Not for public distribution
Document adopted and modified from ProjectManagementDocs.com

All work in this document is subject to NDA. This work is confidential and MUST not be shared with others.

Business Case: Project LoRaWAN

Team UMP

Team Member	Sections
Mattia Pulvirenti	1. Executive summary 2. Business case analysis team and stakeholders 3. Problem definition
Ben Poulton	4. Project overview 5. Strategic alignment 6. Cost Benefit analysis 7. Alternatives analysis 8. Approvals
Isaac Potts	9. Introduction 10. Project management approach 11. Project scope and milestone list 12. WBS + Appendix A
Annie Place	13. Change management plan 14. Communications management plan 15. Cost management plan 16. Procurement plan + Appendix D
Ryan Petrie	17. Project scope management plan + Appendix B 18. Schedule management plan 19. Quality management
Joey Hall	20. Risk management plan + Appendix C 21. Staffing, resource, and cost 22. Quality

ABERTAY UNIVERSITY
DUNDEE, DD1 1HG

DATE:

<Note: You should delete the bold green text in brackets before submission of this document as your assessment. While you are filling in this template, keep the green text for guidance in relation to content and points you need to address. Text in black font should be replaced with your own text, covering the relevant areas of your project. The text in black font is merely text for an example project for the client 'Smith Consulting' (note: this is a different example than that used in the template for the Project Management Plan) to give you an idea of the elements you need to cover. While the content of the template provides some of the information you need for this document, you should not copy text *verbatim* from the template or indeed, leave in the black text in normal font in this document or just exchange names and figures with your own names and figures. Replace the normal font text in black with your own words and expand it, providing justifications for decisions and statements using references etc. The already provided text is merely used here for illustration and guidance regarding content. Copying text would be considered plagiarism and it is bad practice, generally. YOU MUST REPLACE THE TEXT IN THE TEMPLATE WITH YOUR OWN TEXT COMPLETELY. Again, you should only *consider* the content for guidance. Provide as much detail as you can while still staying close to the word limit for your sections of the proposal.

Replace content in the text, tables, and figures with your own content, but keep the format the same, that is, what is asked for in the table or figure or text.

For text content, it is recommended that you read the template content for each section, note what it should be, and then write your own section without looking at the template. Then check whether you covered the content that was asked for.

Make sure that both Business Case and the Project Management Plan you provide contain consistent information. There will be some overlap between the two components as both are referring to the same project.

Note: Different example projects have been used in different sections in this template document for illustrative purposes only.>

Table of Contents

1. Executive Summary

This document outlines a proposed project to conduct a comprehensive security assessment of LoRaWAN technology. PA Consulting Group requires an in-depth understanding of the security strengths and weaknesses of LoRaWAN's network and infrastructure, to make informed decisions about its implementation and ensure the protection of sensitive data. This project will deliver a detailed report analyzing LoRaWAN security across all layers, identifying potential vulnerabilities, and recommending mitigation strategies to enhance the overall security posture of their LoRaWAN deployment.

1.1 Issue

PA Consulting Group recognizes the potential benefits of LoRaWAN technology for clients who design, manufacture, sell, and consume LoRaWAN networks, gateways, or devices. However, concerns have surfaced about the security implications of deploying this technology, particularly in relation to data confidentiality, integrity, availability, and compliance with relevant security standards. A thorough understanding of LoRaWAN's security mechanisms and potential vulnerabilities is crucial to mitigate risks and ensure the long-term success of their IoT applications.

Moreover, failing to address these security challenges could expose the firm to significant risks, including a potential loss of credibility and competitive disadvantage. This project will help the firm better understand the intricacies of LoRaWAN security, enabling it to navigate and address potential risks proactively. Doing so will ensure that PA Consulting is prepared to support its clients in securely implementing and managing their IoT solutions and will strengthen the firm's internal expertise to tackle future technological challenges effectively.

1.2 Anticipated Outcomes

This security assessment project will deliver:

Comprehensive Security Report: A detailed document analyzing LoRaWAN security architecture, identifying potential threats and vulnerabilities at all layers (physical, MAC, network, and application), and evaluating the effectiveness of existing security mechanisms.

Risk Assessment: An in-depth evaluation of the potential risks associated with LoRaWAN deployments, considering both current and emerging threat landscapes. This assessment will include the likelihood and impact of potential attacks, enabling PA Consulting to understand which vulnerabilities pose the greatest threat and prioritize them accordingly. The analysis will also encompass the potential impact of these risks on business operations, compliance requirements, and overall system resilience.

Mitigation Strategies: Actionable recommendations and best practices to enhance the security of their clients' LoRaWAN deployments, including device-level security, network security, and data protection measures. This will include guidance on configuring network infrastructure securely, ensuring strong encryption and authentication mechanisms, and implementing robust access control policies. The strategies will also cover periodic security audits, updates to firmware, and other proactive measures to keep the infrastructure protected against evolving threats.

Informed Decision-Making: The assessment will empower PA Consulting Group to make informed decisions regarding the implementation and management of their clients' LoRaWAN networks, ensuring the confidentiality, integrity, and availability of their data. With clear insights into the strengths and weaknesses of LoRaWAN security, PA Consulting will be able to guide clients with confidence on optimal practices for secure deployments, adjust security strategies in response to new developments, and meet regulatory compliance standards.

The end state of the project will provide PA Consulting Group with a clear understanding of LoRaWAN security, enabling them to confidently advise on deploying and operating a secure and resilient LoRaWAN network. By establishing a strong foundation of knowledge and well-defined security practices, PA Consulting will be better positioned to support their clients in building trust and achieving long-term success with their IoT and IoT-based initiatives. This project ensures that PA Consulting maintains its leadership role in cybersecurity and continues to deliver exceptional, forward-thinking solutions that protect clients against current and future cyber threats.

