maximum of attacks that it cannot repel and is able to recover quickly with a minimum of damage caused from the attacks it cannot tolerate. Development of high assurance security software requires knowledge and techniques which are not usually known to or used in practice by most software developers.

Usually, in a customary software life cycle (SDLC), security is taken up as the last issue to be covered and all its scenarios like probabilities, estimation and solution are resolved at the very end after the software has been developed. Vulnerabilities are an emergent property of software which appears throughout the development phases.

When the security aspect is ever considered during the system life cycle, they are in general, features like password protection, firewalls, virus detection tools and so on. These are, in fact, not security requirements at all but rather implementation mechanisms that are intended to satisfy unstated requirements, such as authenticated access. Thus, system specific security requirements which provide protection to essential services and assets are often overlooked. Even the view point of attackers is not calculated, so the net result is that the security features even which are present are inadequate. Thus, a scientific approach that is step by step dealing with the security requirements will help to avoid the problem of generic lists of features and to take into account the attacker's perspective.

Including security at the beginning of the SDLC is often considered the most cost-effective approach for two reasons: (1) it is usually more difficult to add functionality into a system after it has been built, and (2) it is frequently less expensive to include the preventive measures to deal with the cost of a security incident.

4.2 SECURE SOFTWARE DEVELOPMENT LIFE CYCLE (SSDLC)

The Need for Security to Protect Software

The selection and employment of appropriate security for software system should be done very carefully as this is an important task that can have major implications on the operations and assets of an organization. Security measures are the management, operational and technical safeguards or countermeasures prescribed for a software to protect the confidentiality, integrity and availability of the system and its information. The concerned people should make an assessment by putting forward several important questions that should be answered when addressing the security considerations for their software system:

- What security features should be there to adequately protect the information systems that support the operations and assets of the organization in order for that organization to achieve its goal, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions and protect individuals?

- Have the selected security measures already been implemented or is there a realistic plan for their implementation?

- What should be the desired or required level of assurance (i.e. grounds for confidence) that the selected security features, when implemented, are effective in their application?

The answers to the above questions are to be given in a broader context for the organization that is effective in identifying, controlling and extenuating risks posed to its information and software. The security measures should be employed as part of a well-defined and documented information security program. An effective security program should include the following:

- Risk assessment should be the basis of policies and procedures that can cost-effectively reduce information security risks to an acceptable level and address information security throughout the life cycle of each software system.

- Plans for providing adequate security for networks, facilities, information systems as appropriate.

- Security awareness training to inform personnel (including contractors and other users of software that support the operations and assets) of the security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks.

- Periodic testing and evaluation of the effectiveness of security policies, procedures, practices and security features to be performed with a frequency depending on risks.

- A process for planning, implementing, evaluating and documenting remedial actions to address any deficiencies in the security policies, procedures and practices of the organization.

- Procedures for detecting, reporting and responding to security incidents.

- Plans and procedures for continuity of operations for information systems that support the operations and assets of the organization.

It is of importance that responsible officials understand the risks and other factors that could adversely affect operations, assets or individuals. Moreover, these officials must understand the current status of their security programs and the security features planned or in place to protect their systems in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

When the risks/defects are detected as early as possible in the life cycle then it costs least expensive to software development. Requirements analysis usually takes care of the functional aspects of the product, but when security is important, additional analysis of non-functional requirements must also be used to identify security concerns. Usually, the security requirements are in the form of Don’ts, which should not happen but can still be tracked to closure in the same manner as other requirements and can also be a mix of functional and non –functional requirements. Threat modeling is especially important to requirement phase of the life cycle since it can help in the preparation of test strategies and use cases. A fresh look into the architectural concerns is there when the risk-based view of development is done during the design phase. When security features are correctly incorporated in design, that is, implemented correctly, the code that is constructed minimizes the attack ability of the final product. Again, effective code policies can be tracked for compliance during design and then for the remainder of the life cycle.

In the context of cyber application, security concerns may take the form of

- architecture security, which addresses the specified security requirements,
- secure design criteria, where security requirements can be traced, and
- secure coding practices, where integrity can be assessed and measured.

In the requirements phase, it is useful to know whether security-related concerns have been included in defining system requirements. This could be initially as ‘yes’ or ‘no’. As experience progresses with time, this could develop in characterizing the extent that requirements have been checked and tested against security concerns. Determining the extent that security objectives are implemented during the design and coding phases will make use of tools as well as inspections or reviews. Most of the inspection will be in the form of traditional defect identification checklists, to which security-oriented items have been added.

4.3 GENERAL CODE INTEGRITY ISSUES

Web Applications:

- Scripting issues
- Sources of input
- Forms, text boxes, dialog window etc.
- Regular expression checks
- Header integrity

- Session handling
- Cookies
- Framework vulnerability (Java, .NET etc.)
- Access control: front and back door vulnerability assessment
- Penetration attempts versus failures.
- Depth of successful penetrations before detection.

4.4 LIFE CYCLE PROCESS

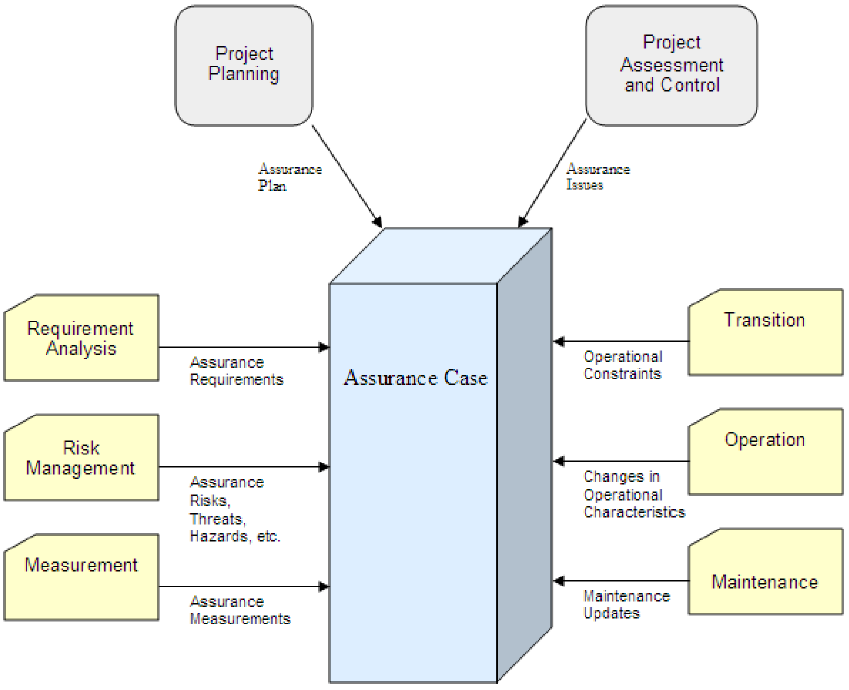


Fig 4.1: Life Cycle Process

4.5 SECURE SOFTWARE DEVELOPMENT MODEL (SSDM)

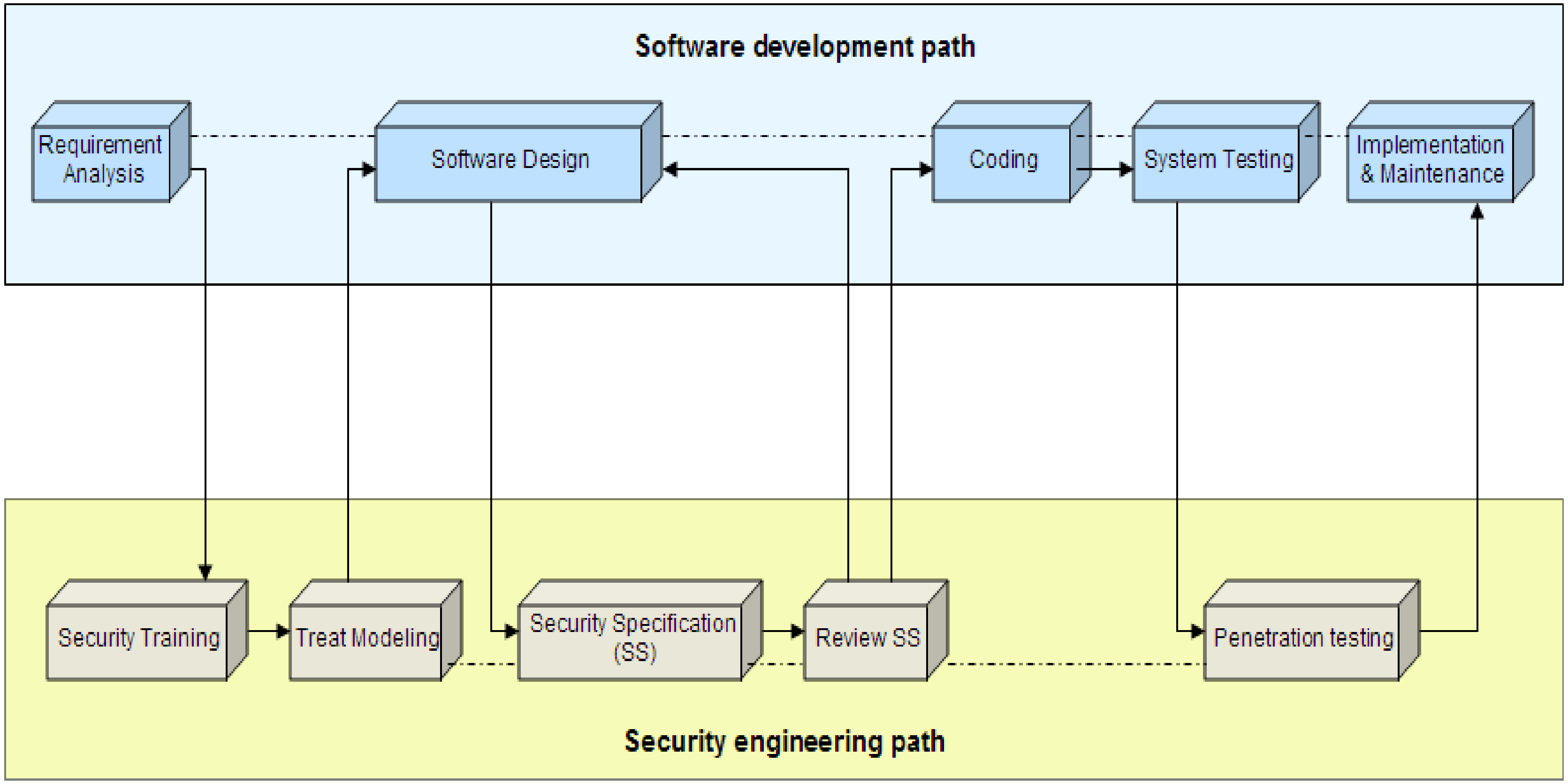


Fig 4.2: Secure Software Development Model

4.6 THE PRESCRIPTIVE FRAMEWORK

Including security early in the system development life cycle (SDLC) will usually result in less expensive and more effective security than adding it to an operational system. Here we present a framework for incorporating security into all phases of the SDLC process, from initial to disposal.

A general SDLC is discussed in here that includes the following phases: initiation, acquisition/development, implementation, operations/maintenance and disposition. Each of these five phases includes a minimum set of security steps needed to effectively incorporate security into a system during its development.

4.6.1 INITIATION PHASE

- Security Categorization: - defines three levels (i.e., low, moderate or high) of potential impact on organizations or individuals should there be a breach of security (a loss of confidentiality, integrity or availability). Security categorization standards assist organizations in making the appropriate selection of security measures for the information system.

- Preliminary Risk Assessment: - results in an initial description of the basic security needs of the system. A preliminary risk assessment should define the threat environment in which the system will operate.

4.6.2 ACQUISITION/DEVELOPMENT PHASE

- Risk Assessment: - analysis that identifies the protection requirements for the system through a formal risk assessment process. This analysis builds on the initial risk assessment performed during the Initiation phase, but will be more in-depth and specific.

- Security Functional Requirements Analysis: - analysis of requirements that may include the following components (1) system security environment (i.e. enterprise information security policy and enterprise security architecture) and (2) security functional requirements.

- Security Assurance Requirements Analysis: - analysis of requirements that address the developmental activities required and assurance evidence needed to procedure the desired level of confidence that the information security will work correctly and effectively. The analysis, based on legal and functional security requirements, will be used as the basis for determining how much and what kinds of assurance are required.

- Cost Considerations and Reporting: - determines how much of the development cost can be attributed to information security over the life cycle of the system. These costs include hardware, software, personnel, and training.

- Security Planning: - ensures that agreed upon security measures, planned or in place, are fully documented. The security plan also provides a complete characterization or description of the information system as well as attachments or references to key documents supporting the agency’s information security program (e.g. configuration management plan, contingency plan, incident response plan, security awareness and training plan, rules of behavior, risk assessment, security test and evaluation results, system interconnection agreements, security authorizations/accreditations and plan of action and milestones).

- Security Control Development: - ensures that security controls described in the respective security plans are designed, developed and implemented. For systems currently in operation, the security plans for those systems may call for the development of additional security measures to supplement the measures that are deemed to be less than effective.

- Developmental Security Test and Evaluation: - ensures that security measures developed for a new system are working properly and are effective. Some types of security measures (primarily those of non-technical nature) cannot be tested and evaluated until the system is deployed – these features are typically management and operational features.

- Other Planning Components: - ensures that all necessary components of the development process are considered when incorporating security into the life cycle. These components include selection of the appropriate contract type, participation by all necessary functional groups within an organization, participation by the certifier and accredited, and development and execution of necessary contracting plans and processes.

4.6.3 **IMPLEMENTATION PHASE**

- Inspection and Acceptance: - ensures that the organization validates and verifies that the functionality described in the specification is included in the deliverables.

- System Integration: - ensures that the system is integrated at the operational site where the system is to be deployed for operation. Security feature settings and specifications are enabled in accordance with vendor instructions and available security manual.

- Security Certification: - ensures that the measures are effectively implemented through established verification techniques and procedures and gives the concerned officials confidence that the appropriate safeguards and counter measures are in place to protect the organization's information system. Security certification also uncovers and describes the known vulnerabilities in the system.

- Security Accreditation: - provides the necessary security authorization of an information system to process,s store or transmit information that is required. This authorization is granted by a service organization official and is based on the verified effectiveness of security features to some agreed upon level of assurance and identified residual risk to agency assets or operations.

4.6.4 OPERATIONS/MAINTENANCE PHASE

- Configuration Management and Control: - ensures adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment. Configuration management and configuration control procedures are critical to establishing an initial baseline of hardware, software and firmware components for the information system and substantially controlling and maintaining an accurate inventory of any changes to the system.

- Continuous Monitoring: - ensures that features continue to be effective in their application through periodic testing and evaluation. Security features monitoring (i.e. verifying the continued effectiveness of those features over time) and reporting the security status of the information.

4.6.5 DISPOSITION PHASE

- This is the final phase of SSDLC. Even though this is supposed to be the definitive end of the whole life cycle, practically there is no end to it. The changes in technology and requirements result in further evolution of it. Security plans also continually evolve with the system.

