

CPT 6216

TRIMESTER 3, 2024 INDUSTRIAL TRAINING REPORT

**AMD GLOBAL SERVICES (M) SDN BHD**

**BY**

**1201200722**

**NUR AYU AMIRA BINTI IDRIS BACHELOR OF COMPUTER SCIENCE HONS.**

**CYBERSECURITY**

**Table of Contents**

[Company Background 4](#_bookmark0)

[Objectives of the Internship 5](#_bookmark1)

[Overview of Roles and Responsibilities 6](#_bookmark2)

1. [Role Overview: 6](#_bookmark3)
2. [Key Responsibilities: 6](#_bookmark4)
3. [Tools/Framework Used: 7](#_bookmark5)

[Tasks and Methods: Supplier Self-Assessment Questionnaire and Monitoring 8](#_bookmark6)

[Tasks and Methods: Cyber Hygiene Risk Score Monitoring for Suppliers 10](#_bookmark7)

[Achievement of the Tasks 12](#_bookmark8)

[Problems Encountered & Way to Improve 13](#_bookmark9)

[Skills Developed & Other Knowledge Gained 14](#_bookmark10)

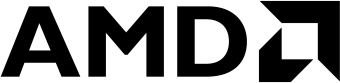
[Conclusion 16](#_bookmark11)

[References 17](#_bookmark12)

[Appendices 18](#_bookmark13)

1. [Reporting Form 18](#_bookmark14)
2. [Meeting Log – Week 1 19](#_bookmark15)
3. [Meeting Log – Week 2 21](#_bookmark16)
4. [Meeting Log – Week 3 24](#_bookmark17)
5. [Meeting Log – Week 4 26](#_bookmark18)
6. [Meeting Log – Week 5 28](#_bookmark19)
7. [Meeting Log – Week 6 30](#_bookmark20)
8. [Meeting Log – Week 7 32](#_bookmark21)
9. [Meeting Log – Week 8 34](#_bookmark22)
10. [Meeting Log – Week 9 36](#_bookmark23)
11. [Meeting Log – Week 10 38](#_bookmark24)
12. [Meeting Log – Week 11 40](#_bookmark25)
13. [Meeting Log – Week 12 42](#_bookmark26)
14. [Meeting Log – Week 13 43](#_bookmark27)

# Company Background



Advanced Micro Devices (AMD) is a global leader in the design and production of innovative semiconductor devices. The company was founded in 1969 and is headquartered in Santa Clara, California.

AMD operates globally, and one of its key branches is in Cyberjaya, known as the AMD Global Services Centre. This branch focuses on providing various services to support AMD's global operations. Through these services, AMD ensures that its internal and external stakeholders benefit from efficient operational practices.

The company's core products include microprocessors (CPUs), graphics processing units (GPUs), and system-on-chip (SoC) solutions. These products are used in many major areas, such as personal computers, gaming consoles, data centers, and enterprise systems. AMD's innovations continue to push the limits of high-performance computing, enabling enhanced gaming, professional workstations, and server capabilities.

The company follows a clear vision: "High performance and adaptive computing is transforming our lives." This reflects AMD’s commitment to improving computing power that have tangible impacts on industries and daily lives around the world. AMD’s mission, which supports this vision, is to "Build great products that accelerate next-generation computing experiences."

As of today, AMD is still a strong competitor in the semiconductor industry. AMD continues to expand its impact in areas such as personal computing, gaming, data centers, and artificial intelligence (AI). The nature of AMD's business is firmly rooted in technological innovation, with a focus on producing hardware that enhances computational capabilities across diverse platforms.

# Objectives of the Internship

The objective of this internship is:

* 1. To gain real-world experience by working in a professional environment and becoming familiar with organizational structures, business operations, and administrative tasks.
  2. To apply and reinforce the knowledge gained in university through hands-on experience in relevant fields.
  3. To learn and work with new technologies while also improving important soft skills such as communication, teamwork, and problem-solving.
  4. To foster collaboration between the industry and academic knowledge, promoting a deeper understanding of practical work.
  5. To develop the necessary skills, knowledge, and abilities required for a successful career, enhancing employability and readiness for the workforce.

# Overview of Roles and Responsibilities

## Role Overview:

In my role within the Third-Party Cyber Risk Management team at AMD, I am responsible for conducting cyber risk assessments on third-party suppliers, particularly focusing on Level 1 suppliers. These suppliers are identified by both direct and indirect procurement teams as having access to sensitive organizational data and systems. The primary objective of these assessments is to evaluate and monitor the information security risks these suppliers may pose to our organization's operational stability and reputation. This helps mitigate potential threats, such as cyberattacks, data breaches, or other security incidents that could lead to significant business disruptions or damage to AMD’s reputation.

## Key Responsibilities:

* **Supplier Self-Assessment Questionnaires (SAQs):**

I manage the collection, and continuous monitoring of supplier self-assessment questionnaires. These questionnaires provide insights into each supplier's security posture by evaluating their compliance with industry standards and their ability to mitigate potential vulnerabilities. The information gathered is used to assess whether the suppliers meet the necessary security standards required to work with AMD.

* **Cyber Hygiene Risk Score Monitoring:**

I am also responsible for continuously monitoring the suppliers' Cyber Hygiene Risk Scores, which provide an overview of the suppliers' security health. This monitoring ensures that suppliers maintain security levels aligned with AMD’s standards.

## Tools/Framework Used:

In my role, I utilize several key tools and frameworks that enable effective third-party cyber risk management:

1. **UpGuard:**

UpGuard is a cybersecurity platform that assists in assessing and monitoring the security posture of third-party suppliers. It offers detailed insights into potential vulnerabilities and provides security ratings that help identify suppliers with critical levels of risk. UpGuard facilitates a self-assessment process, allowing suppliers to evaluate their own cybersecurity standing according to their specific risk profile.

1. **NIST Cybersecurity Framework 2.0:**

The National Institute of Standards and Technology (NIST) Cybersecurity Framework

2.0 is a set of updated guidelines designed to help organizations, manage and reduce cybersecurity risks. This version of the framework continues to provide a flexible, risk- based approach for identifying, protecting, detecting, responding to, and recovering from cybersecurity threats. By applying NIST 2.0, I ensure that our suppliers adhere to industry security standards, strengthening AMD’s ability to protect its systems and data.

1. **Resilinc:**

Resilinc is a platform that helps in supply chain risk management. It plays a vital role in identifying potential disruptions in the supply chain and managing risks related to third- party suppliers. This tool is essential for understanding supplier risk across different tiers and ensuring continuous operation through risk mitigation strategies.

1. **Microsoft Office (Excel):**

Microsoft Excel is a key tool in managing and tracking the self-assessment questionnaires and cyber hygiene risk scores of suppliers. I use Excel to maintain detailed records of the collected data, and track progress over time. Excel allows me to efficiently organize the vast amount of data generated by our assessments and monitoring processes, ensuring that the right information is available to drive supplier security improvements.

# Tasks and Methods: Supplier Self-Assessment Questionnaire and Monitoring

In this section, we will discuss the detailed process of managing supplier self-assessment questionnaires and their monitoring, which is based on NIST Cybersecurity Framework (CSF) 2.0. This cybersecurity self-assessment consists of 107 questions, and it is designed to evaluate the cybersecurity posture of third-party suppliers, helping to mitigate potential risks to AMD.

1. **Managing Questionnaire Scores and Tracker Updates:**

My first task involves managing the scores from supplier self-assessment questionnaires using UpGuard. Once I joined the team, the questionnaires had already been distributed to suppliers. I track and update the scores in our internal tracker to ensure that all self-assessments are properly recorded. After receiving a completed self-assessment, I also download the responses and save them in SharePoint. For suppliers classified as medium to highest risk, I make sure that supporting documents are collected and saved as evidence to verify their self-assessment responses.

1. **Sending Email Reminders for Completion:**

To keep suppliers on schedule, I send email reminders at different phases of the self- assessment process. These reminders are phase-based and include first, second, final, and overdue notifications, depending on each supplier's progress in UpGuard. This helps ensure that suppliers meet their submission deadlines and remain engaged in the risk assessment process.

1. **Responding to Suppliers and Managing Invitations:**

I address any raised issues, such as portal access problems, and manage communications with suppliers. Depending on the supplier's risk level, I extend invitations for further steps in the assessment process, if required. This ensures that all issues are resolved efficiently, and that the assessment process continues smoothly.

1. **Reviewing Responses for Low-Risk Suppliers:**

For low-risk suppliers, I conduct a review of their responses by verifying their compliance with global information security standards, such as ISO 27001. Once I review the completed self- assessment, I summarize the risk level and the results. If necessary, I initiate follow-up actions, such as requesting improvement plans or evidence for further validation.

1. **Ongoing Reviews for Medium and High-Risk Suppliers:**

For medium to high-risk suppliers, I conduct continuous reviews, ensuring that their security practices align with required standards. I refer to Cybersecurity Audit NIST Framework

* 1. as a guideline to ensure these suppliers adhere to industry-standard security measures. After reviewing the responses, I conduct a review session with my supervisor to thoroughly evaluate the self-assessment. If necessary, I follow up with the supplier by requesting additional artifacts or evidence to support their responses. This ongoing review process allows us to closely monitor and ensure that suppliers maintain the necessary cybersecurity posture.

# Tasks and Methods: Cyber Hygiene Risk Score Monitoring for Suppliers

In this section, we will discuss the detailed process of Cyber Hygiene Risk Score Monitoring for Suppliers, which is conducted using UpGuard and follows industry best practices. This monitoring is essential for evaluating and maintaining the cybersecurity posture of third-party suppliers, helping to mitigate potential risks to AMD.