1.3 Recommendation

To ensure the success of this project, the team will adopt a rigorous and methodical approach. This will involve extensive research into the current state of LoRaWAN technology, including the latest developments and documented vulnerabilities. The team will employ a comprehensive and well-established testing methodology, such as the OWASP IoT Top Ten, to systematically evaluate the security architecture at all layers, including physical, MAC, network, and application. This methodology provides a structured framework for identifying potential risks and ensuring thorough assessment coverage.

Collaboration and cross-checking will be integral to the project approach. The team will work closely with subject matter experts within PA Consulting and draw on external industry resources to ensure a well-rounded analysis. Regular peer reviews and collaborative workshops will be conducted to validate findings and ensure consistency and accuracy in the assessment. This team-based approach will facilitate comprehensive insight, enabling the identification of critical vulnerabilities and the development of robust, actionable mitigation strategies.

Additionally, the team will continuously benchmark their findings against industry standards and best practices to maintain objectivity and ensure alignment with security regulations and client expectations. This approach will lay the groundwork for developing a detailed security report that offers PA Consulting valuable insights and recommendations for strengthening the security posture of LoRaWAN deployments.

1.4 Justification

The proposed security assessment project for PA Consulting Group is crucial for maintaining its leadership in cybersecurity and IoT solutions. With LoRaWAN technology gaining traction due to its cost-effectiveness and scalability in IoT deployments, the risks associated with security vulnerabilities have also risen. Industry data highlights that the average cost of a data breach in IoT environments can be substantial, with breaches involving lost business and operational downtime contributing the most to the costs. For example, the 2024 IBM Breach Report cites an average breach cost of $4.88 million, with nearly $2.8 million tied up in lost business and post-breach activities, such as customer support and regulatory compliance measures.

This project is justified as it mitigates these risks by offering a comprehensive assessment of LoRaWAN security. Early identification of vulnerabilities through this initiative can prevent potential data breaches that could lead to severe financial losses, regulatory penalties, and damage to PA Consulting’s reputation. Moreover, the adoption of enhanced security practices based on the findings will help ensure compliance with evolving IoT security standards, bolstering trust among clients and positioning PA Consulting as a proactive leader in secure IoT solutions.

Failing to move forward with this project risks PA Consulting's competitive edge. Without a thorough understanding of LoRaWAN's security, the company could face missed opportunities for business growth and client retention, especially as cybersecurity becomes a critical decision factor for clients selecting IoT partners. This project is therefore not just an investment in security but also a strategic measure to uphold PA Consulting's market position and service credibility.

(Source: https://socradar.io/ibms-cost-of-data-breach-report-2024-cybersecurity/)

1.1. Team Experience

Our team comprises highly motivated and skilled individuals, each currently pursuing a 3rd-year Ethical Hacking degree at the University of Abertay. We are actively involved in extracurricular activities within the cybersecurity domain, and several members possess practical industry experience (including the Cyber & Fraud Center for Scotland and Accenture consulting). This blend of academic knowledge and real-world expertise equips us with the necessary qualifications to execute this project with the utmost professionalism and deliver exceptional results.

2. Business Case Analysis Team and Stakeholders

2.1. Business Case Analysis Team

The following individuals comprise the business case analysis team:

Role	Description	Name
Project Manager	Team activities coordination and main client contact point	Isaac Potts

2.2. Project Team

The following individuals comprise the project team:

Role	Description	Name/Title
Project Manager	Team activities coordination and main client contact point	Isaac Potts
Developer	Technology and setup management	Ben Poulton
Evaluator	Strategy consultancy	Annie Place

Role	Description	Name/Title
Coder	Tools and software management	Joey Hall
Evaluator	Strategy consultancy	Ryan Petrie
Quality assurance tester	Testing and delivery controll	Mattia Pulvirenti

2.3. Client and External/Internal Stakeholders

In addition to the client listed below we have identified the following stakeholders:

Role	Description	Name/Title
Client (PA Consulting)	Sponsor for project	Peter Bennett/client

3. Problem Definition

3.1. Problem Statement

Leading innovation and transformation consultant PA Consulting Group is dedicated to guiding customers through the challenges of a technologically advanced environment. With a comprehensive understanding of strategy, design, technology, and engineering, PA Consulting provides comprehensive solutions for innovation. Acknowledging the growing significance of cybersecurity in the Internet of Things (IoT) space, PA Consulting is concentrating on the security of LoRaWAN technology in an effort to enhance its capabilities in the areas of digital trust and cybersecurity.

The Low-Power Wide-Area Network (LPWAN) technology known as LoRaWAN has become more popular due to its low power consumption, long-range communication capabilities, and cost-effectiveness, making it an ideal choice for industrial IoT applications.
However, security worries have surfaced, jeopardizing broader market acceptance. These worries are related to flaws found in the protocols and design of LoRaWAN, such as:

Vulnerabilities at the device level: Devices can be compromised by insecure firmware upgrades, weak encryption, and hardcoded keys.

Vulnerabilities at the network level: Data disclosure during transmission, replay attacks, and man-in-the-middle attacks are possible.
Vulnerabilities at the gateway level: including incorrect setups, unreliable communication routes, and the possibility of protocol downgrade attacks.

Such flaws may result in data breaches, denial-of-service attacks, unauthorised access, and manipulation of private data transferred across LoRaWAN networks. Through in-depth investigation and useful analysis of LoRaWAN threats and vulnerabilities, this project seeks to address these security concerns.

3.2. Organizational Impact

The findings of this project will support PA Consulting in enhancing its cybersecurity service offerings by integrating these insights into existing frameworks. The project outcomes can be leveraged to strengthen client advisory services, refine risk assessment methodologies, and develop tailored security solutions that address client needs. By embedding these findings into PA Consulting's strategic approach, the company will be better positioned to provide robust, informed guidance to clients adopting or managing LoRaWAN technologies. This integration ensures the project aligns with PA Consulting's commitment to delivering cutting-edge, secure technology solutions.
The following are some ways that this project will greatly improve PA Consulting's capabilities:

Enhanced Expertise: Gain a deeper comprehension of the protocols, architecture, and possible attack vectors of LoRaWAN security.
Tool Development: frameworks and tools might be develop to identify and address LoRaWAN vulnerabilities.
Thought Leadership: Through vulnerability disclosure reports and client presentations, establish PA Consulting as a reliable resource for information on LoRaWAN security.
Service Expansion: Make it possible for PA advisory to provide clients implementing LoRaWAN solutions with specialist security assessment and advisory services, and enhance PA Consulting's competitive advantage in the quickly changing IoT security industry.

