Defense In Depth Exercise

You have implemented your product into the customer's production environment. The customer has integrated it with their own tools to augment their day-to-day business. They will need their own end customer to utilize your software and will input data. The customer will manipulate their data using your tool and will have administrative access to your software to make custom configuration changes. What technical controls, operational controls, and personnel controls do you and your customer need to put in place? What risks are there? What is the residual risk?

CLICK HERE TO SEE THE SLIDES

Part 1: Individual participation (if you do not participate you can not receive a grade for the presentation)
Part 2: Personnel Controls (30% of Presentation each type of control) 3 Risks for full credit
Part 2.a: What risks are specific to your personnel?
Part 2.b: What is the impact of this risk?
Part 2.c: How likely is this risk?
Part 2.d: What control are you putting in place?
Part 2.e: What is the residual risk after the control you put in place?
Part 2.f: Where does this risk overlap with the other types of controls operational and technical.

Part 3 and 4 are the same as 2 but for Technical and Operational Controls.

Part 5: 10% of presentation is based on creative way to demonstrate control or risk in presentation

Speaking Order

Everlee: Introduction & Personnel Controls

Introduction

Good afternoon, Pineapple team! Welcome to today's meeting. We are the Risks & Cyber Security Management Department of Pineapple, and today we'll be discussing the critical risks our company faces in the production environment.

As we continue to grow and expand our Inventory and Supply Chain Management tools to directly compete with Apple, managing risks—especially in areas like data security, system reliability, and customer trust—becomes more important than ever. In this session, we'll focus on the three main types of controls: personnel, technical, and operational, and how these measures will help us avoiding risks while ensuring smooth operations.

First, let's talk about Personnel risks. I will talk about 3 risks: **insider threats, human error and lack of training**

First, we have **insider threats**. This risk, even though it is not very common, can have serious consequences. For example, an employee might misuse customer information for personal gain, like selling it online. If this happens, it could lead to fines, loss of trust from our customers, and even legal trouble. To prevent this, we will conduct background checks and use **role-based access control (RBAC)**, so each employee can only access the information they really need.

Next is **human error**, which happens more often. Employees might accidentally share sensitive information in emails or delete important files. For instance, a team member could mistakenly send customer data to the wrong person, putting that data at risk. To tackle this, we're going to set up strong access controls and an **automated backup system**. This way, we can quickly recover any lost data and avoid major problems.

Finally, there's the risk of **lack of training**. If employees aren't trained properly, they might not follow the right security practices. For example, someone might not recognize a phishing email and end up compromising our system. This risk is fairly common, especially if we don't offer regular training. To address this, we'll have **mandatory security training** sessions to make sure everyone knows how to protect our data and use our systems safely.

By focusing on these three areas and using clear examples, we can reduce risks and keep our operations secure.

Demi: Personnel Controls and Technical Controls

Now, I'll continue by discussing the residual risks associated with both personnel and technical controls, and how these risks overlap with operational measures. Let's break it down step by step.

First, the residual risks after controls are put in place:

- **Insider Threats**: While controls like role-based access and background checks help, there's still a small residual risk. An insider could bypass some controls, intentionally or unintentionally, but we can further reduce this risk through regular audits and continuous monitoring.
- **Human Error**: Despite automation and strict access controls, human error can't be entirely eliminated. Even with robust controls, mistakes can still happen—such as an employee accidentally deleting important files or mishandling sensitive data.
- **Lack of Training**: Training significantly reduces the likelihood of issues, but it's important to remember that not every employee will follow best practices perfectly, especially newer hires. Even with regular training, there is still a residual risk of non-compliance or oversight.

Next, let's look at where these risks overlap with other types of controls:

- **Insider Threats**: These overlap with **technical controls** like logging and monitoring, which help us detect any suspicious behavior early and respond quickly to insider threats.
- **Human Error**: This risk is managed not only through personnel controls but also through **operational controls**, such as incident response and recovery plans, which allow us to quickly address and recover from mistakes when they do occur.
- **Lack of Training**: Here, we see an overlap with both **technical** and **operational controls**. Training includes teaching technical aspects, such as the secure use of software, while operationally, we ensure staff follow defined procedures that keep us aligned with security practices.