* + 1. **Monitoring Supplier Risk Scores in UpGuard:**

I am responsible for monitoring supplier risk scores using UpGuard. During the first week of each month, I update these scores in the Master file and generate a vendor risk report for each active supplier. These reports are saved in SharePoint for future reference and further review.

* + 1. **Sending Resilinc Scores to AMD Contacts:**

On a monthly basis, I send the Resilinc scores to the designated AMD contact, focusing specifically on the Direct Procurement Portfolio. In this process, I manage the data preparation and validation to ensure the accuracy of the scores before sharing them.

* + 1. **Performing External Scans and Risk Reporting:**

Part of my role involves conducting external scans using UpGuard and sharing the vendor risk report with active suppliers. If the scan identifies any risks, I request an improvement plan based on the severity of the identified risks. This task is performed as part of our quarterly communication process with both AMD and the suppliers to ensure that security risks are effectively managed.

* + 1. **Providing Cybersecurity Updates to Lead Source Managers (LSMs):**

I regularly provide cybersecurity updates to AMD contacts, also known as Lead Source Managers (LSMs). These updates include supplier risk scores and details about their participation in self-assessment programs. This communication forms part of our quarterly reporting process from the Third-Party Risk Management (TPRM) team to the LSM, ensuring that AMD leadership remains informed of supplier risks.

* + 1. **Following Up on Improvement Plans:**

Finally, I follow up on the improvement plans requested from vendors. This involves tracking identified risks and ensuring that suppliers establish a timeline for addressing these issues. I monitor their progress and, once the risks are resolved, cross-check the vendor’s report and UpGuard to verify that the issues have been fully addressed.

# Achievement of the Tasks

In this section, we will discuss the various tasks I completed and how their implementation contributed to achieving the goals of my internship. These tasks helped me build essential skills and gain practical experience in cybersecurity and supplier risk management.

1. **Completion of Tasks:**

All tasks were completed within the given period, except for ongoing review responses, which require continuous follow-up and monitoring.

1. **Improved Confidence in Communication:**

Through regular interactions with suppliers, I improved my confidence in managing communications, leading to more effective engagement with suppliers and ensuring timely responses.

1. **Gained Knowledge in Risk Monitoring:**

I gained valuable knowledge in risk monitoring, particularly in understanding detailed risks, their potential impact on AMD, and the strategies for recommending and implementing remediation.

1. **Deeper Understanding of Review Responses and Policies:**

I developed a deeper understanding of how to conduct review responses for cybersecurity self-assessments. I also familiarized myself with relevant policies and standards like ISO 27001, Business Continuity Plans, etc. to ensure compliance in risk assessments.

1. **Application of Cybersecurity Frameworks:**

I gained a comprehensive understanding of cybersecurity frameworks, such as NIST Cybersecurity Framework 2.0, and applied the fundamental knowledge learned in university to real-world tasks. At AMD, I had hands-on experience in reviewing responses, identifying risks in systems, etc.

# Problems Encountered & Way to Improve

In this section, we will discuss the challenges I faced during my internship and the improvements I made to overcome them. These experiences helped me grow both professionally and personally, enhancing my ability to manage key tasks more efficiently.

1. **Writing Formal Business Emails**
   * **Problem:** Initially, I struggled with writing formal business emails due to a lack of experience.
   * **Improvement:** To overcome this, I consistently reread my emails before sending them and asked for feedback from my supervisor. Over time, I improved my writing skills and became more confident in crafting proper formal emails that effectively communicate valuable information.
2. **Conducting Review Responses:**
   * **Problem:** While conducting my first review responses for medium-risk suppliers, I faced some confusion with specific questions and struggled to fully understand the process.
   * **Improvement:** After completing the initial review response, I had several review sessions with my supervisor. My supervisor guided me through the process, helping me understand how to conduct review responses effectively. I also referred to the NIST Cybersecurity Framework 2.0 as a reference, which made these process clearer and more structured.

# Skills Developed & Other Knowledge Gained

In this section, we will discuss the various skills and knowledge I developed throughout my internship. These experiences have contributed to both my professional growth and my ability to manage key responsibilities effectively.

1. **Time Management:**

Successfully managed tasks within deadlines, ensuring that all projects and assessments were completed efficiently.

1. **Business Communication:**

Improved formal email writing skills, allowing for professional correspondence with suppliers and internal stakeholders. Developed confidence in communicating clearly and effectively.

1. **Cyber Risk Assessment:**

Gained a solid understanding of conducting review responses using frameworks such as NIST Cybersecurity Framework 2.0, helping to assess and mitigate risks associated with third- party suppliers.

1. **Vendor Risk Monitoring:**

Acquired hands-on experience in monitoring cyber hygiene scores using tools like UpGuard. Participated in monthly training sessions and catch-ups with the UpGuard team to stay updated on monitoring best practices and features.

1. **Data Management:**

Became proficient in tracking supplier progress, updating supplier and AMD contact details, and managing risk data. Developed skills in analyzing and organizing data for risk assessment processes.

1. **Employee Engagement:**

Participated in events such as Merdeka Day, Happy Diwali Day and AMD Q3 Townhall, which provided valuable opportunities to build connections, engage with peers, and improve networking skills.

1. **Continuous Learning:**

Enrolled in LinkedIn Learning courses provided by AMD and participated in AMD's security awareness training. These courses helped enhance knowledge and skills in cybersecurity and communication.

1. **Other Knowledge:**

Expanded knowledge on the fundamentals of cybersecurity, cloud security, and regulations such as GDPR, PDPA, and IT audits. Through my internship at AMD, I gained hands-on experience in applying these concepts in real-world scenarios, improving my understanding of security best practices.

# Conclusion

Overall, my internship at AMD has been a highly valuable and rewarding experience. I am grateful for the opportunity to be selected as an intern, where I had the chance to apply my academic knowledge in real-world settings and gain practical experience in the field of cybersecurity. Throughout this journey, I have developed critical skills in areas such as risk management, vendor monitoring, and data analysis, which have significantly broadened my understanding of the cybersecurity landscape.

I would like to express my sincere thanks to my supervisor for her guidance and support. Their mentorship not only helped me successfully complete my assigned tasks but also encouraged me to grow professionally, pushing me to continually improve and build confidence in my abilities. The feedback I received has been important in shaping my skills and approach to handling complex responsibilities. I would also like to extend my gratitude to my lecturer for taking the time to visit and support me during my internship.

As a cybersecurity student, this hands-on experience has greatly enhanced my knowledge and equipped me with practical skills that I will carry forward into my future career. The exposure to industry-standard tools and frameworks has provided me with a solid foundation, and I am excited to apply what I have learned in my future career.

# References

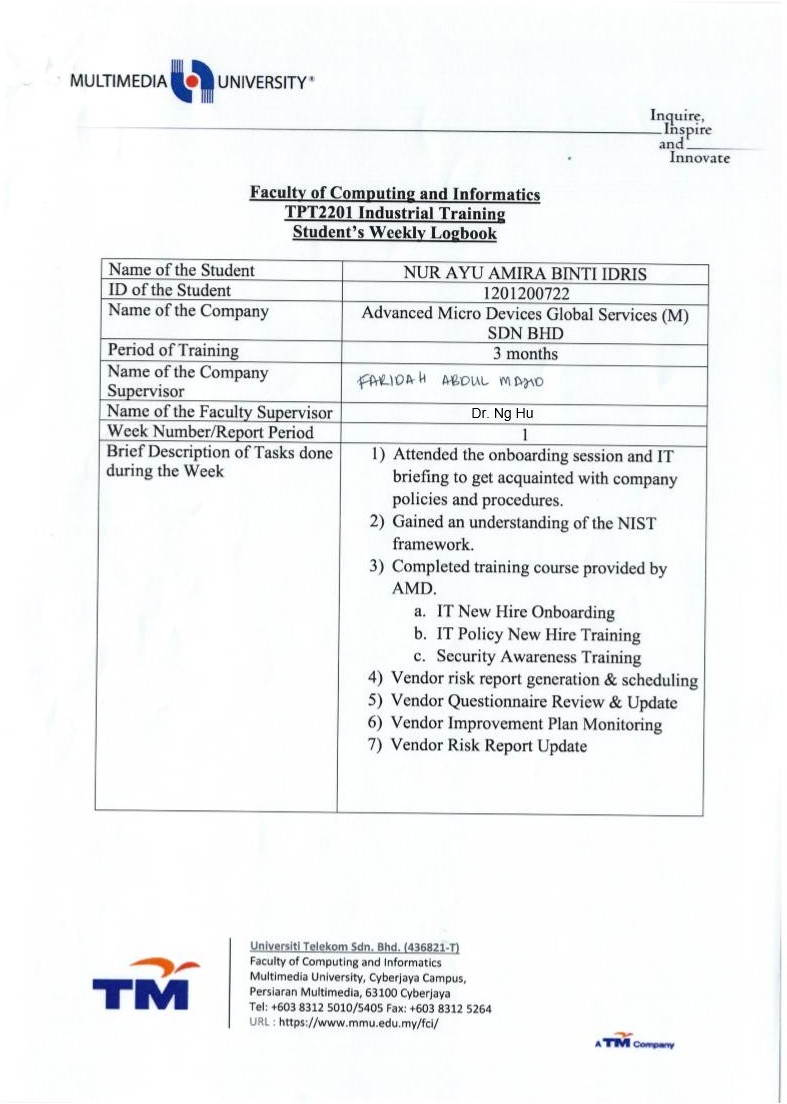
1. *Cybersecurity Framework | NIST*. (2024, October 15). NIST. https:/[/www.nist.gov/cyb](http://www.nist.gov/cyberframework)e[rframework](http://www.nist.gov/cyberframework)
2. *Third-Party risk and attack surface management Software | UpGuard*. (n.d.). https:/[/www.upguard.c](http://www.upguard.com/)o[m/](http://www.upguard.com/)
3. Resilinc Solutions Pvt Ltd. (2024, October 11). *Supplier & Supply chain Risk Management - Supply chain Management | Resilinc*. Resilinc. https:/[/www.resilinc.com/](http://www.resilinc.com/)
4. Kosutic, D. (n.d.). *Mandatory ISO 27001 documents 2022 revision | Get the full list*. 27001Academy. https://advisera.com/27001academy/knowledgebase/list-of-mandatory- documents-required-by-iso-27001-revision/
5. Woerner, R. (2020, October 1). *Reducing risks using the NIST Risk Management Framework - Implementing the NIST Risk Management Framework (2020)* [Video]. LinkedIn. https:/[/www.linkedin.com/l](http://www.linkedin.com/learning/implementing-the-nist-risk-management-)e[arning/implementing-the-nist-risk-management-](http://www.linkedin.com/learning/implementing-the-nist-risk-management-) framework-2020/reducing-risks-using-the-nist-risk-management-framework?u=2140730
6. Lovelace, D. (2019, August 5). *Email: An extension of your brand - Tips for Writing Business Emails* [Video]. LinkedIn. https:/[/www.linkedin.com/l](http://www.linkedin.com/learning/tips-for-writing-)e[arning/tips-for-writing-](http://www.linkedin.com/learning/tips-for-writing-) business-emails/email-an-extension-of-your-brand?u=2140730

