MIS 5203
Requirements Analysis - Data

- Unit 6 -

Agenda

- Adding security requirements to use case template
- Adding security requirements to functional requirements specification
- Deriving data requirements from functional requirements specification
- Quiz

Use Case Template

Use Case Template

Use Case ID:	1		
Use Case Name:			
Created By:		Last Updated By:	
Date Created:		Date Last Updated:	

Actors:	
Description:	
Trigger:	
Preconditions:	
Postconditions:	
Normal Flow: Sunny Day Scenario:	
Alternative Flows: Rainy Day Scenario:	
Exceptions:	
Includes:	
Priority:	
Frequency of Use:	
Business Rules:	
Special Requirements:	
Assumptions:	
Notes and Issues:	

3. Use Case Definition

3.1. Actors

3.2. Trigger

3.3. Description

3.4. Preconditions

3.5. Postconditions

3.6. Normal Flow

3.7. Alternative Flows

3.9. Includes

3.10. Priority

3.11. Frequency of Use

3.12. Business Rules

3.13. Special Requirements

3.14. Assumptions

3.15. Notes and Issues

Security Enhanced Use Case Template – Raisa Ahmed

3. Use Case Definition

3.1. Actors

3.2. Trigger

3.3. Description

3.4. Preconditions

3.5. Postconditions

3.6. Normal Flow

3.7. Alternative Flows

3.9. Includes

3.10. Priority

3.11. Frequency of Use

3.12. Business Rules

3.13. Special Requirements

3.14. Assumptions

3.15. Notes and Issues

3.16. Time

3.17 Stakeholders

3.18 Security

3.19 Expenses

3.20 System Impact

Use Case Template

Use Case ID:	1		
Use Case Name:			
Created By:		Last Updated By:	
Date Created:		Date Last Updated:	

Actors:	
Description:	
Trigger:	
Preconditions:	
Postconditions:	
Normal Flow: Sunny Day Scenario:	
Alternative Flows: Rainy Day Scenario:	
Exceptions:	
Includes:	
Priority:	
Frequency of Use:	
Business Rules:	
Special Requirements:	
Assumptions:	
Notes and Issues:	

Security Enhanced Use Case Template – Raisa Ahmed

3.16. Time

List time-based initiators of processing any activity for the system. Common timers include daily, weekly, bi-weekly, and monthly.

3.17. Stakeholders

A stakeholder is a person who takes interest in the project or a person who must ensure that the use case links to the business and project vision and objectives.

3.18. Security

Indicate where technology is implemented in the project, its role and identify any area where security may be at risk (new software; vendors; between users or procedures). As the project goes on, the use case should help to keep track of any risk that have surfaced since the project was first initiated.

3.19. Expenses

Identify costs of any system or instrument needed to successfully complete the project.

3.20. System Impact

List any existing system that will be impacted by the implementation of the new project.

Security Enhanced Use Case Template – Penghui Ai

3. Use Case Definition
3.1. Actors
3.2. Trigger
3.3. Description
3.4. Preconditions
3.5. Postconditions
3.6. Normal Flow
3.7. Alternative Flows
3.9. Includes
3.10. Priority
3.11. Frequency of Use
3.12. Business Rules
3.13. Special Requirements
3.14. Assumptions
3.15. Notes and Issues
3.16. Secure/Security Requirements (Q1)

3.16. Secure/Security Requirements (Q1)

List any secure requirements (standard requirements) that has security built into them to determine the necessary constraints to protect the system. List any security requirements (separate entities) that support an overall security objective.

Use Case Template (Q1)

Use Case ID:	1		
Use Case Name:			
Created By:		Last Updated By:	
Date Created:		Date Last Updated:	

Actors:	
Description:	
Trigger:	
Preconditions:	
Postconditions:	
Normal Flow: Sunny Day Scenario:	
Alternative Flows: Rainy Day Scenario:	
Exceptions:	
Includes:	
Priority:	
Frequency of Use:	
Business Rules:	
Special Requirements:	
Assumptions:	
Notes and Issues:	
Secure/Security Requirements	

Security Enhanced Use Case Template – Shuyue Ding

3. Use Case Definition

3.1. Actors

3.2 Alert

3.3. Trigger

3.4 Alert Trigger

3.5. Description

3.6. Preconditions

3.7 Preconditions of a Alert

3.8. Postconditions

3.9 Postconditions of a Alert

3.10. Normal Flow

3.11. Alternative Flows

3.11.1 Alert triggered flow

3.12. Includes

3.13. Priority

3.14. Frequency of Use

3.15. Business Rules

3.16. Special Requirements

3.17. Assumptions

3.18. Notes and Issues

3.2. Alert - A warning that the user interaction violate the rule or policy that could potentially entity/entities in danger.

3.4 Alert Trigger - Identify the violation that initiates the alert, and it could be a user mistake or a external attack. It should be the first step of the alternative flows of a alert triggered flow.

