Fac-simile:

Q1: Describe the main objectives of the NIST CyberSecurity Framework and its structure.
Through the CEA(Cybersecurity Enhancement Act of 2014), NIST(National Institute for Standards and Technology) must identify a repeatable, flexible, cost effective and performance based approach, including security controls that can be used by owners of critical infrastructures to identify, manage and respond to cyber risk.
NIST CSF focuses on using the business drivers to guide the cybersecurity activities and making the organizations consider the cyber risk as part of the risk management process.
It is composed of the CORE, the IMPLEMENTATION TIERS and the PROFILES.
So the final goal of the CSF is to help organizations that want to "get in touch" with cybersecurity, keeping in mind the risk perspective.
This framework was developed to improve cybersecurity risk management of critical infrastructures and it is intended to be used by organizations that rely on technology, whether their cybersecurity is based on IT, IoT, Cyber-physical systems and Industrial controls.
The main feature is that it is technology-neutral, in the sense that it does not focus on a specific technology like IoT, but it abstract the technology identifying which is the main problem that you may have in this particular context.
Note that the framework is not used to compute the risk, but rather a tool that we can use to address the critical elements that we should consider in the computation of the risk. and it can also be used as a parameter to identify the level of risk that you can accept.
The CORE of the framework provides a set of activities to achieve a specific cybersecurity outcome and address some examples on how to reach it.
It is composed by 4 elements that are:

- Functions: Identify, Protect, Detect, Respond, Recover
- Categories: contribute to the definition of function and subdivide the functions in group of elements
- Subcategories: specialization of the categories
- Informative references: points to the elements and existing standards and best practices that you may want to compare(shows a method to achieve the outcome associated with each Subcategory)

The IMPLEMENTATION TIERS takes an orthogonal perspective, while in the core we try to identify which are the elements that we should consider, the implementation tiers provides some criteria to evaluate your security defenses in terms of "maturity of the process".
Practically speaking, it checks how you structured the process.
The PROFILES perform the alignment of the functions, categories and subcategories with the business requirements, risk tolerance and organization resources.
It describes the current state and the target one of specific cybersecurity activities.
The CSF can be used for different reasons, for example, it can be used for self-assessment, to improve or establish a cybersecurity program or also for buying decisions(decide what we have to buy and what we can develop by ourselves).

Q2: With reference to the depth dimension of Von Solms's ISG model, describe the main characteristics of the Directive vertical block.
Security policy documents are required by Standards and Best Practices, for example, from ISO 27002 we have Information Security policies.
To be compliant with the requirements(e.g. the ones of ISO 27001) and have a documented Direct process(of the Direct and Control loop), it's fundamental to define a mechanism to create, manage and distribute policy related documents.
The Architecture of Information Security policies is composed by the Board Directives(they identify the IT assets and provide a mandate for protecting those assets), the Corporate Information Security

Policy(an high-level document that provide the basis for all the other lower-level documents related to Information security aspects), the Sub-policies(these may vary between companies but some of them are always present, and define specific important aspects in more detail) and Procedure(defines the way in which the sub-policies should be implemented).
Some guidelines to create an effective CISP are that it should not be too long(around 4-5 pages) and not written in a complex way, also it should be stable and vary not too often.
The CISP should specify which is the owner of the policies and which are the people that will be subject to the policy.
Some of the sub-policies that are usually present in all the companies are the one related to Malicious Software, the one related to the Email Usage and Access Control policy for example.

18/12/2019:

Q1: With reference to the depth dimension of Von Solms's ISG model, discuss the front dimension and its two core principles.
The Front Dimension(Core part) represents the execution of processes and actions and the influence of the Direct and Control loop on these processes.
It is based on two core principles, the first one says that it covers all the 3 well known levels of management, the Strategic level, which is the one of the Board of directors where they define *what* to do, so an objective, the Tactical level, composed by major and medium managers, they define *how* things should be done, so a set of policies and procedures, and the Operational level, where *things are actually done* and they put in place the procedure.
The second core principle says that across the 3 levels there are some specific actions, which are Direct, Execute and Control.
The Direct actions starts from the Strategic level and goes down to the Operational one, where an objective is defined and then translated into policies and then procedures.
The Strategic level identifies the assets, their relevance and their required level of protection and they do this by taking in input internal and external factors.
Then the objective is taken as input in the Tactical level, where they expand this objective into sets of policies, procedures and standards.
At the end the Operational level expands the input taken from the upper level into administrative guidelines and procedures defining how the things must be done in practice.
Then the objective defined by the board that has been translated into procedures is executed(Execute activity) and from the bottom to the top starts the Control activity.
In this activity we have to keep in mind the concept that "we can manage only what we can measure", so to properly control we need to measure and to do it correctly we need to know which kind of information and data to collect.
The Operational level extracts some measurement data from different entities and provides a technical report to the tactical level that will "translate" it into a Tactical Management report indicating the level of compliance of the approach.
At the end the Strategic level has all the information required to understand if the objective that they generated was successful or if they need to change something and restart the Direct and Control loop.

Q2: 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.
We have seen 3 strategies for thread modeling as pointed out in the question, the asset-centric, the attacker-centric and the software-centric.
The asset-centric tries to identify what can go wrong taking a double perspective, one focusing on what is important for the defender, and one for what is important for the attacker.
Note that the things that are important for the attacker are usually tangible things, while the ones for the defender are not tangible(like the reputation of the company).

So we should consider all the enabling steps to reach the goal, which are all the elements that the attacker may want, what you want to protect and that could be an instrument for reaching a higher target for the attacker(the attacker may perform some lateral movements to reach its goal).
The steps to implement this type of threat modeling are first identify and list all the assets and then consider how an attacker can threaten them, the connect each item in the list with a computer system or a set of systems and at the end draw the system showing the assets and other components as well as interconnections until you came up with a concrete solution.
PRO: if you want to support the risk by putting the emphasis on the business component from the asset side you should use this technique.
CONS:

The attacker-centric is a type of threat modeling that takes the point of view of the attacker(think as an attacker), so it first identifies which are all the possible attack techniques, analyse and review them to identify which is the set of possible attackers and how these attacks can be applied on our system.
This procedure is performed by the analyst manually and typically it allows them to identify threats that try to exploit human vulnerabilities(not software ones).
PRO: if you are trying to identify remediation plans or you are trying to provide more awareness you should use this one.
Also, it is more useful when you need to come up with the human side of the system.
CONS:

The software-centric threat modeling approach starts from the idea that from the point of view of the programmer, the software that you have is different from the ideal software that you want essentially.
An ideal software should be defined by the set of requirements that generate it and the set of features that we put in place in order to cover those requirements.
Practically speaking this does not happen, in fact, at the end we have a software that covers some of the requirements but then others are not covered.
Also, the final software may have additional features that were not required but the developer thought that these would be useful - these are called hidden functionalities, and since they are not required are also usually not documented.
Moreover there can be designing bugs that make some features not working properly.
When we perform this type of modelling we have to keep in mind that the software is not just the application, but also the OS on which it is run and the network that it utilizes to communicate.
So we need to focus on the application, but then look also at how the application is run on the OS(maybe there may be buffer overflow vulnerabilities) and how it uses the network to communicate.
Ideally, this type of analysis should be done during the designing phase of the software, but in reality this is usually done in the maintenance phase.
PRO: if you want to protect your system, so you are in the designing phase and you want to check that the security features are implemented and the system will not be subject to specific threats, then you'll need this technique.
CONS:

Q3: Describe the main phases of the Incident Management Process putting particular emphasis on the organizational structures and professional profiles involved.
First, an incident is an event that leads to loss of, or disruption of organization operations, functions and services, so every possible event that may cause damage to the organization.
Incidents may be related to both tangible and intangible things(like a service that you provide).
Incident Management is the process that tries to identify, analyse and correct incidents, so essentially it consists of all the activities that you put in place to prevent the incident from occurring, managing the incident when it happens and recovering from it, and then using the lesson learned for the next time.