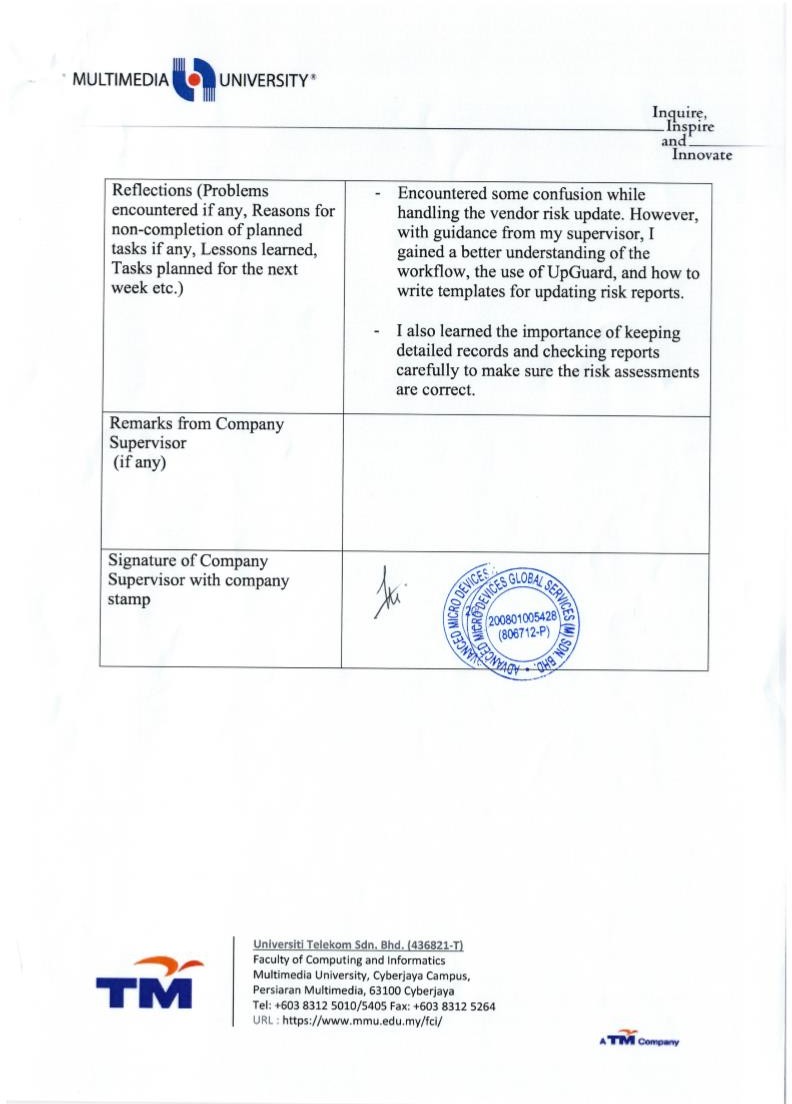
# Appendices

## Reporting Form

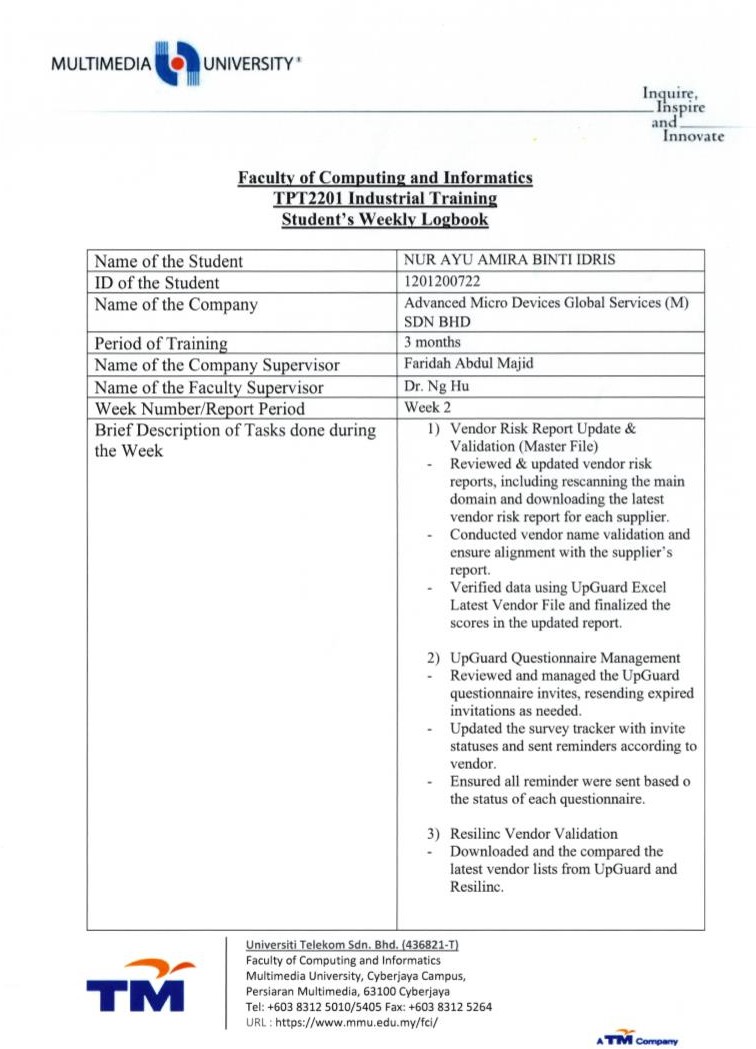


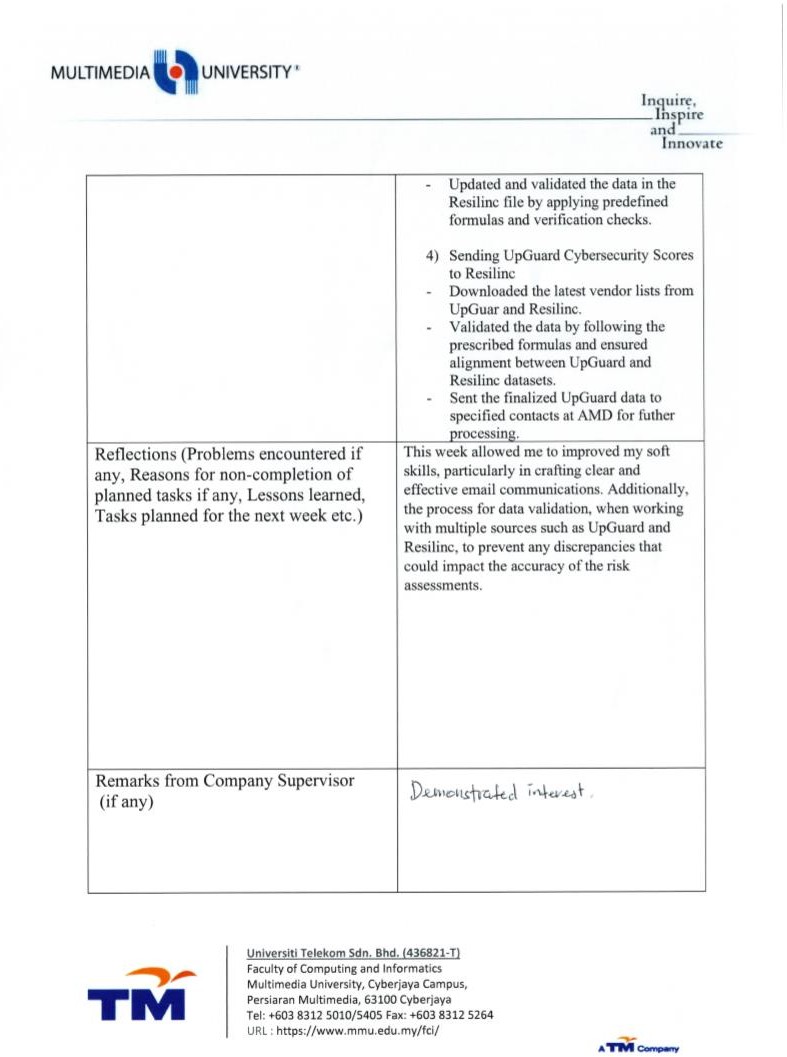
## Meeting Log – Week 1

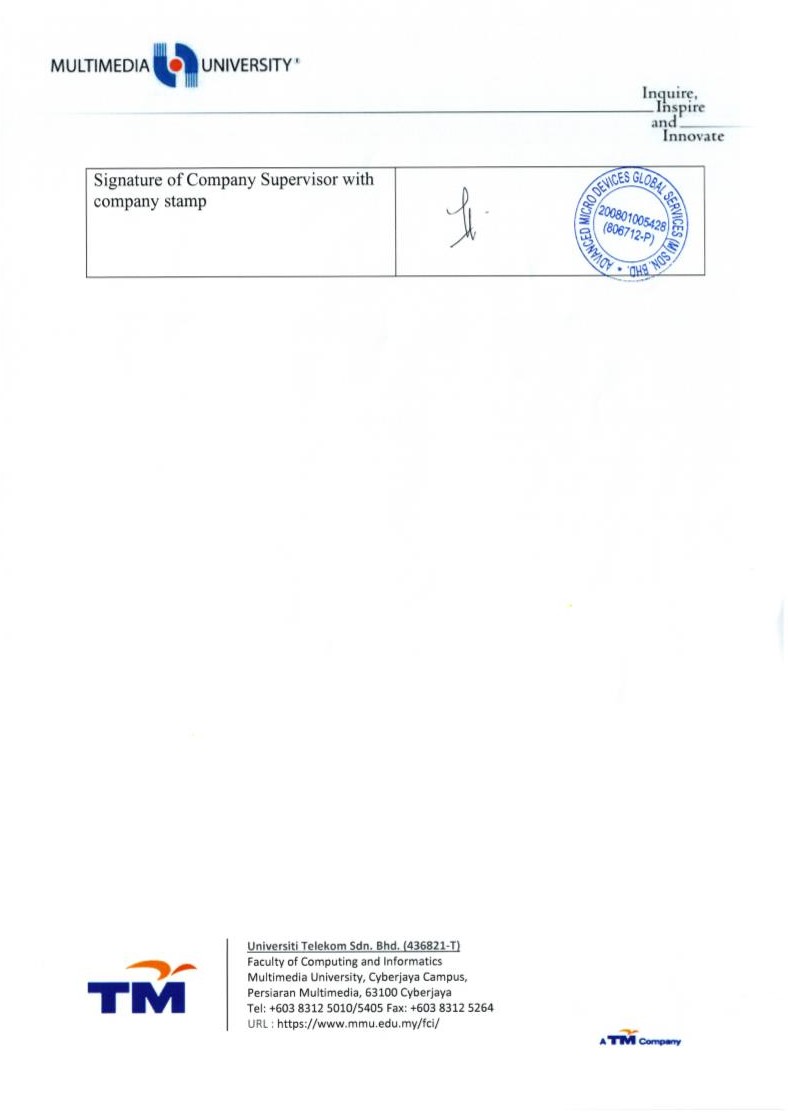