3.7 Preconditions of a Alert - Activities that must happen before start a alert. Number each precondition. Examples:

1. User opens the login page
2. User enters the wrong password number three times

3.9. Postconditions of a Alert - Describe the system outcomes of a alert. Number each postcondition. Examples:

1. Reject the user login
2. Ask user if they want to reset the password.

3.11.1 Alert triggered flow: Document scenarios that can take place because of a alert. Number each Alert triggered flow in the form “X.A.Y”, where “X” is the Use Case ID, “A” states for alert, and Y is a sequence number for the flow. For example, “5.A.3” would indicate the third alert triggered flow for use case number 5.

Use Case Template

Use Case ID:	1		
Use Case Name:			
Created By:		Last Updated By:	
Date Created:		Date Last Updated:	

Actors:	
Alert	
Description:	
Trigger:	
Alert Trigger	
Preconditions:	
Preconditions of a alert	
Postconditions:	
Postconditions of a alert	
Normal Flow: Sunny Day Scenario:	
Alternative Flows: Rainy Day Scenario: Alert triggered flow:	
Exceptions:	
Includes:	
Priority:	
Frequency of Use:	
Business Rules:	
Special Requirements:	
Assumptions:	
Notes and Issues:	

Security Enhanced Use Case Template – Feng Gao

3. Use Case Definition
3.1. Actors
3.2. Trigger
3.3. Description
3.4. Preconditions
3.5. Postconditions
3.6. Normal Flow
3.7. Alternative Flows
3.9. Includes
3.10. Priority
3.11. Frequency of Use
3.12. Business Rules
3.13. Special Requirements
3.14. Assumptions
3.15. Notes and Issues

Use Case Template

Use Case ID:	1		
Use Case Name:			
Created By:		Last Updated By:	
Date Created:		Date Last Updated:	

Actors:	
Description:	
Trigger:	
Preconditions:	
Postconditions:	
Normal Flow: Sunny Day Scenario:	
Alternative Flows: Rainy Day Scenario:	
Exceptions:	
Includes:	
Priority:	
Frequency of Use:	
Business Rules:	
Special Requirements:	
Assumptions:	
Notes and Issues:	

Security Enhanced Use Case Template – Feng Gao

3. Use Case Definition
3.1. Actors
3.2. Trigger
3.3. Description
3.4. Preconditions
3.5. Postconditions
3.6. Normal Flow
3.7. Alternative Flows
3.9. Includes
3.10. Priority
3.11. Frequency of Use
3.12. Business Rules
3.13. Special Requirements
3.14. Assumptions
3.15. Notes and Issues

Use Case Template

Use Case ID:	1		
Use Case Name:			
Created By:		Last Updated By:	
Date Created:		Date Last Updated:	

Actors:	
Description:	
Trigger:	
Preconditions:	
Postconditions:	
Normal Flow: Sunny Day Scenario:	
Alternative Flows: Rainy Day Scenario:	
Exceptions:	
Includes:	
Priority:	
Frequency of Use:	
Business Rules:	
Special Requirements:	
Assumptions:	
Notes and Issues:	

Security Enhanced Use Case Template – Imran Kharabsheh

3. Use Case Definition

3.1. Actors

3.2. Trigger

3.3. Description

3.4. Preconditions

3.5. Postconditions

3.6. Normal Flow

3.7. Alternative Flows

3.9. Includes

3.10. Priority

3.11. Frequency of Use

3.12. Business Rules

3.13. Special Requirements

3.14. Assumptions

3.15. Multi-factor Authentication

3.16. Logging

3.17. Authentic Failsafe

3.18 Honeypot Quarantine

3.19 Secondary Power

3.20 Encryption Method (and Hashing)

3.21 Input Field Restrictions

Use Case Template

Use Case ID:	1		
Use Case Name:			
Created By:		Last Updated By:	
Date Created:		Date Last Updated:	

Actors:	
Description:	
Trigger:	
Preconditions:	
Postconditions:	
Normal Flow: Sunny Day Scenario:	
Alternative Flows: Rainy Day Scenario:	
Exceptions:	
Includes:	
Priority:	
Frequency of Use:	
Business Rules:	
Special Requirements:	
Assumptions:	
Multi-Step Authentication:	
Logging:	
Authentication Failsafe:	
Honeypot Quarantine:	
Secondary Power Sypply:	
Encryption Method (and Hashing):	
Input Field Restrictions:	
Notes and Issues:	

3.15. Multi-Factor Authentication - The authentication procedure required to be completed prior to an actor being granted access to the software system. Minimum requirement of two factors of authentication which meet two or more of the following conditions: something the verified user is, something the verified user has, or something the verified user knows.

3.16. Logging - Hidden and restricted access document(s) that contain a systematic record of all events and transactions carried out by the system. Includes sufficient detail for auditors to be able to tell which users accessed the system, when they accessed it, where they accessed it from, and all actions performed by the users or system.