The Incident management process is structured in 6 activities and the one that we have studied is the Incident Handling one.
In particular we have seen this activity in a more general life-cycle, that starts with the preparation phase, which is the set of activities related to the prevention and to preparing the structure to react.
Then there is the actual loop where you perform the 4 actions of the incident handling activity, which are, Detection & Reporting, Analysis, Triage and Incident Response.
These 4 activities are executed in a loop because after the response to the incident, you have to continue to observe the environment to reevaluate the situation in order to assess if the response that you put in place was effective to solve the incident or if it just mitigated it(so it is still present).
Once the incident is solved, you go with the Post Incident activity where you start an analysis that provides you a feedback about what lead the system to be exploited, you analyse the techniques that have been put in place to perpetrate the incident, the way in which you managed the incident and then you may decide to restart the loop modifying something.
The preparation phase is composed of two activities, preparing to handle incidents and preventing them.
In the first activity you have to define 4 elements:

1. Communication and facilities - in this phase the most important thing is that you have to define the list of people that are involved in the incident management process and specify also how to contact them
2. Analysis hardware and software tool - equipment for the Incident management team
3. Incident Analysis resources - documentation, cryptographic hashes and a list of the critical assets
4. Incident Mitigation software - clean OS and application for recovering from the incident

Sometimes it's also useful to preparare a jump kit, which is a portable case that contains materials that may be needed during the analysis.
Then, fundamental activities to prevent incidents from occurring are Risk assessment and Risk Management processes, Host/Network security, Malicious software prevention, employees training and awareness.
In the section that I described we can see that there is the involvement of a lot of people, from the team of essentially analyst that will be involved in the Incident management process, the expert that will perform activities of Risk Management/Assessment and Host/Network security(also for the malicious software prevention) and the employees that should be trained and make aware about some incidents and in particular how those incidents can became a reality, so the threats and vulnerabilities that they need to know(credentials managing, legal software usage, etc).
Going on, at this point we can start to think about how to detect that an incident is happening, so identifying that something bad is affecting the system.
In this phase we have to keep in mind the concept of signs of incidents, which are essentially indicators that an incident is occurring or will occur.
There are two types of signs, *precursors* and *indicators*.
Then there is the analysis of the incident phase, here the best suggestion is to create a team of experts that will analyse the precursors and indicators and define the appropriate actions.
At this point we can perform the triage activity, which is related to the prioritization of the incidents and handling should be performed based on some factors, such as the functional impact of the incident, information impact of the incident and recoverability from the incident.
So now that we have identified the severity of the incident, we need to put in place communication policies to notify that a specific incident is in place and there's the need to manage it.
Here we should go back to the list of people involved in the Incident Management process that we have created in the preparation step.
At this point we can start the containment phase, which essentially consists in defining remediation actions for the incident that we can put in place immediately and that could solve the issue.
A factor that contributes here is the decision making(shutting down a system, disconnecting from the network, etc).

Then there is the eradication and recovery step, which aims to remove the root cause of the incident(with the containment we may have just limited it) and the perform the proper actions to recover from it - this is done by the administrators that will restore completely the system to normal operations, check that the system is working normally and then remove all the vulnerabilities to prevent similar incidents.
The last step is the lesson learned where you analyse the process that you observed.

02/2020:

Q1: 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.
We know that all the levels are involved in the Information Security Governance process, so, every information user of the company must be trained and aware about the policies, procedures and practices that we put in place.
The SETA(Security Education Training and Awareness) is an extension of the knowledge that people already have to do their job and the extension comprehends the skills on how to do their job securely.
The goals of the SETA are:

1. improve the awareness of the importance and need to protect organizational information resources
2. acquire the necessary skills and know how to do their jobs more securely
3. create an understanding and insight into why it is important to protect organizational information assets

The employees must be trained about aspects such as why information is such an important asset, and these training should typically address issues such as, user identification and authentication, so everything related to the password management ranging from how to choose a strong password up to how to store it(not on post-it left on the desk), legal usage of software, virus control, and so on.