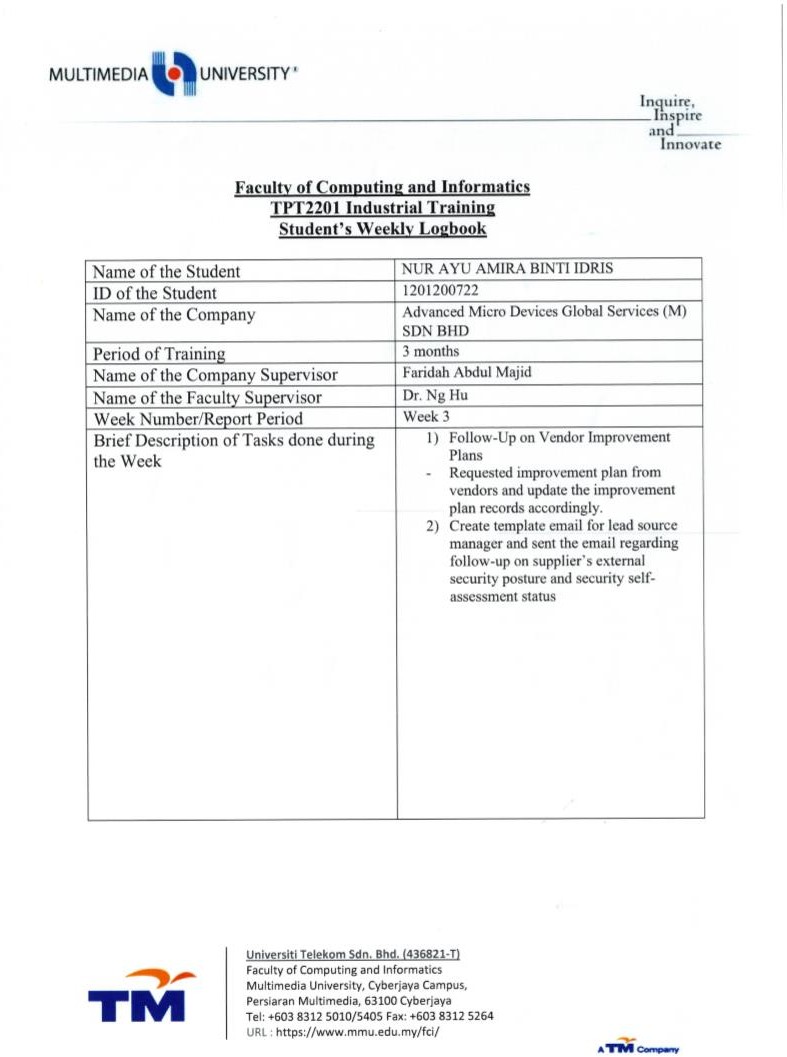
## Meeting Log – Week 2

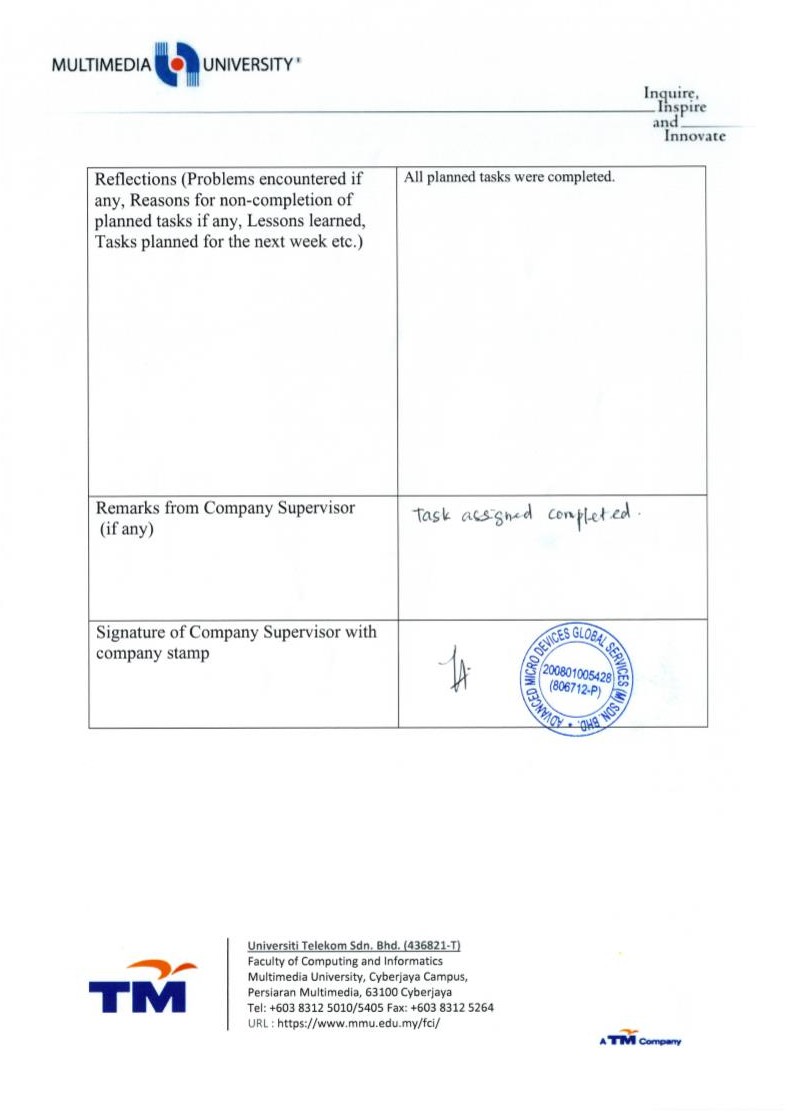




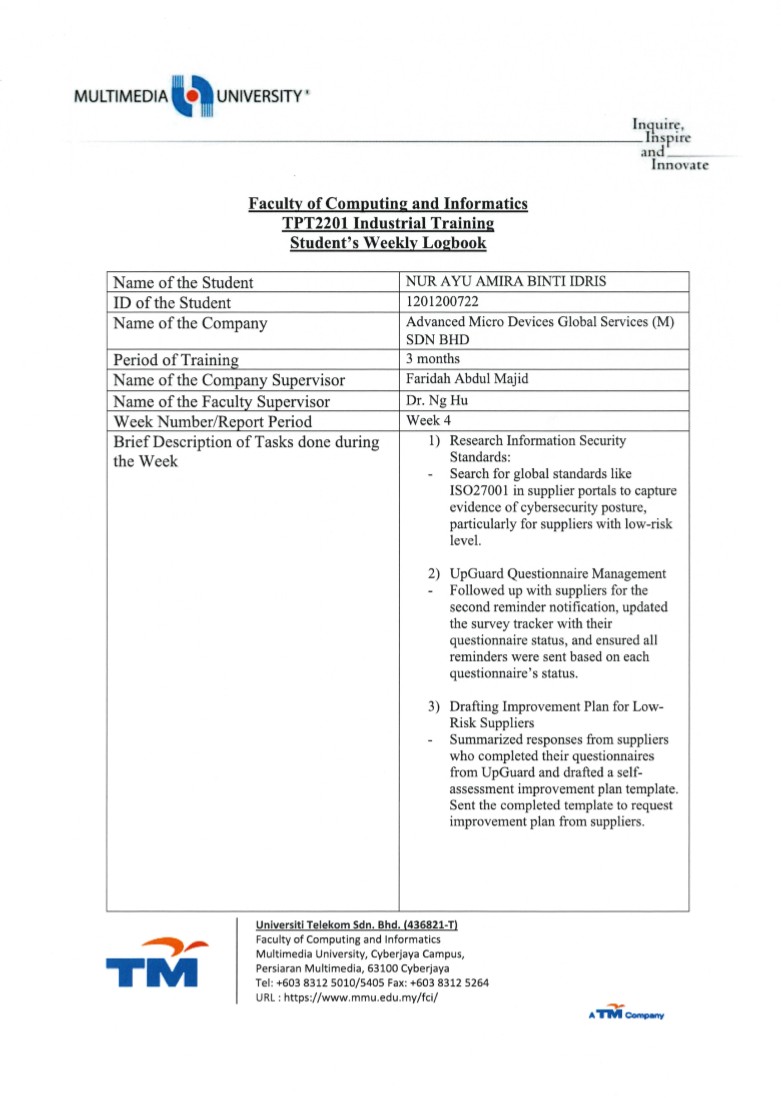


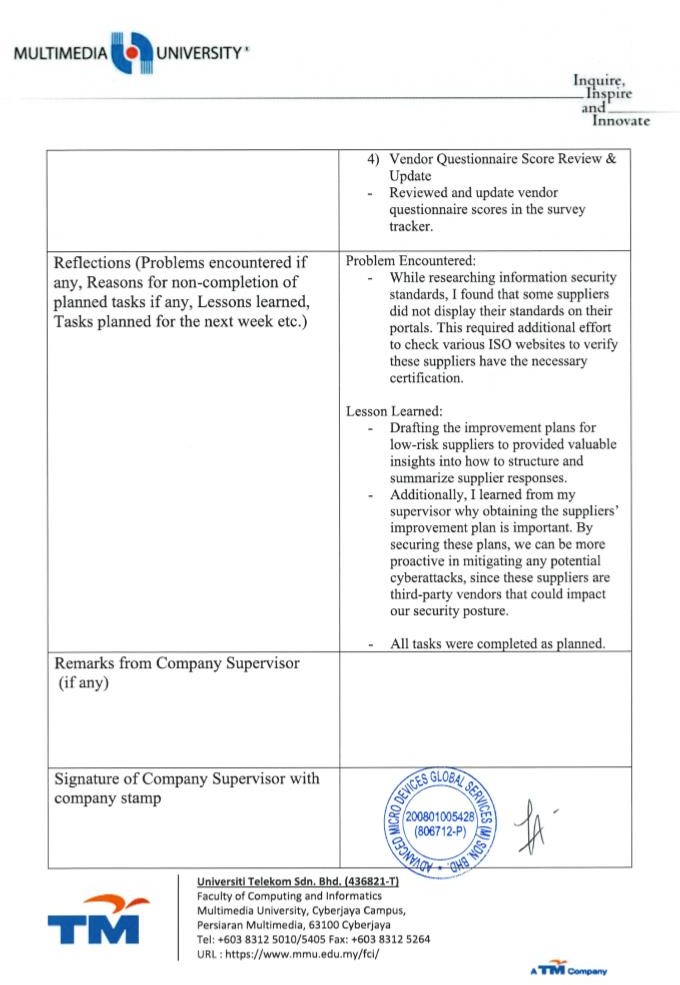