3.3. Technology Integration and/or Migration

This project focuses on security research and vulnerability analysis of LoRaWAN technology. It does not involve direct technology integration or migration within PA Consulting's internal systems. However, the findings and tools developed during this project can be integrated into PA Consulting's existing cybersecurity frameworks and service offerings.

The vulnerabilities identified and mitigation strategies proposed through this research will be evaluated for integration into the firm's existing methodologies, tools, and client offerings. This may include updating PA Consulting's risk assessment models, refining incident response processes, and incorporating specific LoRaWAN security considerations into client engagement strategies. By embedding the project's findings into its broader consulting framework, PA Consulting will be better equipped to address the unique security challenges of LoRaWAN technology, positioning itself as a leader in providing comprehensive, forward-thinking solutions for IoT security.

4. Project Overview

<This section describes high-level information about the project. Include a project description, goals and objectives, performance criteria, assumptions, constraints, and milestones. This section consolidates all project-specific information into one chapter and allows for an easy understanding of the project since the baseline business problem, impacts, and recommendations have already been established.>

The LoRaWAN Project overview provides information for the solutions that this project will put forward to meet the goals outlined in the project brief provided by PA Consulting. A project description, list of goals and objectives for the project, the criteria we will use to measure the project's performance, the assumptions made about the project, the constraints of the project, and the major milestones to measure the progress made in the project. As the project moves forward and the scope expands, each of these components will be updated to match the scope in both coverage and detail.

4.1. Project Description

<This section describes the approach the project will use to address the business problem(s). This includes what the project will consist of, i.e., a general description of how it will be executed, and the purpose of it.>

The LoRaWAN Project will focus on testing and gathering data on the security measures of the LoRaWAN IoT devices, with a focus on the exploitation of these devices and what information can be obtained from this exploitation. This will be done by focusing on several varied types of attacks, ranging from network captures to reverse engineering attempts. The data gathered will be used to create a report that focuses on any weaknesses found and how these can potentially be mitigated, as well as the strengths of the LoRaWAN system.

This project will help reduce costs of IoT projects for the client, and will allow the, to provide services based on the LoRaWAN devices with a lot more confidence that they are offering the best service available. Additionally, the potential for using IoT to help with other areas of the business rises if it is known that the solution is secure and provides everything that is needed.

Any insecurities that are found can be reported to the relevant provider so fixes can be worked on for all products, leading to better security both within PA Consulting, and for the general consumer.

PA Consulting will provide the LoRaWAN devices and all testing will be performed on these devices, whilst staying within the scope specified by PA Consulting at the beginning of the project.

4.2. Business Goals and Objectives

<This section lists the business goals and objectives which are supported by the project and how the project will address them. You should talk to the client about their business goals.>

The LoRaWAN Project directly supports several of the corporate goals and objectives established by PA Consulting. The following table lists the business goals and objectives that the LoRaWAN Project supports and how it supports them **<Replace table content with your own content.>**

Business Goal/Objectives	**Description**
"We accelerate new growth ideas from concept, through design and development to commercial success."	The work done on the LoRaWAN Project will allow PA Consulting to provide more support to clients making use of the IoT networks we are testing. By making sure the LoRaWAN systems are secure, any ideas needing IoT technology will now have a strong base to develop from.
"We revitalise organisations with the leadership, culture, systems and processes to make innovation a reality."	IoT technology is a staple part of engineering new and productive systems within a workspace, and the assurance that any of these projects using LoRaWAN as their IoT network of choice will have a high level of security that's been tested will help solidify the

4.3. Project Performance

<This section describes the measures that will be used to gauge the project's performance and outcomes as they relate to key resources, processes, or services. Consider how success is measured.>

The following table lists the key resources, processes, or services and their anticipated business outcomes in measuring the performance of the project. These performance measures will be quantified and further defined in the detailed project plan. **<Replace table content with your own content.>**

Key Resource/Process/Service	**Performance Measure**
Gateway User Interface	The LoRaWAN Gateway interface should be tested for various vulnerabilities, and attempts to exploit it whilst both authenticated and not should be made.
Network captures	Capturing the data sent by the LoRaWAN devices to see if they don't meet encryption standards, or disclose any sensitive information.
Reverse Engineering	The firmware of the LoRaWAN devices should be examined and reverse engineering of this should be attempted.
Other Testing	Other Testing

4.4. Project Assumptions

<This section lists the preliminary assumptions for the proposed project. These assumptions are what the project manager/team expects to have or be made available without anyone specifically stating so. As the project is selected and moves into detailed project planning, the list of assumptions will most likely grow as the project plan is developed. However, for the business case there should be at least a preliminary list from which to build. Note: You are not describing risks in this section – risks are different from assumptions and constraints. A discussion of risks will go into the Project Management Plan, the other document that needs to be filled in.>

The following assumptions apply to the LoRaWAN Project. As more assumptions are made the list will be updated in accordance.

- The required software will be available and pre-configured as needed
    - Where this is not the case, configuration will be sorted out by
- Funding is available for training
- Funding is available for purchasing hardware/software for the LoRaWAN system

- The required software for the use of the LoRaWAN hardware will be setup and provided as needed
- The university will provide a working network for connectivity between devices.
- No security policies on the university network will disrupt the project

4.5. Project Constraints

<This section lists the preliminary constraints for the proposed project. As the project is selected and moves into detailed project planning, the list of constraints will most likely grow as the project plan is developed. However, for the business case there should be at least a preliminary list from which to build. Constraints are restrictions or limitations that the project manager must deal with pertaining to people, money, time, or equipment. You will probably use words like 'restricted', 'limited', 'constrained by' etc.>

The following constraints apply to the LoRaWAN Project. As project planning begins and more constraints are identified, they will be added accordingly.