4.7 IT SECURITY IN THE SOFTWARE DEVELOPMENT LIFE CYCLE

Table 4.1: IT Security in SDLC

	Initiation	Acquisition/ Development	Implementation	Operations/ Maintenance	Disposition
SDLC	Needs Determination: • Perception of a Need • Linkage of Need to Mission and Performance Objectives • Assessment of Alternatives to Capital Assets • Preparing for investment review and budgeting	• Functional Statement of Need • Market Research • Feasibility Study • Requirements Analysis • Alternatives Analysis • Cost-Benefit Analysis • Software Conversion study • Cost Analysis • Risk Management Plan • Acquisition Planning	• Installation • Inspection • Acceptance testing • Initial User training • Documentation	• Performance measurement • Contract modification • Operations • Maintenance	• Appropriateness of disposal • Exchange and sale • Internal organization screening • Transfer and donation • Contract closeout
SECURITY CONSIDERATIONS	• Security Categorization • Preliminary Risk Assessment	• Risk Assessment • Security functional Requirements Analysis • Security Assurance Requirements Analysis • Cost Considerations and Reporting • Security Planning • Security Control Development • Developmental Security Test and Evaluation • Other Planning Components	• Inspection and Acceptance • System Integration • Security Certification • Security Accreditation	• Configuration Management and Control • Continuous Monitoring	• Information Preservation • Media Sanitization • Hardware and Software Disposal

4.8 APPLICATION SECURITY LIFE CYCLE

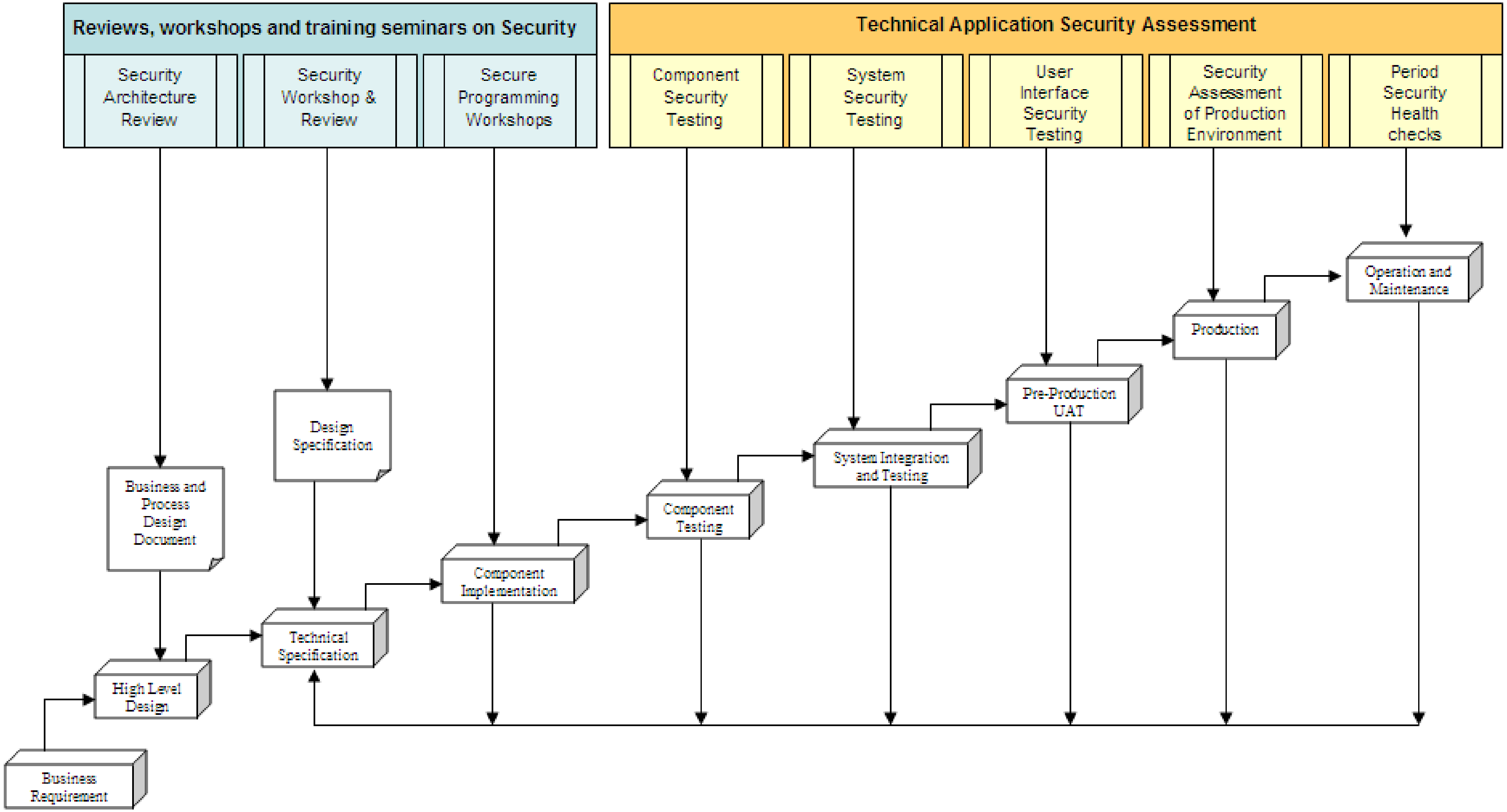

Reviews, workshops and training seminars on Security
Security Architecture Review
Security Workshop & Review
Secure Programming Workshops
Technical Application Security Assessment
Component Security Testing
System Security Testing
User Interface Security Testing
Security Assessment of Production Environment
Period Security Health checks
Business and Process Design Document
Design Specification
Operation and Maintenance
Production
Pre-Production UAT
System Integration and Testing
Component Testing
Component Implementation
Technical Specification
High Level Design
Business Requirement

Fig 4.3: Application Security Life Cycle

CHAPTER 5

INFRASTRUCTURE, PROCESS AND SECURITY AUDIT FOR COMPUTER BASED EXAMINATIONS

5.1 INTRODUCTION

Any Examining Body which is conducting Online Examinations needs to go for Infrastructure, Process and Security Audit for Online Examination at all the centres in all the centre cities. The security audit agency needs to be different from the one which is conducting the online examination. There is a need to carry out an infrastructure, process and security audit by a CERT-In empanelled auditing agency to ensure provision of adequate infrastructure, process review and network security for the smooth conduct of the examination.

5.2 DETAILS OF AUDIT

The audit may be planned in different phases concurrently. These are:

(a) ***Phase I-Examination Software Application Security Audit*****:**

This is the application security audit to find out any vulnerabilities which could be exploited and may result in data leakage or denial of service. OWASP Web Application Standard may be used for auditing during this phase.

(b) ***Phase II-Check of Encryption Process:***

Verification of encryption and decryption technology, being used for uploading of question paper and other exam related data at Examining Body's premises and Central Server location, may be done. FIPS-140 Standard may be used preferably to check symmetric algorithm and the key size (minimum 128 bits).

(c) ***Phase III-Auditing of Exam Centres across Cities:***

- **Module 1:** Physical and Environment Security Audit at each centre.
- **Module 2:** Network Security Audit at each centre.

(d) ***Phase IV-Review of Process on the Days of Examination:***

Verification of encryption and decryption process, being used for uploading of question paper and other exam related data at Examining Body's premises and Central Server location on the days of examination, may be carried out.

5.3 AUDITING OF EXAMINATION CENTRES

Audit of all the examination centers need to be completed well before the date of the examination, so as to give response time to the conducting agency for rectifying flaws if any reported during the audit. A re-audit needs to be done by the auditing agency to ensure rectifications done by the conducting agency. ATR in this regard may be taken from the conducting agency.

5.4 ADMINISTRATIVE CHECKS

The salient requirements are explained in detail below:

(a) ***CCTV Cameras****:* All the centres should ideally be equipped with CCTV cameras to capture the entry of the candidates and any other personnel entering the examination hall. The siting of the cameras must be such so as to cover all entry points appropriately. The CCTV network must have a recording facility with good image resolution, along with the date and time stamps, to enable sufficient evidence in the eventuality of an enquiry subsequently. In case that a centre does not have a CCTV network, arrangements must be made for **'videography'**, that is, to imply that the entire process, commencing from the entry of candidates, the examination and the exit of candidates, must be video-filmed.

(b) ***Power Back Supply Backup:*** All the centres should ideally be equipped with a UPS and DG Set of adequate capacities. In centres, where there is no UPS, there must be a DG Set and a stand-by DG Set.

(c) ***Systems Backup****:* To ensure smooth conduct of the examinations, additional 20% desktops must be made available at each examination centre, i.e., if there are 100 candidates scheduled to appear for the examination at a particular centre on a specific date, there must be at least 120 desktops available at the centre on that date. In addition, there must be a 100% backup for the server(s) at each centre.

(d) ***Illumination****:* Sufficient illumination must be provided in the examination centre for the candidates appearing for the examination. It must also be ensured that sun rays are not falling directly into the centre that may cause discomfort to the candidates. If there is such a case, adequate provision of blinds must be catered for. It must also be ensured that proper ventilation exists in the centre.

(e) ***Air Conditioning****:* It must be ensured that air-conditioners, wherever installed, must be in working condition and not noisy. However, where weather conditions preclude the usage of air-conditioners or the same are not installed, it must be ensured that adequate number of fans are fitted in the centre and are functioning properly.

(f) ***Access Control****:* There must be an effective Access Control System provided at each examination centre to ensure that no unauthorized person gains access into the centre. Ideally, there must be a Biometric Registration of all the candidates, wherein finger-printing facility must be available. Security guards must be stationed to ensure that they permit only authorized personnel and candidates to enter the centre after thoroughly checking the authorized passes and admit cards.

5.5 TECHNICAL CHECKS

The Technical Checklist for the conduct of audit is given at the end of this chapter. However, the salient points pertaining to the technical checks are enumerated below:

(a) ***Network Architecture:*** All examination machines (desktops) should be connected to the server. This will be checked automatically by using network discovery tool. Antivirus logs on the enterprise server are required to be checked for signature updating and presence of any malware which couldn’t be quarantined or deleted.

(b) ***Server:*** Server configuration should be checked to ensure adequate hardening of the server. This will cover local security policy settings, update of patches, disabling of guest account, open ports, setting of audit logs, encryption/ decryption process, presence of any malware, running of any unnecessary services/ applications etc.

(c) ***Audit of Desktops:*** 20% of desktops are planned to be checked for meeting the minimum configuration requirements, presence of malware (if any) and connectivity with the server.

5.6 RISK MITIGATION

Daily reporting needs to be planned to be made to Examining Body with audit reports and recommendations for risk mitigation, if any. All critical gaps are required to be patched by conducting agency, few days before conduct of the examination.

5.7 ADMINISTRATIVE AND TECHNICAL AUDIT CHECK LIST

Table 5.1: Administrative and Technical Audit Check List

Audit Check List: Online Exam Centre
Address of the Centre:
Name of the City :
Date of Auditing :
Name of the Auditor :
Number of Desktops :
Number of Servers :
Maximum Number of Candidates :
Physical Security Audit

S. No.	**Audit Check**	**Description of Check**	**Observation**	**Recommendation**
1	**CCTV**	Is CCTV Installed?	YES/NO	If answer is 'No' then Videography is to be done.
		Is installation appropriate for capturing entry of all the candidates?	YES/NO	
		Are recording of logs with date and time stamp checked?	YES/NO	

		Is quality of Image being recorded satisfactory for identifying the person?	YES/NO	
2	**Electrical Power Supply backup**	Is UPS available to take the load of the Exam Centre?	YES/NO	If YES note down the Capacity: KVA: _____ and backup time: ____ Minutes
		Is stand-by DG set available?	YES/NO	If YES, note down its rating: KVA ______
3	**Back Up System (20% Extra)**	Max no of candidate (a)		
		Max no of Desktop (b)		
		% of Backup system **Method:** (b-a/a) %		20% Backup systems should be available
		No. of Servers		100% backup should be available
4	**Illumination**	Is illumination sufficient for writing exam?	YES/NO	
5	**Air Conditioning**	Are air-conditioners installed and working in the examination hall?	YES/NO	
6	**Access Control**	Is security guard available at the entrance to check any unauthorized access?	YES/NO	
7	**Biometric Registration of Candidates**	Is Biometric Registration for finger printing available?	YES/NO	

Network Security Audit

S. No.	Audit check	Description of check	Observation	Recommendation
1	**Network Architecture**	Check all desktops (clients) properly for connection to the local server. **Methods:** Network discovery tool to be used		
		Check connectivity of the local server with the main server and signal strength of Photon. **Methods:** Check through Modem.		
2	**Server**	Check open ports in both the servers. **Methods:** Using NMAP command.		
		Check Antivirus logs, signature update and firewall enabling status **Methods:** Look for all the malware found, quarantined or could not be quarantined/deleted.		
		Check unnecessary shares on the server and installed software **Methods:**		

		(Start>Run>Services.msc) / cmd->net start		
		Check details of user account and disabling of guest account **Methods:** Check user account settings.		
3	**Audit of Desktop (20%)**	Check for presence of malware in any of the system **Methods:** Start>Run>netstat -an		
		Blocking of Internet connection and disabling of Wireless Connection (as per the procedure).		
		Check that only user access should be provided.		
		Check configuration.	OS: XP/ Vista/Win7, RAM:	

CHAPTER 6

SIGNIFICANCE OF IT SECURITY IN PUBLIC EXAMINATIONS (COMPUTER BASED EXAMS)

6.1 INTRODUCTION

Online Examinations (a.k.a. Computer Based Examinations or CBE) act as an effective solution for mass evaluation for Educational, Entrance, Certification etc. purposes, also referred to as ‘Public Examinations’. Security of such exams is one of the most prime learning and evaluation challenge in today’s connected world. The specific requirements for examination security are to prevent disruption due to a network failure, to avert cheating, and to implement monitoring so that when under question, the proof of the exact happening for the duration can be produced.

Examinations, regardless of their type and purpose, have been increasingly using technology for their conduct. From the pen and paper mode to OMR and OCR for evaluation and recording to desktop application based examinations and Web Application based examinations, the world has seen a major evolution in the way people are assessed. This evolution has brought about a radical enhancement in the swiftness and convenience of the examination process, for both the examinees and the examination organizers.

But, like any other assessment, online exams are vulnerable to various threats and disruption due to miscellaneous factors. In this chapter, an online examination management system has been proposed with comprehensive security, with special focus on IT security, where all the examination-related information is stored digitally. The model uses a diverse set of controls to accomplish this objective.

6.2 BACKGROUND: SECURITY ISSUES IN PUBLIC EXAMINATIONS

The five security requirements have been identified for the security of any Examination System:

6.2.1 CONFIDENTIALITY

To ensure that data are private, and accessible only by authorized entities. Threats to confidentiality may be of the following forms:

- Threats to the question paper / question database confidentiality
- Threats to confidentiality of an examinee’s responses to questions in the exam

6.2.2 INTEGRITY

To ensure that data are original and have not been modified by unauthorized parties, either accidentally or intentionally. Threats to integrity may be related to

- Data from the servers to the examination workstations, and
- Data to the servers from:
  - Examination workstations
  - Authentication equipment
  - Monitoring equipment

Integrity may be ensured by implementing a secure networking architecture and secure configurations on systems throughout the network.

