Case Study 3
SDLC

Scenario

EasyCash Pvt Ltd is a virtual pre-paid cards company operating in India. It has its corporate and registered office in Mumbai. There are various franchisee and distributors of the EasyCash for distribution of prepaid cards. The cards issued by the company are of 2 types. One is a virtual card to be used on Internet and the other is a mobile based card to be used on mobile phones as mobile wallets. The company has its IT systems, but outsourced the data centre to a company located in Hyderabad called as Netizens India Pvt Ltd. The DR site of the company is located in Chennai.

EasyCash has about 15 in-house programmers, system administrators, database administrators, network administrators and security manager. It also outsources key development of code for new systems which are being planned. HR dept looks after recruitment, termination, and other HR related matters. Legal dept has about 3 people who look after agreements and initiating changes to the financials in the agreement, thru back-end system. All changes to the data are done by IT dept. IT dept also has operations team which looks after various IT operations such as monitoring of servers and networking devices, firewall administration, network monitoring, security monitoring, database monitoring and tune up, transaction logs monitoring and resorting to customer / merchants / franchisees queries. Since the business of the company is fast expanding, the company has set-up a separate call centre which is outsourced.

IT Dept has recently developed a MIS system in-house which has gone live recently. However, users are facing many functionality and other issues in the system. Therefore, users are suggesting changes to be made to the software. This was also going on when the system was under development. The management feels that the method used by IT Dept for developing system is not proper. Users should have been involved more in the system development. The management also feels that the testing of the software has not been carried out properly.

Later on, System Audit was initiated by the company. Some important observations of the System Auditors are given below:

1. The system accepts any amount even zero or –ve amounts are accepted by the system
2. All the users can view all the columns of important database tables such as customer master, customer’s ledgers etc.
3. DBA carries out direct updation of database tables by accessing database directly
4. Developers have followed agile development methodology

5. Patches for operating system have not been installed

6. The same old hardware is being used for the system, which hampers the efficiency of the system

Discussion points

1. Roles & responsibilities of programmers, system administrators, database administrators, network administrators and security manager should be discussed.

2. Various types of Application Controls – Source data generation, Input, Processing, Output etc

3. Various types of Information Systems viz Operator Information System, MIS, DSS etc

4. Various types of operations carried out by IT Dept – e.g. monitoring of centralised IT equipment, configuration management, user creation etc

5. Importance of users' involvement in various stages of SDLC

Questions

Based on the above case study, please answer the following questions

1. The management wants to know from the auditor about this recently developed project. The IS auditor should evaluate which of the following?

A. Business case document

B. Requirements gathered so far

C. Feasibility study document

D. Design and development document

2. The management feeling that, high level of user interaction and participation is required for system development, will be satisfied by which of the following methodology?

A. Prototyping model

B. Waterfall model

C. V-model

D. Object oriented model

3. System auditor has stated that users are able to view all the columns of some important tables, to which IT Dept claims that, only authorised users can modify the data in the important master tables. System auditor should point out which of the following risks?

A. Confidentiality

B. Integrity

C. Availability

D. Hacking

4. Direct back-end database correction of data by DBA poses which of the following risks, which is GREATEST?

A. Misappropriation by DBA cannot be ruled out

B. Wrong updation of data by DBA

C. There is no risk, this is a standard practice

D. Users will not know about the changes done by DBA

5. Which of the following will help IT Dept in identifying issues due to lack of applying operating system patches?

A. A simulated test server for testing patches

B. Install the patches since security is most important

C. Do not install patches for smooth functioning of business application software

D. Modify the business application software

Guidelines to Faculty:

1. In all questions, explanation of each incorrect option may be given in a properly delineated form for easy understanding.

2. Relevant Standards / regulations / frameworks like COBIT 2019, ISO27001, and GDPR may be referred to and explained in the class while discussing the answers.

3. The faculty can teach some theory which s/he might not have covered during the class.

Practice Manual 3
Input Validation

Learning Objective

Student shall learn about various Input Validations, which are a part of Application Controls. Input validations ensure that errors are prevented or detected and users are forewarned about the errors.

Scenario

A company wishes to analyse the bills submitted by various employees for reimbursement. The newly joined DISA qualified CA from Accounts & Finance Dept has been asked to develop a system in Excel to enter the mobile bills submitted by the employees. The company also wants to analyse age wise, area wise amount of bills. The following Excel columns were identified by the CA and designed the Excel sheet accordingly. However, when the data was entered by the accounts dept clerks, on a test basis, it was observed that, erroneous data is being entered in all the columns. Therefore, the CA decided to redesign the Excel sheet by providing certain Input controls, so that the errors would be minimum. The following input validation checks were to be designed. You may help the CA to design these validation checks, in Excel as given below.