- There are certain sections that remain out of scope, for example the cloud interface.
- University failure to provide us with correct DNS information and whitelist MAC address, resulting in delays to setup
- Forced to use the university network, so any security policies that are applied may limit what we can or cannot do.
- The network configuration is difficult and may cause issues when proceeding with the project if not configured correctly.

4.6. Major Project Milestones

<This section lists the major project milestones and their target completion dates. Since this is the business case, these milestones and target dates are general and in no way final. Replace what is in the table with your own dates and milestones/deliverables. It is important to note that as the project planning moves forward, a base-lined schedule including all milestones will be completed. >

The following are the major project milestones identified at this time. As the project planning moves forward and the schedule is developed, the milestones and their target completion dates will be modified, adjusted, and finalized as necessary to establish the baseline schedule. **<Replace table content with your own content.>**

Milestones/Deliverables	Target Date
Project Plan Review and Completion	09/12/2024
Project Kickoff	20/01/2025
Phase I Complete xxxx	xx/xx/xxxx
Phase II Complete xxxx	xx/xx/xxxx
Phase III Complete xxxx	xx/xx/xxxx
Phase IV Complete xxxx	xx/xx/xxxx
Phase V Complete xxxx	xx/xx/xxxx
Product xxxx	xx/xx/xxxx
Completed Investigation/Product xxxx	xx/xx/xxxx
Closeout/Project Completion	04/05/2025

5. Strategic Alignment

<All projects should support the client organization's strategy and strategic plans in order to add value and maintain executive and organizational support. All organizations have some sort of 'vision' that your project should address. This section provides an overview of the organizational strategic plans that are related to the project. This includes the strategic plan, what the plan calls for, and how the project supports the strategic plan. For your project, you need to find out about Abertay's strategic plan if Abertay is the client organization (you can 'work' for and be in the same client organization) you are working for. Alternatively, you may have an external client – talk to them about their vision. You can also invent a client, if you received your project from a module instructor that invented a client, for example. Talk to the person who created the brief for clarity. You still need to identify what the invented client's strategic plan is, i.e., you have to make this up.>

Plan	Goal	Relationship to Project
20xx Smith Consulting Strategic Plan for Information Management	Improve record keeping and information management	This project will allow for real-time information and data entry, increased information accuracy, and a consolidated repository for all payroll and administrative data
20xx Smith Consulting Strategic Plan for Information Management	Utilize new technology to support company and department missions more effectively	New technology will allow many payroll and administrative functions to be automated reducing the levels of staff required to manage these systems

Plan	Goal	Relationship to Project
20xx Smith Consulting Strategic Plan for Human Capital	Engage the workforce and improve employee retention	This project allows the employee to take an active role in managing his/her payroll and administrative elections

6. Cost Benefit Analysis

<Many consider this section one of the most important parts of a business case as it is often the costs or savings a project yields which must win final approval to go forward. It is important to quantify the financial benefits of the project as much as possible in the business case. This is usually done in the form of a cost benefit analysis. The purpose of this is to illustrate the costs of the project and compare them with the benefits and savings to determine if the project is worth pursuing. You may not have figures here, in which case you may have to make them up, or you focus on non-financial benefits (that potentially could be converted to financial benefits. For example, if you use a library in a system you are implementing (or coding), it means less time required for development and a lower initial investment for the web application. You should provide actual figures - the idea is that the identified costs are 'reasonable', which means you should also provide some information as to how you estimated these. Use references for your costs – do some research here. These costs should be realistic.>

The following table captures the cost and savings (benefits) actions associated with the LoRaWAN Project, descriptions of these actions, and the costs or savings associated with them through the first year. At the bottom of the chart is the net savings for the first year of the project. **<Replace table content with your own content.>**

Action	Action Type	Description	First year costs (-indicates anticipated savings)
Purchase of LoRaWAN equipment for initial testing	Cost	Initial investment for LoRaWAN Project	£400
Prevent Data Breaches	Savings	The Average cost of a data breach is £3.42 million, so preventing a data breach means massive savings	-£3,420,000.00
Net First Year Savings			**£1,620,000.00**

If a single data breach is prevented by the research done in this project, the average saving will be £1.62 Million.

7. Alternatives Analysis

<All business problems may be addressed by any number of alternative projects and/or existing systems, tools etc. While the business case is the result of having selected one such option, a summary of considered alternatives should also be included—one of which should be the status quo, i.e. doing nothing. The reasons for not selecting the alternatives should also be included. If the bullet format is not appropriate, provide an in-depth discussion of alternatives. In all cases, you have to do some research as to what existing or related systems/sites etc. are out there that would be suitable for the delivery of the project.>

The following alternative options have been considered to address the business problem. These alternatives were not selected for a number of reasons which are also explained below. **<Replace table content with your own content.>**

No Project (Status Quo)	**Reasons For Not Selecting Alternative**
Not incorporating anything IoT related	• Potential loss of clients who are specifically looking for services requiring LoRaWAN technology • Unable to make use of the benefits of IoT within the organisation
Alternative Option	**Reasons For Not Selecting Alternative**
Just leaving the IoT running without testing	• Unidentified risks – Could potentially lead to a massive loss of data if a vulnerability that can be exploited is found • Data loss would be a significant expense to deal with
Alternative Option	**Reasons For Not Selecting Alternative**
Only testing with an automated tool	• Likely to miss vulnerabilities that require more creativity • Reliant on known issues, cannot create/find new issues • Potentially a higher cost to obtain these tools to begin with

8. Approvals

<The business case is a document with which approval for a project is sought. Approval is granted or denied. Therefore, the document should receive approval or disapproval from its executive review board. Get a signature of the relevant subject specialist.>

