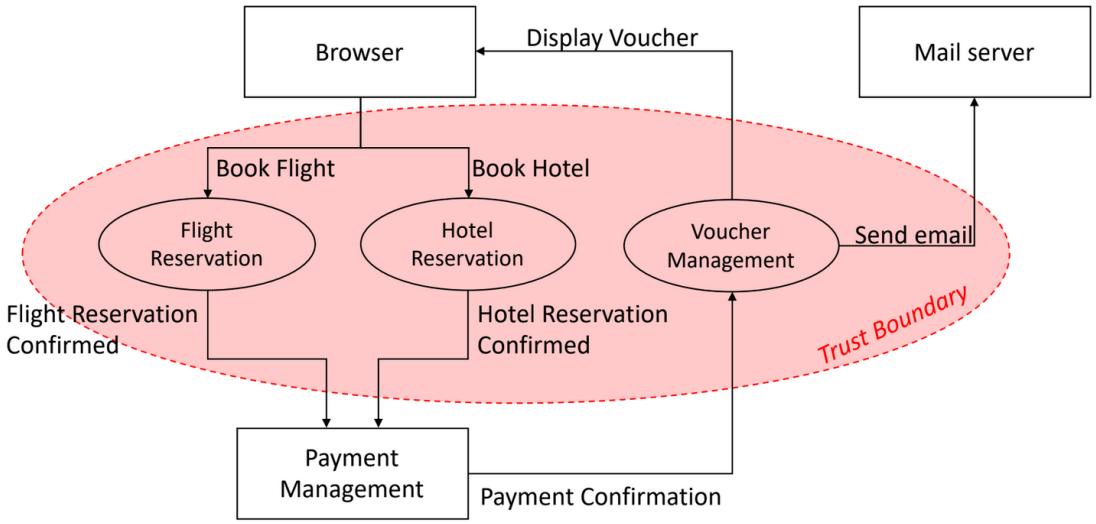
1. (Q1 XX/XX/XXXX) Describe the main objectives of the NIST CyberSecurity Framework and its structure
2. (Q2 XX/XX/XXXX) With reference to the depth dimension of Von Solm's ISG model, describe the main characteristics of the Directive vertical block.
3. (Q3 XX/XX/XXXX) Let's consider a software application supporting the travel reservation process. The application DFD is shown in the following figure:

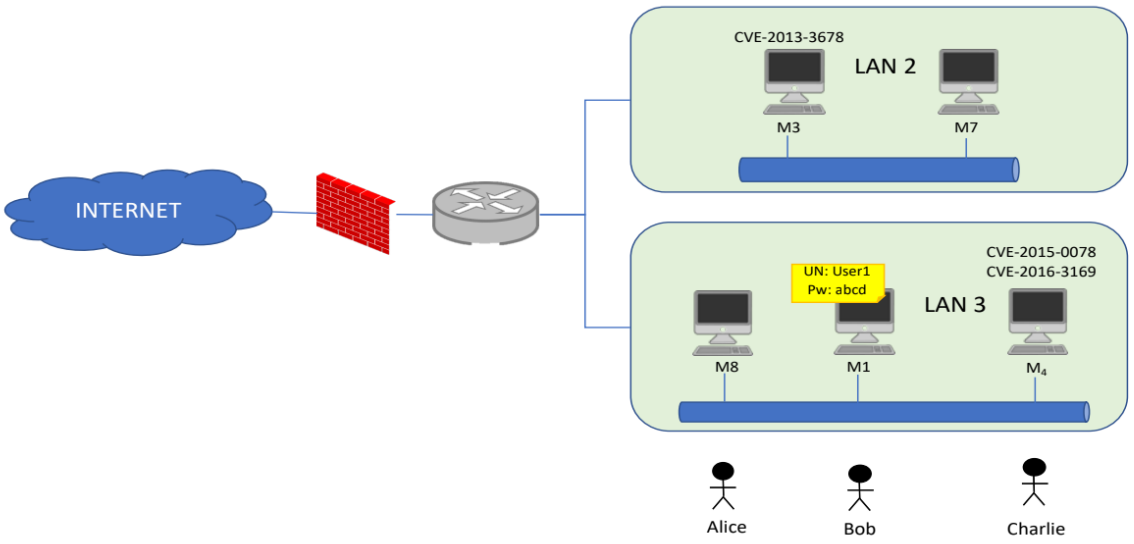


Elicit the main threats to the reservation system by assuming that:

- communications between the Browser and the reservation processes are implemented by using non-encrypted protocols
- communication between the reservation processes and the payment management system are implemented through secure communication protocols
- the mail server is hosted and managed internally to the company but from another department

For everything that is not clearly stated, the student should make assumptions and provide a consistent model.