Bill Number	Bill Date	Mobile Number	Account Code	Check digit	Name of Customer	Ag e	Birth Date	Gend er	PIN Code	PIN Code Location	Amoun t

Hardware and Software Requirements

- Student's laptop, Microsoft Excel

Step-by-Step Activities to be performed

1. **Sequence Check** – Data should be entered in sequence – Bill number entered by a user should be in sequence only. i.e. 1,2,3,4 …..

2. **Duplicate Check** – Bill date entered by a user should not be duplicate in subsequent rows

3. **Completeness, Length Check and Numeric Check -** Mobile number entered by a user should be 10(not less than or more than 10), only digits and should not be duplicate

4. **Check Digit -** Account code entered by user should be appended with a check digit calculated by modulus 11

5. **Existence Check -** User should be able to enter only A-Z. No digits.
6. **Range Check -** Age should be between 18 to 60
7. **Logical relationship Check -** Birth date and age should match
8. **Validation Check** - Gender should be either 'M', 'F', 'T' – validity check
9. **Table Lookup** - Pin code name should be picked up from next sheet. Pincodes for Maharashtra are given in 2nd sheet. Any other state's table may be used by the faculty.
10. **Limit Check** - Amount – Should be > 0 and <= 10000 – Limit check

Note: 2 more input validation checks are not given in the above list which are: ***Reasonableness check*** *and* ***Key verification check****. Reasonableness check requires history of transactions. Key verification check requires input by two separate operators.*

Case Study 4
Testing

Scenario

Newline Software Systems Pvt Ltd is a software development company based in Pune, India undertakes software projects in India and outside India. The company has many developers and other staff such as quality assurance, testers, functional experts, DBAs etc.

Newline has many developers and undertakes development in various platforms. The company was very small about 5 years ago but has rapidly grown since and now employs about 400 people.

A new CIO joined the company. After about 6 months in the company, the CIO got a grip on the company's software division. CIO discussed and called for meetings with various teams, users, departmental heads, testers, developers etc.

CIO has made the following observations and put forth them in several meetings:

1. We are undertaking feasibility studies before going ahead with the purchase of the software or development of a software. However, we are doing only technical studies. We have to carry out all types of feasibility studies.
2. Recently we have purchased a software based on Internet information. Have we taken management approval for such a procedure?
3. We carry out UAT which is good. But what about other testing? E.g. have we carried out a stress testing for our recent web site project for a university? University users have complained about a very slow response for the web site.
4. Some of the old systems were being reworked to take advantage of new technology. These systems were successfully implemented and were operational and useful. In doing so, the old system's design and some of the developed code was reused and reengineered. This has been done nicely and I want to congratulate the team for it.
5. How do we decide cost of developing a software? Our accounts department has no clue about it and when I enquired, I was told that, the developers count the number of lines of source codes and arrive at the size or the software and number of days it would take. This is very old method and may not work correctly for modern development methodology. We have to use latest methods of software size estimation and then arrive at its cost.
6. I have also found that, we are not using project management practices. We manage projects haphazardly. We have to follow project management techniques such as PERT/CPM.

7. Our project on medical diagnosis, which is based on artificial intelligence and which we are developing on a pilot basis for a super speciality hospital has been halted. It was informed to me that, some expert doctors working on this project have left this hospital and joined another hospital. This new hospital is now launching the same product which we thought of.

8. In one of the banking projects, there was a conflict between company's developers and bank's user management. The bank management insisted on exact mapping of the software modules with the current manual processing done in the bank, which involves heavy customisation of the software. The bank has appointed an IS auditor to review the development done by the company so far.

9. Developers are using their own laptops and also take them home, which pose security threats. Can we eliminate this?

Discussion points

1. What other areas should be included in a Feasibility Study? Can the company accept or reject in part or full, the feasibility study done by an expert? Who will approve the Feasibility Study?

2. What are the different types of testing which need to be carried out apart from UAT?

3. How to decide cost of the software? Who will decide it? As mentioned in the case, if Accounts dept should decide the cost of software, what inputs/training the accounts dept will require? Which costing model/methods will be used for arriving at cost of software development?

4. What are important considerations for developing and protecting AI based systems?

5. What is meant by customisation of software? Why it is needed? Can a customisation be done on a purchased software?

6. If developers have to work from home, should company provide them the laptops or can company have BYOD policy? If so, what are the precautions the company/developers should take?

Questions

Based on the above case study, please answer the following questions

1. Which of the following testing will be done to check by putting limit on the hard disk space availability or memory space availability?