The signatures of the people below indicate an understanding in the purpose and content of this document by those signing it. By signing this document you indicate that you approve of the proposed project outlined in this business case and that the next steps may be taken to create a formal project in accordance with the details outlined herein. **<Replace table content with your own content. Do NOT fake signatures. Get a client or one of the module team to sign the form, digitally or otherwise. Get the signatures as soon as you can – clients are busy and need to be able to review your document before they can sign it.>**

Approver Name	Title	Signature	Date
Bennett, P.	Client (PA Consulting), Sponsor	P.Be	
Callum, D.	Client (PA Consulting), Sponsor		

PROJECT MANAGEMENT PLAN: SMARTVOICE PROJECT <Your Project Name>

TEAM SMARTVOICE <Your Team Name>
ELENA BLACK, JOE GREEN <Your Team Members' Names>

ABERTAY UNIVERSITY
DUNDEE, DD1 1HG

DATE:

<Note: You should delete the bold green text in brackets before submission of this document as your assessment. While you are filling in this template, keep the green text for guidance in relation to content and points you need to address. Text in black font should be replaced with your own text, covering the relevant areas of your project. The text in black font is merely text for an example project for the client 'Total Software Incorporated (TSI)' (note: this is a different example than that used in the template for the Business Case) to give you an idea of the elements you need to cover. While the content of the template provides some of the information you need for this document, you should not copy text *verbatim* from the template or indeed, leave in the black text in normal font in this document or just exchange names and figures with your own names and figures. Replace the normal font text in black with your own words and expand it, providing justifications for decisions and statements using references etc. The already provided text is merely used here for illustration and guidance regarding content. Copying text would be considered plagiarism and it is bad practice, generally. AGAIN, YOU MUST REPLACE THE TEXT IN THE TEMPLATE WITH YOUR OWN TEXT COMPLETELY. You should only *consider* the content for guidance. Provide as much detail as you can while still staying close to the word limit for your sections of the proposal.

Replace content in the text, tables and figures with your own content, but keep the format the same, that is, what is asked for in the table, figure, or text.

For text content, it is recommended that you read the template content for each section, note what it should be, and then write your own section without looking at the template. Then check whether you covered the content that was asked for.

Make sure that both Business Case (sections 2-8) and the Project Management Plan (starting from section 9) you provide contain consistent information. Note: Different example projects have been used in different sections in this document. Remember to replace the entire example text with your own. The text is for guidance only (e.g., just replacing a project name is not sufficient). What you write should reflect your project components and ideas.>

9. Introduction

PA Consulting has approved EH8 to penetration test specific IoT products that use LoRaWAN networking protocols. This project will result in various reports being submitted to the client, with the success of the project depending on the quality of these reports. The project will involve following the OWASP IoT penetration testing methodology. This methodology involved various types of testing on the devices, all of which are in scope for this project. A condensed version of the methodology is talked about on a high level below.

The OWASP methodology began with testing the Processing unit, defining this as A processing unit is a device internal element that can only be accessed with physical access. This stage will focus on Authorization, business logic and side channel attack vulnerabilities. This will involve affirming authorization level needed for access, privilege escalation vectors, and discovering edge cases in the business logic.

The next stage is testing memory of devices. This involves testing cryptography, secrets and information gathering. Source code and detail exposure will attempt to be found by exploring the effected system. It will also be discovered how secrets and other information is stored. Cryptography will also be examined in this case.

In the next stage the installed firmware will be examined. This is another stage of enumeration, and finding authorization level, privilege escalation vectors and further cryptographical information.

Data exchange services will then be examined. A data exchange enables the secure, standardized and monetized exchange of IoT data between devices, organizations and applications. This stage involves ensuring data exchange security through both physical access and man in the middle (MitM) attacks.

Internal, physical, wireless and user interfaces will be tested. These will explore the following bullet points in all of the identified interfaces

- Authorization
- Information Gathering
- Cryptography
- Configuration and Patch management
- Secrets
- Cryptography
- Business Logic
- Input Validation

This methodology ensures full coverage of all vulnerabilities. This is used to demonstrate to the client project success even if no vulnerabilities were found, we can show security robusteness by following a comprehensive methodology.

It will also involve the LoRaWAN penetration testing framework to identify and exploit the network. The LoRaWAN penetration testing framework was created by IOActive. It is designed to provide a series of tools to craft, parse, send, analyse and crack LoRaWAN packets.

PA Consulting has provided the products to the client. The university has provided relevant setup information to EH8.

While Penetration tests against LoRaWAN products have been completed before, we believe that we can build off those and other existing resources to uncover new vulnerabilities and attack vectors. This penetration test will be conducted to make PA Consulting aware of vulnerabilities within the IoT devices, to contribute to PA Consulting’s purpose, to build a positive human future. The project will deliver a variety of deliverables to the client, specifically:

- Regular progress updates to all relevant stakeholders
- 1 hour presentation covering all vulnerabilities with Q&A
- Academic report
- Disclosure reports
- Project proposal
- RAID log

Team EH8 will achieve these by following the Agile manifesto, performing bi-weekly sprints, and regular check-ins with all relevant stakeholders. EH8 will follow premade methodologies in order to provide a consistent reliable outcome throughout the penetration test. Due to the wide scope of the penetration test the duties will be split up between all Team members. All team members will be allocated a section of the scope to test that they have expressed interest in, and all results will be collated into the final deliverables. The project manager will also ensure that at least 2 individuals are present during any part of the penetration test to ensure scope adherence.

PA Consulting has become a successful consultancy thanks to following their purpose of Believing in the power of ingenuity to build a positive human future. These values directly correlate to the project, as it will contribute towards PA consulting people-first mindset. It will do this by protecting individuals information through vulnerability disclosure. PA Consulting itself is a management consultancy, that contributes greatly towards cyber security, and creating secure, trustworthy products. This penetration test will align with this goal.

10.Project Management Approach

The Project Manager for EH8, Isaac Potts, has responsibility to ensure the project corresponds to this project plan, and other created management plans. The team consists of a project manager, developer, two evaluators, a coder and a quality assurance tester, as listed below.