## Meeting Log – Week 3



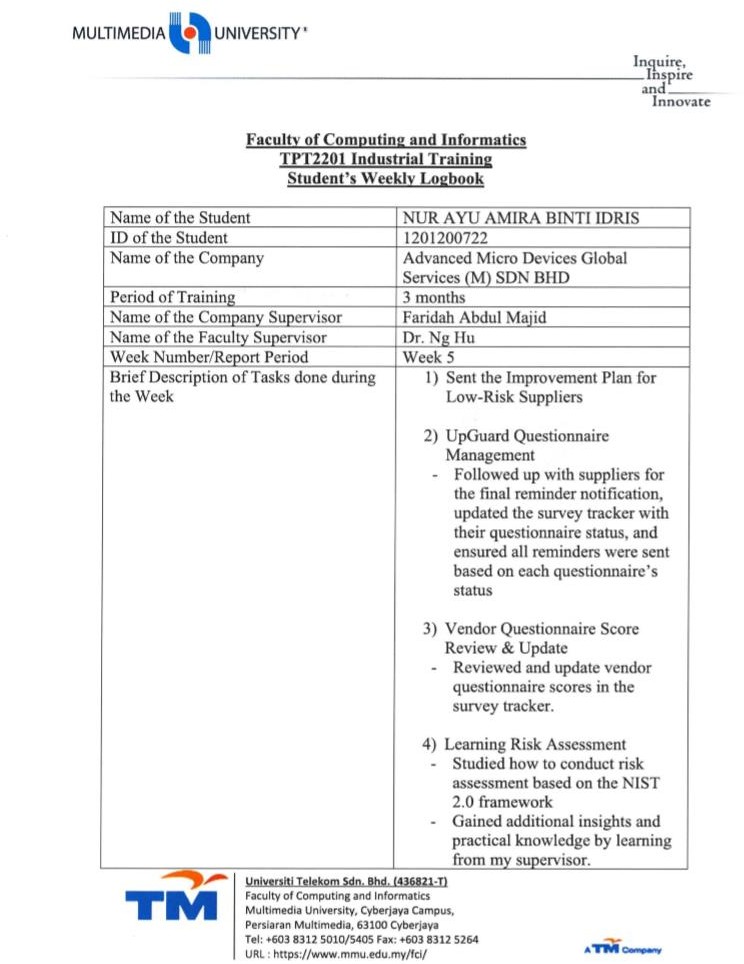


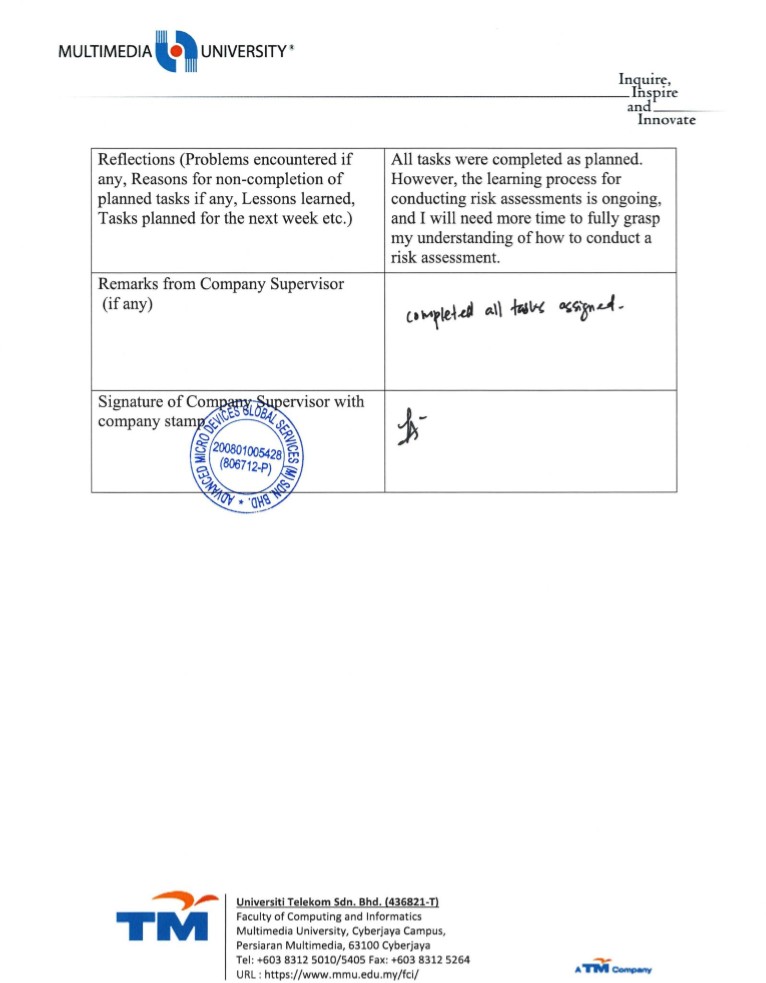
## Meeting Log – Week 4



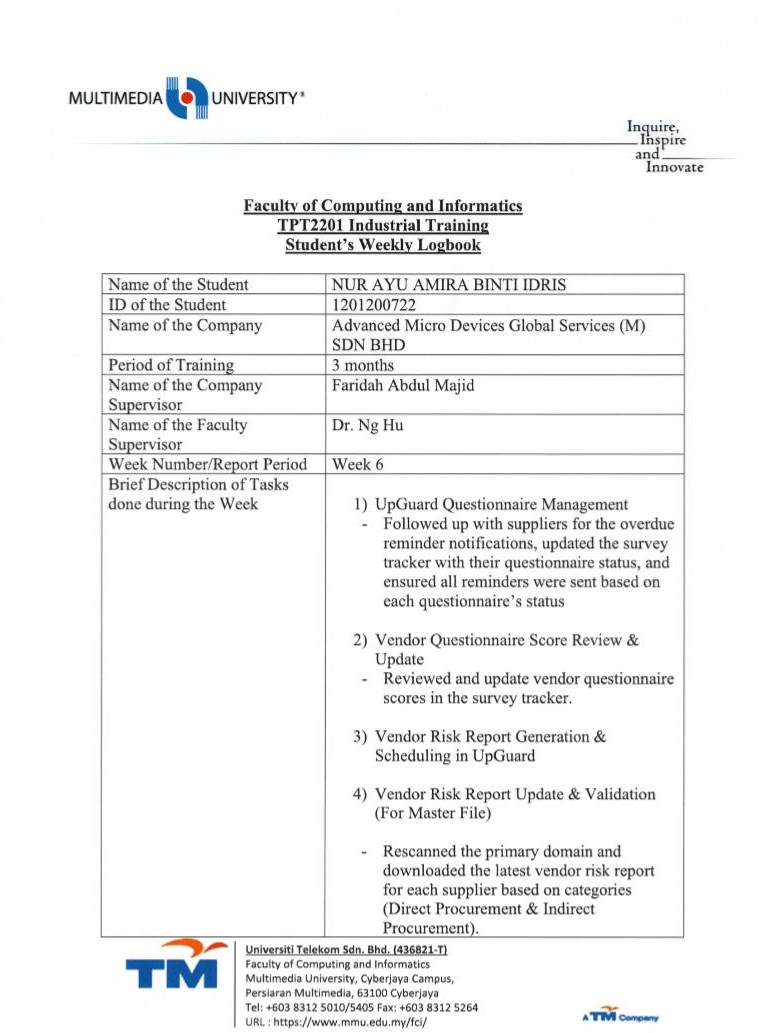


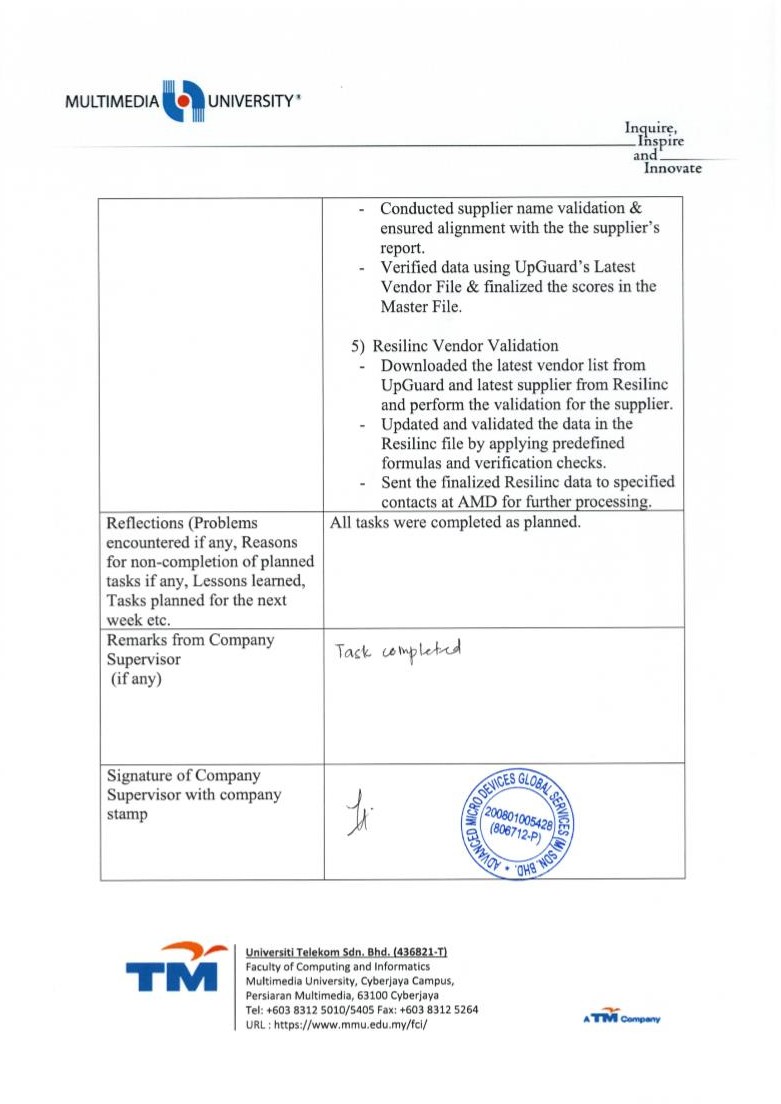