3.17. Authentication Failsafe - The procedure put in place on the occasion that several login attempts are attempted unsuccessfully in a short span of time (eg. 5 repeated failed attempts). In order to secure the system, the account will become locked and users will be notified to visit IT office in order to have their accounts reinstated with renewed credentials.

3.18. Honeypot Quarantine -After securing and renaming the official administrative accounts related to the software system, it can be beneficial for organizations to create isolated, false and monitored accounts with zero access to anything as a detective measure against intruders. By enabling extensive logging and monitoring for these accounts, an organization can better understand and identify aggressors and their means of infiltration.

3.19. Secondary Power Supply - On the occasion of a disaster that disables the primary source of power to an organization's software systems, an organization must prioritize restoring the functionality and ensuring the integrity of their systems. To this end, securing a second power supply will help prevent the systems suddenly shutting off and corrupting all information being used at the time of the disaster.

3.20. Encryption Method (and Hashing) - As sensitive information circulates both inside and outside of the system through interactions between the actors and the software systems, the need to secure the confidentiality and integrity of the information becomes apparent. To facilitate this, encrypting data and creating hashes pertaining to this data will reduce the likeliness that outside actors will retrieve anything meaningful, and the inside actors can ensure the sanctity of the transmitted data upon arrival.

3.21. Input Field Restrictions - Input fields in the software systems run the risk of being abused through the injection of code by actors with access to enter characters into these input fields, which could have severe consequences to the confidentiality and integrity of the information systems. In order to avoid this, all input fields must have specific requirements and controls that prevent the reading of non-relevant characters placed in the field.

Security Enhanced Use Case Template – Deepa Kuppuswamy

3. Use Case Definition

3.1. Actors

3.2. Trigger

3.3. Description

3.4. Preconditions

3.5. Postconditions

3.6. Normal Flow

3.7. Alternative Flows

3.9. Includes

3.10. Priority

3.11. Frequency of Use

3.12. Business Rules

3.13. Special Requiremer

3.14. Assumptions

3.15 Notes and Issue

3.16. Use Case Path

3.17. Scope

3.18. Security Threat

3.19 Stakeholders and Risks

3.21 User Interaction

3.22 Misuser Interaction

3.23 System Interactions and System Actions

Use Case Template

Use Case ID:	1		
Use Case Name:			
Use Case Path:			
Created By:		Last Updated By:	
Date Created:		Date Last Updated:	
Actors:			
Description:			
Trigger:			
Preconditions:			
Postconditions:			
Normal Flow: Sunny Day Scenario:			
Alternative Flows: Rainy Day Scenario:			
Exceptions:			
Includes:			
Priority:			
Frequency of Use:			
Business Rules:			
Special Requirements:			
Assumptions:			
Notes and Issues:			
Scope:			
Security Threat:			
Stakeholders and Risks:			
Abstraction Level:			

User Interactions	Misuser Interactions	System Requirements	
		System Interactions	System Actions

3.16. Use Case Path - Use case paths helps to maximize the reusability of the use case specifications that describes the security control requirements.

3.17. Scope - This field represents the scope of modeling, e.g., an entire business, an information system of users and computers, or just the computerized information system. Business level models can show how an outsider interacts with humans inside the organization instead of only showing how someone interacts with the system. This is important, because the techniques used to capture misuse attempts may be of a physical or organizational nature, in addition to designing security into the computerized information system.

3.18. Security Threat - Analyze the security threats from which the assets and services should be protected. The analysis and documentation of security threats and security requirements has received considerably less attention. Therefore, relationships between assets and services, which are vulnerable to security threats, which necessitate security requirements, which require security mechanisms that counter these security threats and thereby protect the assets and services.

3.19. Stakeholders and Risks - List the various stakeholders' w/motivations. This field lists the various stakeholders and what their motivations are. For misuse cases this slot is actually even more important. On an abstract level, risks could simply be described textually (e.g., system unavailable for customers for several hours; potential employer gets sensitive data about patient, who thus loses job opportunity, …).

3.20. Abstraction Level - This field indicates what level of abstraction a use case is on. This can be e.g., summary, user goal, or sub-function. Misuse cases can be specified at several levels of abstraction.

3.21. User Interaction - Describe the interaction between the user and the system to achieve the goal without violating any security requirements.

3.22. Misuser Interaction - Unlike normal use cases that document interactions between an application and its users, misuse cases concentrate on interactions between the application and its misusers (e.g., cracker or disgruntled employee) who seek to violate its security and It is a specialized kind of use cases that are used to analyze and specify security threats. Because the success criteria for a misuse case is a successful attack against an application, misuse cases are highly effective ways of analyzing security threats.

3.23. System interactions and System Actions - Carefully differentiate requirements (e.g., by using the word "shall") from ancillary information. System interactions, system actions, and the postconditions should be specified as requirements on the system and clearly distinguish between externally-visible system interactions and hidden system actions.

