1- Not all existing devices (endpoints) within the offices are well secured.
Assets valuation
CEO
Dear CEO we have a high risk which is the endpoints are one of the most important parts of the company because these devices have a lot of customers data and data for the company so they will be in risk because of the weak security on the ends point
The endpoints it is an entry point for the threats so if any hacker attacked one of these endpoints it will have a big negative effect on the reputation of Bombay and can damage a lot of things because they have access to what this endpoint can do business continue
Threats on assets

1- customers data could be published
2- losing customers

Cfo
Dear CEO we have a high risk which is that we have a weakness in the security of the endpoints and that is a very dangerous thing so we are vulnerable to theft at any time if this happened we going to lose around 300k and very important data which means we are going to lose money and customers but if we want to improve the security to be safe we have to pay 100k so its worthy
Threats on assets
Finance
There will be a financial deficit, which will lead to employees not paying their salaries And the inability to spend on company cars

HR
Dear CEO we have a high risk which is that we have security weakness in our endpoints which means we are vulnerable to theft and if this happens we are going to need 4 days to fix errors that might happen instead of working and making money which means we will make the employees work 9 hours instead 5 days to fix downs besides of losing customers trust and data
Threats on assets
employee and productivity
Employees will be very tired so they will work for a lot of time without having the productivity that you want because they have two jobs to do in this situation

Vulnerabilities on assets

1- no HTTPS

2- there is no protocol to scan the data that is coming from outside

3- all the pcs ports are available for the employees

The impact

It is a frequency loss because we have faced the same issues last year and before 2 years too so we have a money loss and customers and their trust lose, time lose

Controls

Malicious Code Protection (Anti-Malware):
mechanisms to utilize anti-malware technologies to detect and eradicate malicious code.

File Integrity Monitoring:
(FIM) technology to find and report unwanted adjustments to operating systems and data.

Host Intrusion Detection and Prevention Systems (HIDS / HIPS):

methods for using Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS) on delicate systems.

2- One subnet is used for all devices in all monitoring stations.

CEO
Dear CEO we have a problem which is a medium risk too that all the devices are connected to the same network which is very dangerous which means if any hacker access any device and interrupts the network, all the network will be down so the business will stop so the customers won't be able to track their shipments.
Also, the hackers can control all the devices by accessing one so they can see private Information and they can publish anything on the webpage which will make the customers not trust our company and make our competitor happy and people will think that other companies more trustworthy so that means we will lose customers too

Threats on assets
-customer will have trust issue with the company: which means a lot of customers will not work with us
-Accessing confidential data
-errors in connection
-losing data

CFO
Dear CFO we are facing a medium risk which is all the devices are connected to the same network which means if w faced any attack we will have our services down and will have to work for a couple of days to solve this and it will cost around 400k In addition to the losses and we don't know if we are going to work again because if the hacker published anything on our web will make customers go for others company so we will face two problems the first one that it will cost 400k to solve it and the other one we won't have a god profit if we lose customers.
Threats on assets
- Liquidity

- Return on investment (ROI)

HR
Dear HR we are facing a medium risk that is all the devices are connected together on the same network so if this happened we will have to make the employees work 24h until we solve the problem which means we have to play them more money and they will not be happy and working for 3 days without sleeping will cause two things the first one they will not focus because of tired and the second one the productivity will increase because all the network is down and because of tired

Threats on assets
employee and productivity: because they will have to work for Bart Tim that means why will not do their work because the network is down and because they have to fix the error
And we Will have to make training courses for the employees that means we will no have time for productivity

Vulnerabilities on assets

All the devices are connected to the same network

Not having a firewall: which make filtering can provide attacked

Ports that are not needed

We don't have an organization for the data traffic

Controls

I want to divide the subnet into small subnets which will increase the security and the speed

If we don't put this control we will lose 400k instead of paying 150k to put this control and this control will improve the efficiency of the network, and the productivity will increase

3-Data processed by conveyer system (related to the shipments) in each branch well be uploaded to the system on the cloud via Internet connection and will be stored there in a database server for analysis and reporting. The transmission of data is done through a published web application over the Internet (front-end back-end architecture). Such information should be highly secured since it is considered of customer privacy and protected by law and regulations.

Dear CEO we have a risk that our cloud is over the network and our data is so important and this is the way that we are using to send data through to the server the other risk is that we have just one data center and that is a big danger so if the risk happens we will lose all our data and we don't have a backup to restore it, so we will have priceless that means our business will stop for a long time and it will cost us over a million to pass this. And if the competing companies knew that we lost everything we had, it would be an opportunity to stand out

CFO

Dear CFO we have a risk that our cloud is over the network and our data is so important and this is the way that we are using to send data through to the server the other risk is that we have just one data center and that is a big danger that will cost us over a million to begin standing out again which is a very big number so we can't pay the employees their money and we will not have money to spend on our transportations but if we want to put some controls wall cost 550k