A. Stress Testing

B. Functional Testing

C. Structural Testing

D. Performance Testing

2. The technique of reworking old systems into new systems, is known as :

A. reengineering.

B. reverse engineering.

C. prototyping.

D. software reuse.

3. Which of the following shall be checked to ensure availability of technical and skilled human resources required for developing/acquiring and implementing the required solution?

A. Resources Feasibility

B. Technical Feasibility

C. Economic Feasibility

D. Operational Feasibility

4. In a software development project, if the project is going to overrun, which of the following should be critically examined? Activities :

A. that have zero slack time.

B. whose sum of activity time is the shortest.

C. that give the longest possible completion time.

D. whose sum of slack time is the shortest.

5. Which of the following method is MOST useful when the project manager is faced with challenge in delivering on time and with acceptable quality?

A. Assign expert resources to complete critical path activities of the project

B. Use GANTT chart to allocate 100% of time of expert resources for 90% of work

C. Use GANTT chart to define milestones and make experts responsible for milestones

D. Identify some activities with slack times and allocate them to expert resources to reduce slack time.

Guidelines to Faculty

1. In all questions, explanation of each incorrect option may be given in a properly delineated form for easy understanding.

2. Relevant Standards / regulations / frameworks like COBIT 2019, ISO27001, and GDPR may be referred to and explained in the class while discussing the answers.

3. The faculty can teach some theory which s/he might not have covered during the class.

Practice Manual 6
RACI Matrix & Threat Modelling

Learning Objective

- Learn RACI matrix for various roles in requirement analysis phase of SDLC
- Identify security objectives of the software, threats to software, vulnerabilities in the software being developed

Scenario

RACI Matrix is the name given to a table, which is used to describe the type and degree of involvement that stakeholders have in completing tasks or deliverables for a project or business process. Also sometimes called the Responsibility Assignment Matrix or Linear Responsibility Chart, it is a common tool used by business analysts and project managers for establishing roles and responsibilities early on in a project. In this way it reduces project risk and sets expectations about the level of involvement that is expected by various stakeholders.

Hardware/ Software Requirements

- Windows OS 7, 8 or 10
- MS-Office (Word and Excel)
- Suggested Time is 1 Hour 30 Minutes
- This is a group activity.

Step-by-Step Activities to be performed

1. Activity 1: Identifying Responsibility, Accountability, Consulted or Informed definitions to different roles for requirement analysis phase.

Steps for development of RACI matrix:

- Identification of all the tasks involved in delivering the project.
- Identification of all the project roles
- Identification of who has responsibility, accountability and who will be consulted and informed for each task.
- Ensure every task has a role responsible and a role accountable for it.

- No tasks should have more than one role accountable. Resolve any conflicts where there is more than one for a particular task.
- Share, discuss and agree the RACI Matrix with your stakeholders before your project starts.

	RACI Definitions
R	**Responsible**: person or role responsible for doing or completing the item
A	**Accountable**: person or role accountable for ensuring that the item is completed
C	**Consulted**: person or role whose subject matter expertise is required in order to complete the item
I	**Informed**: person or role that must be kept informed of the status of item completion

Activities and Roles are given in the table for Requirement Analysis phase of SDLC. You need to identify and map the RACI role definitions for various activities and roles.

Roles	Definitions
Project Manager	Project managers have the responsibility of the planning, procurement and execution of a project, in any undertaking that has a defined scope, defined start and a defined finish; regardless of industry.
Application Developer	An Application Developer is responsible for developing and modifying source code for software applications.
Business Analyst	A business analyst analyzes an organization or business domain and documents its business or processes or systems, assessing the business model or its integration with technology.
Solution Architect	A solution architect is responsible for the design of one or more applications or services within an organization, and is typically part of a solution development team. A solution architect is the person in charge of leading the practice and introducing the overall technical vision for a particular solution.
Enterprise Architect	An enterprise architect is someone who is responsible for making sure that a company's business strategy uses proper technology systems architecture to achieve its goals.

Roles	Definitions
Technology Architect	Technology architects are responsible for designing the high-level structure of new technology solutions, including the emerging technologies that development teams may use. This also includes planning the resources needed to implement the new solution and identifying potential roadblocks.
Technology Support	Technical Support provides assistance and maintenance to all computer systems and hardware. Their work may include installing, configuring, and updating hardware and software, as well as fixing any issue related to the equipment that may come up on a daily basis.
Program/Project Sponsor	The Program/Project Sponsor is an executive with overall accountability for the project. A Program/Project Sponsor acts as the link between the project, the business community, and strategic level decision-making groups.
Account Manager	The account manager role is to ensure that client needs are understood and satisfied. They build and manage client relationships, collect information, and ensure that company offerings meet the individual needs of clients.
Work Product Reviewer	Work Product Reviewer prepares the test scenarios executes tests on product usability, analyzes test results on database impacts, errors or bugs, and usability. Also Participates in design reviews and provides input on requirements, product design, and potential problems.
Key User	A key user is a representative of a number of its own business processes and they have a leading role within a system implementation. They represent during (and after) the project some of the processes in which they are involved.
Steering Committee	The Steering Committee's role is to provide advice, ensure delivery of the project outputs and the achievement of project outcomes.