Q2: Describe what is a SOC, its main responsibilities and design principles.
A Security Operation Centre(SOC) is a centralized security organization that helps companies in identifying, managing and remediating to distributed security attacks.
So the main goal is to improve the security posture of such companies by detecting and responding to threats before they have an impact on the business.
The main services that are provided by SOCs and for which they are going to take care of are:

- Log Management
- Security Incident Management
- Security Monitoring and Alerting

Additional services provided are:

- Vulnerability assessment(identify vulnerabilities in the system - not just technically)
- Security Operation Management

The most modern versions of SOC provide also some advanced functionalities such as:

- Service Security Assessment: taking a list of controls applicable to the organization(e.g. from ISO family) and provide an audit concerning the current coverage of the control and the assessment about the maturity of the control implemented
- Security analytics starting data collected from SIEM: collecting data from SIEM and then correlating the data extracted from the environment and perform further analysis wrt to the data collected outside of the company(e.g. trying to identify whether some specific types of threats are going to affect the company)
- Threat Intelligence: supporting the organization with some mechanisms that analyze information collected inside/outside the company and identify possible future threats to the organization

The SOC is in the centre of 3 elements that we should always keep in mind when we try to build a successful SOC which are, the People, the Process and the Technology.

The People are essential because looking at the services that a SOC may provide, most of them need the analysts in order to accomplish their tasks and so they cannot be fully automated.
In particular, when you have to select the person that should be included in the SOC, you have to keep in mind that they have to be specialized.
So the first step is to perform training activities and then consider people that have some kind of experience in these kinds of activities.
Then you also need to perform vendor-specific training to train people to use a particular platform that is used in the company.
The last step to consider is to continuously train people to update their knowledge to keep up with the evolution of the technologies that they have to analyse.
The Process is the same as the Incident Handling life-cycle that we have seen when we studied the Incident Management, so it starts with the preparation, then there is the identification, containment, eradication, recovery and the last one is the lesson learned.
We have this because the services provided by the SOC are mostly related to the Incident management process.
For Technology, we cannot design a successful SOC without taking into account it, which is at the end the instrument used by the person to build and support the process in which they are involved.
So when we consider the person and the role inside the process, we have to keep in mind laso the technology and the technological competences that these people have.
At the end, to design a successful SOC we need to consider these 3 elements together and once we understand how to combine them, we need to assign roles to the people inside the SOC.
The generic structure of a SOC's organizational chart is defined in a hierarchical form, where at the top we have the SOC manager that represents the strategic level.
Then in the bottom(1st level) we have the *Frontlines* that represent the operational level, which are essentially analysts that acquire data from the environment and provide the input for the response.
In the 2nd level we have the people working for the response, so they have to identify which are the response actions that could be put in place to limit the action of the attacker based on the analysis provided by the 1st level.
In the 3rd level we have people grouped according to different services that they provide and are called *Hunters*.
We can have hunters for different aspects, for example for the Network(they manage and control all the responses related to the network), for the Malwares and hunters for specific endpoints of the company.
At the end the hunters should provide the input for the SOC manager that based on the feedback that receives it will identify new directions and implement in the hierarchical structure the Direct and Control loop.
From the pov of the techniques used that these roles need to use to support the Incident Management process and Incident handling life-cycle, what they are going to do is acquire data from heterogeneous data sources and implement a kind of correlation and selection mechanism that will filter not relevant data and keep the relevant data aggregated and enriched to provide increased situational awareness to the analyst that at this point will take decisions.
The most typical types of data needed to acquire in this process are Network traffic, Network flows, System logs, Endpoint data, Threat feeds, Security events and Identity/asset context.

Q3: Describe what is an attack graph and its three main usage scenarios.
An attack graph represents the possible ways in which a potential attacker may intrude into the target network by exploiting a set of vulnerabilities on various network hosts and gaining different levels of privileges at each step.
In the nodes we have the privileges gained and in the edges the vulnerabilities that have to be exploited in order to acquire those privileges.
The nodes that we can use to build an attack graph are:

- privilege nodes: represent the privileges gained on a machine identified with its IP address

- vulnerability nodes: represent the vulnerability that affects an host
- information source: represent the additional information needed to the attacker in order to continue with the exploit
- conjunction node(and node): combine more that one privilege required an attacker in order to successfully exploit a vulnerability or use an information source