HR

Dear HR

Dear CFO we have a risk that our cloud is over the network and our data is so important and this is the way that we are using to send data through to the server the other risk is that we have just one data center and that is a big danger that means there will not be any productivity because we don't have any data to work with and on the other side if all the branches want to send data to the database in the same time we will have traffic and it will take a lot of time to finish the tasks

Threat on asset

Losing money

Losing customers because we will not have data about them

Losing time instead of working and gaining money

Employees will be under stress and depression

Losing big data

Vulnerable on assets

Vulnerabilities on assets

Not having a backup database

Not having a backup system in every branch

Using a public network to communicate with the data center

controls

Making a private network the communications the branches with the data center

Putting a backup system in every branch

Putting a backup system for the main data center but in another location

4-Customers are able to create profiles on an online tracking system hosted on premise and to be moved on the cloud. Such profile contains some personal and private information that should not be disclosed to other parties.

Dear CEO we have a high risk which is the customer's profiles are online on the cloud and also all the customer's data are stored on the cloud too, that is a very dangerous problem because the cloud storage is nut will secure so the hackers will be able to get the customer's privet information and hack them and if this happens you will lose your customer because they will not trust u anymore and this will effect on the reputation too because if just one customer was hacked and all his privet data were published he will tell everyone not to work with us and the last point if we lost data we will be not able to continue our work except after restoring it

Threats on asset
Losing our reputation
Losing customer and their trust

Dear CFO we have a high risk which is the customer's profiles are online on the cloud and also all the customer's data are stored on the cloud too, that is a very dangerous problem because the cloud storage is nut will secure so the hackers will be able to get the customer's privet information and hack them and if this happens you will lose around 90k Financial compensation And the company will bear the responsibility and in case you need to appoint a lawyer is you also have to pay around 30k so the magnitude is so high

Threats on asset

Losing a big amount of money
Losing data

Dear CHRO, we have a high risk which is the customer's profiles are online on the cloud and also all the customer's data are stored on the cloud too, that is a very dangerous problem because the cloud storage is not will secure so the hackers will be able to get the customer's privet information and hack them and if this happens the productivity of the employees will decrease so much because they will be working to solve the problem

Threats on asset
Losing time instead of working and making money
Employees will be under stress
Losing employees

Vulnerabilities on assets

The cloud is online

Controles

Making physical storage to store the customer's data in it when they create a profile online

5-When you checked the current data centre as well as the warehouse in each branch, you noticed that the door is easily opened. So, shipments, servers and networking devices are easily accessed by anyone. You also noticed that the humidity and temperature inside the servers' room are not well controlled

Dear CEO as you know we have a weak door for our data center which is a high risk so it will be easy to hack physically by accessing through the door and if any hacker did access the door he will be able to put a usp that contains a virus in any server and he will be able to copy all the data that will effect on the business continuity of the company because we will not be able to work without data
And on the other hand, we have another risk which is the temperature of the data center which can cause a faler in the server means customers can't see their pages and track their shipments Which leads to damage to the company's reputation
Threat on asset

Losing customers

Losing money

Losing data

Dear CFO
Dear CEO as you know we have a weak door for our data center which is high risk so it will be easy to hack physically by accessing through the door, if any hacker did access the door in this situation we will lose all data and a big amount of money around 900k and the profit will decrease because we will not have the same number of customers
The other risk is the temperature of the database if any server is affected by the temperature it will go down and customers will not be able to yes for example the website so we will lose profit because it will need time to fix it and in this time you might have hundreds of operations

Threat on asset

Losing money

Dear HR we have a high risk which is the door of the database is weak which means anyone will be able to access and if that happens we going to lose big data and the employee's data too and the servers might stop in this situation the productivity will decrease because we don't have servers and the employees will work 4h more
The other risk is the temperature it will effect the same effect as the previous risk because servers are very sensitive to temperature if the server got overheated it will stop so as I said productivity will stop because the server is not working so the employees don't have work to do without servers.

Threat on asset

Losing time to solve the problem instead of making work and money

Vulnerabilities on assets

Not having a strong door

Not having physical security on the door like passwords and cameras

No air condition

No thermostat rot tracking the temperature

The mitigation will increase to 30%

Controls

I want to put a metal door with some security methods like 3 keys and cameras on the entrance and a fingerprint also I want to put a motion sensor inside the data center and connect it to an alarm system(detective)

I want to put a central air conditioner under the floor and a thermostat with an alarm to let me follow the temperature changes in my office without accessing the database

6- Some employees have VPN access to the data centre to run some applications remotely

Dear CEO we have a high risk which is some employees have access to the VPN which means they can access the data center and the data center contains all the company and customers' information and that is so dangerous because any of these employees can take data and sale it to others companies so all you company information will be between everyone and also can take some customers Information and blackmail customers so you going to lose customers because they will not trust you anymore that means it will effect on the business continuity and on the reputation of the company so the profit will decrease