Security Enhanced Use Case Template – Panayiotis Laskaridis

3. Use Case Definition
3.1. Actors
3.2. Trigger
3.3. Description
3.4. Preconditions
3.5. Postconditions
3.6. Normal Flow
3.7. Alternative Flows
3.9. Includes
3.10. Priority
3.11. Frequency of Use
3.12. Business Rules
3.13. Special Requirements
3.14. Assumptions
3.15 Notes and Issue

3.10 Security Requirements

List security requirements: i.e. login requirements, password requirements, security questions, alternative email, access settings, two-step verification, etc…

Security Enhanced Use Case Template – Alexander H. Reichart-Anderson

3. Use Case Definition

3.1. Actors

3.2. Trigger

3.3. Description

3.4. Preconditions

3.5. Postconditions

3.6. Normal Flow

3.7. Alternative Flows

3.8. Contingency to Normal Operations

3.9. Security Requirements

3.10. Secure Requirements

3.11. Security Constraints

3.12 Data Collection and Privacy

3.13 Associated Risks

3.14 Exceptions

3.15. Includes

3.16. Priority

3.11. Frequency of Use

3.12. Business Rules

3.13. Special Requirements

3.14. Assumptions

3.15 Notes and Issue

Use Case Template

Use Case ID:	1		
Use Case Name:			
Created By:		Last Updated By:	
Date Created:		Date Last Updated:	

Actors:			
Description:			
Trigger:			
Preconditions:			
Postconditions:			
Normal Flow: Sunny Day Scenario:			
Alternative Flows: Rainy Day Scenario:			
Contingency to Normal Operations:	Fail Case	Consequence to Failure	
Security Requirements:			
Secure Requirements:			
Security Constraints:			
Data Collection & Privacy:	Confidentiality	Integrity	Availability
Associated Risks:			
Exceptions:			
Includes:			
Priority:			
Frequency of Use:			
Business Rules:			
Special Requirements:			
Assumptions:			
Notes and Issues:			

3.8. Contingency to Normal Operations - Outline the affects and effects of a failure to the MIS system. This includes the *Fail Case* — what to do when things go wrong. In addition, include the *Consequences of Failure* — the negative business affects when a technological issue occurs.

3.9. Security Requirements - To what length is this use case utilizing and enforcing specific security requirements? Outline how the attack surfaces are being protected from external attackers. In addition, outline how inherent vulnerabilities of running this use case will be handled — either mitigated, accepted, or avoided

3.10. Secure Requirements - How does this used case address the overall 'systematic' security of the systems involved, business processes, and individual business units.

3.11. Security Constraints - What constraints does this use case and business processes put on the security of the system and/or processes? How does the use case limit the capabilities of security software, hardware, and/or procedures?

3.12. Data Collection & Privacy - Of the data being collected, what is the Confidentiality, Integrity, and Availability of the process, the data being collected, and the privacy of the overall system.

3.13. Associated Risks - What are the risks (security specific) the come along with running this use case?

Security Enhanced Use Case Template – Haixin Sun

3. Use Case Definition

3.1. **Actors**

3.2. Trigger

3.3. Description

3.4. Preconditions

3.5. Postconditions

3.6. Normal Flow

3.7. Alternative Flows

3.14 Exceptions

3.15. Includes

3.16. Priority

3.11. Frequency of Use

3.12. Business Rules

3.13. Special Requirements

3.14. Assumptions

3.15 Notes and Issue

3.16. Issues and to-do

3.17. Variations

3.18. Assumptions

3.19 Additional Notation

Use Case Template

Use Case ID:	1		
Use Case Name:			
Created By:		Last Updated By:	
Date Created:		Date Last Updated:	

Actors:	
Description:	
Trigger:	
Preconditions:	
Postconditions:	
Normal Flow: Sunny Day Scenario:	
Alternative Flows: Rainy Day Scenario:	
Exceptions:	
Includes:	
Priority:	
Frequency of Use:	
Business Rules:	
Special Requirements:	
Assumptions:	
Notes and Issues:	
Additional Notation:	

3.1 Primary Actor - List the primary actor who has the primary interest in the outcome of this Use Case here

Supporting Actor -List the supporting actors who have a supporting role in helping the Primary Actor achieve his or her goal

Stakeholders and Interests - List the various entities who may not directly interact with the system but they may have an interest in the outcome of the use case

3.5 Post Conditions -Success end condition, Failure end condition, Minimal Guarantee

3.16. Issue and to-do -List any issues related to the definition of the use case and any follow-up works that remain to be done on this use case

3.17. Variations -Enter any data entry or technology variations like different data input

3.18. Assumptions - List any assumptions made while planning about this use case.

3.19. Additional Notation - List communication into and out of the system as part of the use case diagram to specify that information is passing across the association lines:

[E] placed on any association between actor and procedure or procedure and procedure that crosses over the external boundary of the system.