- Isaac Potts – project manager
- Ben Poulton – developer
- Annie Place – evaluator
- Joey Hall – coder
- Ryan Petrie – evaluator
- Mattia Pulvirenti – quality assurance tester

All project other management plans and funding decisions reviewed and approved by the relevant stakeholders (Abertay University, or PA Consulting). If any delegation authority is delegated to the project manager, it must be done so in writing and must be signed by the stakeholders and the project manager.

The project manager is responsible for communication with relevant stakeholders, on the progress of the project and the performance of the team. The project manager will also ensure clear communication between Abertay University, PA Consulting and EH8. Meaning they are responsible for relaying questions the team has to the client and vice versa. The project manager will be responsible for the filling in of the Risk, assumptions, issues and dependencies log. This involves identifying problems with the project and sorting them into the above sections.

The team will use the agile approach to this task, as the finished product is clearly defined, however there is a wide scope, and many different approaches to achieve the end goal. The team will follow and embody the principles of the Agile manifesto and use team communication to define goals and tickets. This also allows the team to accommodate for discovered issues with the product and dpenednenices and adapt our timeline accordingly.

Various constraints and limitations have been placed on EH8. These are detailed in the raid log for the client. And further in 4.4 and 4.5, these limitations revolve around the scope and identified issues and challenges with the LoRaWAN technology.

EH8 has developed an estimate of the effort required for each main componenet. Utilising a top-down estimate the project will take approximately 100 days, or 3 and a half months. Each section will be allocated several weeks that we believe the section should require. As the group has 6 individuals, each with a different speciality, they will be allocated sections of the methodology to spend up to 10 weeks on their allocated sections. The sections to be allocated can be seen below.

- Processing Units
- Memory
- Firmware
- Installed Firmware
- Firmware Update Mechanism
- Data Exchange Services
- Internal interfaces
- Physical Interfaces
- Wireless interfaces
- User interfaces

This will allow the team the following 30 days for further testing as deemed necessary and to finish deliverables. If work is completed early more time will be allocated to completion of deliverables. Time estimation is approximate, and collaboration will be used on some sections of the methodology.

11.Project Scope and Milestone List

The scope of the project includes the planning of the project, plan of the penetration test, the penetration test and reporting. The scope of the penetration test is as follows:

- Compromise device level security
- Compromise network level security
- Compromise gateway security.

The only feature out of scope are all cloud features. The team will hope to test the product against the UKs IoT code of conducts. The scope of this project also includes deliverables, such as vulnerability disclosure reports for the manufacturer of the LoRaWAN products. A 45 minute presentation will also be made at the end of each term to the relevant stakeholders, with a 15 minute Q&A. Videos of applicable vulnerabilities will also be submitted. Project completion will be completed when the team has exhausted their penetration testing methodology and completed deliverables for all applicable devices and services has been given to the client.

All of this penetration testing work will be performed internally in Abertay University, and none of this project will be outsourced.

The below chart lists the major milestones for this penetration test. The chart is composed of major project milestones such as completion of a project phase. There are also smaller milestones which are not included; however these will be included in the project schedule and WBS. If any delays occur the project manager will be notified immediately so proactive measures may be taken to let us provide the best service to PA Consulting. Any approved changes to these milestones or dates will be communicated to the project team by the project manager.

Milestone	**Description**	**Date/Week**
Completion of Initial network setup	LoRaWAn network functioning within the university	30/10/2024
Initial scoping and preparation	Define the scope, limitations and objectives of the penetration test with client	1/11/2024
Begin penetration test following OWASP methodology	Begin the penetration test following an approved methodology	20/1/2025
Compile findings into a comprehensive report detailing vulnerabilities,	All findings are compiled into a report for the client.	30/04/2025
Presentation to client	A 45 minute PowerPoint will be created and presented to the client.	30/04/2025

The following products will be handed over to the client:

Product	**Description**	**Date/Week**
Project proposal document	This document	12/12/2024

Presentation to client with all steps done thus far	45 minute PowerPoint at the end of this term	30/04/2025
Academic report	Academic report detailing vulnerabilities	30/04/2025
Disclosure reports for device manufacturer	Reports documenting any discovered vulnerabilities for the LoRaWAN manufacturer	30/04/2025
Video demonstration of successful hacks.	Any applicable videos demonstrating effect of successful hacks.	30/04/2025
RAID log	Log detailing Risks, assumptions, issues and dependencies of the project.	Continuous

12.Work Breakdown Structure (WBS)

The schedule for this penetration test has been derived with input from all project members. The schedule was completed and reviewed by PA Consulting and approved and baselined by the project manager. The schedule was maintained using a RAID log, weekly updates with the university and following a Gantt chart. Any requested changes will follow the Change Management Plan outlined below. If any established boundary controls may be exceeded, a change request will be submitted to the Project manager. The project manager and teams will determine the impact of any changes created, including schedule, costs, resources, scope and risks. If the impact exceeds the boundary conditions the change will be run by PA Consulting. Due to this project not having a set budget or costs, this will be estimated with CPI meaning This projects boundary conditions are as follows:

Work breakdown followed the 5/50 rule. This means no individual work package will require no less 5 hours and no more than 50 hours. The work packages were developed in collaboration with the team in order to ensure each package is relevant to the project.

CPI less than 0.8 or greater than 1.2
SPI less than 0.8 or greater than 1.2

While either CPI or SPI are significantly above or below 1, the group will meet and consider the most effective way to manage the groups time and resources to get the group

The Work Breakdown Structure is provided in Appendix A.

13.Change Management Plan

A Change Management Plan lays out the framework for the project used by the team to manage and support the parties involved. The LoRaWAN systems may be altered, changed, and misused during the testing process. Due to this, the team requires a process where in the group will go about changes to methodology, scope, and planning. The Change Management Plan can help the project team achieve these goals as well as maintain the path to success of this project.