Threats on asset

Losing customers
Losing data

Dear CFO we have a high risk which is some employees have access to the VPN which means they can access the data center and the data center contains all the company and customers' information and that is so dangerous because any of these employees can take data and sale it to others companies and also can take some customers Information and blackmail customers so you are going to lose customers because they will not trust you anymore that means no customer no work no money so you will lose money also you will have to pay compensation for the affected customers around 20k per affected customer

Threats on asset
Losing money
Losing financial Information

Dear CHRO, we have a high risk on our company which is some employees have access to the VPN of the data center which means they can see all the private data such as the company's private information and the employee's private information so It is considered a breach of privacy it will effect on the employees you might lose some employees because they will lose the trust of the company that means you will not have enough employees so the productivity will decrease

Threats on asset
Losing employees
Losing employees trust
The productivity will decrease

Vulnerabilities on assets

Some employees have a VPN access

control
Take the access from everyone and give it just to the CEO
Put a password on the VPN

7- Some other third parties are granted VPN access for support reasons, like the companies that provided and installed the conveyer system

Dear CEO you have another high risk which is that third parties can access the VPN so which means they can see all the data on our private network and that is a big problem because if any of these third parties took some private data and published it will effect on the reputation of the company and if they took some data the business continuity will be affected too but if you give me 1k I can handle all that

Threats on asset

Losing money

Losing customers trust

business stop

Dear CFO

Dear CFO you have another high risk which is that third parties can access the VPN so which means they can see all the data on our private network and that is a big problem because if any of these third parties took some private data and published it will effect on the profit because the customers will not trust us anymore so they will not work with us anymore and our loss will be around 50k

And the magnitude will increase tho 40% so I need 1k to handle all that

Threats on asset

Losing money and profit

Publishing privet financial Information

Dear CHRO, we have another high risk which is that third parties can access the VPN so which means they can see all the data on our private network and that is a big problem because if any of these third parties took some private data and published it will effect on the productivity of the employees and the business because if we lose data we will need 10 days to restore the data and we will need to give the employees a training course to know how to restore the data with less damage

Threats on asset

Losing employees

productivity decrease

Vulnerabilities on assets

There are no contracts guaranteeing the rights of the company

Controls

Companies sign contracts that include laws to ensure the confidentiality of the company and its rights

8-Very minor security procedures taken by Bombino as well as some misconfigurations on some network security devices like firewalls and VPN.

Dear CEO the risk that u have is that there is a misconfiguration on the security devices so it is a very high risk that can lead to stopping the business and can damage the reputation of the company because this misconfiguration allows the hackers to enter the data easily because the VPN is a privet network and if this VPN stops you will lose the communication with the employees and with the customer so that means the business will stop

Dear CFO you have a high risk which is the misconfiguration of the VPN and firewall as you know the VPN is a private network its an interior system so the misconfiguration of the VPN will cause a big loss on the profit of around 3k per hour because all the servers will stop so plus the firewall will cost you around 10k loss because without the firewall it will be easy to hackers to get the privet information

Dear CHRO, you have a high risk which is the misconfiguration of the VPN and firewall as you know the VPN is a private network so if the VPN stops we need all the employees to work on this problem and we don't know how much time they need to fix it so the productivity will decrease so much because the all the business will stop

Threats on asset
losing profit
Losing customers trust
And losing customers
Losing data

Vulnerabilities on assets

Not checking on the updates

Controls

On on updates

Making another VPN network in case one is down

Part B

Discuss risk assessment procedures

One of the key elements of a risk analysis is risk assessment. Risk analysis is a multi-step process with the goal of identifying and analyzing all potential risks and problems that might be harmful to the organization. This is a continuous procedure that is updated as required. These ideas are related and adaptable on their own.

1-Establish the context: before you identify the risk, determine the activity's scope, including your objectives, and gain knowledge of your operational environment.

2- Identify the risks: Identifying risks entails considering what might go wrong as you deliver your target.

3- Analyse the risks: To calculate the total level of risk,

Initial risk assessments are made on an inherent basis, taking into consideration the possibility and consequences of the risk without taking into account the firm's controls. This clarifies the significance of controls in risk mitigation.

4- Evaluate the risks: Determine whether the degree of risk is acceptable and the best way to handle each risk by evaluating it. The risk rating levels are related to the levels of acceptability, and they are defined as:

- Extreme
- High
- Medium
- Low

5- Treat the risks: Your response to a danger by:

By weighing the advantages gained from each activity's implementation against its expenses, the best risk treatment may be chosen. Generally speaking, the expense of risk management must match the rewards realized. The larger context should also be considered when weighing cost vs benefit decisions.

- Avoid: picking a different, more acceptable action that satisfies company objectives, choosing an alternate less hazardous strategy or procedure, or opting not to move further with the activity that produced the unacceptable risk.

- terminate: putting in place a plan that divides or transfers the risk to one or more parties, such contracting with service providers, outsourcing the administration of physical assets, or purchasing insurance. This requirement should be known to and accepted by the third party taking on the risk.