[I] placed on any association between actor and procedure or procedure and procedure that indicates communication is internal to the system boundary but does communicate externally beyond a single host machine.

[C] placed on any association to indicate the transmission of sensitive data such as a password or mission critical data.

[A] placed on location of a potential attack.

Security Enhanced Use Case Template – Ryu Takatsuki

3. Use Case Definition
3.1. Actors
3.2. Trigger
3.3. Description
3.4. Preconditions
3.5. Postconditions
3.6. Normal Flow
3.7. Alternative Flows
3.14 Exceptions
3.15. Includes
3.16. Priority
3.11. Frequency of Use
3.12. Business Rules
3.13 Security Requirements
3.13. Special Requirements
3.14. Assumptions
3.15 Notes and Issue

Use Case ID:	0		
Use Case Name:	**Outage Notification**		
Iteration:	Focused		
Created By:	Analyst 1	Last Updated By:	Analyst 1
Date Created:	7-7-2015	Date Last Updated:	7-7-2015
Actor:	Customer Service Representative (CSR) Customer Service Supervisor (CSS) Utilities Operations Manager (UOM) Customer Information System (CIS)		
Description:	The User (CSR, CSS or UOM), in response to an ongoing or planned outage of sewer system pumpstations, generates a report and updates CIS with records of customers affected by the outage event.		
Triggers:	Outage event has occurred or is planned.		
Preconditions:	§ GIS Outage Notification Application online. § CIS online.		
Postconditions:	CIS updated with database records documenting the outage event and the affected parcels (i.e. customers).		
Priority:	High		
Frequency of Use:	Moderate		
Normal Course of Events:	1. User receives information that an outage has occurred, or is planned. 2. User invokes the GIS Outage Notification Application. 3. GIS Outage Notification Application updates CIS with database records documenting the outage event and the affected parcels (i.e. customers).		
Alternative Courses:	None		
Exceptions:	None		
Extensions:	None.		
Includes (Uses):	Use Cases 1, 2, 9		
Related Business Rules:	None.		
Security Requirments:	Confidentiality: ensure that the outside party cannot get users data. • Access control Integrity: only authorized people could modify the outage notification. • Login identification • Policies • Two-factor authentication Availability: It should be available when the users need to get the data Repeated Information: Make sure there is no repeated information to users, which might cause confusion.		
Special Requirements:	None.		
Assumptions:	None.		
Notes and Issues:	Fault tolerance is required to assure that a backup way of notifying customers of outage events exists, in the case that the Outage Notification Application, CIS, or interface between the two is not working.		

3.13 Security Requirements - I would add the security requirements after the Business Rules and before Special Requirments. The definition would be Security Requirments: identify and list the possible security risks might be facing in the Use Case, at least from three aspects, confidentiality, integrity, and availability. Also, provide the appropriate control for each risk.

Security Enhanced Use Case Template – Yuqing Tang

3. Use Case Definition

3.1. Actors

3.2. Trigger

3.3. Description

3.4. Preconditions

3.5. Postconditions

3.6. Normal Flow

3.7. Alternative Flows

3.14 Exceptions

3.15. Includes

3.16. Priority

3.11. Frequency of Use

3.12. Business Rules

3.13. Special Requirements

3.14. Assumptions

3.15 Notes and Issue

Use Case Template

Use Case ID:	1		
Use Case Name:			
Created By:		Last Updated By:	
Date Created:		Date Last Updated:	

Actors:	
Actors account:	
Description:	
Trigger:	
Preconditions:	
Postconditions:	
Normal Flow: Sunny Day Scenario:	
Alternative Flows: Rainy Day Scenario:	
Exceptions:	
Includes:	
Priority:	
Frequency of Use:	
Business Rules:	
Special Requirements:	
Assumptions:	
Notes and Issues:	

Security Enhanced Use Case Template – Mei Wang

3. Use Case Definition
3.1. Actors
3.2. Trigger
3.3. Description
3.4. Preconditions
3.5. Postconditions
3.6. Normal Flow
3.7. Alternative Flows
3.14 Exceptions
3.15. Includes
3.16. Priority
3.11. Frequency of Use
3.12. Business Rules
3.13. Special Requirements
3.14 Secure Requirements
3.15 Security Requirements
3.16. Assumptions
3.17 Notes and Issue

Use Case Template

Use Case ID:	1		
Use Case Name:			
Created By:		Last Updated By:	
Date Created:		Date Last Updated:	

Actions	
Trigger	
Preconditions	
Postconditions	
Normal Flow	
Sunny Day Scenario	
Alternative Flows	
Rainy Day Scenario	
Exceptions	
Includes	
Priority	
Frequency of Use	
Business Rules	
Special Requirements	
Secure Requirements	
Security Requirements	
Secure Requirements	
Nonfunctional Requirements	
Functional Requirements	
Assumptions	
Notes and Issues	

3.14. Secure Requirements
Identify standard requirements that have security built into them to determine the necessary constraints to protect the system as a whole. They must facilitate security across entire system and be systematic.