4. (Q4 XX/XX/XXXX) Consider the fragment of the network depicted in the following figure:



Assess the risk that an attacker is able to compromise the availability of M3 by assuming that:

- M3 is reachable only from machines in LAN2 and from M4
- Alice has user access to M8 and she has the bad habits of sharing her credentials with all her colleagues
- Bob has user access to M1 and he has poor memory. He leaves all his credentials written around on post it
- Charlie has access to M4 and he is very careful in managing his credentials. However, he tends sometimes to leave his machine logged in while he is out for a coffee.
- The details of the three CVE are reported in the following table:

CVE TABLE HERE

5. (Q1 18/12/2019) With reference to Von Solm's ISG model, discuss the front dimension and its two core principles.
6. (Q2 18/12/2019) With reference to the threat modelling, describe the asset-centric, the attack-centric and the software centric approaches highlighting for each of the advantages and disadvantages.
7. (Q3 18/12/2019) Describe the main phases of the Incident Management process putting particular emphasis on the organizational structures and professional profiles involved.
8. (Q4 18/12/2019, Q4 08/06/2021) Let us consider the XYZ company that is rapidly growing both in terms of market and size. The company passed in one year from 20 to 50 employees and most of them have no technical background, but they have been just trained in order to be able to use the XYZ applications. Given its small size in the past, XYZ has no strict and encoded security process and almost every employee was able to perform all the tasks. As a consequence, there were just two types of credentials used to access systems and applications (one as administrator and one as user) that were shared by every employee.

However, XYZ realized that its growth in the last period requires an investment in order to manage security risks deriving from improper accesses and that can lead to data breaches in terms of confidentiality and integrity.

Considering the context described above and the set of controls reported in Table 1, address the following points:

1. Identify the set of controls that XYZ company should implement, providing a motivation for each of them
2. For each control selected, provide an implementation plan that XYZ company can follow
3. Provide a prioritization of all actions identified by implementation plans.

NOTE: for every relevant aspect not explicitly stated, the student should make assumptions and provide answers accordingly.

TABLE HERE

9. (Q5 18/12/2019) Let us consider the network fragment depicted in the following schema:

SCHEMA HERE

Let us assume the following reachability conditions:

- Inside each LAN, every machine can reach any other machine
- Machines in LAN1 can reach all machines in DMZ
- Machines in LAN2 can reach only S1 in DMZ

Let us assume the business process BP_i that is performed by orchestrating some applications (App_1, App_2, …, App_n) and has the following constraints:

- Confidentiality of BP_i only depends on the confidentiality of App_1
- Integrity of BP_i only depends on the integrity of App_1
- Availability of BP_i only depends on the availability of all the applications

Applications are deployed on S1 and S2 as follows:

- On S1 we have running all the applications and we have the vulnerability CVE-2013-3678 and the vulnerability CVE-2016-3169 (cfr. detailed table at the bottom)
- On S2 we have running App_1 and App_3 and we have the vulnerability CVE-2013-3678 (cfr. detailed table at the bottom).

Evaluate the following risks:

1. Loss of availability of BP_i
2. Loss of confidentiality of BP_i

CVE-2013-3678	
Multiple unspecified vulnerabilities in SAP Governance, Risk, and Compliance (GRC) allow remote authenticated users to gain privileges and execute arbitrary programs via a crafted (1) RFC or (2) SOAP-RFC request.	
Base Score (CVSS v2)	9.0 HIGH
Access Vector (AV)	Network
Access Complexity (AC)	Low
Authentication (AU)	Single
Confidentiality (C)	Complete
Integrity (I)	Complete
Availability (A)	Complete
Additional Information:	Provides unauthorized access Allows unauthorized disclosure of information Allows disruption of service

10. (Q2 08/06/2021) In the context of incident management activities, describe and discuss the incident handling lifecycle.
11. (Q3 08/06/2021) Describe what a SOC is, its main responsibilities and design principles. Finally, discuss the main differences and common points between activities carried out by a SOC and by a CERT
12. (Q5 08/06/2021)