- Accept: Decide on your own if the cost of the therapy surpasses the potential benefits or the risk rating is at an acceptable level. This choice may also be appropriate when other treatment alternatives have been implemented but there is still a residual danger. The danger is not treated further; nevertheless, continuous monitoring is advised.

- Reduce: adopting an approach that is intended to lower the risk's chance or consequences to a manageable level in cases where eradication would be too time- or money-consuming.

Part C

Explain how you can take benefit of the ISO risk management methodology (ISO 31000) by summarizing it and highlighting its application in IT security of this project

gives businesses rules and general recommendations to help them create, operate, maintain, and continually improve their risk management framework.

It can be used by any public, private, or community enterprise, association, group, or individual because it is not particular to any industry or sector. A wide range of activities, including plans and decisions, operations, procedures, functions, projects, goods, services, and assets can all be covered by this standard over the course of an organization's existence.

So we use the ISO because it has a lot of benefits because it separated everything and analyses everything for us such as:

Risk Elements

- The probable FREQUENCY and probable MAGNITUDE of FUTURE loss
- Frequency: How often in the future an event might occur.
- Magnitude: How large the event is expected to be.
- Future: A defined time horizon

The following questions can be used to assist in identifying risks:

- What could go wrong?
- How could we fail?
- What must go right for us to succeed?
- Where are we vulnerable?
- What assets do we need to protect?
- Do we have liquid assets or assets with alternative uses?
- How could someone steal from the firm?
- How could someone disrupt our operations?
- How do we know whether we are achieving our objectives?
- On what information do we most rely?
- On what do we spend the most money?
- How do we bill and collect our revenue?
- What decisions require the most judgment?
- What activities are most complex?

Risk types

- Initial Risk: is Risk before any mitigating actions are taken.
- Residual Risk: is the Risk remaining after mitigating actions have been taken.
- These mitigating actions are called “Controls”

Approaches to Managing Risk

- Accept
- Mitigate
- Avoid
- Transfer

Probability versus Possibility

Possibility: Something that might be done or might happen.

Probability: The chance that something will happen.

taxonomy

- Taxonomies are organized methods of decomposing complex systems to explain how they work.

Elements of Risk: Loss Event Frequency and (LM) Loss Magnitude

Loss Event Frequency:

The probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset.

- LEF is driven by:
- Threat Event Frequency (TEF)
- Vulnerability (Vuln)

Loss Magnitude is:

✓ The probable magnitude of loss resulting from a loss event

✓

✓ The first phase, referred to as Primary Loss, occurs directly as a result of the threat agent's action upon the asset

✓

✓ The second phase, Secondary Loss, occurs as a result of secondary stakeholders reacting negatively to the primary event

Risk Definition

The probable frequency and probable magnitude of future loss.

Six forms of loss

- Productivity
- Response
- Replacement
- Fines and Judgments
- Competitive Advantage
- Reputation

Types of Risk Analysis

An overall risk rating is often assigned to each of the risk events found during a risk analysis.

1-Analyse inherent risk

2-Identify and evaluate controls

3-Analyse residual risk

What is risk analysis :

A project's likelihood of success or failure, the variation of portfolio or stock returns, the likelihood of future economic conditions, and the uncertainty of predicted cash flow streams are all examples of fundamental uncertainties that are studied through risk analysis.

Quantitative Risk Analysis

A quantitative assessment is a risk analysis that is done with an emphasis on the existing dangers' numerical numbers. You may assess a project's potential risk using a quantitative risk analysis. This might assist you in determining if a project is worthwhile. It is also helpful in creating project management plans since it enables you to prepare for hazards you can't completely remove while simultaneously reducing the chance of others.

Qualitative Risk Analysis

Using a predetermined rating scale, a qualitative risk analysis ranks the identified project hazards in order of importance. Risks will be graded according to their chance of happening and how they would affect the project's goals if they did.

Risk evaluation:
Establishing qualitative and/or quantitative correlations between benefits and related risks in order to determine risk management priorities.

Risk treatment

Risk treatment is creating a variety of risk-mitigation choices, evaluating those possibilities, and then creating and carrying out action plans. The greatest hazards should be taken care of right away.

By weighing the advantages gained from each activity's implementation against its expenses, the best risk treatment may be chosen. Generally speaking, the expense of risk management must match the rewards realized. The larger context should also be considered when weighing cost vs benefit decisions.

the following options are available:

Avoid:
picking a different, more acceptable action that satisfies company objectives, choosing an alternate less hazardous strategy or procedure, or opting not to move further with the activity that produced the unacceptable risk.

Reduce:
into practice a plan that is intended to lower the risk's chance or consequences to a manageable level when eradication would be too time- or money-consuming.

Transfer:
putting in place a plan that divides or transfers the risk to one or more parties, such contracting with service providers, outsourcing the administration of physical assets, or purchasing insurance. This requirement should be known to and accepted by the third party taking on the risk.