3.15. Security Requirements
Identify separate entities that support an overall security objective. These are often contributed by security personnel and specialists. They assert what is needed within the system to support overall business security objectives and emphasize security in particular places

Security Enhanced Use Case Template – Yuchong Wang

3. Use Case Definition
3.1. Actors
3.2. Trigger
3.3. Description
3.4. Preconditions
3.5. Postconditions
3.6. Normal Flow
3.7. Alternative Flows
3.14 Exceptions
3.15. Includes
3.16. Priority
3.11. Frequency of Use
3.12. Business Rules
3.13. Special Requirements
3.14. Assumptions
3.15 Notes and Issue

Use Case Template

Use Case ID:	1		
Use Case Name:	Secure/Security requirements		
Created By:	Yuchong Wang	Last Updated By:	2/17/19
Date Created:	2/17/19	Date Last Updated:	2/17/19

Actors:	User, search engine
Description:	Searching engine that will try to find what the users' are looking for
Trigger:	Users enter their questions to the text box
Preconditions:	Needs to have internet access and get on google.com
Postconditions:	Searching keywords must make sense
Normal Flow: Sunny Day Scenario:	You type what you want to search, you get what you are looking for. 1: go to google.com 2: Typing your search keywords 3: click the link that gives you the answer
Alternative Flows: Rainy Day Scenario:	You type what you want to search, but there is no answer 1:search your keywords 2: no actual answer 3: system will update your question and looking for answer 4: upload the answer as soon as possible
Exceptions:	Keywords do not make any sense
Includes:	Other languages searching
Priority:	Medium
Frequency of Use:	10 times every day per user
Business Rules:	Protect users' IP address while searching
Special Requirements:	User must obeys the rule of federal law
Assumptions:	User wants to find something he or she does not know
Notes and Issues:	The website needs strong firewall protection in order to not alter the search results.

Security Enhanced Use Case Template – Adam Wolf

3. Use Case Definition

3.1. Actors

3.2. Trigger

3.3. Description

3.4. Preconditions

3.5. Postconditions

3.6. Normal Flow

3.7. Alternative Flows

3.14 Exceptions

3.15. Includes

3.16. Priority

3.11. Frequency of Use

3.12. Business Rules

3.13 Data Privacy Requirements

3.14 Identity and Access Control Requirements

3.15 Data Integrity Requirements

3.16. Special Requirements

3.17. Assumptions

3.18 Notes and Issue

Use Case Template

Use Case ID:	1		
Use Case Name:			
Created By:		Last Updated By:	
Date Created:		Date Last Updated:	

Actors:	
Description:	
Trigger:	
Preconditions:	
Postconditions:	
Normal Flow: Sunny Day Scenario:	
Alternative Flows: Rainy Day Scenario:	
Exceptions:	
Includes:	
Priority:	
Frequency of Use:	
Business Rules:	
Data Privacy Requirements:	
Identity & Access Control Requirements:	
Data Integrity Requirements:	
Special Requirements:	
Assumptions:	
Notes and Issues:	

3.13. Data Privacy Requirements -Describe any requirements that need to be addressed when considering the confidentiality of the data related to this specific use case. Also, acknowledge any broad security requirements (i.e. data policies, database security procedures, company security standards, etc.) related to confidentiality that would need to be considered for the use case.

3.14. Identity and Access Control Requirements - Describe any requirements that need to be addressed when considering the availability of the data related to this specific use case. Also, acknowledge any broad security requirements (i.e. identity/access policies, login procedures, company security standards, etc.) related to availability that would need to be considered for the use case.

3.15. Data Integrity Requirements - Describe any requirements that need to be addressed when considering the integrity of the data related to this specific use case. Also, acknowledge any broad security requirements (i.e. data maintenance policies, data validation techniques, traceability metrics, company security standards, etc.) related to integrity that would need to be considered for the use case.

Security Enhanced Use Case Template – Xinye Yang

3. Use Case Definition
3.1. Actors
3.2. Trigger
3.3. Description
3.4. Preconditions
3.5. Postconditions
3.6. Normal Flow
3.7. Alternative Flows
3.14 Exceptions
3.15. Includes
3.16. Priority
3.11. Frequency of Use
3.12. Business Rules
3.13. Special Requirements
3.14. Assumptions
3.15 Notes and Issue
3.16 Security Requirement

Security Requirement -

A: Unauthorized activity on operational systems shall be continuously monitored, recorded and reported

B: recording of unauthorized activity shall be initiated with 50 ms of completion operator input request

Use Case Template

Use Case ID: 1	
Use Case Name:	
Created By:	Last Updated By:
Date Created:	Date Last Updated:
Actors:	
Description:	
Trigger:	
Preconditions:	
Postconditions:	
Normal Flow:	
Sunny Day Scenario:	
Alternative Flows:	
Rainy Day Scenario:	
Exceptions:	
Includes:	
Priority:	
Frequency of Use:	
Business Rules:	
Special Requirements:	
Assumptions:	
Notes and Issues:	
Security Requirement:	

Security Enhanced Use Case Template – Li Zhu

3. Use Case Definition

3.1. Actors

3.2. Trigger

3.3. Description

3.4. Preconditions

3.5. Postconditions

3.6. Normal Flow

3.7. Alternative Flows

3.14 Exceptions

3.15. Includes

3.16. Priority

3.11. Frequency of Use

3.12. Business Rules

3.13 Special Requirements

3.14. understanding of system requirements without actually developing a final operational system

3.18 Notes and Issue

3.14. understanding of system requirements without actually developing a final operational system.