The steps below lay out the EH8 change control process for projects and will be used during our LoRaWAN project.

Step 1: Identify a change
PA Consulting will contact the project manager and request a change.
Step 2: Contact parties involved
The team leader will contact the university as well as the team member involved in making the change.
Step 3: Evaluate Change
The contacted team member will identify if the change is feasible.
Step 4: Sprint
The change will be included in the team's next sprint.
Step 5: Implement Change
The change will be implemented during the teams next sprint and added to the project if it follows the criteria above.

Any team member or party involved may submit a change request. All proposed changes will go through the same process as laid out above and treated by the same entities during each evaluation. Every change request will be logged by our team leader in the change log on our project's GitHub page. The GitHub will maintain a log of all changes implemented and not implemented, with a history of who implemented each change and who pushed the changes through. This will allow for the team to maintain a track record of what sections of the project need the most adjustments and how to better implement those adjustments as they transpire.

14.Communications Management Plan

The project requires an outline for communicating with one another, which is where the Communications Management Plan is necessary. These guidelines set will server to ensure proper communication throughout the entire length of the project. The plan outlines proper role allocation and a defined framework for proper interpersonal interaction. There will also be a table that properly defines the roles given to each task member as well as a directory which includes the contact information of everyone involved.

The leader for proper communication in this project would be our Project Manager, Isaac Potts. Below is a Matrix documented the proper role allocation for each member. This Communication Matrix ensures proper communication by properly displaying who communicates what to one another in an ordered manner.

Communication Type	Description	Frequency	Format	Participants/ Distribution	Deliverable/ Product	Owner
Weekly Status Report	Message evaluating weekly project status	Weekly	Discord	Project Sponsor, Team and Stakeholders	Status Report	Project Manager
Weekly Project Team Meeting	Meeting to review action register and status	Weekly	In Person	Project Team	Updated Action Register	Project Manager
Project Biweekly Review (PMR)	Present metrics and status to team and sponsor	Biweekly	Teams	Project Sponsor, Team, and Stakeholders	Status and Metric Presentation	Project Manager
Project Gate Reviews	Present closeout of project phases and kick-off next phase	As Needed	In Person	Project Sponsor, Team and Stakeholders	Phase completion report and phase kickoff	Project Manager
Technical Design Review	Review of any technical designs or work associated with the project	As Needed	In Person	Project Team	Technical Design Package	Project Manager

Project team directory for all communications is:

Name	Title	E mail
Andy Bridden	Project Sponsor	Andy.Bridden@PACONSULTING.COM
Isaac Pouts	Project Manager	2200980@abertay.ac.uk
Mattia Pulvirenti	Senior Programmer	2205049@abertay.ac.uk
Ben Poulton	Programmer	2300558@abertay.ac.uk

Ryan Petrie	Sr. Quality Specialist	2401114@abertay.ac.uk
Joey Hall	Quality Specialist	2205024@abertay.ac.uk
Annie Place	Technical Writer	2301241@uad.ac.uk

Communications Conduct:
The conduct of communication between parties in the project will maintain a formal, workplace tone throughout all avenues of communication. Through emails, the parties will maintain proper work communication etiquette that is clear, concise and to the point of the topic at hand. This will ensure that the team and the parties involved maintain proper focus and scope of the project as well as ensure that proper standards are set in place. A proper formal standard will ensure that the team is treating the LoRaWAN tools and properties with the utmost care and seriousness required for the task.

Meetings:
The Project Manager will inform the team every week on which days the team will meet with one another. There will be a timekeeper during each meeting to ensure the team is focused and on task. The role of timekeeper will be allocated to the group by the Team Leader and their role will maintain itself for the duration of the project. If the timekeeper is unable to be present for the Team Meetings, then at the meeting the Team Leader will assign the role temporarily to another Team Member. The timekeeper will log the times spent at each meeting on the GitHub to ensure the group remains poignant to the tasks at hand. The members are expected to arrive on time and to be on task during the meetup, minimizing all distractions. The talking points for the meeting will be given the day beforehand via email as well as through the appropriate discord channels. Any questions that a team member might have can be brought up within this 24-hour window through either of these communication avenues, and the team leader will be expected to deal with these inquiries prior to the meeting.

Email:
All emails for the LoRaWAN Project are to be formal, grammatically proper, and conducted in a professional manner. All information within the emails should be properly read over and sent to all appropriate parties involved. All emails should have the Project Manager tagged and involved inside them to ensure proper conduct. All attached files should be available to all team members and easily accessible within the GitHub or discord server.

Informal Communications:
Most communication about the project should happen between all appropriate members within the discord server, email, or in person. The etiquette within these channels is allowed to be looser, and less formal than otherwise. However, the team must maintain the same

communication expectation that one would have within an office work environment. If any information needs to be communicated about an issue that information should be communicated as soon as possible. These issues should be handled by the appropriate parties as well as the team leader.

15.COST MANAGEMENT PLAN

The devices allotted to the team have been pre provided by the sponsor PA consulting. From this, there is no overhead cost from the sponsor or the team aside for the price previously allotted to the IoT devices. The team, being one of several that have had the opportunity to work these systems, does not need to factor in this cost to the project overhead. The university has not been required to provide any other services aside for computer laboratory usage. This service will also not be added to the project cost overhead as it is a pre expected requirement from the university and not project related. Due to this, the project will cost a minimal amount since everything used during this project has been provided by the sponsor and university.

The Project Manager will be in constant contact with the Project Sponsor to ensure that our tasks remain on budget. The Sponsor will have a final say on all budgeting constraints and decisions made by the group at large. The finances will be delegated to whomever the Project Manager dictates will handle these when the time arises. This person will oversee keeping a log of all purchase and expenses during each sprint of the project as well as reporting these logs to both the Project Manager and the Project Sponsor.