## Meeting Log – Week 5



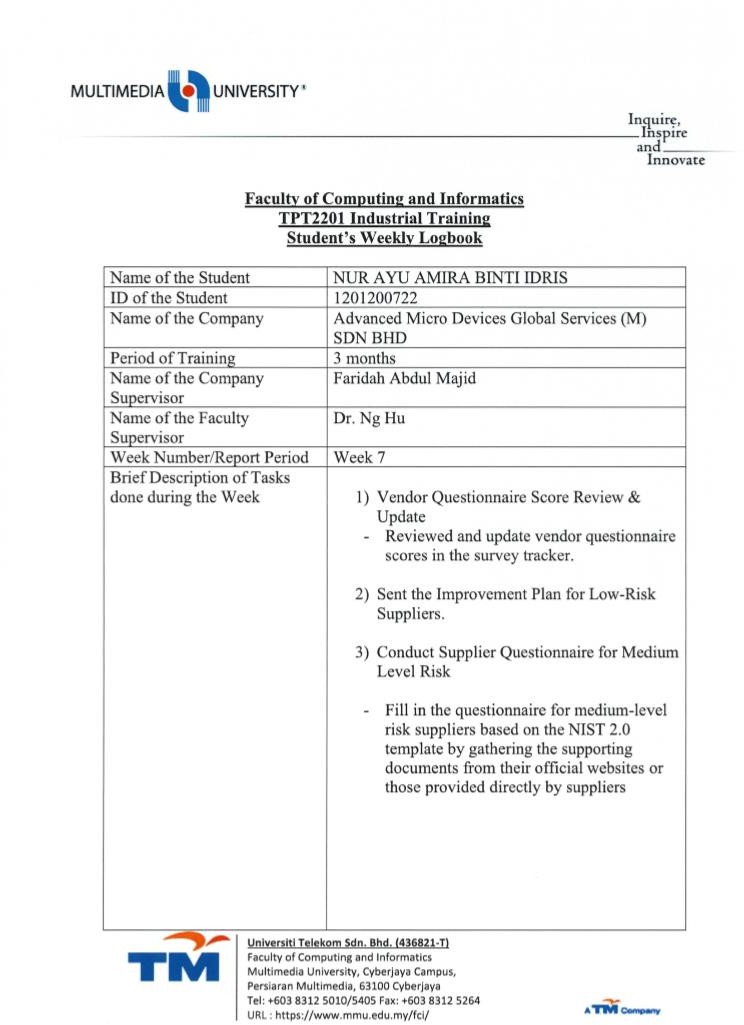


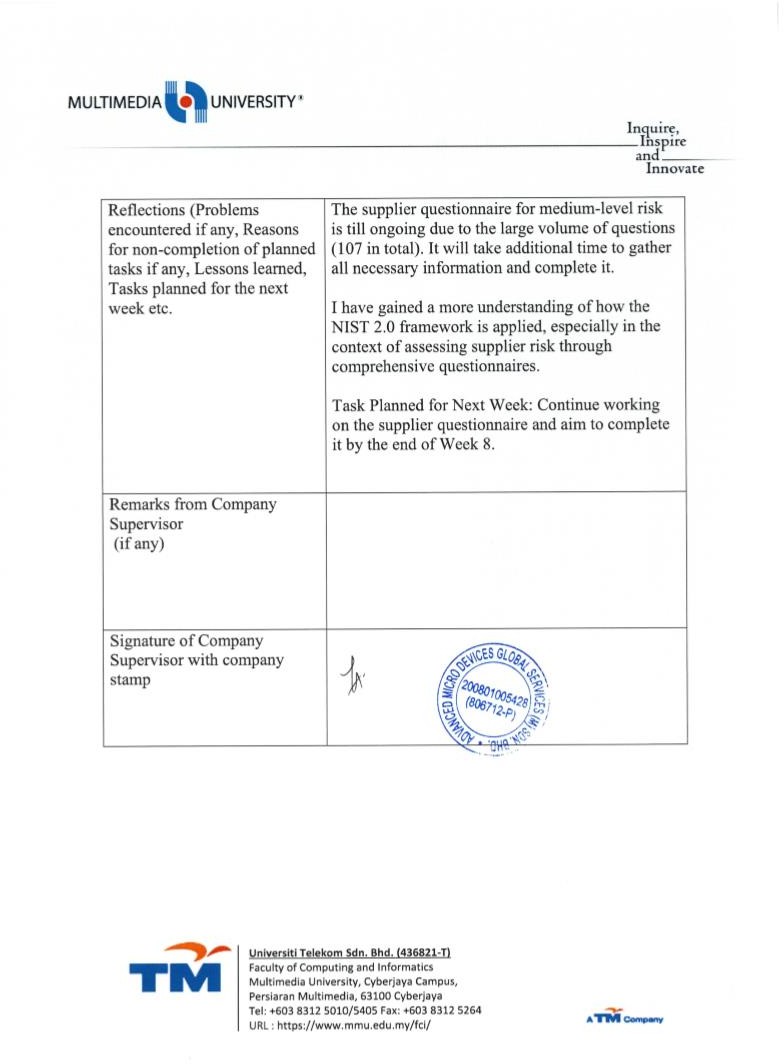
## Meeting Log – Week 6



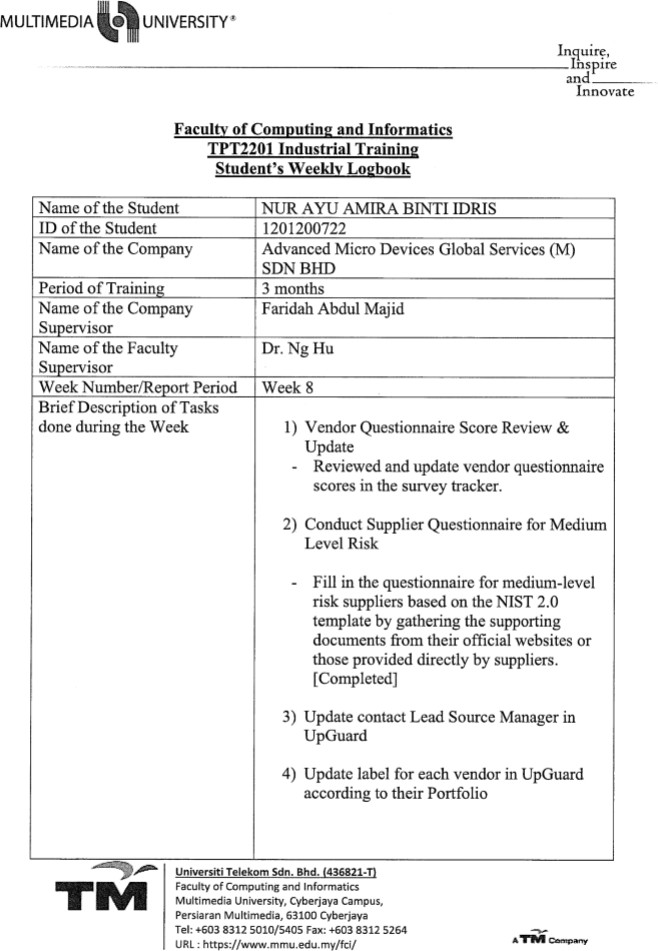