Use Case Template

Use Case ID:	1		
Use Case Name:			
Created By:		Last Updated By:	
Date Created:		Date Last Updated:	

Actors:	
Description:	
Trigger:	
Preconditions:	
Postconditions:	
Normal Flow: Sunny Day Scenario:	
Alternative Flows: Rainy Day Scenario:	
Exceptions:	
Includes:	
Priority:	
Frequency of Use:	
Business Rules:	
Special Requirements:	
Assumptions:	
Notes and Issues:	

Security Enhanced Use Case Template – Sarah Puffen

3. Use Case Definition

3.1. Actors

3.2. Trigger

3.3. Description

3.4 Security Vulnerability

3.5 Secure Requirement

3.6 Security Requirement

3.7. Preconditions

3.8. Postconditions

3.9. Normal Flow

3.10. Alternative Flows

3.11 Fail Case

3.12 Consequence of Failure

3.13 Associated Risk

3.14 Misuse Management Method

3.15 Misuse Action

3.16 Fail Case Exit State

3.14 Exceptions

3.15. Includes

3.16. Priority

3.11. Frequency of Use

3.12. Business Rules

3.13 Special Requirements

3.18 Notes and Issue

Use Case Template

Use Case ID:	1		
Use Case Name:			
Created By:		Last Updated By:	
Date Created:		Date Last Updated:	

Actors:		
Description:		
Trigger:		
Security Vulnerability:		
Secure Requirements:		
Security Requirements:		
Preconditions:		
Postconditions:		
Normal Flow: Sunny Day Scenario:		
Alternative Flows: Rainy Day Scenario:		
Fail Case:		
Consequence of Failure:		
Associated Risk:		
Misuse Management: Method:		
Description:	Misuse Action	Fail Case Exit State
Exceptions:		
Includes:		
Priority:		
Frequency of Use:		
Business Rules:		
Special Requirements:		
Assumptions:		
Notes and Issues:		

3.4. Security Vulnerability - Identify threat relative to the use case which may compromise the confidentiality, integrity, and/or availability of the system.

3.5. Secure Requirement - List the systematic approach used to ensure security across the system itself. Number each requirement. Examples:

1. Confidentiality – How data is protected to ensure no unauthorized personnel may obtain access to sensitive information.
2. Integrity – How to ensure accuracy and consistency of data stored within the system.
3. Availability – How data will remain accurate and consistent in the event of a disaster.

3.6. Security Requirement

Identify the entities necessary to support the security objective. Number each requirement. Examples:

1. Authentication – Verify user identity and eligibility to access information.
2. Authorization – Level of privilege a user has regarding access to information.

3.11. Fail Case - Describe the event(s) in which security constraints may fail, whether by misuse attack or by system control failure.

3.12. Consequence of Failure - Describe the result(s) of the fail case. The result is the system response in the event of violation of system control boundaries.

3.13. Associated Risk - Identify the risk(s) associated with control failure. Risk describes any negative impact that may derive from the result of the fail case.

3.14. Misuse Management Method - Identify and describe what a malicious attack on the use case may look like. This includes the misuse action and the resulting fail case exit state.

3.14.1 Misuse Action - Describe a malicious attack on the system. Identify the method of the activity. Example: Special characters injected into input field.

3.14.2 Fail Case Exit State -Describe how the system will handle the misuse action. Example: System reroutes to an Error Page.

Agenda

✓Adding security requirements to use case template

- Adding security requirements to functional requirements specification
- Deriving data requirements from functional requirements specification
- Quiz

Agenda

- ✓Adding security requirements to use case template
- ✓Adding security requirements to functional requirements specification
- Deriving data requirements from functional requirements specification
- Quiz

Agenda

- ✓Adding security requirements to use case template
- ✓Adding security requirements to functional requirements specification
- ✓Deriving data requirements from functional requirements specification
- Quiz

Quiz

The use of object-oriented design and development techniques would MOST likely:

a) facilitate the ability to reuse modules
b) improve system performance
c) enhance control effectiveness
d) speed up the system development life cycle (SDLC)

During which of the following phases in system development would user acceptance test plans normally be prepared?

a) Feasibility study
b) Requirements definition
c) Implementation planning
d) Postimplementation review