6.2.3 AVAILABILITY

To ensure that system resources are up and available for authorized parties at any given time. Threats to availability may result from the following:

- Malfunctioning of examination workstation or disruption in its performance
- Disruption of local communications network
- Disruption of the link to the Internet, where required
- Malfunctioning of examination server or disruption in its performance
- Malfunctioning of examination application or disruption in its performance

This may be ensured by implementing a secure networking architecture and secure configurations on systems throughout the network.

6.2.4 USER AUTHENTICITY

To verify a user’s identity whilst trying to access system resources by ensuring who is granted access to which resources, i.e. to ensure that impersonation may not be allowed to take place.

Impersonation threats in e-assessment are the most vital risks (i.e. cheating scenarios), that might be encountered during an e-exam. They occur when an examinee pretends to be somebody else. They have been divided into three types:

- **Type I,** where impersonation might occur in two cases - if undetected, or, knowingly allowed due to force, sympathy or bribery.

- **Type II**, which occurs when a student may pass his security information to another, who uses it to answer the exam on his behalf. Username-password pairs fall in this type.
- **Type III**, which occurs when a student just logs in to an exam, letting another to continue on his behalf. Non-shareable attributes such as biometrics fall in this type.

6.2.5 FAIRNESS OF CONDUCT

To ensure that the examination is conducted in such a manner that no examinee can use any unfair means during his attempt of the examination to obtain the correct responses to the questions asked therein.

Usage of unfair means may happen in many ways. The examinee, while attempting, may take help in knowing the responses to the questions from:

- physical material (e.g., handwritten/printed) in the examinee's possession during the exam,
- persons present in the same room (Examinees/ Invigilator(s)/ any other),
- persons available to him through communication media,
- resources available in a digital format on any device in the examinee's possession during the exam,
- resources available locally on the examination workstation/ Local network (in case of computer based examinations),
- resources available on the Internet (in case of internet based tests or any computer based examinations), and
- exploiting the vulnerabilities in the examination application.

6.3 CONTROLS FOR MITIGATION OF RISKS FROM VARIOUS THREATS

Table 6.1: Controls for Mitigation of Risks from Various Threats

Threats	**Assurance measure(s) for offline mode**	**Assurance measure(s) for online mode**
Threats to Confidentiality	Safeguarded through Secure Packaging and Transportation Procedures	▪ Secure networking architecture ▪ Secure configurations on all systems/ devices throughout the network. ▪ Distributed Firewall
Threats to Integrity		
Threats to Availability		
Malfunctioning of examination workstation or Disruption in its performance	Ensured through Robust Packaging and Transportation Procedures	▪ Secure, Homogenous System Configuration on all Examination Workstations
Disruption of local communications network		▪ Robust network architecture, to prevent any delay or disruption due to the network
Disruption of the link to the Internet, wherever required		
Malfunctioning or Disruption in		▪ Secure Server Configuration, audited

performance of the Examination Server		and certified by a competent auditor
Malfunctioning or Disruption in performance of the Examination Application		▪ Secure Examination Application audited and certified by a competent auditor
Threats to User Authenticity		
Type I Impersonation	▪ Strict Identification through Govt. issued Photo ID + Admit card ▪ Penalizing the Personnel responsible for candidate authentication in case of violation	▪ Requiring Authentication for launch of examination
Type II Impersonation	▪ Penalizing the candidate for Fraud and complicity to Impersonation ▪ Penalizing the Personnel responsible for candidate authentication in case of violation	▪ Requiring Multimodal Biometrics in addition to other Authentication Measures for launch of examination
Type III Impersonation		▪ Continual/Synchronous Biometric Authentication (like facial recognition, Keystroke Biometrics)

Use of Unfair Means		
From physical material (e.g., handwritten / printed) in the examinee’s possession during the exam	▪ Physical and Environmental Security Controls ▪ Penalizing the candidate for use of unfair means under the generally accepted definition ▪ Penalizing the accomplice for complicity ▪ Video (CCTV) Surveillance	▪ Physical and Environmental Security Controls ▪ Video (CCTV) Surveillance ▪ Cheating Indication System
Persons present in the same room (Examinees / Invigilator(s) / any other)		
Persons available to him through communication media		
Resources available in a digital format on any devices in the examinee’s possession during the exam		
Resources available locally on the examination workstation / Local network (in case of		

any computer based examination)		
Resources available on the Internet (in case of internet based tests or any computer based examinations)		
Unfair edge, by exploitation of vulnerabilities in the examination application		

6.4 DESCRIPTION OF CONTROLS USED

6.4.1 PHYSICAL AND ENVIRONMENTAL CONTROLS

- The following should be prohibited from being carried into the Examination center:
  - Electronic computing and communication devices
  - Storage media
- Visual facial verification of the candidate should be carried out with the *photo* given during the registration and photo-ID proof issued by a government/ educational/ banking organization.
- The access to the room where the exam is to be conducted shall be given only after what has been stated above has been executed.

6.4.2 CONTINUAL/SYNCHRONOUS MULTIMODAL BIOMETRICS, IN ADDITION TO OTHER AUTHENTICATION MEASURES

In order to achieve comprehensive security in e-learning systems, multiple biometric approaches are required to be combined, in addition to authentication using *username and password*. This provides reliable user security for the duration of the exam rather than instantaneous login. For instance, fingerprint might be combined with keystroke dynamics and/or with facial recognition/ head-geometry detection using a webcam. Then a user's authenticated presence at his system may be verified by continuously/ periodically/ randomly taking inputs from his webcam/ keyboard to authenticate him and verify his presence at the workstation.

Fingerprint Recognition

Fingerprint authentication is proposed to be implemented for user authentication in e-examination. A special hardware, which might be a portable fingerprint scanner with USB connector, is required to scan a user's imprint. The main steps for the enrolment and authentication process can be summarized as follows:

- Creating user-ID and password for each user, scanning each user's thumb, and storing them in a secure server.
- Logging in to the site using user-ID and password.
- In case of access to sensitive data, the fingerprint scanning device will be enabled and the user will be prompted to get his thumb scanned.
- After getting correct recognition, the device will be disabled and the user will be able to access sensitive data.

Keystroke Biometrics

A keystroke biometric system collects raw keystroke data and uses a feature extractor and pattern classifiers to make identification or authentication related decisions. The system can accurately identify or authenticate individuals if the same type of keyboard is used to produce the enrollment and questioned input samples. Input length of 300 keystrokes is considered sufficient for the purpose.

Here, a training set of keystrokes is captured for each student by typing a passage using a computer dedicated for this purpose.

Face recognition

A still photo is captured by a high-resolution camera attached to the registrar’s computer, and a short video (around 1 min) is recorded using an arc-moving video camera.

6.4.3 VIDEO SURVEILLANCE

A proven approach for high security has been monitoring of student activities during online examination using video capture. Random video monitoring has been proposed for secure internet examination. A password has been required for login and a proctor is supposed to watch the video either live or recorded.

6.4.4 CHEATING INDICATOR SYSTEM (USING VIDEO MONITORING, GESTURE RECOGNITION AND MACHINE LEARNING)

This is a proposed system that uses gesture recognition to catch cheating. Gesture Recognition is a technology that has developed in sufficient sophistication to handle the system’s requirements. This is evident from its use on the latest video game consoles, which can track limb movements, facial expressions and eye movements to translate the same into in-game actions. The system logs the video for the duration of the exam attempt and generates a cheating probability score at the end, by analyzing the gestures made by the examinee in the exam duration. The system is to be designed in such a way as to report more false positives (which may be manually verified under protest or in case of disqualifying cheating probability scores) than false negatives.

The outcomes of such human interventions, governed by an effective change management process, are the input to the learning module of the cheating indicator system and help making it increasingly more effective.

6.4.5 SESSION REPORT (INCLUDING THE SESSION VIDEO FOOTAGE AND CHEATING INDICATOR SYSTEM LOGS)

After the exam is terminated either by submission or by a timeout, a session report is generated and saved onto the server. This report includes the video monitoring footage for the exam duration and the logs and the output of the cheating indicator system.

6.4.6 INPUT OF GRADING RESULTS

The exam is graded, where auto-graded questions (e.g. multiple-choice and matching) are corrected, otherwise they are sent to the examiner who is to grade them manually and enter the score into the system using his examiner's credentials.

6.4.7 PENALTY BASED ON THE CHEATING INDICATOR RATE EXTRACTED FROM THE GENERATED SESSION REPORT

A penalty is applied on the total score, based on the cheating indicator's output – the cheating probability score in the generated session report. For instance, the penalty on a cheating probability score of 60% and more could be Failure/

Rejection/ Being debarred from re-attempting the exam, either for a period or for lifetime; while for lower scores, an equation could be set according to each institution's standards.

6.4.8 SECURE EXAMINATION APPLICATION AUDITED AND CERTIFIED BY A COMPETENT AUDITOR

A full screen locks the examinee's desktop to prevent access to any resources from local disks, by the network or the Internet. Windows shortcuts are disabled, and the system relinquishes full control of the hardware only on exam termination. In addition, the system must:

- be free from any vulnerabilities to the extent of existing knowledge of vulnerabilities at the time, and
- implement Robust Encryption (Preferably AES).

6.4.9 SECURED NETWORK TO CONNECT THE EXAMINATION WORKSTATIONS AUDITED AND CERTIFIED BY A COMPETENT AUDITOR

The local area network connecting the examination workstations should be suitably secured with MAC binding, and various router and switch security related best practices in place. Also, the connectivity to the server administering the examination must be either through an isolated network (if local) or through a secure VPN (if remote), as is generally the case.

6.4.10 SECURE, HOMOGENOUS SYSTEM CONFIGURATION ON ALL EXAMINATION WORKSTATIONS

All Examination Workstations must be configured centrally with relevant policies for security.

6.4.11 SECURE SERVER CONFIGURATION, AUDITED AND CERTIFIED BY A COMPETENT AUDITOR

The servers administering the examination (and grading, if applicable) and interacting with the security systems like the Cheating Indicator System or other biometric systems should be configured with the best security practices, like:

- access should be limited to specific authorized IPs while all other requests dropped by a reverse proxy,
- effective logging must be configured to take place, and periodic log review procedure must be in place,
- there should be no services installed unless required, and that requirement is documented,
- there should be no open ports except those required,
- the server should have its relevant policies configured, e.g.,
    - Audit Policy
    - Password Policy
    - Account Lockout Policy
- *default* banner of the server should be modified,
- Admin User must be renamed, and unique as well as separate user accounts must be created for all users, and
- *Default Shares* must be disabled.

6.4.12 DISTRIBUTED FIREWALL

The model prescribes the use of distributed firewall techniques to control the network packets of all machines, and to centralize the security policy management to control the security policies of all machines.

6.4.13 ROBUST NETWORK ARCHITECTURE TO PREVENT ANY DELAY OR DISRUPTION DUE TO THE NETWORK

Networking robustness is a critical issue and a high priority in Online Examination Systems. The explosion of the Internet made the use of effective congestion control algorithms for the TCP/IP protocol, which was designed for best effort services, a necessity. The design of effective congestion control strategies is known to be difficult because of the networks' structural complexity, the nature of services supported, and the QoS parameters involved. As a result, the network architecture must be designed with the ability to cope with these difficulties in order to devise effective, robust congestion control techniques as an alternative (or supplement) to traditional control approaches.

6.5 PROPOSED POSSIBLE PRACTICES FOR ONLINE EXAMINATIONS

- Antivirus software should be installed and updated with the latest signatures.
- The operating system should be updated with the latest patches.
- Internet should be disabled on all the examination workstations.
- WLAN, USB and CD/DVD should be disabled on all the examination workstations.
- Guest account should be disabled in the server and workstations.

- All browser plug-ins should be removed.
- No remote administration (e.g., VNC, Rlogin, RDP etc.) tools should be installed on the examination workstations.
- All examination workstations should be capable of operating continuously for 3-4 hours.
- All examination workstations should be cleaned of malware prior to the examination.
- Performance of mice and keyboards should be ensured.
- Sufficient power cables and patch chords should be available in case of any failure of cables.
- There must be sufficient power back-up to support the entire system for 1.5 times the examination duration.

6.6 LIMITATIONS AND CHALLENGES

The proposed model, like in case of any system, has certain challenges and limitations due to technology or human error or wrongdoing. Some of these obstacles or challenges need to be resolved technologically yet, while others, procedurally, to obtain the optimal security and performance. Some of these challenges are listed below:

1) Video Processing and Feature Extraction: Still needs to be enhanced for better accuracy in feature extraction and matching.
2) Internet Speed and Robustness: This model requires high-speed and stable internet connection, especially at the peak times. This challenge is being tackled day by day.

3) Performance and Capacity: It requires high specification for the VFKPS server in terms of processor speed and disk space.

4) Implementation Complexity: Automatic video processing and feature extraction is still complex to be implemented, and researches are still being conducted to overcome this issue. Moreover, its users require special-purpose hardware. Hence, it is hard to be implemented nowadays.

5) Failure Penalties: In failures such as internet disconnection or power failures, which are highly probable in many countries, the answered questions cannot be reviewed for security purposes.

6.7 CONCLUSION

The model presents an effective system which uses multiple safeguards, both preventive (technological, psychological) and detective (technological), against any of the vectors of the security breach. That been said, it is emphasized that 100% security can never be achieved. This is because of discovery of new vulnerabilities and exploits. Therefore, it is necessary, as a good practice, to test and monitor information systems and their associated controls at least every six months, along with keeping the Operating Systems and Applications patched up and updated.

CHAPTER 7

PROPOSED SECURITY PROCESSES AND PROTOCOLS IN DIGITAL ASSESSMENT

7.1 DATA CENTRE

First and foremost, need for Digital Assessment, i.e. computer based examination, is a secure Data Centre (at least tier 4) with a disaster recovery data centre in a different seismic zone. All modules of Digital Assessment except Content Engine (Local Instance) and Assessment Examination Centre (AEC) should be hosted in secured, centralised Data Centre. Independent auditors to audit the service provider for compliance with ISO 27001. There has to be a security policy governing all data centre operations. There has to be internal audit periodically. Primary DC and Secondary DC have to be in different seismic zones to ensure operation continuity. DC Virtual Machines, servers and network devices should also be CERT-In certified.

The Data Centre (DC) IT infrastructure that hosts all web-based applications comprises of several tiers. Each tier handles a particular set of functions, such as serving content (web servers), implementing business logic (application servers) or processing database transactions (Database servers). When the end user issues a request via a web browser to the web server, the web server pre-processes the request and relays it to the application server. The application server obtains necessary information from the database, processes the request and responds to the web server. The web server, in turn, formats and displays the response to the user.

A multi-tier architecture offers the following benefits:

- It is easier to modify or replace any tier without affecting other tiers.

- Adequate security policies can be enforced within the server tiers without hindering the customers.