All of these nodes can include information like the IP address, the CPE id, the application name and specific nodes allows also for specific additional information, like the CVE of a vulnerability for the vulnerability nodes.
When we want to generate an attack graph we have to consider 4 main problems in the generation process:

1. reachability analysis: when we start the generation of an attack graph we may have a picture of all the hosts in a network and how they are physically connected, but we also need additional information to create a good graph such as firewall and routing rules
2. attack template determination: which information that we want to represent in the attack graph
3. attack structure determination: the meaning of each node and edge
4. attack graph core building mechanism: the algorithm that we are going to use when we compute the graph

For the first problem, the typical solution is to build a *reachability matrix* where in the columns and rows we have all the different hosts and in the interception we represent if two hosts can communicate with each other(e.g. from host 192.168.1.2 I can reach host 122.67.80.5).
In the interception we can either use boolean values to indicate the reachbilitty or also specify the protocol used by the two hosts to communicate(so the matrix can represent any type of connection among the hosts, physical, transport, application, network).
For the template what we have to do is to identify which is the level of details of the attack that we want to capture and include in the representation of the exploit.
We can define the attack template as the set of conditions required by an attacker to perform a specific attack and describe the conditions gained by an attacker after the successful corresponding attack.
Here we have to identify also which level of privileges we want to consider(common access privileges - none, user, root - or also more sophisticated ones).
For the attack structure we have to keep in mind that due to the number of hosts that are in a network, the size of the graph may grow exponentially and so here we have to find additional graph elements that have to be introduced to reduce the space complexity of a full attack graph and also the time complexity of building an attack graph.
At the end, for the core building mechanism, we should consider that for both partial and full attack graphs the current privileges of an attacker and the target one should be passed as input for the attack paths determination.
For full attack graph generation each possible attack path from the initial to target privileges if found and the full attack graph generation process can be formulated as a general graph traversal problem.
The main problem of attack graphs is the scalability, but we have some techniques to try to overcome this problem, such as pruning the attack paths, monotonicity assumption or computing the shorter attack path or paths with fixed length.
The main usage scenarios of an attack graph are:

1. Computing Network Security Metrics: here you can include all the analysis that contributes to the computation of security metrics indicating the security level of the target network and in particular in our case we are going to use it to support the risk analysis.
   In this way you can identify the source and target in the system and set them as source and target of the attack graph and then evaluate the risk of the specific situation;
2. support Network hardening: we compute the attack graph and use it in order to identify the best set of mitigation actions, typically expressed in terms of vulnerability batches(how to remove a specific set of vulnerabilities or which is the set of vulnerabilities that we should remove to mitigate the problems in the network) or it can be used to reason of mitigations in

terms of reachability so you can try to change configuration like firewall rules, etc.
It can be used also to deploy intrusion detection filters;

3. support near real-time security analysis: the idea is to use the attack paths as possible patterns that an attacker may exploit and you monitor whether these attackpaths are exploited or not by an attacker - so you monitor through the analysis of IDS alerts whether the attacker is matching over specific attack paths and you can identify how to respond to a specific attack by cutting the edges of the specific path that the attacker is going to follow.

09/01/2020:

Q1: Discuss the role of Best Practices and Standards in the design and realization of an Information Security Governance system.

ISG should help in "doing the right things right" and every Information Security Manager should be able to answer to the following questions:

1. How do I know which are the right things?
2. Even if I know, how do I know that I'm doing right?

The answer to these questions is to look at the best practices.
The best practices(or standards) are documents that include the experience and the solution of other ISM(on which experts have reached consensus on) that provides an internationally accepted framework that can be used as a building block for ISG.
Examples of best practices can be NIST, ISO 27k family, etc.
We have seen in particular ISO 27001 and 27002 as examples of best practices.
ISO 27001 is an international standard that specifies the set of requirements to establish, implement, maintain and continually improve an ISMS within the context of an organization.
ISO 27002 is an international standards that is intended to be used by organizations that want to:

- select controls within the process of implementing an ISMS based on ISO/IEC 27001
- implement common accepted information security controls
- develop their own information security management guidelines

Each clause defining security controls contains one or more security categories, where each of them contains a control objective stating what is to be achieved and a set of controls that can be applied to reach this objective.
The difference between those two standards is in the fact that ISO 27001 is very strict and goes down in detail, while ISO 27002 is more high-level and provides help to companies that want to build an ISMS based on the experience of other companies.