Now, let’s transition to the **technical controls** and their associated risks.

3.a: What risks are specific to your technical controls?

- **Software Vulnerabilities**: As we all know, no system is entirely bug-free. These bugs can be exploited by attackers to gain unauthorized access, manipulate data, or cause system failures. Regular vulnerability assessments and automated testing are critical to identifying these weaknesses early.
- **Weak Authentication**: Without strong authentication, such as multi-factor authentication (MFA), it becomes easier for unauthorized users to gain access to our systems. For instance, if an employee’s password is compromised, it opens a door to sensitive company data.
- **Unpatched Systems**: If we don't apply patches and updates on time, we expose our systems to vulnerabilities that attackers can easily exploit. In a worst-case scenario, this could lead to major security incidents, including data breaches or operational downtime.

3.b: What is the impact of these risks?

- **Software Vulnerabilities**: Exploits from bugs in our systems could lead to data breaches, downtime, or ransomware attacks, which could be financially devastating and erode customer trust.
- **Weak Authentication**: If authentication is weak, unauthorized access could result in stolen data, altered system configurations, or manipulation of our critical infrastructure.
- **Unpatched Systems**: Hackers can exploit unpatched systems with known vulnerabilities, causing significant damage, including security breaches, data loss, and long-term operational impacts.

3.c: How likely are these risks?

- **Software Vulnerabilities**: Unfortunately, these risks are quite likely because no system is entirely free of bugs, despite our best efforts.
- **Weak Authentication**: This risk is moderately likely if we don’t enforce strong security practices like MFA across the board.
- **Unpatched Systems**: This risk is highly likely if we do not prioritize timely patch management. Keeping our systems updated is key to reducing this risk.

By addressing both the residual risks of personnel controls and the inherent risks of technical controls, we can maintain a robust security posture that mitigates potential threats to our systems and operations.

Calla: Technical Controls and Operational Controls

- **3.d**: What control are you putting in place?
- **3.e**: What is the residual risk after the control you put in place?
- **3.f**: Where does this risk overlap with other types of controls (personnel and operational)?

Operational Controls (Part 4)

- **4.a**: What risks are specific to your operational controls?
- **4.b**: What is the impact of this risk?

When managing **technical risks**, several **controls** are crucial. For **software vulnerabilities**, regular **security testing** helps identify weaknesses, and updates are issued to close those gaps. To address **weak authentication**, we implement **multi-factor authentication (MFA)** for all users, which adds a second layer of protection. For **unpatched systems**, a **patch management policy** ensures updates are applied in a timely manner, reducing the risk of system exploitation.

Even with these measures, **residual risks** remain. Despite regular testing, unknown vulnerabilities, like **zero-day threats**, can still be exploited before we are aware. With **MFA**, attackers may bypass security through **social engineering**. For **unpatched systems**, the risk is reduced if patches are applied promptly, though new vulnerabilities may still emerge between updates.

These technical risks overlap with **operational** and **personnel controls**. For example, if **software vulnerabilities** are exploited, operational controls like a strong **incident response** plan are critical for damage control. **Weak authentication** relates to personnel controls, as employees need proper training to use **MFA** correctly. Managing **unpatched systems** depends on **operational processes**, like a structured **patch management plan** to ensure timely updates.

Operational controls also bring specific risks. A **poor incident response** can slow recovery and worsen damage. **Change management failures** can introduce vulnerabilities or cause system breakdowns if changes aren't well controlled. Finally, **inadequate backup procedures** risk critical data loss during an incident.

The impact of these risks is significant. A **slow incident response** can lead to prolonged downtime, causing financial losses and reputational damage. **Change management failures** can destabilize systems, and **inadequate backups** can result in permanent data loss, particularly after attacks like ransomware.

Kelvin: Operational Controls and Conclusion

- **4.c**: How likely is this risk?
- **4.d**: What control are you putting in place?
- **4.e**: What is the residual risk after the control you put in place?
- **4.f**: Where does this risk overlap with other types of controls (personnel and technical)?

Alright, to continue **Operational Controls**,...