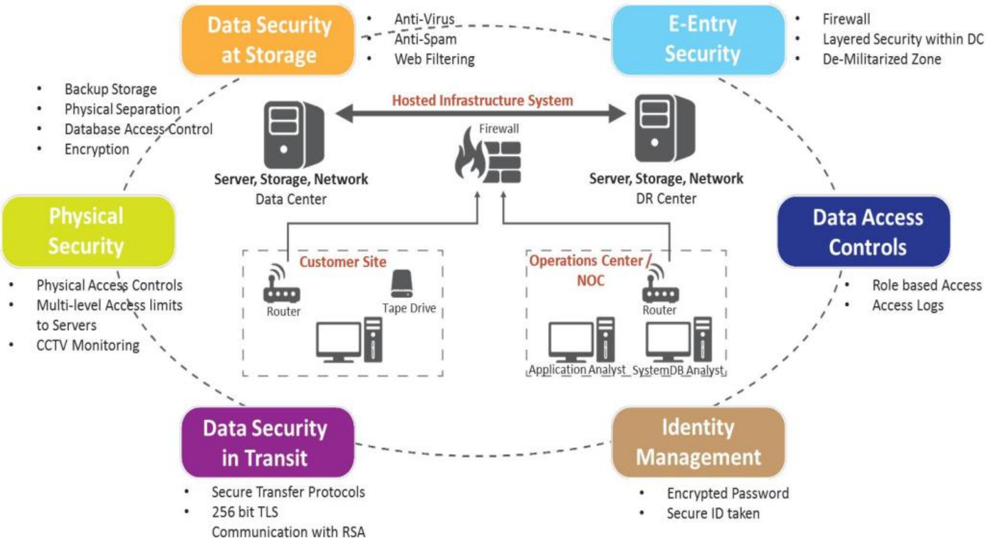


Fig 7.1: Comprehensive Security Framework Encompassing Data Security, Physical Security, Application and Network Security

7.1.1 FIREWALL

There has to be hardening controls in operating systems, applications, databases, network, and server components. A layered, firewall architecture segregates all servers across different network segments. The firewall provides stateful packet inspection for all the incoming traffic towards any of the servers. The firewall rule base and policies implement access restrictions should be for servers in each tier. For example, a database server may require additional layer of protection because it is more sensitive than the web server that provides the front-end of the application.

The Firewall components deployed in the data centre as under:

- Separate setup for Internet and for MPLS (both in High Availability mode)
- Layer 3/4 stateful packet inspection capabilities

- IPSec VPN connection supported
- VLANs for isolation
- FWSM Firewall Switch Module on core switches providing packet firewall features

7.1.2 INTRUSION PREVENTION SYSTEM (IPS)

An inline IPS from Tipping Point needs to be used along with the firewall in the perimeter layer. An IPS prevents external attacks on vulnerable applications and OS. It will prevent attacks such as Denial of Service, Sync Floods, etc. IPS will provide efficient protection against zero-day attacks as it automatically updates virus signatures and provides the necessary protection without user intervention.

7.1.3 SERVER HARDENING CHECKLISTS

The policies need to be in place to define Linux and Windows Server hardening checklists. These are reference checklists, organized as a collection of risk areas required to be covered as part of installation of new server operating systems. The aim has to be successfully hardened Linux and Windows Operating Systems so that there are no vulnerabilities left, making the environment secure. All servers need to be hardened in line with these checklists.

7.1.4 OTHER SECURITY CONTROLS

Apart from firewalls, IPS and server hardening checklists, several other controls need to be employed to comprehensively secure the infrastructure:

1. Transport Layer Security (TLS) is used to authenticate and access hosted web applications. F5 load balancers implement TLS.
2. FWSM controls access to servers. Access to the unified storage system (FC, iSCSI, NFS and CIFS) too is configured through FWSM.
3. A demilitarized zone is implemented for Internet or public-facing services such as email relay and DNS.
4. 24/7 manned security and video surveillance in DC premises.
5. Biometric based physical access controls in the DC premises.

6. A managed antivirus system is deployed in the DC. Anti-spam and anti-spy-ware systems are implemented.
7. An isolated management LAN runs services to proactively monitor and manage servers.
8. Proactive patch management policies and deployment procedures are implemented in the DC.
9. Database schemas for each exam to be maintained separately.

7.1.5 LOG CORRELATION TO TRACE SECURITY INCIDENTS

Details about incoming requests and its subsequent processing need to be captured in individual tiers. In case of disputes and incidents, the logged details to be co-related across tiers to create a complete trace.

Web Server logs

The web server logs should capture all requests that come to the Apache Web Server. They should capture the following:

- The URL that was requested
- Time at which the request was made
- The IP address from which the request was made
- The cookie that could give an indication of the user making the request
- The amount of data that was sent out
- HTTP status
- Time taken to serve the request

Application Access Logs

Application Access logs should capture the following:

- The URL that was requested
- The time at which the request was made
- The amount of data that was sent as part of the request
- The amount of data that was sent back for the user
- The time taken to serve the request

Application Monitoring Logs

- The user and the organization that made the request
- The time taken to execute the main methods in the request
- The queries executed and the time taken to execute each query
- Application exceptions

Application Exception logs

Application level logs will capture all errors, warnings and exceptions that are generated in applications along with the time at which they occurred.

Audit logs

Audit logs need to capture the following:

- For a database record, the last user who created or updated the record
- For a database record, the last create or update time

Additionally, it is possible to turn on audit logs for a specific application table. In this case, all changes to the data records are logged in a parallel audit table and all past versions of a record are maintained here.

Time on all the servers is maintained in-sync using an NTP server. Based on timestamps in different logs mentioned above, it is possible to track the progress of a request, from the time it hit the web server, through the Application Server, and through the queries executed and the data updated in specific tables. It is thus possible to track data changes that have occurred due to different actions taken by users of an application. Logs are maintained for normal users as well as privileged users such as application administrators.
Privileged users cannot turn-off logs; all activities of all types of users can be traced and audited.

7.2 CANDIDATE RELATED PROCESSES

7.2.1 PRE-EXAM: APPLICATION FORM

Application form is hosted in secure Data Centre (DC). Candidate will initially connect to via internet, click on Registration link and get re-directed to the application form hosted in DC. Candidate will fill in the application form, make the required payment and submit the application form. Post successful submission, candidate will be provided with a User Name and Password, which will get shared by Email. Post this, the candidate can login using the assigned credentials and post successful authentication, will be allowed to view the submitted application.

7.2.2 PRE-EXAM: DOWNLOAD OF ADMIT CARD

Candidate will login using the assigned credentials and post successful authentication, will be allowed to view and download the system generated admit card.

7.2.3 EXAM DAY: CAPTURE OF PHOTO AND BIOMETRICS

Candidate's photo and biometrics are captured prior to exam, at the registration machine which will be located at the entrance of the test centre's lab. The captured files are directly saved in the corresponding Assessment Primary Server, used in the test centre.

- Biometric files are stored in FPT format - Fingerprint Image Data ((ISO/IEC 19794-4:2005) / FMD - Fingerprint Minutiae Data ((ISO/IEC 19794-2:2005) formats which are binary image maps and as per the guidelines of UIDAI.

- Digital Persona device which is UIDAI compliant and which follows ISO / IEC standard, is leveraged to capture the biometric data.

- Depending on the requirement, at the time of interview, biometric files can be captured again and verified against the biometric file captured on the day of exam.

7.2.4 EXAM DAY: ATTENDING THE EXAM

Candidate system should be booted using specially developed OS through image from Assessment Primary Server.

Key advantages of specially developed OS include:

1. Same OS is made available in all the candidate systems to have better control on candidate system
2. OS of the candidate's system cannot be tampered, as it is always loaded from the Primary server.
3. No linkage from primary OS, and thus RAM utilization is low.

In every candidate system, Launcher module of software would be installed as part of pre-exam process. Exam conducting staff/invigilator would then start the launcher and also input the corresponding system number. Since the candidate is bound to a system, candidate login page would be displayed along with candidate's photo, name, subject for which the candidate is appearing in the exam. The Launcher module will ensure that there are no background applications running when the login page is brought up or anytime during the exam. In the login page, the roll number of the candidate would already be pre-populated. Candidate would not be allowed to edit/delete the displayed roll number. Candidate would be allowed to only key-in the password.

Other key advantages of Launcher would be as follows:

1. Prevent candidate from moving out of candidate console.
2. Continuously check for firewall state and Internet connectivity during assessment.
3. Have control on keyboard and ensure that only the required keys are enabled.
4. Disable all inbound and outbound ports (except Port 80).
5. Allow candidates to login to the systems as per the seating plan.

At the stipulated first login time, candidate will enter the provided login credentials (printed in the admit card/announced in the test centre) and login to the assessment. Post the first login, candidate will be able to read the instructions. At the stipulated exam start time, candidate will click on a provided start link and start the exam.

When the candidate's request will come for the first time to the test centre's primary server, unique question paper (based on question/option shuffling) will get created in the primary server. Every time, a question would be rendered to the candidate from the primary server and every response will be stored back in the primary server.

The exam is conducted over Local Area Network (LAN). Following checks are implemented to ensure security of candidate systems -

- Port Blocking (Inbound and Outbound except operationally required port to connect to LAN)
- Dynamic Internet Checking
- Detection of virtualized hardware
- Detection of additional hardware

7.2.5 EXAM DAY: CHANGE IN CANDIDATE SYSTEM (OPTIONAL)

Before the start of the exam or during the exam, when there is an issue noted in the candidate system, in the primary server, the candidate would first be de-mapped from the allocated system. This will automatically get recorded in the corresponding audit log of the candidate.

When the new system is identified for the candidate and the Assessment Launcher is started from the machine, the new system is now bound for the candidate. This will also get automatically recorded in the corresponding audit log of the candidate. The login screen in the new system would then display the name and photo of the candidate and the name of the subject for which the candidate is appearing. The candidate can then login and continue with the exam.

7.2.6 EXAM DAY: TRANSFER OF RESULTS FROM LOCAL TEST CENTRE TO DATA CENTRE

Post the completion of exam, technical person in-charge of conducting the exam will connect the Primary Server to Internet and then upload the following information from the Primary Server to the Data Centre

- Encrypted Candidate Responses
- Candidate’s Audit Trail
- Candidate’s Biometric Files
- Error Log
- Access Log
- Incident Register
- Drive manager Log
- IT Manager Log
- Transaction Log
- Performance Log

Candidate responses are encrypted using 128-bit AES encryption. These encrypted files are uploaded using HTTPS protocol.

To enhance the security of highly confidential data like the candidate responses and to prevent any kind of data tampering, MD5 Hash Algorithm is also implemented. By this, prior to the data transfer, a hash value is created for the data which is being transferred. Both the data and the hash value are transferred to Data Centre. In the Data Centre, hash value of the received data would be recalculated and both the hash values (generated in the test centre primary server prior to the transfer and generated post the receipt of data in the Data Centre) are compared. When the values are matched, it will give an assurance that the data has been transferred in a safe and secured way and there was no possibility of data tampering.

7.3 QUESTION PAPER RELATED PROCESSES

7.3.1 CREATION OF QUESTION PAPER BUNDLE

The Content Authoring Engine (Local Instance – LI Server) will be installed in authorized system in examination control room. Assessment Engine Authentication (AEA) file would be provided to authorized personnel. Only with the upload of AEA file as a one-time activity, authorized user would be able to connect to CAE LI Server.

Post this, Assessment Specific Authentication (ASA) file will be uploaded and then content authoring can begin. Post the process of creation, review and sealing of question paper (QP), question paper bundle will be created. QP bundle will be 256-bit encrypted file.

7.3.2 UPLOAD OF QUESTION PAPER BUNDLE

VPN Tunnel is established between CAE LI Server and DC. Using the credentials, authorized personnel will login and upload the password protected encrypted QP bundle to DC.

7.3.3 DOWNLOAD OF ASSESSMENT DRIVE

Assessment Drive is a combination of password protected encrypted QP bundle and the list of candidates mapped to the assessment server of the test centre. The technical person in-charge of conducting the exam will initially login to the server using System Access Password and then download the drive (with encrypted QP bundle) using the provided Drive Credentials.

At the stipulated time to enter the QP Bundle Password, the designated person-in-charge of QP Bundle upload will input the password centrally. Test Centre Assessment Server, which is connected to the Internet, at this point in time will pull the password and have it displayed in a masked manner. By this, the IT Manager will also not be able to view the password. Post this, the Drive Commencement Password will be entered at the stipulated time. Question Paper would still be encrypted. QP will get decrypted only when the first candidate’s login request (at the stipulated start time) comes to the assessment server.

7.4 ENCRYPTION AND DECRYPTION

There are 3 parts of encryption implemented in Digital Assessment Solution

QP Bundle Encryption - AES 256 Bit Client Key Encryption is leveraged for QP bundle encryption. This is a patent pending solution in which data is encrypted by a string provided by the customer and converting it to 256-bit key. In this scenario, the development team who has built the solution will also not be able to decrypt the data through code.

Result Data Encryption - RSA Algorithm is leveraged for Result Encryption where private key is kept in customer's instance of Content Authoring Engine (CAE) and only public key is shared for result encryption. Unless private key is shared in the system by the customer, result cannot be processed. From a security perspective, keys and algorithm are maintained separately.

Report Data Encryption - RSA Algorithm is leveraged for Report Data Encryption. All the report files that are generated from system are encrypted again with another key using RSA algorithm. RSA private key used for Result Data Encryption is different from the key used for Report Data Encryption. This is kept different to ensure that no one is able to use the same keys across different phases of exam (Pre-Exam / Post Exam / Report Generation and Sharing)

All keys are stored in CAE software which is installed at customer location in an isolated LAN, which has no internet connectivity. Only public keys are shared for encryption purpose, which cannot be used for decryption. Bundle Encryption and Decryption is automated. For any reason, if the entered password is incorrect, question paper cannot be decrypted. Also, there is no manual mechanism of sharing of bundle password on the ground. On the day of exam, at the stipulated time, when the customer enters the password, the same is automatically transmitted to all the assessment servers, securely in a masked manner. Password is not known to anyone (apart from customer representative) on the day of the exam. All communication to DC is SSL enabled over and above the encryption process mentioned above. Every end point is protected with MD5 Hash checksum to ensure that there is no loss of data in transit.

7.5 ANALYSIS OF LOGS

Log Analysis happens at 3 different levels:

- Several automated checks are part of conduct of the examination and automated incidents are generated and logged. Based on the issues reported and the subsequent analysis, the test centres are kept on hold, till the time issues are resolved by the Centre Head and detailed Root Cause Analysis (RCA) is completed. These test centres, which are on hold status, are not allowed to be reserved for any future exams.

- Detailed checks are done as part of Result Processing to find out abnormalities. Centre level incidents are analysed to identify any unforeseen issue that had happened during the exam.

- All incidents recorded in the assessment servers are visible in real time at the Command Centre. For all the recorded incidents, process is followed to ensure that detailed Root Cause Analysis (RCA) is done and the details are captured in the system.

CHAPTER 8

RECOMMENDED INFORMATION SECURITY POLICIES

8.1 WEB APPLICATION SECURITY

Following are the most critical vulnerabilities which need to be addressed, and hence remedial actions need to be ensured for a secure web based application:

1. **Injection Flaws -** Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.

Impact - *Injection can result in data loss or corruption, lack of accountability, or denial of access. Injection can sometimes lead to complete host takeover.*
Remedial action- Preventing injection requires keeping not trustworthy data separate from commands and queries.