Q2: Describe the structure of the NIST CSF and explain how it can be used to plan investments related to cybersecurity.

<Same answer as the first question in page 1>

This framework can be used for different things, but related to investments we can define the following aspects:

- improving the cybersecurity program: we can define which is the level of security that we can to reach in specific functions
- Buying decisions: evaluate what we can should buy and what we should create by ourselves in the company

So it can be used to plan investments related to the creation or improvement of the security program of a company and also to decide what the company should buy(as a service from other companies for example) and what instead we can create inside the company on our own.

Q3: Discuss a taxonomy of IDS systems putting particular emphasis on the different techniques that can be used to perform the analysis.

The taxonomy of an IDS is composed of the *Information Source, Analysis Strategy, Time Aspects, Architecture and Response*.

For the Information Source we have different alternatives which are Host-based, Network-based, Application Logs, Wireless networks and sensor alerts.
The most used are for sure the host and network based.
The first one is related to everything that concerns a specific host, so it focuses on analysing the events that happen in that host, including the network traffic, permissions, file access, processes, logs etc and it can also be used to inspect encrypted data.
Typically it is used on critical hosts(e.g. servers) because it requires managing a lot of information and for a normal host can be too resource consuming.
Other downsides are the fact that focusing on a single host does not have a picture of the context in which the host is working and also since it needs to manage a lot of data, the configuration of the IDS may be complex.
For the network based solution we focus on the communication between typically two hosts, so not only the traffic on the interfaces but also the between.
The type of data that you analyse is related to the type of protocol you use, so application, transport or lower layers(mac, arp).
The sensor here is placed not on a specific host but rather in the link between them, so *in line*.
In this way we can perform active detection, but also the passive one is allowed by creating a copy of the traffic toward the machine that is acquiring the traffic and analyzing it.
The good point of this solution is that it works in a stealth mode(no IP) and it is not intrusive for other operating systems in the network.
The downside is that it cannot inspect encrypted data.
The Analysis Strategies are the Misuse and Anomaly Detection.
The first one focuses on the knowledge of the attack, so the idea is that we know which are the common attacks and the strange behaviors and we compare the events that we are observing and acquiring from the environment with these attacks.
If we get a match, we trigger an alarm.
The main problem is that if the attack changes a bit from the version that is known to the IDS(stored in the knowledge base typically) then the attack may go undetected.
Example of this technique are the signature based(used by Snort IDS) which compares the events observed with the fingerprints of attacks or the rule-based systems that performs the match by evaluating the “if then” condition, so evaluating whether something happens and if the condition is verified they associate the label corresponding to the class of attacks that they try to match.
For the Anomaly Detection we try to detect anomalies wrt the normal behavior of the system, so the opposite of the Misuse detection.
Here we know which is the normal behavior of the system/network/etc and so we check that the events that we are observing matches with this concept of “known behavior”.
We can do this with a Programmed system and such systems work with fixed models, Default deny(model of the normal behavior where only the modeled states are allowed) or Descriptive statistics(statistical model of the normal behavior).
To detect the anomalies we can use time or non-time series, so either we consider the time correlation between events or not.
For the time aspects we may have online and offline tools, the first allows us to analyze the events online, so there is a flow of data that goes from the monitored system to an online service and this improves the timeliness because we can analyse in real time, but we need specific resources to do that.
The second solution analyzes the data offline by collecting all the data in a storage and then analyzing it all together to improve the performances since we can chunk the data in the right size, but the timeliness here is worse because we don’t analyze in real time.
For the Architecture instead we can use Centralized or Distributed solutions, the first we have a single element that analyse the data(easier to configure but we have a single point of failure) while the second solve the problem of the centralized one but required particular configuration since all the system must be synchronized.