First up, we've got **Poor Incident Response**. This happens when there's no solid plan in place to quickly handle security incidents. If we don't react fast enough, it could lead to downtime or data loss. And solution? A clear incident response plan that's regularly updated and backed by training so everyone knows exactly what to do. Even with this, there's still a small risk if the plan isn't followed or kept current.

Next is **Change Management Failures**. This risk pops up when changes to the system aren't reviewed or tested properly. Rushing through changes can break things or create new vulnerabilities. To manage this, we implement a formal change management process - everything needs approval, documentation, and testing. But, there's always a small chance emergency changes could slip through, so we need to stay on top of that.

Finally, we have **Inadequate Backup Procedures**. If we're not backing up data regularly, or don't have a solid recovery plan, we risk losing critical data. The fix? Automated backups and regular recovery testing to make sure everything works. This significantly reduces the risk, but there's always a chance something could go wrong with the recovery itself, so regular testing is key.

Now, where do these risks overlap? It's all connected. **Incident response** ties into personnel training - our team has to know the plan. **Change management** links to technical controls because system changes need to be secured and tested. And **backups**? That's both technical automation and personnel monitoring to ensure it all runs smoothly.

Conclusion

So, what's the key takeaway? By combining all these controls such as personnel, technical, and operational - we can build a layered defense that drastically reduces the risks our customer's environment faces. But let's not forget: even with these in place, risks evolve, which is why **continuous monitoring, regular updates, and adapting to new threats** are crucial to maintaining a strong security posture.

Now, as we wrap things up, I just want to say this: **security is not a one-time thing**. It's an ongoing effort, and every layer of defense we've discussed today is part of that journey.

So, with that said, I'd like to thank you all for your attention. This concludes today's team meeting for the security department. Let's keep pushing forward, stay vigilant, and continue improving our defenses. Thanks and I look forward to seeing how we can further strengthen our security posture together!

Part 2: Personnel Controls (30%)

Part 2.a: What risks are specific to your personnel?

1. **Insider Threats**: Employees with access to sensitive data may misuse it for personal gain or malicious purposes.
2. **Human Error**: Employees may accidentally share, delete, or expose sensitive information.
3. **Lack of Training**: Untrained employees may not follow proper security practices, leading to data breaches or configuration errors.

Part 2.b: What is the impact of this risk?

1. **Insider Threats**: Unauthorized data disclosure could result in regulatory fines, loss of customer trust, and legal action.
2. **Human Error**: Data loss or corruption could disrupt business operations or expose sensitive data to external threats.
3. **Lack of Training**: Poor security practices increase the likelihood of breaches or system misconfigurations that compromise security.

Part 2.c: How likely is this risk?

1. **Insider Threats**: Uncommon, but can have a significant impact when it occurs.
2. **Human Error**: High likelihood, as human mistakes happen frequently, especially under stress or poor procedures.
3. **Lack of Training**: Moderately likely, especially if regular security training and updates are not provided.

Part 2.d: What control are you putting in place?

1. **Insider Threats**: Conduct background checks and enforce strict role-based access control (RBAC) to limit employee access to only necessary data.
2. **Human Error**: Implement strong user access controls and an automated backup system to recover lost data.
3. **Lack of Training**: Regular, mandatory training sessions on security best practices, data protection, and system usage.

Part 2.e: What is the residual risk after the control you put in place?

1. **Insider Threats**: There is still a small residual risk, as an insider could still bypass some controls, but regular audits can further reduce this risk.
2. **Human Error**: The risk is reduced but not eliminated, as mistakes can still happen even with the best controls.
3. **Lack of Training**: Training minimizes the likelihood of issues, but not every employee may follow practices perfectly, especially new hires.

Part 2.f: Where does this risk overlap with the other types of controls (operational and technical)?

- **Insider Threats**: Overlaps with technical controls, such as logging and monitoring, to detect suspicious activity.
- **Human Error**: Overlaps with operational controls like incident response and recovery plans to manage mistakes.
- **Lack of Training**: Overlaps with both operational and technical controls. Training includes technical aspects (like secure use of software), while operationally, it aligns with the procedures staff must follow.