Quiz

An IS auditor finds that a system under development has 12 linked modules and each item of data can carry up to 10 definable attribute fields. The system handles several million transactions a year. Which of these techniques could an IS auditor use to estimate the size of the development effort?

a) Program evaluation review technique (PERT)
b) Function point analysis (FPA)
c) Counting source lines of code
d) No answer provided

The most common reason for the failure of information systems to meet the needs of users is that:

a) users' needs are constantly changing
b) the growth of user requirements was forecast inaccurately
c) the hardware system limits the number of concurrent users
d) user participation in defining the system's requirements was inadequate

Quiz

When identifying an earlier project completion time, which is to be obtained by paying a premium for early completion, the activities that should be selected are those:

a) whose sum of activity time is the shortest.
b) that have zero slack time.
c) that give the longest possible completion time.
d) whose sum of slack time is the shortest.

Which of the following should be developed during the requirements definition phase of a software development project to address aspects of software testing?

a) Test data covering critical applications
b) Detailed test plans
c) Quality assurance (QA) test specifications
d) User acceptance test specifications

Quiz

Many IT projects experience problems because the development time and/or resource requirements are underestimated. Which of the following techniques would provide the GREATEST assistance in developing an estimate of project duration?

a) Function Point Analysis (FPA)
b) Program evaluation review technique (PERT) chart
c) Rapid application development
d) Object-oriented system development

Which of the following is a prevalent risk in the development of end-user computing (EUC) applications?

a) Applications may not be subject to testing and IT general controls.
b) Development and maintenance costs may be increased.
c) Application development time may be increased.
d) Decision-making may be impaired due to diminished responsiveness to requests for information.

Quiz

Which of the following is MOST relevant to an IS auditor evaluating how the project manager has monitored the progress of the project?

a) Critical path diagrams
b) Program evaluation review technique (PERT) diagrams
c) Function point analysis (FPA)
d) Gantt charts

An IS auditor who is auditing the software acquisition process will ensure that the:

a) contract is reviewed and approved by the legal counsel before it is signed.
b) requirements cannot be met with the systems already in place.
c) requirements are found to be critical for the business.
d) user participation is adequate in the process.

Quiz solutions…

The use of object-oriented design and development techniques would MOST likely:

a) facilitate the ability to reuse modules
b) improve system performance
c) enhance control effectiveness
d) speed up the system development life cycle (SDLC)

During which of the following phases in system development would user acceptance test plans normally be prepared?

a) Feasibility study
b) Requirements definition
c) Implementation planning
d) Postimplementation review

Quiz solutions…

An IS auditor finds that a system under development has 12 linked modules and each item of data can carry up to 10 definable attribute fields. The system handles several million transactions a year. Which of these techniques could an IS auditor use to estimate the size of the development effort?

a) Program evaluation review technique (PERT)
b) Function point analysis (FPA)
c) Counting source lines of code
d) No answer provided

The most common reason for the failure of information systems to meet the needs of users is that:

a) users' needs are constantly changing
b) the growth of user requirements was forecast inaccurately
c) the hardware system limits the number of concurrent users
d) user participation in defining the system's requirements was inadequate

Quiz solutions…

When identifying an earlier project completion time, which is to be obtained by paying a premium for early completion, the activities that should be selected are those:

a) whose sum of activity time is the shortest.
b) that have zero slack time.
c) that give the longest possible completion time.
d) whose sum of slack time is the shortest.

Which of the following should be developed during the requirements definition phase of a software development project to address aspects of software testing?

a) Test data covering critical applications
b) Detailed test plans
c) Quality assurance (QA) test specifications
d) User acceptance test specifications

Quiz solutions…

Many IT projects experience problems because the development time and/or resource requirements are underestimated. Which of the following techniques would provide the GREATEST assistance in developing an estimate of project duration?

a) Function Point Analysis (FPA)
b) Program evaluation review technique (PERT) chart
c) Rapid application development
d) Object-oriented system development

Which of the following is a prevalent risk in the development of end-user computing (EUC) applications?

a) Applications may not be subject to testing and IT general controls.
b) Development and maintenance costs may be increased.
c) Application development time may be increased.
d) Decision-making may be impaired due to diminished responsiveness to requests for information.

Quiz

Which of the following is MOST relevant to an IS auditor evaluating how the project manager has monitored the progress of the project?

a) Critical path diagrams
b) Program evaluation review technique (PERT) diagrams
c) Function point analysis (FPA)
d) Gantt charts

An IS auditor who is auditing the software acquisition process will ensure that the:

a) contract is reviewed and approved by the legal counsel before it is signed.
b) requirements cannot be met with the systems already in place.
c) requirements are found to be critical for the business.
d) user participation is adequate in the process.

Agenda

- ✓Adding security requirements to use case template
- ✓Adding security requirements to functional requirements specification
- ✓Deriving data requirements from functional requirements specification
- ✓Quiz