    SCHEMA HERE

    Let us assume the following reachability conditions result from the routing tables and firewall chains:
    - there is full reachability inside every subnetwork
    - W_LAN1_2 can reach only S_DMZ_SVN in DMZ
    - W_LAN1_1 can reach only W_LAN2_0 in LAN2

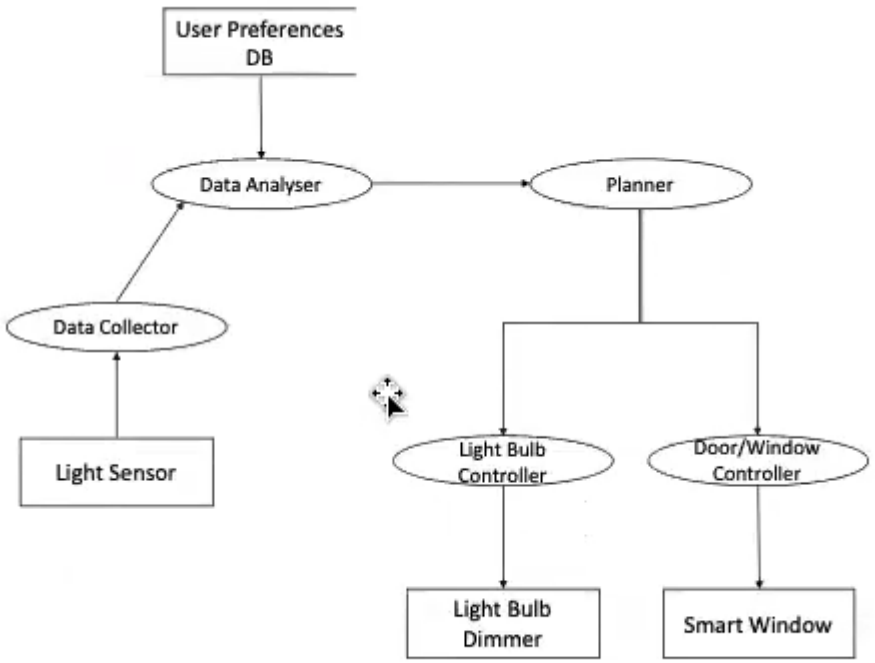
    In addition, there are two employees (Bob and Alice) owning the following credentials:
    - Bob owns credential C1 giving ROOT access on W_LAN1_0
    - Alice owns credential C2 giving USER access on W_LAN1_1

    Form a vulnerability scanner, we also found the following vulnerabilities:
    - CVE-YYYY-0004 on T_LAN2_PRINTER1 and on W_LAN1_1
    - CVE-YYYY-0001 on W_LAN2_0
    - CVE-YYYY-0003 on W_LAN2_0
    - CVE-YYYY-0002 on S_DMZ_SVN
    - CVE-YYYY-0005 on W_LAN1_2
    - CVE-YYYY-0006 on W_LAN1_1

The detailed description of the vulnerability is reported in the appendix.
Evaluate the following risks:

1. Loss of availability of the printing service guaranteed by T_LAN2_PRINTER1 assuming that its impact is LOW.
2. Loss of confidentiality of data stored on S_DMZ_SVN assuming that its impact is HIGH.

13. (Q1 02/2020) With reference to the depth dimension of Von Solms's ISG model, describe the main characteristics of the Awareness with particular emphasis on the SETA program.
14. (Q2 02/2020) Describe what is a SOC, its main responsibilities and design principles.
15. (Q3 02/2020) Describe what is an attack graph and its three main usage scenarios.
16. (Q1 09/01/2020) Discuss the role of Best Practices and Standards in the design and realization of an Information Security Governance system.
17. (Q2 09/01/2020) Describe the structure of the NIST CSF and explain how it can be used to plan investments related to cybersecurity.
18. (Q1 09/01/2020) Discuss a taxonomy of IDS systems putting particular emphasis on the different techniques that can be used to perform the analysis.
19. (Q4 09/01/2020) Let us consider the domotic system represented by the following DFD:

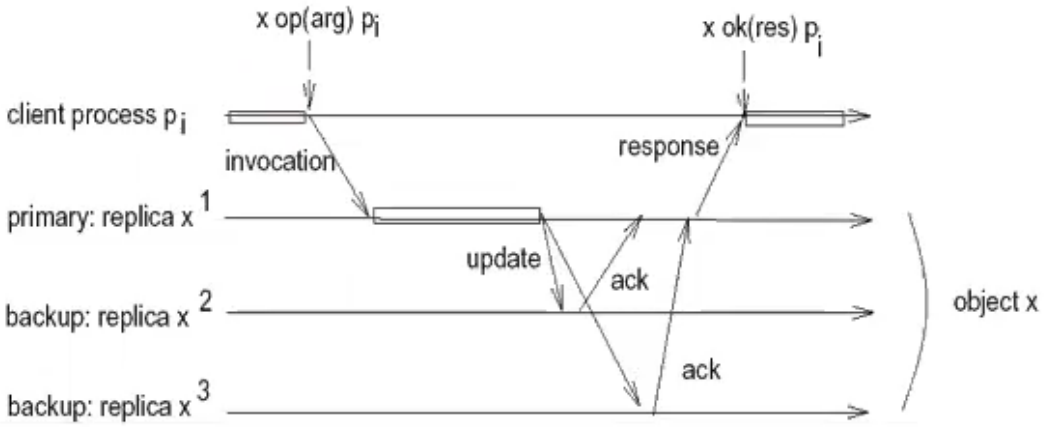


Using one of the approaches presented during the course, elicit the main threats to the system considering that:

- Communications between modules are encrypted
- The User Preferences DB has been configured to not require any authentication to access data
- The two controller processes have been developed by an external third party

20. Let us consider the XYZ company owning a private cloud where all relevant data are stored in a replicated database X. The database is composed of 3 replicas r1, r2, and r3 located on three different machines m1, m2 and m3, two inside the XYZ main building (i.e., m1 and m2) and one located in a secondary building 100 m far away (i.e. m3).

    The replication schema adopted is the primary-backup as described in the following figure where m1 acts as primary and m2 and m3 are backups.



    Considering that:

    - m3 is fully dedicated to manage the replica of the database
    - m1 and m2 also host other applications
    - m1 is also exposed on Internet
    - m1 and m2 can accessed by XYZ's employes with user privileges and by the system administrator with root privileges
    - m1 and m2 have the vulnerability CVE-2013-3678 and the vulnerability CVE-2016-2169 (cfr. Detailed table at the bottom)

    Evaluate the following risks:

    1. loss of availability of the database
    2. loss of integrity of data stored in the replicated database.

CVE-2013-3678	
Multiple unspecified vulnerabilities in SAP Governance, Risk, and Compliance (GRC) allow remote authenticated users to gain privileges and execute arbitrary programs via a crafted (1) RFC or (2) SOAP-RFC request.	
Base Score (CVSS v2)	9.0 HIGH
Access Vector (AV)	Network
Access Complexity (AC)	Low
Authentication (AU)	Single
Confidentiality (C)	Complete
Integrity (I)	Complete
Availability (A)	Complete
Additional Information:	Provides unauthorized access Allows unauthorized disclosure of information Allows disruption of service

CVE-2016-3169		
Multiple unspecified vulnerabilities in SAP Governance, Risk, and Compliance (GRC) allow remote authenticated users to gain privileges and execute arbitrary programs via a crafted (1) RFC or (2) SOAP-RFC request.		
Access Vector (AV)	Network	1
Access Complexity (AC)	Low	0,71
Authentication (AU)	Single	0,56
Exploitability	Partial	1
Report Confidence	Partial	1
	λ_CVE-2013-3678	0,40

CVE-2016-3169	
The User module in Drupal 6.x before 6.38 and 7.x before 7.43 allows remote attackers to gain privileges by leveraging contributed or custom code that calls the user_save function with an explicit category and loads all roles into the array.	
Base Score (CVSS v2)	6.8 MEDIUM
Access Vector (AV)	Network
Access Complexity (AC)	Medium
Authentication (AU)	None
Confidentiality (C)	Partial
Integrity (I)	Partial
Availability (A)	Partial
Additional Information:	Provides unauthorized access Allows unauthorized disclosure of information Allows disruption of service

CVE-2016-3169		
The User module in Drupal 6.x before 6.38 and 7.x before 7.43 allows remote attackers to gain privileges by leveraging contributed or custom code that calls the user_save function with an explicit category and loads all roles into the array.		
Access Vector (AV)	Network	1
Access Complexity (AC)	Medium	0,61
Authentication (AU)	None	0,704
Exploitability	Partial	1
Report Confidence	Partial	1
	λ_CVE-2016-3169	0,43