Sr. No .	Requirements Analysis Phase	Roles											
	Activity	Project Manager	Application Developer	Business Analyst	Solution Architect	Enterprise Architect	Technology Architect	Technology Support	Program/Project Sponsor	Account Manager/Service M	Work Product Reviewer	Key User	Steering Committee
1	Confirmation of Requirement Definition from Subject Matter Expert												
2	Development of Process model												
3	Development of Use Cases												
4	Identification of Technology Platform												
5	Evaluation of Technology Vendor												
6	Definition of Reliability, Availability, SLA Requirements												
7	Definition of performance needs												
8	Identification of Security, legal, Regulatory and Compliance Requirements												
9	Mapping Existing Solution to Requirements												
10	Identification of Functional Gaps												
11	Identification of phases for implementation												
12	Conducting Requirements Review												

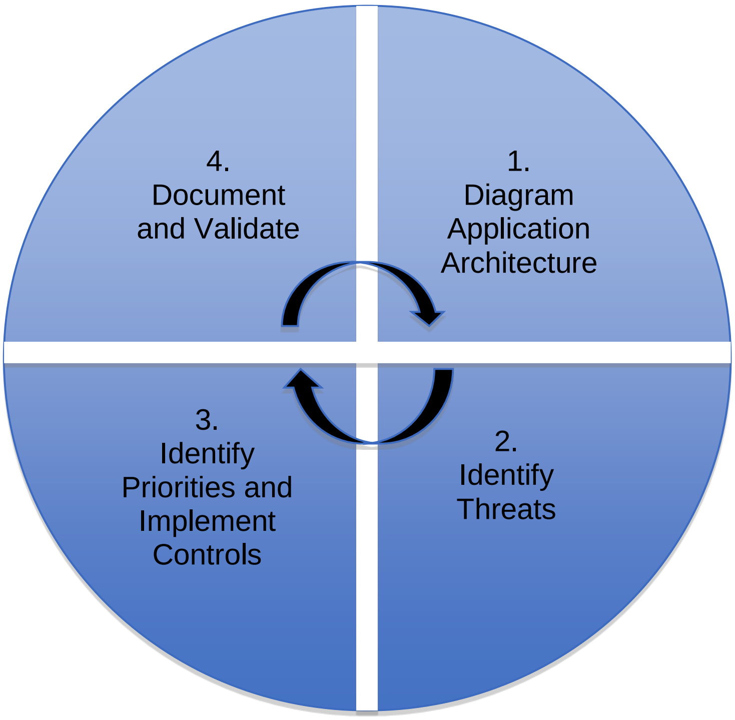
2. Activity 2: Model the Secure SDLC process.

Threat modelling is a systematic, iterative, and structured security technique that should be taken into consideration during the design phase of the software development. It should be performed to identify security objectives of the software, threats to software, vulnerabilities in the software being developed. It provides the software development team an attacker's or hostile users' view point, as the threat modelling exercise aims at identifying entry and exit points that an attacker can exploit. It also helps the team to make design and engineering trade-off decisions by providing insight into the areas where attention is to be prioritized and focused, from a security viewpoint.

The primary benefit of threat modelling during the design phase of the project is that design flaws can be addressed before a single line of code is written, thereby reducing the need to redesign and fix security issues in code at a later time.

Before we start the process of threat modelling, we must first determine the security objectives that need to be met by the software itself. This is some times referred to as the "Security Vision" for the software in threat modelling terminology. These include the requirements that impact the core security concepts such as confidentiality, integrity, availability, authentication, authorization, and accountability.

Threat Modelling Process



- Classify the following items into four groups of "Threat Modelling Process"

- Technologies (physical /Logical)
- Categorized Threat list
  (STRIDE/ OWASP to 10/ CWE Top 25)
- Error handling
- Authorization
- Data Elements
- Verification and Validation report
- Dependencies
- Entry and exit points
- Mis-actors
- Input Validation
- Residual Risk

- Services, Port and Protocols
- Attack trees
- Identities and Authentication
- Replication
- Multi-factor authentication
- Access control lists
- Logging
- Parameterized Queries
- Documented Threat Profile
- Encryption Hashing
- Auditing controls
- Trust boundaries
- Actors
- Data flows

1. Diagram Application Architecture	**3. Identify, Prioritize and Implement controls**
2. Identify Threats	**4. Document and Validate**