Accept:
deciding on your own if the cost of the therapy surpasses the potential benefits or the risk rating is at an acceptable level. This choice may also be appropriate when other treatment alternatives have been implemented but there is still a residual danger. The danger is not treated further; nevertheless, continuing monitoring is advised.

Recording and reporting

The risk management process should include monitoring and evaluation as a scheduled step that involves routine inspection or observation. The outcomes must to be documented and appropriately communicated both internally and internationally. The outcomes ought to be used as input for the firm's risk management framework's evaluation and ongoing development.

The firm's monitoring and review processes should encompass all aspects of the risk management process for the purposes of:

- Ensuring that controls are effective and efficient in both design and operation
- Obtaining further information to improve risk assessment
- Analysing and learning lessons from risk events, including near-misses, changes, trends, successes and failures
- Detecting changes in the external and internal context, including changes to risk criteria and to the risks, which may require revision of risk treatments and priorities
- Identifying emerging risks.

Part D

1-Describing different security procedures that Bombino could apply to protect customers & business-critical data and equipment

We have two kinds of controls

physical controls and virtual controls

The physical: like a strong metal door for the data center to prevent theft access and damage to our assets (preventive)

And put a fingerprint panel on the door of the data center to To prevent the entry of any unauthorized user (preventive)

And give every driver a device for saving the customer's voice when they receive their shipments to avoid fraud and security complaints in this case I will be protected the driver from the customers and the opposite

Virtual controls: like antivirus at the endpoints and Firewall (preventive)

quarantine a virus, Patch a system (corrective)

These controls will protect the customer and the business data too because if I build strong security control for the database the database has data for customers and for the business so if I used the previous controls I will protect the data of both of them.

2. Explaining data protection processes and regulations that might help Bombino to enhance IT security.

1- Lawfulness, Fairness, And Transparency:

they must not break the law or keep any important information from information subjects hidden.

You also must explain to users of your website or app what sort of information you collect and why.

2-Purpose Limitation:

According to this concept, particular information must be obtained in a specified way for a certain purpose. Additionally, it is prohibited to use the information in any way other than what was intended when it was collected.

3-Data Minimization

It simply suggests that no data can be collected at all if it is not required for a certain reason.

Additionally, clear and latest data must be obtained in order to minimize data. Outdated information must, by law, be deleted.

4-Accuracy:

It suggests that the information gained is accurate and updated to remain exact across time. Information assurance depends on the accuracy of each individual piece of data.

5-Storage Limitation:

Storage capacity refers to how specific information should be stored within a structure.

In other words, data should be kept in a way that allows access for as long as required. The data may be kept for whatever long it is necessary to achieve the stated goal.

Businesses must delete customer information when it is deemed unnecessary in order to create room for new data.

6-Integrity And Confidentiality:

Individual information should be handled to ensure the maximum protection of the person's information, as required by the GDPR. This includes protection against unauthorized or illegal data processing.

7-Accountability:

This third principle basically tells companies that they are totally responsible for any noncompliance with the GDPR regulation, as its name implies.

3. Discussing the benefits of IT security audit and its impact to Bombino IT security.

- the benefits of audit

1-evaluates your existing security setup and practices, and uses the audit findings to help you establish a goal for your business.

2-reduces hacker threats via early detection of security holes and possible hacker entry sites.

3-enables you to comply with regulations by confirming that your IT infrastructure complies with the highest regulatory authorities.

4-lets you make well-informed decisions for the improvement of your organization's security awareness and training by identifying gaps in these areas.

- **The impact**

It will increase the security and safety of your valuable information which means the customer will trust us more

It will save time for the IT employee because vulnerable points and problem areas will be easy

It keeps the business continuity in its best case and it will decrease the threats which means it will decrease the risks that we might face

because of the audit, we can detect the threats early

And also it will increase productivity because we will not lose time for solving errors

E. Discuss, in details, the security impact of any misalignment of IT security with Bombino policy.

if we have a misalignment with any policy we will be exposed to many risks and hackers
first, it will affect the reputation for example if any customer data was established in any way we will lose all the customer's trust which means we will lose customers, if we lose customers that mean productivity will decrease which the profits will decrease too
And also
Examples
Let's begin with the password policy if we have misalignment and we don't have the control that checks the policy that means we have misalignment
For example, if two devices have the same password and a hacker finds out the password the loss will be huge which means magnitude because will access the other device which has the same password as the one that he accessed so he can hack all the data on the two devices

The second policy is the branch's cameras which means all the branches must have cameras as I mentioned before. the CCTV does not prevent theft so the control is to put an employee to monitor the cameras system.
if we have a misalignment between the policy and the control it will cause a big impact on the security of the company
And on the reputation of the company and on their profit because if anything got hacked we will lose the object which means we will lose money

Part F

Design and implement a security policy for Bombino.
passwords police
1-we must have a sheet with all the passwords of the users and must be in a safe in the CEO's office
1-the password must be 8 digits
1-password must be complex
2-No similarity between the user passwords
3-the endpoints devise password must be changed every week