- Server side and client-side validation. Server-side validation is mandatory.
- The preferred option is to use a safe API or stored procedures using bound and typed parameters, which avoids the use of the interpreter entirely or provides a parameterized interface. If a parameterized API is not available, you should carefully escape special characters using the specific escape syntax for that interpreter.

- Use positive or ‘white-list’ input validation, and appropriate canonicalization is also recommended.
- Ensure that a customized error message is shown for any error that has occurred, which gives out very limited information.

2. Cross Site Scripting (XSS) - XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface websites, introduce worms etc.

Impact - *Attackers can execute scripts in a victim’s browser to hijack user sessions, deface websites, insert hostile content, redirect users, hijack the user’s browser using malware etc.*

Remedial action - Preventing XSS requires keeping not trustworthy data separate from active browser content.

- The preferred option is to properly escape all the non-trustworthy data based on the HTML context. Include data escaping techniques in their applications.
- Use positive or ‘white-list’ input validation for protection against XSS.
- Use HTML and URL encoding for applications which accept special characters and meta tags. Such validation should decode any encoded input, and then validate the length, characters, and format on that data before accepting the input.
- Client side and server-side validation should be implemented. Server-side validation is mandatory.

3. **Broken Authentication and Session Management -** Application functions related to authentication and session management are often not implemented

correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.

***Impact** - Such flaws may allow some or even all accounts to be attacked. Once successful, the attacker can do anything the victim could do. Privileged accounts are frequently targeted.*

Remedial action –

a) **Session Fixation:** The following solution can be implemented for fixing the session fixation flaw:
   - Follow a secure session management lifecycle which includes proper initialization, maintenance, authentication and termination of the session token.
   - Application should generate different tokens for pre-authentication and post authentication. It is mandatory for the web application to provide a unique, random and fresh session token after the user has authenticated to the web site.
   - Do not allow the login process to start from an unencrypted page. Always start the login process from a second, encrypted page with a fresh or new session token, to prevent credential or session stealing, phishing attacks and session fixation attacks.
   - Consider regenerating a new session upon successful authentication or privilege level change.
   - Only use the inbuilt session management mechanism. Do not write or use secondary session handlers under any circumstances.
   - Do not accept new, preset or invalid session identifiers from the URL.

b) **Improper Session Termination:** The following solution should be implemented to fix this vulnerability:
   - Follow a secure session management lifecycle which includes proper generation, maintenance and expiration of session tokens.

- Session tokens should expire or get destroyed from the server, once user logouts from the application.
- Ensure that every page should have a logout link. Logout should destroy all server-side session state and client-side cookies.
- Back button in the browser should be disabled, once user redirects to login page.

c) Improper Session Timeout: The following solutions should be implemented to fix this vulnerability:

- Follow a secured session management lifecycle which includes proper initialization, maintenance, authentication and termination of the session token.
- Authenticated session should time out/expire automatically, after a certain period of time, when the user is idle.

d) Cache Control Implementation: The following solutions are recommended for the mentioned flaw:

- Access control mechanism should be extensively tested to be sure that there is no way to bypass it.
- Multiple mechanisms, including HTTP headers and Meta tags should be used to ensure that the pages containing sensitive information are not cached by user's browsers.
- Authentication pages should be marked with all varieties of no cache tag to prevent someone from using the back button in a user's browser to back up to the login page. Some of the tags are:
  - **Cache-control: private**
  - **Cache-control: no-cache**
  - **Cache-control: no-store**
  - **Cache-control: pre-check=0**
  - **Cache-control: post-check=0**
  - **Cache-control: must-revalidate**

- **Pragma: no-cache**

To prevent browser caching of internal pages of the application in Mozilla Firefox:

```
<head id="ctl00_Head1"><title>
Untitled Page
</title>
<script type = "text/javascript" >
 function burstCache() {
if (!navigator.onLine) {
        document.body.innerHTML = 'Loading...';
         window.location = 'ErrorPage.html';
       }
  }
</script>
```

Note: Implement the above recommended solution throughout the application.

4. **Insecure Direct Object Reference –** A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

***Impact** - Such flaws can compromise all the data that can be referenced by the parameter. Unless the name space is sparse, it's easy for an attacker to access all available data of that type.*

Remedial action **–** Preventing insecure direct object references requires selecting an approach for protecting each user's accessible object (e.g. object number, filename etc.):

- Avoid exposing your private object references to users whenever possible, such as primary keys or filenames.
- Use per-user or session indirect object references. This prevents attackers from directly targeting unauthorized resources. The application has to map the per-user indirect reference back to the actual database key on the server.
- Check access. Each use of a direct object reference from a non-trustworthy source must include an access control check to ensure that the user is authorized for the requested object.
- Instead of sending primary keys (like code in the above scenario) in URL, it's better to use **session** to send such a kind of information.
- If you must expose direct references to database structures, ensure that SQL statements and other database access methods allow only authorized records to be shown.

5. **Cross Site Request Forgery -** A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate those requests which the vulnerable application *thinks* are legitimate requests from the victim.

***Impact** - Attackers can cause victims to change any data the victim is allowed to change or perform any function the victim is authorized to do.*

Remedial action – Preventing CSRF requires the implementation of the following solutions:

- Use a CSRF guard code. A CSRF guard code is a server-side code that inserts a hidden random value in the requested page of a web application. When that page is resubmitted to the web server with some user input, this hidden value is verified by the CSRF guard code. If the resubmitted page contains the hidden value, it is allowed through for further processing. If the hidden value is not present, the CSRF guard blocks that page with the user input.
- Avoid the inclusion of unique token in the URL, which is subject to exposure, and ensure that length of the token string is large, if possible.
- Use **POST** instead of **GET** requests. Even though the attack shown here was carried out on a POST request, forging fake POST requests is much harder than forging GET requests.
- Another countermeasure which should be considered is using the referrer header field to validate the origin of the request. Even though it can be faked, it makes it more difficult for the attacker.

Note: Implement the above recommendation solution in all the authorized pages in the application.

6. **Security Misconfiguration**– Security misconfiguration can happen at any level of an application stack, including the platform, web server, application server, framework, and custom code. Attacker accesses default accounts, unused pages, un-patched flaws, unprotected files and directories, etc. to gain unauthorized access to or knowledge of the system.

Impact – *Depending on the information, such flaws frequently give attackers unauthorized access to some system data or functionality. Occasionally, such flaws result in a complete system compromise.*

Remedial action –Developers should use tools to try to make their applications generate errors. Applications that have not been tested in this way will almost certainly generate unexpected error output. Applications should also include a standard exception handling architecture to prevent unwanted information from leaking to attackers. Preventing information leakage requires discipline. The following practices have proven to be effective:

- Ensure that a customized error message is shown for any error that has occurred, which gives out very limited information.
- Disable or limit detailed error handling. In particular, do not display debug information to end users, stack traces, or path information.
- Application should be made secured to prevent revealing of any kind of error, and hardening process should be carried out periodically.

7. **Insecure Cryptographic Storage -** Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes.

***Impact** -Can compromise the complete application.*

Remedial action – The following solutions should be implemented to fix the above vulnerability:

- Sensitive data should be kept encrypted within the database and it should never reflect within the web application interface.
- Don’t store sensitive data unnecessarily. Discard it as soon as possible.

8. **Failure to Restrict URL Access -** Many web applications check URL access rights before rendering protected links and buttons. However, applications need to perform similar access control checks each time these pages are

accessed, or attackers will be able to forge URLs to access these hidden pages anyway.

***Impact** - Such flaws allow attackers to access unauthorized functionality. Administrative functions are key targets for this type of attack.*

Remedial action – Preventing unauthorized URL access requires selecting an approach for requiring proper authentication and proper authorization for each page. Frequently, such protection is provided by one or more components external to the application code. Regardless of the mechanism(s), all of the following are recommended:

- The authentication and authorization policies should be role based, to minimize the effort required to maintain these policies.
- The policies should be highly configurable, in order to minimize any hard-coded aspects of the policy.
- The enforcement mechanism(s) should deny all access by default, requiring explicit grants to specific users and roles for access to every page.
- If the page is involved in a workflow, make sure that the conditions are in the proper state to allow access.

9. **Insufficient Transport Layer Protection -** Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic. When they do, they sometimes support weak algorithms, use expired or invalid certificates, or do not use them correctly.

***Impact** - Such flaws expose individual users' data and can lead to account theft. If an admin account was compromised, the entire site could be exposed.*

Remedial action – The following solutions should be implemented to fix the above vulnerability:

- At Login page, the password should be strongly encrypted using salted hashing, before traversing into the LAN.
- Use pure hashing where application generates a new password for the users.

Note: Implement the above recommendation solution throughout the application wherever the application is dealing with sensitive information over the network traffic.

10. **Un-validated Redirects and Forwards -** Web applications frequently redirect and forward users to other pages and websites, and use the non-trustworthy data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Impact *- Such redirects may attempt to install malware or trick victims into disclosing passwords or other sensitive information. Unsafe forwards may allow access control bypass.*

Remedial action – The following solutions should be implemented to fix this vulnerability:

- Simply avoid using redirects and forwards.
- If used, don’t involve user parameters in calculating the destination. This can usually be done.
- If destination parameters can’t be avoided, ensure that the supplied value is valid, and authorized for the user. It is recommended that any such destination parameters be a mapping value, rather than the actual URL or portion of the URL, and that server-side code translate this mapping to the target URL.

11. **Malicious File Upload and Execution -** Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.

Impact - *Whole application server can be compromised.*

Remedial action – The following solutions are recommended to fix this flaw:

- Application should check the allowed File extension and File type (MIME Type) in the upload module using white-list filter at server side.
- File to be uploaded should be restricted to a particular size.
- Server-side check for not allowing long filename with double extension / double dot(.) / nullbyte(%00) / meta characters.
- Assign only Read and Write permissions to the upload folders as required.

12. **Denial of Services –** Attackers can consume web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.

Impact –*Can deny the accessible resource in the application; also choke the server bandwidth by consuming server resources extensively and fill the recipient mail box with spam mails.*

Remedial Action – Implement CAPTCHA's in all the forms which are publicly accessible in a proper way for carrying out transactions in order to prevent Denial of Service attack.

13. **No Lockout Policy -** Weak passwords allowed in the application can make attacker guess the password and brute force for the password if the username is known, if no account lockout policy is implemented in the application to block user after particular invalid attempts.

Impact *– An attacker can access the application as a valid user and can do the entire authentication task privileged by a legitimate user.*

Remedial Action – The following solutions are recommended for the flaw mentioned above:

- The user should be blocked after a failure of three login attempts. The blocked user can be unblocked by a user with administrative privileges or can be unblocked after a certain period of time.
- Alternatilvey, implement CAPTCHA at login page to prevent brute force attack.

14. **Auto-Fill Feature Enabled -** Browser has the feature to remember/cache all field values entered by end user into the application. Sometimes applications are well coded to prevent such caching of information. This can be misused by a malicious user for some social threats.

Impact *– Depends on data cached by the browser.*

Remedial Action – The following solution is recommended for the flaw mentioned above:

- Auto-Fill feature should be disabled in all forms which are publicly accessible, especially at Login and Registration forms in the application.

15. **Password Auto-Complete Feature Enabled -** A malicious user could gain access to the website due to “Remember Passwords” functionality of the client browser.

***Impact** - Can compromise the account of a valid user without his knowledge.*

Remedial Action **–** The following solution is recommended for the flaw mentioned above:

- Remember Password functionality feature should be turned off in the application.

16. **No Audit Trail Report for Admin User -** The application does not maintain any record of the application usage in the form of a report or audit trail. Any malicious activity cannot be monitored or traced back. In case of any misuse or attack, it may be difficult to trace and locate the origin.

***Impact** - Malicious activity will not be traced in the application.*

***Remedial Action* -** The following solutions are recommended for the flaw mentioned above:

Audit trails required:

Description: Applications should have adequate repudiation controls, such as web access logs and audit trails at every tier. A common task, typically required from the audits, is reconstructing the chain of events that led to a certain problem.

The following guidelines are required to be followed for audit trails:

1. Information to be logged includes the following: IP address of the originating Source, Date, Time, Username (No Password), session details, Referrer, Process ID, URL, User Agent, Countries (if any) in addition to other details to be logged in the web application.

2. Logging of Authentication Process, which includes number of successful and failed login attempts.

3. To create audit logs, use auto-numbering so that every logged entry has an un-editable log number. Then if one audit entry is deleted, a gap in the numbering sequence will appear.

4. Report of the web application logs to be generated weekly by the administrator to keep track of the web application activities.

Example: Failure and successful login attempts can be something like below.

User name	**Time Stamp**	**IP address**	**Login/Logout**
Admin	02/02/2017; 2.30.1	192.168.1.77	Login Failed
Username	03/02/2017; 2.30.1	192.168.1.77	Login Successful
Testing	04/02/2017; 2.40.5	192.168.1.77	Logout

It is at the discretion of the application owner to determine which application-specific information is to be logged.

8.2 PASSWORD POLICY

It is recommended that the following password policy for the application may be adopted.

1. Password length must be minimum 8 characters.

2. Password must contain characters from the following four categories:

   - At least one upper case letter: (A – Z)
   - At least one lower case letter: (a - z)
   - At least one number: (0 - 9)
   - At least one Special Characters: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ `{ | }~

3. Password history can also be maintained in order to not use the same password again and again.

8.3 DATABASE SERVER SECURITY

8.3.1 ELEMENTS OF DATABASE SERVER SECURITY

A) Database vulnerabilities

A thorough security analysis of a database server must be much broader, assessing potential vulnerabilities in all possible areas like:

- Risks associated with vendor-supplied software:
  - Bugs
  - Missing operating system patches
  - Vulnerable services
  - Insecure choices for default implementations and configurations
- Risks associated with administration:
  - Security options available but not used correctly
  - Risky default settings
  - Improper granting of excessive privileges to users
  - Unauthorized changes to the system configuration
- Risks associated with user activity:
  - Poor password strength
  - Inappropriate access to critical data
  - Malicious activities, such as stealing contents of databases

B) Database security

Database security can be divided into the following key points:

- Server Security
- Database Connections
- Table Access Control
- Restricting Database Access

All of these vulnerabilities need to be considered when securing database servers.

C) Server security

Server security is the process of limiting actual access to the database server itself. It is the most important aspect of security and should be carefully planned.

- The database server should not be visible to the world.
- There should be no anonymous connection.
- A database server supplying information to a dynamic website should never be on the same machine as the web server.
- If a database server is supplying information to a web server then it should be configured to allow connections only from that web server.
- Every server should be configured to allow only trusted IP addresses.
- A database server supplying information to a homegrown application running on the internal network should only answer to addresses from within the internal network.

D) Database connections

- All updates to a database via a webpage should be validated.
- No data should be allowed to be submitted if a normal user can't input data.
- A super-user account like "sa" should not be used for every connection and data source on the server.
- Only the minimum privileges required by a user to connect with a database should be provided.

E) Table access control

Table access control is one of the most overlooked forms of database security because of the inherent difficulty in applying it. Properly using table access control will require the collaboration of System Administrator, Database Administrator and Database Developer.

F) Physical location of server

Physical protection should be provided to the server, depending upon the importance of data being stored in it.

G) Separate storage area

A separate storage area for keeping the backup of the database and archive should be decided in advance.

