PWC Cybersecurity Job Simulation

TASK 1:

Task 1: Integrated Information Defense

Here is the background information on your task

Boldi AG is a family-owned business in Switzerland with around 90 employees. They are a premium component supplier for the chemical industry, they have 4 people in IT and hire external IT consultants now and then.

Last night the news had a story about a competitor who was hit by a severe ransomware attack. Wake-up call for Boldi AG: their last information risk analysis was conducted in 2014. Management has decided to ask top consultancies to pitch their cybersecurity services.

The team needs your help to prepare a convincing pitch presentation. But first, Stefan, your team leader on this assignment, sets up a call together with you and the Boldi AG management to get more information. They mention, they have heard of the concept of layered, integrated defense but would like to know more about how it works.

You're happy to jump in and explain together with Stefan that integrated defense is a universal concept that applies to deliberate attacks and non-intentional threats such as acts of nature. A layered approach to Boldi AG's information security would involve classification from the innermost layer of vital assets, core functions, processes, data and information to the public-facing boundary points. These interlocking layered strategies, tactical procedures and operational details would reduce the potential impact of information risks.

Then, referring to the recent attack on Boldi AG's competitor, you warn management that there are three dangers/biases that they need to be aware of:

- ignoring "blind spots" in their defenses,
- blindly trusting in their systems, processes, and people, plus
- not checking up to see if these are actually working correctly.

Boldi AG thanks you, and the call ends.

You're about to meet with our Cybersecurity team to set up workflows for preparing the pitch, when you see that a manager at Boldi AG has left you a voicemail message:

[voicemail transcript below]

"Hi, after considering the dangers you flagged, we've identified a potential blind spot. We have been storing our back-up systems images and database back-ups at an offsite facility that is not

monitored 24/7. This means that we cannot exclude with 100% certainty that unauthorised persons could enter that facility. Feel free to call me if you have any questions. Thanks."

A bit surprised, you and Stefan call back to remind Boldi AG management of the absolute minimum of information security best practices:

- physically protect information systems
- control access by all users
- control disclosure and disposal of information
- train all staff regularly

To wrap up the call, you explain that in a broader sense information security must be actively managed. A risk management framework can provide top-down guidance to organisations in setting the necessary organisational attitude and mindset.

Here is your task

Submit a PowerPoint set including both parts below to complete your task.

Part 1

We need to consider the information provided in the voicemail. Please differentiate first due care from due diligence for information risk management. Afterwards, use your new knowledge to analyse what Boldi AG did wrong. Was it due care, due diligence or both?

Our Cybersecurity team will include your findings in the final pitch presentation with your detailed explanation.

Part 2

Based on the key principles of defense, what basic options does Boldi AG have for limiting or containing damage from risk?

Hint: the abbreviation of the options is Deter, Detect, Prevent, Avoid. Please briefly explain each one.

Before you answer in an email to Stefan (please use one PowerPoint slide of your deck), think about how Boldi AG can react to an attack like the one experienced by their competitor.

TASK 2

Here is the background information on your task

Our Cybersecurity team gave an excellent presentation. We won the pitch! Now the action starts: Stefan needs to present a risk assessment of Boldi AG to its management, explaining it in detail step by step. But a risk assessment requires lots of work up front.

You are working with Stefan on location at Boldi to learn as much as possible about the company. First, it is critical to establish a common understanding of information risk at Boldi AG. This means learning about the company and its culture.

- What is their risk tolerance?
- How willing are they to accept risk?
- How do they handle changes in processes and systems?

A risk management framework can provide top-down guidance and establish the attitude and mindset to build consensus about risk. It is also important to understand how Boldi AG controls changes in business processes and systems, particularly Information Technology Systems.

Here is your task

Create and submit a PowerPoint slide deck for Stefan answering step 2 and 3. For the first step, use the memo function of your phone and upload a voicemail to complete your task.

1. To learn more about Boldi AG and its culture, you first need to determine who you should talk to at Boldi AG and what the content of these interviews should be. How does your agenda differ based on the audience, e.g. management vs. engineers? Stefan is currently in a meeting, leave him a voicemail (no longer than 1.5 minutes).

2. Now you are prepared to conduct an information risk impact assessment. In the meantime, you discover that Boldi AG files on paper and the company's cloud-based information systems are inconsistent in format and hard to use for an analysis. Plus, there are no controls over who in the company can access these files.

Does any of this present an information security concern? Please explain your answer in the slide deck. Think of this through the prism of confidentiality, integrity, and availability (CIA) and add slides to your started presentation.

3. After you know enough about Boldi AG, decide what type of risk assessment would be best, a quantitative risk assessment or a qualitative risk assessment. Then explain the difference between quantitative and qualitative assessments. What do you rely on to be able to perform a quantitative assessment? Which method could be more adapted for information security risk assessments?

TASK 3

Here is the background information on your task

After analysing the impact of possible risks at Boldi AG, it's time to determine how we can lower the likelihood of these risks through specific cybersecurity measures. We need to prevent these risks from occurring by decreasing each IT system's threat surface and thus decreasing the total threat surface of Boldi AG.