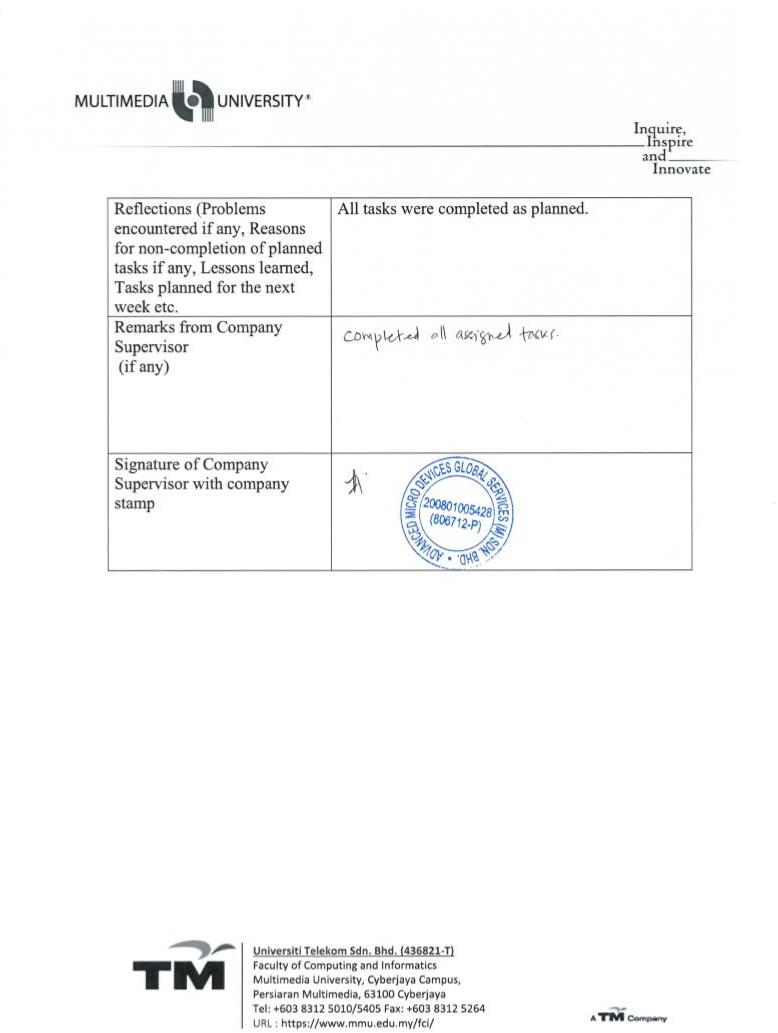
## Meeting Log – Week 7



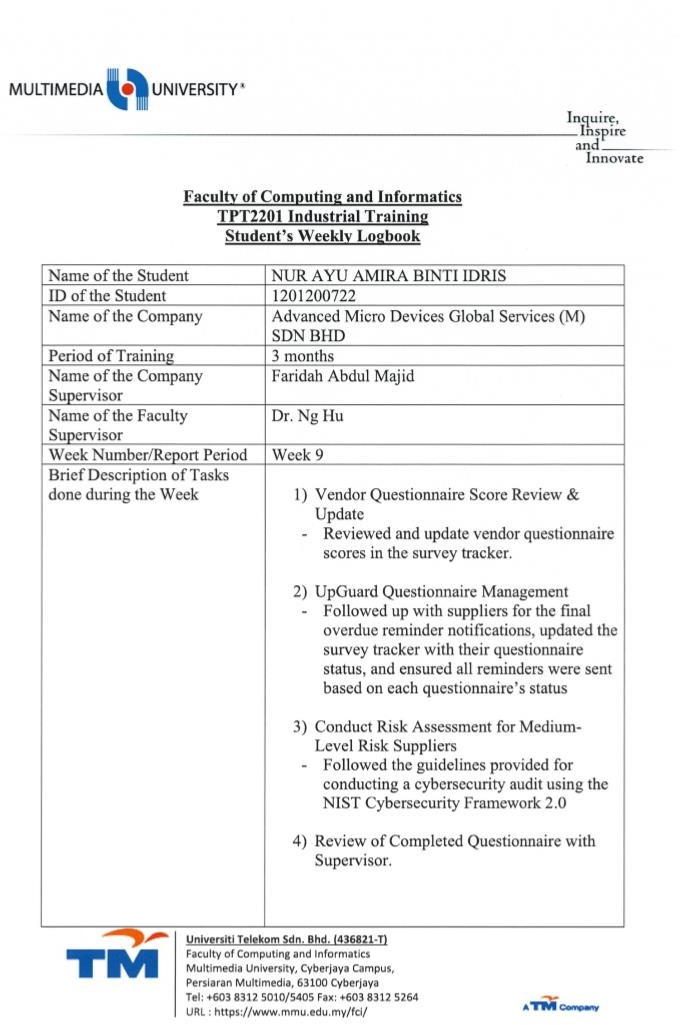


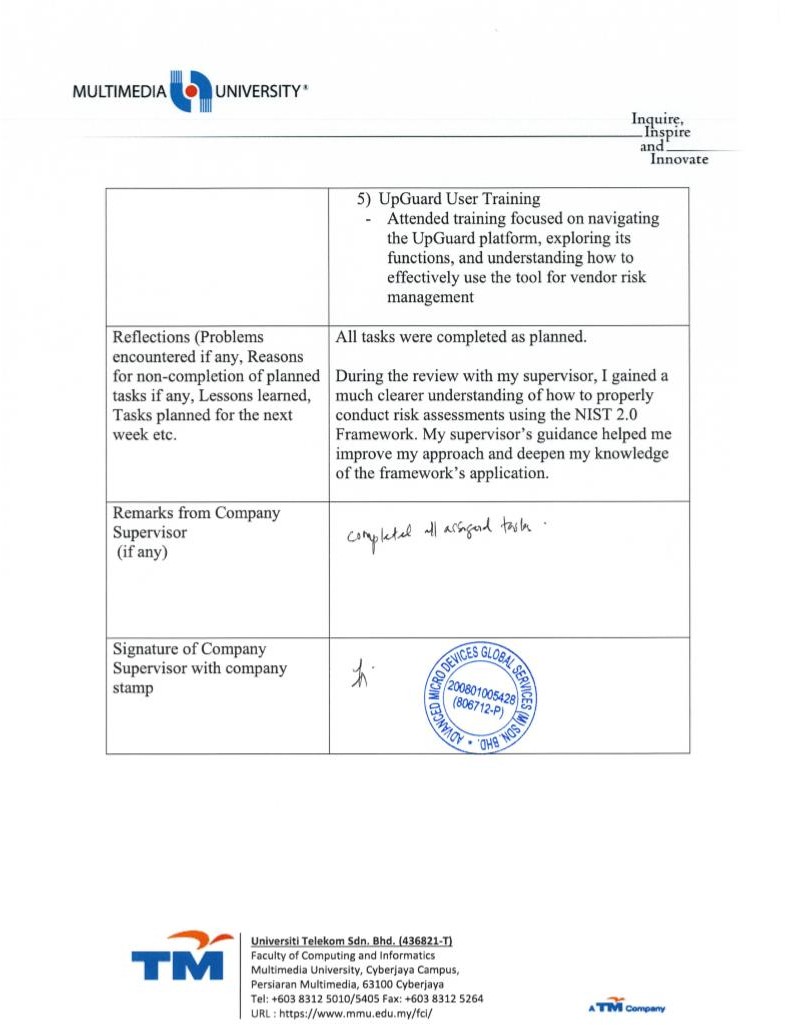
## Meeting Log – Week 8



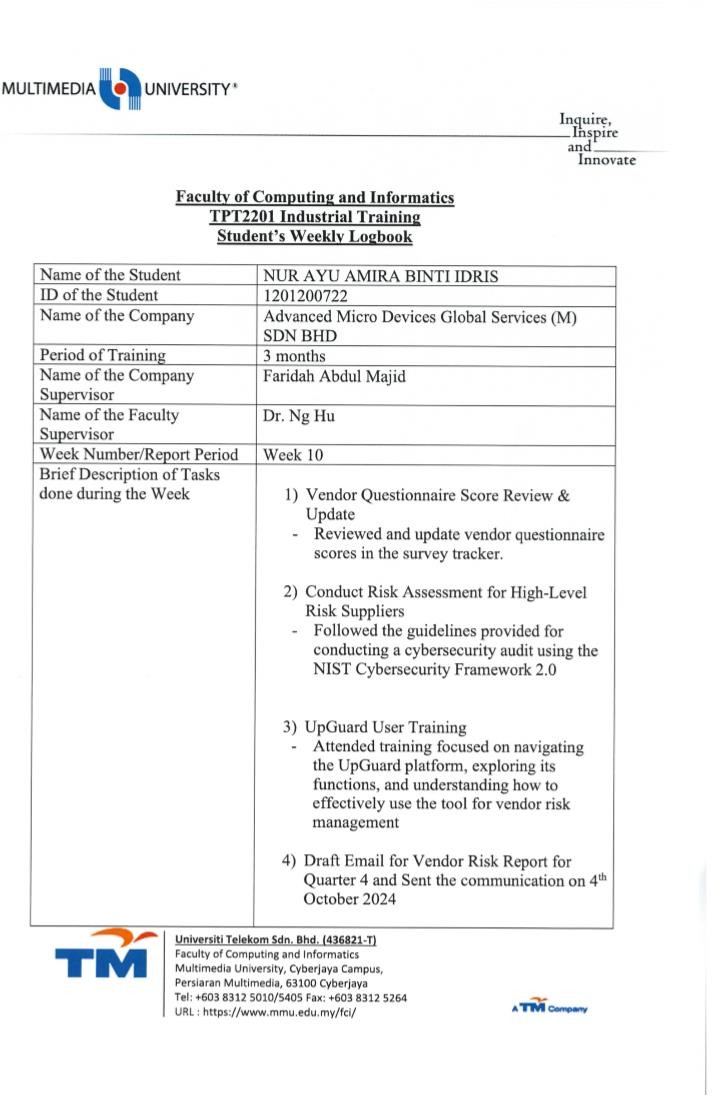