H) Identify users and their needs

Identify the types of users and grant them minimum access permissions to the database, depending upon their needs.

I) Security policy

A security policy consisting of the procedures and regulations, needed to maintain a desired level of system security, should be based on:

- **Identification of Security Requirements**
- Identify the business importance of the data and the associated processing system
- Assign a security priority to the data, based on the business case evaluation
- Identify the classes of users requiring access to Database Server and the data that it controls
- Identify the system resources that require protection to ensure continued availability data to all valid users.

- **Identification of Security Levels**
- Minimal Security: Users have unrestricted access to all database server resources. No one performs security related auditing and no formal security policy exists.

- Moderate Security: A small privileged subgroup has unlimited access. The DBA performs only occasional auditing of security-related events, and no formal security policy exists for the users.
- High Security: The DBA is the only user whom database server permits to perform the following security-related actions:

  - Define username/password combinations to whom database server will grant access.
  - Define and control the auditing of security-related events.
  - Review the results of security-related audits.

J) Guidelines for each user

Each user should receive a document that states the security policy, explains the importance of security, outlines the role of the user in supporting that policy, and defines the guidelines for protecting passwords and data.

8.3.2 INSTALLATION AND CONFIGURATION

A DBA should keep in mind the requirements and applications of the database server before starting the installation. The DBA, in consultation with management and Network Administrator, should:

a) Check the License of the Database Server Software

Ensure that the instance being installed is legal and properly licensed.

b) Check for Appropriate Version

Ensure that the instance to be installed matches with the hardware and software already present in the organisation.

c) Type of Installation

Choose custom mode of installation to change the default values and avoid known vulnerabilities of the database server.

d) Change default passwords

No default passwords should be kept for the database server. Secure passwords should be assigned to all the accounts and objects as defined in the password security policy of the organisation.

e) Disable/Remove unnecessary accounts

Any account created while setting up the server should be disabled or deleted if not required. If the account has to be kept then the password should be changed.

f) Remove Unnecessary Scripts

Any script installed or copied during installation of the server should be deleted as soon as possible to secure the database.

g) Verify the Features Installed

After the completion of installation, ensure that all the required features have been installed and no required feature is missing.

h) View Error Log

After completion of the installation, the error log should be reviewed to ensure that there was no error in the installation.

i) **Calculate Checksum**

Checksum of the files installed should be performed to ensure that all the required files have been installed and there has been no error in the installation.

j) Install All the Patches/Hot-Fixes/Service Packs

Install all the patches available to strengthen the database server. Any hot-fixes and service packs provided by the vendor should be installed immediately.

k) Change Port Number

Change the default ports used by the database in consultation with the Network Administrator.

l) Implement Auditing Policy

Implement the auditing policy of the organization.

m) Create an Extra Administrator Account

Create an extra account with Administrator privileges to recover from any situation in which the database server or administrator account is compromised. It should be kept confidential.

n) Create an Account for Back-up and Archiving

Create a separate account for backing up the database and archiving it. This account should be different from the administrator account.

o) Create Sufficient Tablespace

Ensure that sufficient tablespace has been provided to all the applications, so that no application comes in conflict with system tables for space and resources.

8.3.3 OPERATIONS AND MAINTENANCE

a) User and Application Accounts

- During installation, some default accounts are setup. Keep an inventory of all the accounts and disable or remove the unnecessary ones.
- Assign privileges to application-owner account as per their roles. Make a policy for assigning roles and privileges, and follow that when opening new user accounts.
- It is advisable to secure RMAN account properly, because anyone who can access that account can alter backup schedule and destinations.
- Make sure that the passwords are not visible by file searches (such as use of the UNIX grep command).

b) Control the Distribution of Database Name

Service names and aliases should be used to mask the physical location and name of every database in the system.

c) Encrypt the Contents

Enable encryption of stored data on a high-risk database environment. Any user trying to access the data should need the right password as well as the encryption key.

d) Effective Auditing

Logs should include the time and date of activities, the user ID, commands (and command arguments) executed, ID of either the local terminal or remote computer initiating the connection, associated system job or process number, and error conditions (failed/rejected attempts, failures in consistency checks, etc.)

e) Make Password Changes Mandatory

Users should be required to change their passwords frequently. Force passwords to expire and prevent the reuse of old passwords.

f) Isolate Production Database

A Production Database should be kept separate from development database.

- Revoke operating-system-level access for developers on the production server and implement a standardized change-control process.
- Never publicize the name of the database and server supporting the production application.
- Forbid the use of the production database for development or testing.

g) Dormant Accounts

Accounts must be regularly reviewed for inactivity, and any dormant accounts should be suspended.

h) Privileged Accounts

Passwords for privileged accounts should be given only to people with a need for privileged access. The passwords for these accounts must be encrypted when network is used to access them.

i) Test Security Patches

Vendor or author provided security patches must be evaluated for compatibility, and installed.

j) Display Warning Banner

Wherever feasible, a login banner, stating that the system is for authorized use only, should be displayed for anyone attempting to connect to the system.

k) Hide Vendor & Software Information

Wherever feasible, all operating systems, version/release numbers, and vendor information provided in login/sign-on banners should be limited or disabled.

l) Login Restrictions

Wherever feasible, login restrictions (by time of day, by system address, etc.) should be implemented.

m) Remedial Action

If any unauthorized or undesirable activity is noticed, one of the following remedial actions should be taken to address the problem:

- Change compromised passwords.
- Change access rights.
- Audit intensively all actions of particular users.
- Deny the offending users any access to database.
- Change the security policy.

n) Re-evaluating the Security Policy

A system security policy should not remain static. The following factors make a review of the security policy necessary:

- Changes in the profiles of users who access the system.
- Changes in business needs that raise or lower the value of the data being protected.
- New releases of database server software that might introduce new security features.
- Discovery of security violations, potential violations, or attempted violations.

o) Backup and Recovery

Databases should be protected from accidental data loss. A general backup and recovery strategy must be designed depending on various factors, such as database size, volume of changes, and resources available. Attention must be paid when choosing the backup type (incremental, full) and testing the whole set of procedures to recover the system, in case of a disaster, and in a timely manner.

Backup

Backing up databases should protect against accidental loss of data, database corruption, hardware failures and even natural disasters.

- A database backup records the complete state of the data in the database at the time the backup operation completes.
- A transaction log backup records the state of the transaction log at the time the backup operation starts.

Depending upon the requirements, one of the following ways to back up the database should be selected:

- **Complete database backups**
  Perform a full backup of the database, objects, system tables and data.

- **Differential backups**
  Back up data that has changed since the last complete backup.

- **Transaction log backups**
  Back up all database modifications transaction logs.

- **File and filegroup backups**
  Back up database files and filegroups rather than the entire database.

Recovery

A backup is only as good as the recovery it can provide. A DBA may experience one or more of the following database integrity problems and will be required to recover the lost data.

Invalid Data - This is the smallest, but most common database problem. It occurs when a finite number of invalid entries find their way into the data.

Corrupted Database Object - The next level of database problems includes situations in which a single or limited number of database objects have become corrupted or invalid.

Full Database Corruption - At this level, the scope of the problem is so significant that the database is no longer operational and a full database recovery must be performed.

Multiple Database Corruption - The largest levels of database problems occur when multiple databases within the enterprise have been corrupted and must be recovered as a set.

- **Transaction Recovery**

  Transaction recovery, also known as data-level recovery, allows DBAs to precisely identify and correct the invalid data. The DBA should select and examine each of the changes that were applied to the database by using selection and filtering capabilities.

- **Database Object Recovery**

  Database object recovery allows DBAs to identify and recover only the missing or the damaged objects. DBA should use tools available for Object recovery containing built-in database intelligence to identify all of the objects making up the database from information captured when the backup was taken. This information can be then matched against the existing database environment. Missing or invalid objects can then be automatically recovered from the physical backup of the database, while valid objects remain unaffected.

- **Full Database Recovery**

  The DBA may need to recover the entire database. This requires the database to be closed. During this time, users will not be able to access important business critical applications.

- **Multiple Database Recovery**

  The DBA should select tools that combine an enterprise -wide view of the organization with maximum database recovery capabilities. This enterprise-wide recovery management console allows consistent, reliable backup and recovery plans to be established and automated.

8.3.4 WEB BASED DATABASES

Access to a web based database server is via network connections, such as SQL/net. Authentication is often an automated or scripted task, or the network access is via a single username as far as the operating system on the server is concerned.

a) Configuration for Web-Based Database Servers

It is recommended that in a web-based application, a typical configuration should keep the database with the sensitive information behind a firewall. It will be accessed from an application-server, also located behind a second firewall, which will receive the web server requests. This three-tier design isolates the Web server from the database, isolating the database server from the outside users by two dedicated private networks. Only the Web server can communicate through the firewall with the application-server, and only this can communicate with the database. This configuration is relatively secure and special attention must be paid on securing the information sent to the client from the Web server, the Web server itself and the database/application-server system. The application-server will incorporate the event logging and the security analyzer that recognizes the unauthorized attempts to log into an account.

b) Security Threats to Web Based Database Servers

All web-based database servers have ports that they listen to. Most intruders do a simple ‘port scan’ to look for ports that are open, which popular database systems use by default.

For web security, the following three primary areas must be addressed:

- Server security: Ensure security for the actual data or private HTML files stored on the server.
- User-authentication security: Ensure login security to prevent unauthorized access to information.
- Session security: Ensure that data is not intercepted as it is broadcast over the Internet or Intranet.

8.3.5 SECURITY CHECKLIST FOR A DATABASE ADMINISTRATOR

- Ensure that the database RDBMS version is a vendor supported product version.
- Monitor the RDBMS software on a regular basis to detect unauthorized modifications.
- Ensure that all directories and file permissions created by the installation of a RDBMS are protected in accordance with security evaluation specifications if available or, if not, vendor recommendations.
- Ensure that end user accounts are not granted permissions to change directory or file permissions associated with the database software.
- Ensure that all default installation passwords will not remain on DBA database accounts.
- Change all default database account passwords after the application installation and disable default application accounts that are not required.
- Ensure that the following password management rules are enforced:
- Configure all database accounts to be protected by a password, certificate, or approved network-based authentication.
- Assign a temporary password at account creation.
- Store all passwords in an encrypted format.
- No database account name and password should be visible to the host operating system.
- Passwords should be alphanumeric characters and should include at least one numeric character.

- Passwords should not contain consecutively repeating characters.
- Restrict access to files containing logon credentials and encryption keys to SAs and DBAs.
- Ensure that RDBMS installation default object privileges are not granted to the public, except for those object privileges whose removal is not supported by the RDBMS vendor.
- Ensure that all user accounts are granted roles containing the minimum set of privileges required for the application.
- In a shared production/development environment, ensure that no application developer account is given permission to create, alter, or drop schema objects.
- Ensure that application developer accounts on shared production/development systems are at no time given DBA roles within the database or on the operating system.
- Ensure that all database actions are traceable to an individual user logon.
- All database objects should be owned by the database system, database administrators, or by an account created especially for application object ownership.
- Ensure that a tested and verifiable backup strategy is implemented on all RDBMS databases.
- Ensure that roles or application object privileges are not granted to the public.
- Ensure that the DBA role is restricted to authorized DBA accounts in a production environment.
- Ensure that the DBA role is restricted to DBA accounts and authorized application developer accounts in a development environment.
- Restrict assignment of alter, index, and references object privileges to DBAs, object owners and predefined roles.
- Restrict the assignment of the grant option of any object privilege to DBAs.
- Restrict access to the AUD$ table to DBAs and/or security auditors.
- Do not include a version number, vendor name or any identity thereof in production database instance names.

- Protect the environment variable identifying the location of the password file.
- Configure an idle time limit for all database accounts through the use of profiles.
- Deny ‘Everyone group’ any permissions on any database files or directories.
- Restrict write permissions to database registry keys to the Database Administrators and System Administrators.

8.4 NETWORK SECURITY

8.4.1 DESIGN SCREENED SUBNET

The network architecture should be designed to create different security zones/segments for external users, internal users and the servers. The Web server should be placed in the secure Server Security segment (also referred to as DMZ or screened subnet) isolated from the public network and organization's internal network. The network architecture can be designed as a single layer or multi-layer, as per the requirement of the organization.

A Web Hosting Network should have at least three segments. viz.

- Internet Segment
- Public server segment (Web, Mail, DNS servers)
- Internal Segment

A firewall should be used to restrict traffic between the public network and the Web server, and in between the Web server and internal networks. Servers providing supporting services to the Web server (like Database Server, LDAP Server) should be placed on another subnet isolated from the public and internal networks. In a multi-layer architecture, the traffic to this subnet is filtered using another firewall.

8.4.2 ACCESS CONTROLS

The major access control devices, such as routers and firewalls, can be enforced to the network resources at different levels of the network.

A) Router

It is very crucial to secure the router as it is the ‘first line of defense’ to the network of any system. It is hence strongly recommended to apply the required necessary control so as to stop unwanted traffic and attacks at the perimeter itself. For secure configuration of a router, the following should be considered.

- Deploying proper access management and preferably disable remote administration.
- Enabling secret password
- Changing default SNMP community string
- ACLs (access control lists) should include
  - Applying egress/ingress filter
  - Filtering all RFC 1918, 3330 address space and special/reserved addresses
  - Permitting the required services for the required IP Addresses only
  - Denying everything else.
- Turning on logging to a central syslog server

B) Firewall

A firewall can be defined as a combination of hardware and software, located at a network gateway, safeguarding the resources of a network from users of other networks. It implements a boundary between two or more networks, limiting access between networks and network segments according to the local security policy. It filters all network packets in order to determine whether they should be forwarded to their destination or should be discarded.

Firewalls available commonly use different technologies like

- Packet filter

- Stateful Inspection Firewall
- Application Proxy Firewall

Firewall is available as a software utility as well as an appliance. All the above technologies have their own benefits and disadvantages. Users should choose the optimum combination after analyzing the need of the network to be protected and the servers that shall be deployed for it.

A Firewall should be suitably implemented to sort the networks into different network segments. The following should be considered while implementing a firewall system-

- The host on which the Firewall is installed should be secured if a software firewall is used.
- For the firewall installation in an organization, specific security guidelines as specified by the firewall vendor should also be consulted.
- The firewall should be configured for full logging and a mechanism for generating alerts on any suspicious activity.
- A firewall is effective only when proper rules (local security policy) are applied. Thus, the rules should be carefully framed, after considering all the threats and security essentials. Rules are then applied to secure the organizational network and servers installed behind the firewall.

Do's and Don'ts of firewall rule base

- Clean up rule:
  - Place a 'DENY ANY-ANY' rule, at the end of the rule base.
  - Never design an 'ALLOW ANY ANY' rule.
  - ALLOW rules should be formed only for required services and servers.
  - This will lead to all the traffic being disallowed, unless specifically allowed.
- Lockdown/Stealth rule:

        - All traffic destined for the firewall itself should not be allowed.
    - Anti-spoofing rule:
        - Place anti-spoofing rule as per RFC 1918 and 2827
    - Enable DoS/DDoS prevention features on firewall.
        - Several Firewalls contain features to avert DoS attacks and these should be enabled.
    - Enable Application level filtering features of firewall.
        - If the firewall has abilities to perform Application level filtering then they should be enabled.