2- brunches cameras must be under control 24h 7

3-endpoint physical ports must be disabled

4- doors access cards and fingerprints must be disabled after work ends

5-Bitdefender anti-virus on the endpoints

Part G

Evaluate the suitability of the tools used in this policy

1-The first tool that I used is the camera it was very effective to see all moves but it does not prevent theft so I put an employee, his job is to monitor the cameras 24h 7days in case one of the branches got stolen he can notice at the same time.
If I did not have this employee I will be late to discover the theft and after I discover it I will go to the recording so it will take a lot of time

2-the second tool was a device that cut the electricity when the work time ends to stop the doors access cards and the doors fingerprints it is very effective because it prevents theft, in case the access card was falsified they can't access any door
So this tool will protect the business from the theft of valuable Information and equipment and goods

3- the third tool was a software tool to stop the physical ports on the endpoints which will help me to control the data that is on the endpoints it will give me confidence that it is not possible to obtain company and customer information by a USB or entering any information that is incorrect or harmful to the company’s reputation by a USB

4-The fourth one was a software tool is to put anti-virus on the ends point which will filter the incoming and outcoming files because in some cases you might receive a file (by email etc..) that contains bugs and it will harm the data that you have on the device that receives this packet
And I will choose Bitdefender antivirus because it highly detected for viruses so its excellent virus protection will save my data from any bugs and hackers
And it has zero impact on the preferences of the system which means there will not be any delays in the transaction and there will be no delay in services provided by the company

That means I have high protection on my data and a high speed for the system

H. A discussion of the roles of stakeholders in the Bombino to implement security audit recommendations.

Dear CEO

Some of the roles of the CEO is to save the business continuity and reputation of the company and cost
That is why CEO always needs an audit because he wants to handle any attack that will increase the cost in the company
And he doesn't want to have a lot of policies that are not used or not effective for his business

Dear CFO

Some of the CFO's roles are the get to the biggest mount profit and not to waste money
That is why CFO always needs an audit that contains some policy to protect the financial information of the company and the financial information of the employees, which means not to be in all the people's hands

CHRO

Some of the CHRO's roles are to get the best productivity of the employees and he needs the employee to feel comfortable.
That is why CHRO always needs an audit that contains so policies that control the employee's productivity and he want to be sure that some policies don't waste the employee's time

Part I
List the main components of an organisational disaster recovery plan, justifying the reasons for inclusion.

Take Inventory of IT Assets:

To determine which assets require protection, you must first map out all of your assets. Assets could include:

Hardware

software

cloud services for networks

crucial information

Sort Assets According to Criticality and Context

You must consider things in their context. How are these resources used by your company? Which resources would be most significantly impacted in the event of a disaster if lost or compromised? Sort all of your mapped assets into impact categories, from high to low, by going over each one.

Assess Potential Risks

Threats vary greatly from one another. What are the main dangers to your company as a whole? Which assets are likely to be the target of these threats? Getting feedback from the critical system's workers at this stage is crucial since they are informed about the most likely potential reasons of service disruption. Though you can't foresee every hazard, you can develop a successful strategy by evaluating each threat's likelihood and possible impact.

Define Your RTO and RPO

Recovery time goals (RTO) and recovery point objectives should be used to group recovery objectives (RPO). RTO stands for the maximum period of downtime before recovery, while RPO stands for the maximum amount of data loss you can tolerate. Your disaster recovery plan should include these objectives from the start so that the right arrangement may be chosen.

Select A Disaster Recovery Setup

Propose A Budget

Each company will have different demands for its disaster recovery plan, and with the correct knowledge, management can balance risk and investment in disaster recovery plan technologies.

Test and Review

To make sure it is prepared, the disaster recovery plan has to be tested and revised. Each employee has to be aware of what to do in the event of a real tragedy. Conduct a catastrophe exercise to evaluate employee behavior and the plan's effectiveness. Change the plan if things don't go exactly as you planned.

We should conclude in our business because it effects on

1. **Cost-Efficiency**
2. **Increased Employee Productivity**
3. **Greater Customer Retention**
4. **A Better Understanding of Scalability**

STUDENT ASSESSMENT SUBMISSION AND DECLARATION

When submitting evidence for assessment, each student must sign a declaration confirming that the work is their own.

Student name: saif haddad **Student ID: 21110214** **Is the student repeating this unit? YES NO**		**Assessor name:** Eng. Sami Al-Mashaqbeh
Issue date: 09/08/2022	**Submission date:** 06/09/2022	**Submitted on: 8/9/2022**
Programme: Computing		
HTU Course Name: Security **HTU Course Code:** 30201140	**BTEC Course name:** Security **BTEC Course Code:** Unit 5 (K/615/1623)	
Assignment number and title: Assignment 8: Bombino		

Plagiarism

Plagiarism is a particular form of cheating. Plagiarism must be avoided at all costs and students who break the rules, however innocently, may be penalised. It is your responsibility to ensure that you understand correct referencing practices. As a university level student, you are expected to use appropriate references throughout and keep carefully detailed notes of all your sources of materials for material you have used in your work, including any material downloaded from the Internet. Please consult the relevant unit lecturer or your course tutor if you need any further advice.