Part 3: Technical Controls (30%)

Part 3.a: What risks are specific to your technical controls?

1. **Software Vulnerabilities**: Bugs in the system can be exploited by attackers.
2. **Weak Authentication**: Lack of strong authentication methods makes it easier for unauthorized users to access the system.
3. **Unpatched Systems**: Not applying security patches on time exposes the system to known vulnerabilities.

Part 3.b: What is the impact of this risk?

1. **Software Vulnerabilities**: Exploits can lead to data breaches, downtime, or ransomware attacks.
2. **Weak Authentication**: Unauthorized access could result in stolen data, altered configurations, or system manipulation.
3. **Unpatched Systems**: Hackers can easily exploit outdated software, leading to major security incidents.

Part 3.c: How likely is this risk?

1. **Software Vulnerabilities**: Likely, as no system is free from bugs.
2. **Weak Authentication**: Moderately likely without strong security practices like MFA.
3. **Unpatched Systems**: Likely if patch management is not a priority.

Part 3.d: What control are you putting in place?

1. **Software Vulnerabilities**: Perform regular security testing and issue updates.
2. **Weak Authentication**: Implement multi-factor authentication (MFA) for all users.
3. **Unpatched Systems**: Create a patch management policy that ensures timely updates.

Part 3.e: What is the residual risk after the control you put in place?

1. **Software Vulnerabilities**: Even with testing, unknown vulnerabilities (zero-days) can still be exploited.
2. **Weak Authentication**: Residual risk remains if MFA or other mechanisms are bypassed.
3. **Unpatched Systems**: Residual risk is low if patches are applied, but there's always a chance that new vulnerabilities emerge.

Part 3.f: Where does this risk overlap with operational and personnel controls?

- **Software Vulnerabilities**: Overlaps with operational controls, such as incident response, to manage exploitation of vulnerabilities.
- **Weak Authentication**: Relates to personnel controls, as employees must understand and use MFA correctly.
- **Unpatched Systems**: Involves operational controls, such as creating a patch management process to ensure updates happen on time.

Part 4: Operational Controls (30%)

Part 4.a: What risks are specific to your operational controls?

1. **Poor Incident Response**: Not having a solid plan in place can slow down recovery.
2. **Change Management Failures**: Uncontrolled changes can introduce system vulnerabilities or cause system breakdowns.
3. **Inadequate Backup Procedures**: Failure to back up data regularly can result in data loss during an incident.

Part 4.b: What is the impact of this risk?

1. **Poor Incident Response**: Delayed response times can worsen the impact of security incidents, increasing downtime and data loss.
2. **Change Management Failures**: Improper changes can break the system or introduce security vulnerabilities.
3. **Inadequate Backup Procedures**: Data loss can lead to severe operational disruptions and financial losses.

Part 4.c: How likely is this risk?

1. **Poor Incident Response**: Likely if there is no formal response plan.
2. **Change Management Failures**: Moderately likely if changes are not properly reviewed and tested.
3. **Inadequate Backup Procedures**: Likely if no routine backup schedule is enforced.

Part 4.d: What control are you putting in place?

1. **Poor Incident Response**: Implement a clear, documented incident response plan.
2. **Change Management Failures**: Use a formal change management process, including approval and testing steps.
3. **Inadequate Backup Procedures**: Schedule automatic, regular backups and test recovery plans frequently.

Part 4.e: What is the residual risk after the control you put in place?

1. **Poor Incident Response**: Residual risk remains if the incident plan is not properly followed or updated.
2. **Change Management Failures**: Some risk remains if unauthorized or emergency changes bypass the usual process.
3. **Inadequate Backup Procedures**: Even with backups, there's a small chance of losing very recent data or facing storage issues.

Part 4.f: Where does this risk overlap with technical and personnel controls?

- **Poor Incident Response**: Overlaps with personnel, as trained employees must know how to handle incidents properly.
- **Change Management Failures**: Involves technical controls, as changes may involve system configurations or software updates.
- **Inadequate Backup Procedures**: Tied to both technical controls (automated backups) and personnel (those responsible for monitoring backups).