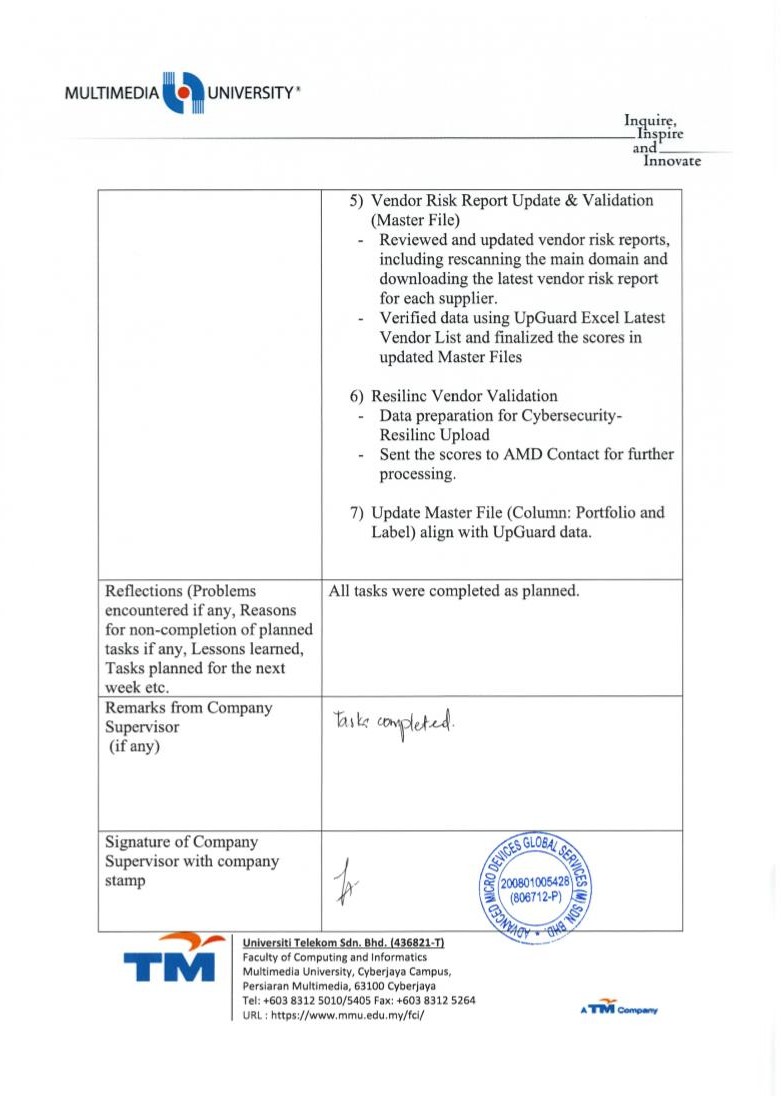
## Meeting Log – Week 9



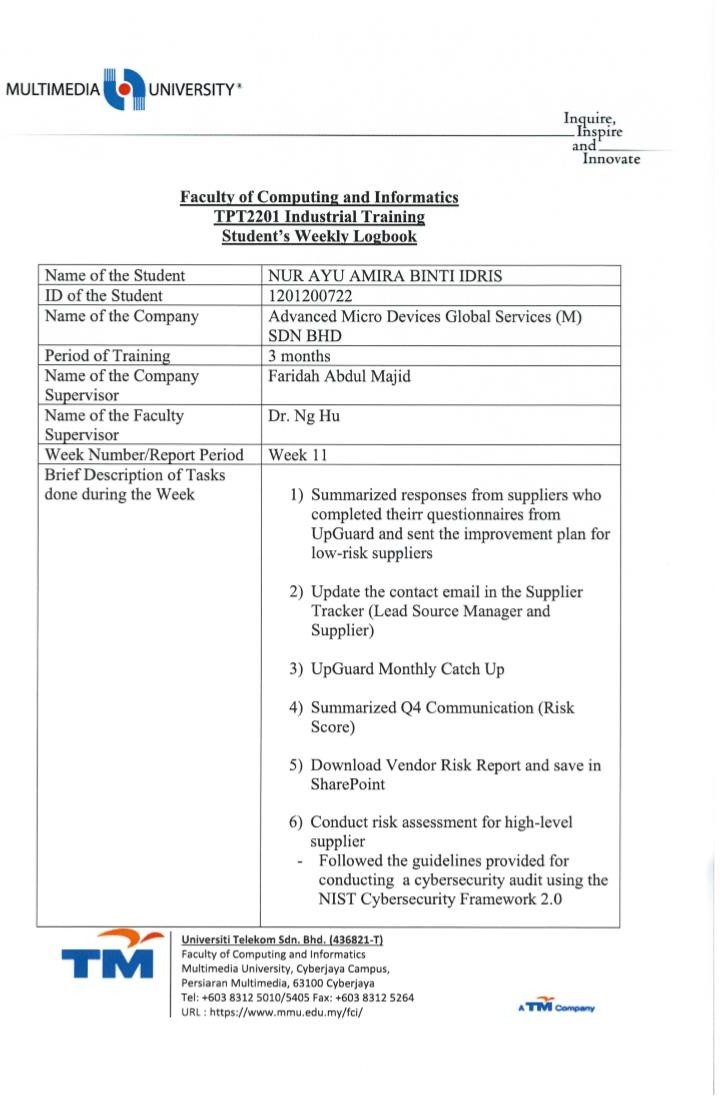


## Meeting Log – Week 10





## Meeting Log – Week 11





## Meeting Log – Week 12

## Meeting Log – Week 13