Student declaration
I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.

Student signature: *saifhaddad* **Date: 8/9/2022**

www.ketch.com. (n.d.). *What Are The Seven GDPR Principles?* [online] Available at: https://www.ketch.com/blog/what-are-the-seven-gdpr-principles [Accessed 6 Sep. 2022].

Quora. (n.d.). *What is the risk if all devices connect in the same subnet?* [online] Available at: https://www.quora.com/What-is-the-risk-if-all-devices-connect-in-the-same-subnet [Accessed 6 Sep. 2022].

preyproject.com. (2021). *Endpoint Security Risks - Why It Matters Now More Than Ever | Prey Blog*. [online] Available at: https://preyproject.com/blog/endpoint-security-risks.

Bika, N. (2019). *CEO vs. CFO: What's the difference?* [online] Recruiting Resources: How to Recruit and Hire Better. Available at: https://resources.workable.com/hr-terms/ceo-vs-cfo# [Accessed 6 Sep. 2022].

Lucidchart Content Team (2018). *A Complete Guide to the Risk Assessment Process | Lucidchart Blog*. [online] Lucidchart.com. Available at: https://www.lucidchart.com/blog/risk-assessment-process.

www2.education.vic.gov.au. (n.d.). *Risk Management — Schools: Step 5 — Risk treatment | education.vic.gov.au*. [online] Available at: https://www2.education.vic.gov.au/pal/risk-management-schools/guidance/step-5-risk-treatment [Accessed 6 Sep. 2022].

PECB (n.d.). *ISO 31000 Risk Management – Principles and Guidelines*. [online] pecb.com. Available at: https://pecb.com/whitepaper/iso-31000-risk-management--principles-and-guidelines#:~:text=ISO%2031000%3A2009%20describes%20a.

ISO. (n.d.). *ISO - ISO 31000 — Risk management*. [online] Available at: https://www.iso.org/iso-31000-risk-management.html#:~:text=It%20can%20be%20used%20by [Accessed 6 Sep. 2022].

ThreatX. (2018). *5 Negative Impacts of Misaligned Security Strategies*. [online] Available at: https://www.threatx.com/blog/5-negative-impacts-of-misaligned-security-strategies/.

Hanna, T. (2018). *6 Hazardous Business Continuity Risks to Look Out For*. [online] Best Backup and Disaster Recovery Tools, Software, Solutions & Vendors. Available at: https://solutionsreview.com/backup-disaster-recovery/6-hazardous-business-continuity-risks-to-look-out-for/ [Accessed 6 Sep. 2022].

www.revbits.com. (n.d.). *The Growing Importance of Endpoint Security*. [online] Available at: https://www.revbits.com/blogs/the-growing-importance-of-endpoint-security [Accessed 6 Sep. 2022].

GitLab. (n.d.). *Endpoint Security Controls*. [online] Available at: https://about.gitlab.com/handbook/engineering/security/security-assurance/security-compliance/guidance/endpoint-security.html [Accessed 6 Sep. 2022].

Avi Networks. (n.d.). *What is Subnet Mask? Definition & FAQs*. [online] Available at: https://avinetworks.com/glossary/subnet-mask/.

Nuggets, C. (2017). *5 Subnetting Benefits*. [online] IT Infrastructure Advice, Discussion, Community - Network Computing. Available at: https://www.networkcomputing.com/data-centers/5-subnetting-benefits.

Process Street. (2019). *What Is ISO 31000? Getting Started with Risk Management | Process Street | Checklist, Workflow and SOP Software*. [online] Available at: https://www.process.st/iso-31000/.

documentation.avaya.com. (n.d.). *Avaya Documentation*. [online] Available at: https://documentation.avaya.com/bundle/AvayaCommunicationManagerSecurityDesign_r7.1.3/page/IntegrityIssues.html [Accessed 6 Sep. 2022].

PECB (n.d.). *ISO 31000 Risk Management – Principles and Guidelines*. [online] pecb.com. Available at: https://pecb.com/whitepaper/iso-31000-risk-management--principles-and-guidelines#:~:text=ISO%2031000%3A2009%20describes%20a.

Anon, (n.d.). *9 Policies For Security Procedures Examples*. [online] Available at: https://www.privacy.com.sg/resources/9-rules-security-procedures-examples/.

Getkisi.com. (2019). *Workplace Security: Sample Policies and Procedures + Audit Checklist*. [online] Available at: https://www.getkisi.com/overview/workplace-security.

Walkowski, D. (2019). *What Are Security Controls?* [online] F5 Labs. Available at: https://www.f5.com/labs/articles/education/what-are-security-controls.