8.4.3 INTRUSION DETECTION SYSTEMS

An intrusion detection system (IDS) protects the network perimeter, extranets, and the internal network in real-time. An IDS system analyzes the network data stream and determines attempts to hack or break into a computer system. It identifies attacks through various ways, including anomaly detection and signature matching, and can generate an alarm or give a reaction to the attempt of attack.

- The IDS should be updated with the latest signatures. Current rules should be applied and tuned so as to prevent generation of false alarms.

- IDS should be deployed with network sensors in all parts of the network. Host IDs should be implemented on all critical servers, including the web server.

- Rapid development has been seen in this field, with Intrusion Prevention Systems (IPS) now being available. IPS has both pros and cons being an inline device. Thus, IPS deployment can be considered only after careful analysis.

8.5 OTHER MISCELLANEOUS SECURITY

8.5.1 ANTIVIRUS AND SPAM PREVENTION

AntiVirus

- An anti-virus package should be installed on the Web Server system, if available on that platform.
- All clients who access the web server for the purpose of administration and content management should use an antivirus package with the latest signatures.
- All files and documents which are hosted on the web server should not be uploaded until checked for virus and trojans.
- If the Web server has provisions for uploading of files from users, appropriate mechanism should be in place at the server side to ensure that the files are virus-free.

Open Proxy

Some web servers have modules to act as an http proxy server. It is recommended that such modules should not be installed as the web server can be misused as an open proxy if proper controls are not in place.

SPAM Prevention

Some websites contain online forms for forwarding links or documents on the website as mail. It is suggested that mail should not be allowed to any external e-mail addresses, as it may be used to spam external users.

8.5.2 HOST SECURITY

The default configurations in Operating System are typically set by vendors to emphasize features, functions and ease rather than security. Thus, the first step in securing a Web server is to secure the underlying operating system as several security issues can be avoided if the operating systems are properly secured.

In the securing of a Host, the following should be considered:

• Include specific security requirements when selecting the Operating System of the web server.

- Security certification level of the chosen platform
- Level of support provided by the vendor
- Compatibility and support issue of the software to be used on this platform
- Support of security features on the platform, like authentication, levels of access control, support for remote administration and logging

• Minimize the Operating system with only essential services by removing all operating system and network services not required, like Telnet, FTP, NetBIOS, NFS, NIS, etc. and unneeded protocols.

• Keep operating systems and applications software up to date with the latest service pack and patches to protect against common attacks.

• Configure computers for user authentication and remove all unneeded users and groups.

• Configure computer operating systems with appropriate object, device, and file access controls.

• Harden TCP/IP stacks.

• A strong password policy should be enforced.

• Enable detailed logging including failed logging etc.

8.5.3 WEB AND APPLICATION SERVER SECURITY

Web Server Security

Web Server is a program that serves Web pages to Web browsers using the Hyper Text Transfer Protocol (HTTP). Some of the Web Server software contain middle-tier software that act as an application server. This enables users to perform high-level tasks, such as querying a database and delivering the output through the Web Server to the client browser as an HTML file.

In securing a Web Server, administrators should take care of the following:

- Based on security needs, check for presence of specific security-related features on the chosen web server. It may include types of authentication, levels of access control, support for remote administration, and logging features.
- Install only the required features of the Application Servers and remove the default features which are not being used.
- Install the latest version of the web server software along with the latest patches.
- Install web server software in a CHROOT cage.
- Remove all sample files, scripts, manuals and executable code from the web server application root directory.
- Remove all files that are not part of the Website.
- Reconfigure the HTTP Service banner so that Web server and Operating System type and version are not reported.
- Create a new custom least-privileged user and group for the Web Server process, unique from all other users and groups.
- Although the server may have to run as root or administrator initially to bind to port 80, the server should not run in this mode.
- The configuration files of the Web Server should be readable by Web Server process but not writable.
- The server should be configured in a manner so that web content files can be read but not written by the Web service processes.
- Consider security implications before selecting programs, scripts, and plug-ins for the web server.

- Various Server-Side Active Content Technologies are available viz. Java Servlets, ASP, ColdFusion, etc. Each has its own strengths and weaknesses along with an associated risk. Thus, the technology to be implemented on the Web server has to be chosen after due consideration.

- Third-party free modules available should not be used without proper checking and verification of their functionality and security.

- Configure the Web server to use authentication and encryption technologies (SSL), wherever required, along with a mechanism to check the latest CRL (certificate revocation list).

Secure coding practices

Server-side applications are written in various programming languages. However, flaws in the scripts may allow attackers to penetrate a Web server. Thus, the scripts need to be written with due consideration to security.

The following are some of the common secure coding practices.

- Consider security implications before selecting the scripting technology.
- Various client-side Active Content Technologies are available viz. Java applets, javascripts, vbscript, etc. Each has its own strengths and weaknesses along with an associated risk. The technology to be implemented should be chosen after careful consideration.
- On Linux/Unix hosts, the code should not run with SUID.
- The code should use explicit path names when invoking external programs and not rely on the path environment value.
- Input data received through a web page form should be filtered for malicious input.
- Encryption mechanism should be deployed to encrypt passwords.

8.5.4 CONTENT MANAGEMENT

Use of remote authoring tools for editing content directly on public Website is not recommended.

- Carrying out administration of the sever on the console itself is recommended. However, in case of requirement of remote adminstration, computers should be configured for remote administration through a secure channel.
- Web content uploading should be configured through a secure communication channel e.g. SSH, and it should be configured for low session time-outs as well as account lockouts.
- Management clients used for content management should be placed in a screened network zone with limited access.
- Management clients should be hardened and patched with latest OS updates.
- Contents uploaded on the Web Server should be verified to ensure that it is free of any malicious content.

8.5.5 LOGGING AND BACKUP

Logging is a crucial component of security of a Web server. Monitoring and analyzing logs are critical activities as log files are often the best and/or only record of suspicious behavior.

In setting up logging and backup mechanisms the following should be considered.

Logging

- Use a centralized Syslog server

- Alert mechanism to alert administrator in case of any malicious activity detected in logs.

- Use the Combined Log Format for storing the transfer Log.

- Establish different log file names for different virtual Websites that may be implemented as a part of single physical Web server.
- Use the Remote User Identity as specified in RFC 1413.
- Ensure procedures are in place so that log files do not fill up the hard drive.
- Ensure log files are regularly archived, secured and analyzed

Backup

- A proper backup policy should be enforced and ensure regular backup of files.
- Maintain a latest copy of Website content on a secure host or on media.
- Maintain integrity check of all important files in the system. This is possible by either generating md5 hashes of important files or by the use of various software integrity checkers such as Tripwire.

8.5.6 PHYSICAL SECURITY

To protect the hosting system resources, establishment of proper physical and environmental security controls should be present. Protection against physical damage, unauthorized disclosure of information, theft and loss of control over system integrity is provided by physical security controls.

Natural calamity threats

Mitigation of effects of different threats should be taken care of, including the cases of natural calamities.

Physical Access Controls

In order to restrict physical access to the servers, proper access control mechanism should be in place. Biometric access controls can be used for this purpose. With the exception of designated administrators, no one else should be permitted to log on to the server locally on the console.

Electromagnetic shielding

Electro-magnetic radiations emitting from the computer servers may lead to data theft. This can be prevented by electromagnetic shielding of the Server room.

Disaster recovery centre

A replica of the entire server infrastructure should also be formed, depending on how critical the situation may be, at a different physical location so as to recover from any disaster. In case of critical websites, disaster recovery site should be prepared to take over web services whenever needed.

8.5.7 SECURITY AUDIT/PENETRATION TESTING

A security audit basically compares current security practices against a set of defined standards. Vulnerability assessment is a study to locate security vulnerabilities and identify corrective actions.

A penetration test is a real-life test of an organization's exposure to security threats and it is performed to uncover the security weakness of a system.

Organization should carry out these tests regularly and also have them verified by empaneled third party Information Security Auditors and Attack & Penetration (A&P) Testing experts.

8.5.8 SECURITY POLICY

A security policy defines the rules that regulate how an organization manages and protects computing resources to achieve security objectives.

Security requirements of web servers should be included in the security policy of an organization. The following should be incorporated in the security policy:

- Network and host security policy
- Web Server backup and logging policy
- Web server administration and Updating policy
- Classification of documents to be published on Web Server
- Password management policy
- Encryption policy
- Physical security

8.5.9 INCIDENT HANDLING AND RECOVERY

A computer security incident is any real or suspected adverse event in relation to the security of computer systems or networks. It is an act of violating explicit or implied security policy resulting in unauthorized access, denial of service/disruption, and unauthorized use of a system for processing or storage of data or changes to system software, hardware, firmware characteristics without the owner’s knowledge.

A formal policy should be created for Incident handling. A Computer Security Incident Response Team (CSIRT) should be created within the organization to handle incidents through the following six stages of Incident handling

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Follow-up

8.5.10 THIRD-PARTY HOSTING

An organization may not have the required infrastructure and expertise and therefore can use a third-party organization to host the Website. The organization can co-locate their own servers in the service provider's network or directly host on the servers of the service provider itself.

Advantages of third party hosting are:

- The service provider may have greater knowledge in securing and protecting Web servers.
- The network can be optimized solely for the support and protection of Web servers.
- DoS attacks aimed at the Web server shall have no effect on the organisation's production network.
- Compromise of the Web server does not directly threaten the organisation's network.

Disadvantages of third party hosting are:

- It requires trusting a third-party with Web server content.
- It is difficult to remotely administer/update Web server.
- There is little control on the security of the Web server.
- The Web server may be affected by attacks aimed at other Web servers hosted by the service provider on the same network.
- In selecting a third-party hosting organization, a user should keep the following in view:
  - Hosting organization should have a security policy and should implement the best practices for the websites as per this document
  - Hosting organization should have its infrastructure and Web servers audited by auditors. Hosting organization should also have their web servers tested by A&P testing experts periodically and should take immediate steps to plug the security weakness unearthed.

8.5.11 WEB SERVER SECURITY THUMB RULES

- Web administrators should be adequately skilled.
- Use software only from trusted source.
- Keep all software updated.
- IS Security audit and A&P test should be carried out regularly.
- A dedicated machine should be used as a Web server.
- Changes to configuration should be documented (revision control program).
- Central syslog server should be used.
- Encryption should be used.

8.6 ASSESSMENT SECURITY CENTRE

In order to address the critical challenges, like storing question paper in the system without any security, or multiple teams within the systems having access to the question paper prior to the encryption of question papers, a strong protocol needs to be conceptualized and implemented which is termed as ***Assessment Security Centre (ASC),*** and is explained below:

Step1: Upload Empty Question Paper Template:

(a) The content creator will connect to Assessment Knowledge Centre (AKC) and download a question paper template.

(b) The template will then be filled with dummy questions and options. The structure of the question paper will be exactly same as the actual question paper, including the number of sections, section name, question type and option count.

(c) The structure of the dummy paper will be uploaded in the AKC module.

Step2: Download Question Paper Meta Data template:

(a) The uploaded question paper meta data can be downloaded using the "Download meta data for Question Paper" feature from AKC.

(b) The meta data template will have all the generated ids (i.e. question paper id, section id, question id, configuration id, option id, language id and subject id).

Step3: Content Creation at ASC:

(a) The content creator will now use the meta data template and provide the actual content in the excel, without editing the ids in the template.

(b) The template with the content will then be uploaded back in to the ASC module.

(c) The template for all the question papers for all the subjects will be uploaded using the same method.

(d) The images required in the question paper will also have to be uploaded in ASC. ASC will then rename the images as '*orgid_imagename'*. The images and question text are encrypted using the 128/256 Bit AES Encryption Algorithm.

(e) The uploaded question paper can be viewed in *Internet Explorer* for proof reading.

(f) After all the question papers are uploaded in ASC, the content creator can view the uploaded question paper in the ASC module and then select one or many question papers, and generate the *question paper bundle* as required by AEC.

(g) The *question paper bundle* is password protected.

(h) The *question paper bundle* is validated at AEC laptop and on providing the required password, it gets uploaded and starts displaying in *proof reading mode*.

Step 4: Generate Content for distribution:

There are two ways in which the content can be distributed:

1) ***Centralized distribution by uploading it at Assessment Data Centre (ADC):***
    1. The content owner can download question papers created at ASC and upload all of them in ADC, on the eve of the exam.
    2. The system admin then will map these question papers subject wise to the created assessment drives.
    3. The drives will be configured at ADC by providing a passcode for drive start.
    4. The content is then centrally distributed from ADC in the normal approach.
    5. To start the drive, the IT managers need to enter the passcode which will be validated with the passcode provided by the admin.

2) ***De-Centralized distribution from External Media:***
    1. The content creator can download the bundle from ASC and write it in CDs.
    2. CDs can be distributed to the IT Managers of various test centres across the country,
    3. The IT managers need to browse and upload the drive in AEC.
    4. On uploading of the bundle, the IT manager will be required to enter the passcode, which will be validated with the passcode given during the bundle creation in ASC.

Step 5: Upload Question Paper Meta Data template with Content (After Exam):

(a) The Question Paper meta data template, with the actual content, is uploaded back to AKC after the exam is started / completed.

(b) The uploaded template is used to update the dummy content from the actual content in the Database.

CHAPTER – 9

IT SECURITY FOR EXAMINATION CONDUCTING BODY

9.1 SECURITY POLICY IN EXAMINATION CONDUCTING BODY

This top-level information security policy is a key component of overall information security management framework of examination conducting body and should be considered alongside more detailed information security documentation, including system level security policies, security guidance and protocols or procedures.

9.1.1 OBJECTIVE

The objectives of examination conducting body Information Security Policy are to preserve:

- **Confidentiality -** Access to data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- **Availability -** Information shall be available and delivered to the right person, at the time when it is needed.

9.1.2 SCOPE

This policy applies to all assets which processes information which includes systems, networks, applications, locations and users of examination conducting body or suppliers under contract to it.

9.1.3 AIM OF THE POLICY

The aim of this policy is to establish and maintain the confidentiality, integrity and availability of information owned or held by examination conducting body by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principals of security and explaining how they shall be implemented in the organization.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining, within the organization, a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organization.

9.2 RESPONSIBILITIES FOR INFORMATION SECURITY

9.2.1 INFORMATION OWNER

Information security is a responsibility of all employees in the organization but the accountability to ensure the security of the information rests with the owner of the information. On a day-to-day basis, the information owner shall be responsible for managing and implementing the policy and related procedures. The ultimate responsibility, on an organization level, to protect the security of the information rests with the Chief Executive Officer.

9.2.2 RESPONSIBILITIES OF OTHER EMPLOYEES

Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

All staff shall comply with information security procedures including the maintenance of data confidentiality, data integrity and data availability. Failure to do so may result in disciplinary action.

The Information Security Policy shall be maintained, reviewed and updated periodically or as and when required. This review shall take place at least annually.

Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.

Each member of staff shall be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

Contracts with external contractors that allow access to the examination conducting body information shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

9.3 LEGISLATION

The examination conducting body is obliged to abide by all relevant legislations, including both local and international legislations. The requirement to comply with this legislation shall be communicated to employees of the examination conducting body, who may be held personally accountable for any breaches of these legislative requirements.