Stefan has met with the Head of IT Infrastructure at Boldi AG to discuss the measures required to follow up on the risk assessment. He acknowledged the need for a detailed vulnerability review as this has not been performed for several years. However, he is not convinced that maintaining an up-to-date Information Systems Security Baseline is worth the effort since the system can be scanned with a vulnerability scan anytime. We need to convince him and you'll help Stefan to create some graphics to do so.

Here is your task

Submit a PowerPoint slide deck to complete this task.

First, you need to learn more about

- **Vulnerability Assessment**
- **Mitigation Planning**
- **Vulnerability Scanning**
- **Hardware and Systems Security**
- **Information Systems Security Baseline**

and why an up-to-date Information System Security Baseline is crucial.

Use your new knowledge to create a graphic using the terms, so we can present it to the Head of IT Infrastructure.

Write notes below your graphic, explaining in your own words the relationship between the terms.

TASK 4

Here is the background information on your task

The Head of IT Infrastructure of Boldi AG does see the need for network segmentation but cannot follow why a segmented network cannot prevent you from every possible issue. In order to give him and his people a broad understanding of the topic, Stefan organises a workshop and need your help.

Task 4: Network Segmentation

Here is your task

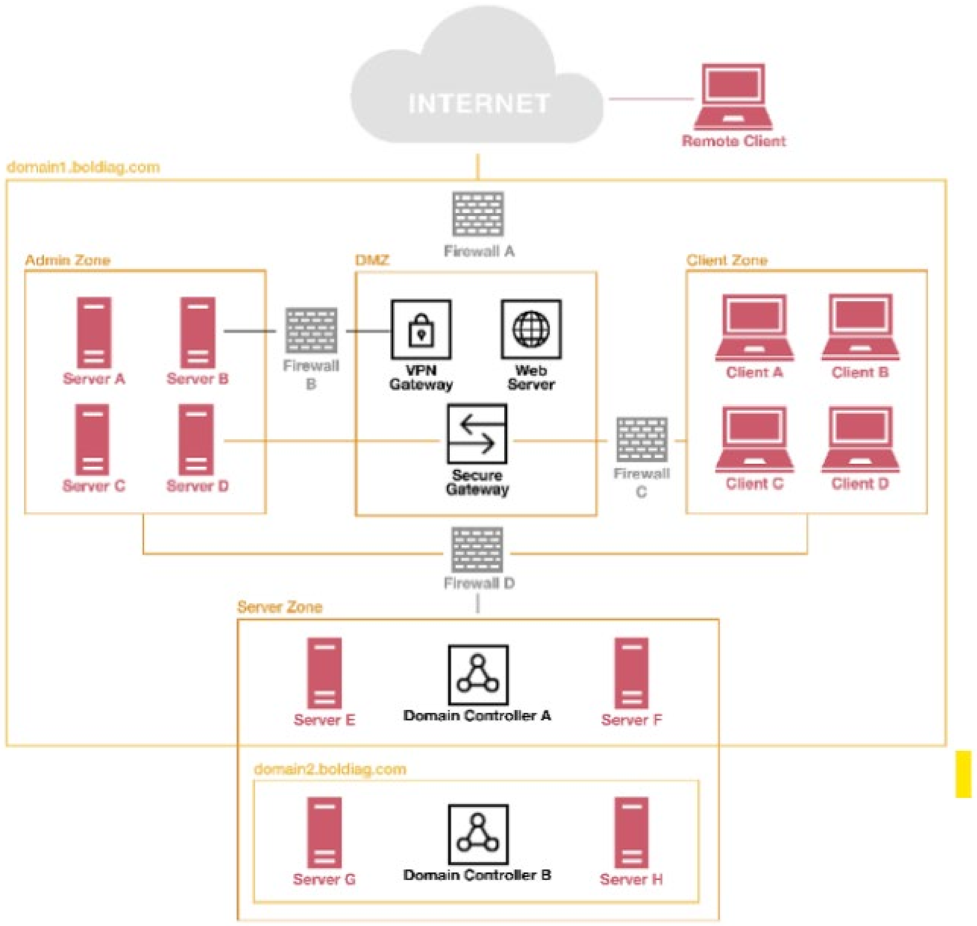
Submit a Microsoft Word document with both parts in it to finalise your work.

Part 1

For Stefans preparation, write in Microsoft Word format detailed notes explaining how segmentation contributes to network security and to the security of the whole organisation. Your notes will help Stefan creating the workshop.

Part 2

The Head of IT Infrastructure of Boldi AG provided Stefan with the following network segmentation:



Domain: A namespace which logically divides an organisation's network objects that share the same directory.

Admin Zone: Special purpose server zone, e.g. central logging, Security Information and Event Management (SIEM)

Server Zone: General purpose server zone, e.g. application servers, database servers

Client Zone: General purpose client zone, e.g. user laptops

Regarding network segmentation and trust architectures, the base configuration and maintenance of firewalls is of great importance. There are two approaches to configuring firewalls: whitelisting the good or blacklisting the bad.

Add to your notes how firewalls A, B, C and D at Boldi AG need to be configured using the concepts of whitelisting and blacklisting and why.

Ready to submit your work? That was your final task. This voice message just in from Stefan.