Varghese, J. (2020). *IT Security Audit: Importance, Types, and Methodology*. [online] www.getastra.com. Available at: https://www.getastra.com/blog/security-audit/it-security-audit/?gclid=Cj0KCQjwmdGYBhDRARIsABmSEeP4aWPDyod1lZZwPSjG-NZ7DJy0kkofguIfpb7n9oO2--H4ytaMISkaAghzEALw_wcB [Accessed 6 Sep. 2022].

Evolve IP. (2019). *4 Benefits of Disaster Recovery Planning | Evolve IP*. [online] Available at: https://www.evolveip.net/blog/4-benefits-disaster-recovery-planning.

Guerra, B. (2020). *7 Components That Make A Great Disaster Recovery Plan*. [online] Axiom. Available at: https://www.axiom.tech/7-components-that-make-a-great-disaster-recovery-plan/#:~:text=There%20are%20seven%20main%20components.

ZEVENET. (2021). *10 Importance of Information Security Audit*. [online] Available at: https://www.zevenet.com/blog/10-importance-of-information-security-audit/.

Bright Security. (2021). *Security Misconfiguration: Impact, Examples, and Prevention*. [online] Available at: https://brightsec.com/blog/security-misconfiguration/.

admin (n.d.). *THE ADVANTAGES OF BITDEFENDER AS VIRUS SCANNER - SoftwareLicense4u*. [online] Available at: https://softwarelicense4u.com/us/advantages-bitdefender-antivirus/.

Catley, C. (2014). *What are the dangers of misaligned strategy?* [online] StrategyBlocks. Available at: https://www.strategyblocks.com/blog/the-dangers-of-misaligned-strategy/ [Accessed 6 Sep. 2022].

www.cypressdatadefense.com. (n.d.). *The Impact of Security Misconfiguration and Its Mitigation*. [online] Available at: https://www.cypressdatadefense.com/blog/impact-of-security-misconfiguration/#:~:text=These%20human%20errors%20lead%20to [Accessed 6 Sep. 2022].

www.restorepoint.com. (n.d.). *What Are Network Security Devices? - Restorepoint*. [online] Available at: https://www.restorepoint.com/topics/what-are-network-security-devices.

www.thousandeyes.com. (n.d.). *How Virtual Private Networks Impact Application Performance*. [online] Available at: https://www.thousandeyes.com/blog/how-virtual-private-networks-impact-performance#:~:text=Sometimes%2C%20a%20misconfiguration%20or%20connecting [Accessed 6 Sep. 2022].

Swanagan, M. (2020). *The 3 Types Of Security Controls (Expert Explains)*. [online] PurpleSec. Available at: https://purplesec.us/security-controls/.

Stepanovich, A. (2014). *Virtual Integrity: Three steps toward building stronger cryptographic standards*. [online] Access Now. Available at: https://www.accessnow.org/virtual-integrity-the-importance-of-building-strong-cryptographic-standards/ [Accessed 6 Sep. 2022].

vmware (2021). *What is Intrusion Prevention System? | VMware Glossary*. [online] VMware. Available at: https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html.

Lauterbach, C. (2019). *Intrusion Detection, Intrusion Prevention, and Antivirus: The Differences*. [online] Be Structured Technology Group. Available at: https://bestructured.com/intrusion-detection-intrusion-prevention-and-antivirus-the-differences/#:~:text=The%20Role%20of%20Antivirus%20Protection&text=Although%20IPS%20and%20IDS%20tools [Accessed 6 Sep. 2022].

www.restorepoint.com. (n.d.). *What Are Network Security Devices? - Restorepoint*. [online] Available at: https://www.restorepoint.com/topics/what-are-network-security-devices.

ramsac. (2018). *5 key benefits of network monitoring - ramsac*. [online] Available at: https://www.ramsac.com/blog/5-key-benefits-of-network-monitoring/.

Hayes, A. (2019). *Risk Analysis Definition*. [online] Investopedia. Available at: https://www.investopedia.com/terms/r/risk-analysis.asp.

Indeed Career Guide. (n.d.). *Quantitative Risk Analysis (Definition, Benefits and Steps)*. [online] Available at: https://www.indeed.com/career-advice/career-development/quantitative-risk-analysis.

Goodrich, B. (2017). *Qualitative risk analysis vs quantitative risk analysis*. [online] PM Learning Solutions. Available at: https://www.pmlearningsolutions.com/blog/qualitative-risk-analysis-vs-quantitative-risk-analysis-pmp-concept-1.

N-able. (n.d.). *Risk Evaluation Definition*. [online] Available at: https://www.n-able.com/features/risk-evaluation-definition.

www.ideagen.com. (n.d.). *ISO 31000: Developing Your Risk Treatment Strategy | Ideagen*. [online] Available at: https://www.ideagen.com/thought-leadership/blog/iso-31000-developing-your-risk-treatment-strategy#:~:text=ISO%2031000%20defines%20a%20control.

survey.charteredaccountantsanz.com. (n.d.). *Risk Management Framework - Monitor & Review*. [online] Available at: https://survey.charteredaccountantsanz.com/risk_management/midsize-firms/monitor.aspx.