9.4 POLICY FRAMEWORK

9.4.1 MANAGEMENT OF SECURITY

The examination conducting body IT Department shall be responsible for implementing, monitoring, documenting and communicating security requirements for examination conducting body.

9.4.2 INFORMATION SECURITY AWARENESS TRAINING

- Information security awareness training shall be included in the staff induction process.
- An ongoing awareness program shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

9.4.3 CONTRACTS OF EMPLOYMENT

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.

Information security expectations of staff shall be included within appropriate job definitions.

9.4.4 SECURITY CONTROL OF ASSETS

Each information asset both IT and non-IT asset shall have a named custodian who shall be responsible for the information security of that asset.

9.4.5 PHYSICAL ACCESS CONTROLS

Only authorized personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

9.4.6 USER ACCESS CONTROLS

Access to information shall be restricted to authorized users who have a legitimate business need to access the information.

9.4.7 IT SYSTEM ACCESS CONTROLS

Access to IT systems shall be restricted to authorized users who have business needs to use the system. Access to data, system utilities and program source libraries shall be controlled and restricted to those authorized users who have a legitimate business need e.g. systems or database administrators. Authorization to use an application shall depend on the availability of a license from the supplier.

9.4.8 EQUIPMENT SECURITY

In order to minimize loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

9.4.9 IT SYSTEM PROCEDURES

Management of IT systems and networks shall be controlled through standard documented procedures published and approved by the IT Department.

9.4.10 INFORMATION RISK ASSESSMENT

Information Risk Assessment should be conducted based on the defined and approved Risk Assessment method. Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all the associated actions shall be reviewed at regular intervals at least once a year. Any implemented information security arrangements shall also be a regularly reviewed feature of examination conducting body's risk management program. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

9.4.11 INCIDENT MANAGEMENT

All information security incidents should be handled based on the defined and approved incident management process. All identified weaknesses should be reported to the IT Department or designated incident response team. All information security incidents shall be investigated to establish their root cause and impacts with a view to avoiding similar events in the future.

9.4.12 CLASSIFICATION OF SENSITIVE INFORMATION

The classification 'Confidential' shall be used for customer sensitive data (customer financial information, customer personal information etc.) and employee sensitive data (eg: salary, medical information etc.).

The classification 'Restricted' shall be used to mark all other sensitive information such as financial and contractual records. It shall cover information disclosure of which is likely to:

- adversely affect the reputation of examination conducting body or its officers or cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness of examination conducting body;
- cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organizations;
- prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- breach statutory restrictions on disclosure of information;
- disadvantage the organization in commercial or policy negotiations with others or undermine the proper management of the organization and its operations.

The classification ‘Public’ shall be used to mark all other information which does not fall under the category of ‘Confidential’ or ‘Restricted’. Knowledge of this information does not expose examination conducting body to financial loss or jeopardize the security of examination conducting body’s information assets. Prior to disclosure, public information may be subject to appropriate review or procedures to mitigate any potential risks of inappropriate disclosure. Example of such content are: public website content, published accounts etc.

9.4.13 INFORMATION SHARING

Secrecy or confidentiality of information owned or operated by examination conducting body should be maintained. Information should be protected in transit or at rest and protection should be adhered to as per the classification of information.

- **Confidential Information –** Information so marked shall be held securely at all times in a locked room to which only authorized persons have access. They shall not be left unattended at any time in any place where unauthorized persons might gain access to them. They should be transported securely in sealed packaging or locked containers or in encrypted form (E-data). Information marked 'Confidential' not in a safe store or in transport should be kept out of sight of visitors or others not authorized to view them. Access to information is restricted when data sets are accessible only through a prescribed process of registration/ authorization by respective. Information having restricted access shall be made available to only the recognized users, through defined procedures. The requester of such data may need to authenticate his/her identity and provide a valid reason to access the information in question by producing the correct documentation and authorizations.
- **Restricted Information –** Information declared as restricted shall be accessible only through and under authorization to selected individuals or organizations based on a need-to-know basis.
- **Public Information –** Information that may be accessible freely and the access is provided without any process or registration/authorization is referred to as public information and is freely available to all.

9.4.14 PROTECTION FROM MALICIOUS SOFTWARE

The information system owners shall use software countermeasures and management procedures to protect the system against the threat of malicious software. The staff shall be expected to co-operate fully with this policy. Users shall not install software on the organization's property without permission from the IT Department. Users breaching this requirement may be subject to disciplinary action.

9.4.15 USER MEDIA

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of IT Department before they may be used on examination conducting body systems. Such media must also be checked for virus before being used on the organization's equipment. Users breaching this requirement may be subject to disciplinary action.

9.4.16 MONITORING SYSTEM ACCESS AND USE

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis. A process should be in place to regularly audit the audit trail to ensure no unauthorized or unlawful actions are done using systems of examination conducting body. The monitoring should be implemented based on the local legislation to avoid any breach of regulation.

9.4.17 ACCREDITATION OF INFORMATION SYSTEMS

All product owners shall ensure that all new information systems, applications and networks include a security plan and are approved by the IT Department before they commence operation.

9.4.18 SYSTEM CHANGE CONTROL

Changes to information systems, applications or networks shall be reviewed and approved by the IT Department Intellectual Property Rights

The product owners shall ensure that all information products are properly licensed and approved by the IT Department. Users shall not install software on the organisation's property without permission from the IT Department. Users breaching this requirement may be subject to disciplinary action.

9.4.19 BUSINESS CONTINUITY AND DISASTER RECOVERY PLANS

The information owner shall ensure that a business impact assessment is conducted for all information assets and business continuity and disaster recovery plan is produced for information assets based on the result of the business impact assessment.

9.4.20 REPORTING

The IT Department shall keep the senior management informed of the information security status of examination conducting body by means of regular reports and presentations.

9.4.21 FURTHER INFORMATION

Further information and advice on this policy can be obtained from IT Department.

9.5 COMPLIANCE: INAPPROPRIATE AND PROHIBITED USE

In the absence of an explicit waiver or approval from the Supervisor, the use of examination conducting body IT systems for activities that might be inappropriate or prohibited is forbidden and may lead to disciplinary action being taken against the staff member.

REFERENCES

- http://www.esigmatechnologies.com/etest-online.html.
- Chi-Chien Pan et al, Secure online examination architecture based on distributed firewall , e-Technology, e-Commerce and e-Service, 2004 IEEE International Conference on , 28-31 March 2004 ,533 - 536 .
- http://eduexamsoftware.weebly.com.
- www.projectcorner.in/online-examination-systemcollege-project-asp-net.
- BhagyashriKaiche et al , Online Descriptive Examination and Assessment System, International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 3, March 2014.
- Borromeo, R.M.H. , Online exam for distance educators using moodle, Educational Media (ICEM), 2013 IEEE 63rd Annual
- Gupta, P.K., Mobile examination system, Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on DOI: 10.1109/PDGC.2012.6449836 ,Publication Year: 2012 , Page(s): 302 – 306.
- Ullah, A. ; Hannan Xiao ; Lilley, M. ; Barker, T. , Usability of profile based student authentication and traffic light system in online examinations, Internet Technology And Secured Transactions, 2012 International Conference for Publication Year: 2012 , Page(s): 220 - 225 .
- Ruhnow, M. ; Kohser, J. ; Bley, T. ; Boschke, E. ; Bulst, M. ;Wegner, S. , Robust multi -parametric sensor system for the online detection of microbial bio films in industrial applications — Preliminary examinations, Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014 IEEE Ninth International Conference on , Publication Year: 2014 , Page(s): 1 - 4
- Jani, H.M. , Benefiting from online mental status examination system and mental health diagnostic system, Information Sciences and Interaction Sciences (ICIS), 2010 3rd International Conference on ,Publication Year: 2010 , Page(s): 66 – 70.
- SweZinHlaing , An Authenticated Paradigm for Mobile Agent System in Online Examination, Computer Engineering and Technology, 2009. ICCET '09. International Conference on ,Volume: 2 , 2009 , 420 – 424.
- Alfreosson, F. (2014). Bring-your-own-device Exam System for Campuses. Presented at the 28th NORDUnet Conference, Uppsala University, Sweden. Retrieved from

https://events.nordu.net/display/NORDU2014/Bring-your-owndevice+Exam+System+for+Campuses

- Proceedings of the International Mobile Learning Festival 2015: Mobile Learning, MOOCs and 21st Century learning, May 22-23, 2014, Hong Kong SAR China
- Alkema, A., McDonald, H., & Ryan, R. (2013). Student Voice in Tertiary Education Settings. New Zealand: Ako Aotearoa. Retrieved from www.akoaotearoa.ac.nz/projects/student-voice-effective-representation-andquality
- Andrews, T., & Tynan, B. (2010). Why the student voice? The case for investigating the distance learners' experience of ICT in distance education (pp. 60–64). Presented at the Australasian Society for Computers in Learning in Tertiary Education Conference, Sydney, Australia. Retrieved from http://ascilite.org.au/conferences/sydney10/procs/Andrews-concise.pdf
- Andrews, T., du Toit, L., Harreveld, B., Backstrom, K., & Tynan, B. (2014). Exploring the Student Voice in Online Education (Final Report No. ID11-2077). Australia. Retrieved from http://www.olt.gov.au/project-quality-learning-spaces-socialnetworking-connectedness-and-mobile-learning-exploring-stud-0
- Barrett, M. E., Swan, A. B., Mamikonian, A., Ghajoyan, I., Kramarova, O., & Youmans, R. J. (2014). Technology in Note Taking and Assessment: The Effects of Congruence on Student Performance. International Journal of Instructional Technology and Distance Learning, 7(1), 49–58.
- Blair, E., & Valdez Noel, K. (2014). Improving higher education practice through student evaluation systems: is the student voice being heard? Assessment & Evaluation in Higher Education, 39(7), 879–894. http://doi.org/10.1080/02602938.2013.875984
- Dahlstrom, E., & Bichsel, J. (2014). ECAR Study of Undergraduate Students and Information Technology 2014. EDUCAUSE Center for Applied Research. Retrieved from http://net.educause.edu/ir/library/pdf/ss14/ERS1406.pdf
- Dahlstrom, E., & diFilipo, S. (2013). The Consumerization of Technology and the Bring-Your-Own-Everything (BYOE) Era of Higher Education (Research Report). Louisville, CO, USA: EDUCAUSE Center for Applied Research. Retrieved from http://www.educause.edu/library/resources/byod-andconsumerization-it-higher-education-research-2013
- Dermo, J. (2009). E-Assessment and the student learning experience: A survey of student perceptions of e-assessment. British Journal of Educational Technology,

- Sotiris Ioannidis, Angelos D. Keromytis, Steven M. Bellovin, and Jonathan M. Smith, "Implementing a Distributed Firewall", ACM Conference on Computer and Communications Security, Athens, Greece, November 2000.
- Steven M. Bellovin, Distributed Firewalls, November 1999. <http://www.research.att.com/~smb/papers/distfw.html>
- Daniel Wan, Distributed Firewall, May 2001, <www.giac.org/practical/gsec/Daniel_Wan_GSEC.pdf>
- Wei Li, Distributed Firewall, December 5th, 2000. <www.cs.helsinki.fi/u/asokan/distsec/documents/li.ps.gz>
- Vadim V.Smirnov, Firewall for Windows 9x/NT/2000, <http://www.ntkernel.com/articles/firewalleng.shtml>
- Microsoft Windows Driver Development Kits, <http://www.microsoft.com/whdc/ddk/winddk.mspx>
- OpenLDAP Project, <http://www.openldap.org>
- Ellen Smith, 'Securely Implementing LDAP', SANS Institute, July 2001.
- PuTTY: A Free Win32 Telnet/SSH Client, <http://www.chiark.greenend.org.uk/~sgtatham/putty/>
- Cetin Kaya Koc, High-Speed RSA Implementation, RSA Laboratory, Nov. 1994, <ftp://ftp.rsasecurity.com/pub/pdfs/tr201.pdf>
- The International PGP Home Page, <http://www.pgpi.org>
- Bhavin Bharat and Bhansali, 'Man-In-the-Middle Attack - A Brief', SANS Institute, Feb. 2001.
- Robert Wagner , 'Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks', SANS Institute, Sep. 2001.
- The Apache Software Foundation, <http://www.apache.org>
- Liang Shi-qing, SUN Bo-cheng. Research and Implementation of Remote Examination System Based on Java[J]. Modem Computer,2009,(2):192-194.
- Tu Zhi-qing.Design and discussion of generation system of random test paper[J]. Fujian Computer,2008,(7):161-170.
- Guo Dong-mei. Design and Realization of a Network Test System based onWeb. Development and Application of the Computer[J], 2011,(24) : 65-72.
- Yuan Zhenming, Zhang Liang,Zhan Guohua. A NOVEL WEB-BASED ONLINE EXAMINATION SYSTEM FOR COMPUTER SCIENCE EDUCATION[J]. 33'd

ASEE/IEEE Frontiers in Education Conference, 2003 , pp: S3F_7 - S3F_10. [5] Xiao Jian-qing ,etc.Key technologies in development of paper analysis system. Computer Engineering and Design [J],

- “Development of an E-Assessment Platform for Nigerian Universities”, Research Journal Applied Sciences, Engineering and Technology 2(2): Page 170-175, ISSN: 2040-7467.
- F. Andrew, Darren Pullen and Colleen Harper (2009). “Case study of a computer based examination system” Australian Journal of Educational Technology, 25(4), 509523
- INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 2, ISSUE 8, AUGUST 2013 ISSN 2277-8616
- IJSTR©2013 www.ijstr.org
- C.K. Ayo, I.O. Akinyemi, A.A. Adebiyi and U.O. Ekong (2007), “The Prospects of E-Examination Implementation in Nigeria”, Department of Computer and Information Sciences, Covenant University, Ota, NIGERIA. Turkish Online Journal of Distance Education - TOJDE. ISSN 1302-6488 Volume: 8 Number: 4 Article 10, page 125-135.
- I.M.M. Emary El and J.A.A. Abu (2006), “An Online Website for Tutoring and E-Examination of Economic Course”, American Journal of Applied Sciences 3 (2): Page 1715-1718, ISSN 1546-9239
- A. Huszti and A. Petho (2008), “A Secure Electronic Exam System”, Informatika felsőoktatásban. Page 1-7.
- B. Ipaye (2009), “E-Learning in a Nigerian Open University”, National Open University of Nigeria, page 111.
- H. Lei (2006), “A novel web-based educational assessment system with Bloom‟s Taxonomy”, Current Developments in Technology-Assisted Education. Page 1861-1865.
- Y. Levy and M.M. Ramim (2007), “A Theoretical Approach for Biometrics Authentication of e- Exams”, Nova Southeastern University, USA. Page 93-101.
- M.Z. Rashad, M.S. Kandil, A.E. Hassan and M.A. Zaher (2010), “An Arabic Web-Based Exam Management System”, International Journal of Electrical & Computer Sciences IJECS- IJENS Vol: 10 No: 01. Page 48-55.
- Y. Zhenming Y., Z. Liang and Z. Guohua (2003), “A Novel Web-Based Online Examination System for Computer Science Education”, 33rd ASEE/IEEE Frontiers in Education