Cost and Schedule Performance Index (CPI and SPI respectively) will be used for calculating the cost of all project's expenses. For any large expense changes there will need to be timely corrections for their adjustments to ensure the project remains on budget. All changes that are made will be reported during the biweekly project reviews with the Project Sponsor to ensure all parties are informed on budgeting constraint and adjustments. When a correction is made the change will have to be approved using the same method described above in the change management plan. If there are any extreme budgeting issues present, the Project Sponsor will be immediately notified to ensure swift action on the issue at hand.

16.PROCUREMENT MANAGEMENT PLAN

For the LoRaWAN Project, the systems and IoT devices have been provided to the team by the Project Sponsor and handed into the University. The Sponsor has informed the team that the products shall remain on campus for the duration of the Project. For any damaged and faulty equipment, the Sponsor has informed the team that the equipment can be replaced at no extra cost to the team. When damage occurs to the equipment, the Project Manager will inform the Project Sponsor of the damages, and a new device will be sent out as soon as possible.

The Sponsor encourages experimentation and rigorous testing on the devices, and thus expects that permanent damages may occur to the provided hardware. These damages will be reported by the appropriate member of the project team and brought up during the biweekly teams meeting with the sponsor.

When permanent, project altering damages do occur to the IoT devices provided, the project manager will inform the appropriate channels at PA consulting of the damages. From there, the team will expect for a new model of the damaged device to be delivered to the University as soon as possible. This delivery will be expected to add no extra overhead cost to the team as the sponsor already has exclaimed that there are several more devices waiting testing in storage. Once these devices are brought to the University building, the team will then acquire the devices from the appropriate staff members at Abertay and proceed to set up and continue onward with the project from that point. Any parts of the testing process that need to be redone will be tasked off the appropriate team members. These team members in order of methodology assigned will redo whatever processes through the test that must be redone to bring the device back to where the damaged device was left off at.

17.Project Scope Management Plan

<It is important that the approach to managing the project's scope is clearly defined and documented in detail. Failure to clearly establish and communicate project scope can result in delays, unnecessary work, failure to achieve deliverables, cost overruns, or other unintended consequences. This section provides a summary of the Scope Management Plan in which it addresses the following:

- **Who has authority and responsibility for scope management**
- **How the scope is defined (i.e. Scope Statement, WBS, WBS Dictionary, Statement of Work, etc.)**
- **How the scope is measured and verified (i.e. Quality Checklists, Scope Baseline, Work Performance Measurements, etc.)**
- **The scope change process (who initiates, who authorizes, etc.)**
- **Who is responsible for accepting the final project deliverable and approves acceptance of project scope**

>

A Project scope management plan is an essential piece of the puzzle in any project. A project scope management plan involves the definition of the projects scope. It is vital that this section covers authority and responsibility for management of the project scope, the project scope definition, the measurement of the project scope, the process of changes within the project scope, and all parties who are responsible for final acceptance of the project scope.

The project scope management plan for Team EH8 working on the LoRaWAN project for PA Consulting Group with Abertay University will be the team's project manager responsibility or any other team members assigned to this work by said project manager will be responsible for the overseeing of and managing of the project scope management plan. The project scope is initially defined from documents provided to the team EH8 for example the project brief, NDA agreement and IP agreement provided. Further definition is from the other sections in this proposal template such as work breakdown structure. Any and all Parties involved in the LoRaWAN Project including Team EH8, Abertay University and PA Consulting Group will ensure proper completion and delivery of documents to relevant parties such as quality checklists to confirm all work is being completed to the agreed upon standards from all parties involved(Team EH8, Abertay University and PA consulting Group) and individual Activity Logs from each team member for each work week to ensure equal and adequate contribution to the project work and goals. Documentation like this is vital to the project as it helps track progress, quality, and deadlines.

Any and all changes to the project scope proposal can be suggested by any team members of EH8, Instructors from Abertay University, and relevant sponsors from PA Consulting Group. Any Scope changes however necessary must be authorized by project manager after a thorough evaluation of the proposed changes with relevant team members if applicable. After this evaluation the project manager will propose the changes to the Instructor from Abertay University and PA Consulting Group to ensure all parties are happy with the proposed changes. Once all parties are in agreement with the proposed changes the project manager and any relevant team members involved will update any and all documentation and apply the agreed upon changes. This helps to ensure stakeholders in the project whether from team EH8, Abertay University, or PA Consulting Group will all agree and understand the suggested changes helping reduce and negative impacts to the project and allowing preparation to advance through the project with these changes in mind.

The acceptance and approval of finalized project deliverables and the project scope for the LoRaWAN Project is the responsibility of the client PA Consulting Group. This would come after a review of all relevant documents and work by PA Consulting Group to ensure that all project requirements and standards are met to ensure an effective and through path towards the end goals and outcomes.

To summarise the project management plan is a critical tool to be used in any project for maintaining a structured approach ensuring all parties involved (Team EH8, Abertay University and PA consulting Group) are happy with the project timeline, standards and goals.

18.Schedule Management Plan

<This section provides a general framework for the approach which will be taken to create the project schedule. Effective schedule management is necessary for ensuring tasks are completed on time, resources are allocated appropriately, and to help measure project performance. This section should include discussion of the scheduling tool/format, schedule milestones, and schedule development roles and responsibilities.>

The schedule management plan provide a overview of the approach towards the development of the projects schedule. This is vital to the projects work as it ensures appropriate delivery and completion of project work not only this it helps to see and properly allocate resources to the correct tasks and their related team members.

The schedule for the LoRaWAN project will be created and documented in word and the project deliverables as well as their relevant connections will be seen in this document in the WBS also known as the Work Breakdown Structure, Gantt Chart and precedence overview network with an identifiable critical path. These areas of the proposal template will ensure a clear path of work for the project helping limit delays. The estimation of time for each project deliverable will be calculated using the precedence overview network. A precedence overview network is a tool often used for projects helping to layout a clear roadmap for project deliverables. This is seen through the display of the earliest start, earliest finish, latest start, latest finish and the float value (which represents the amount of time each deliverable can be allowed to delay). This detailed and clear diagram streamlines the projects workflow not just for task management but also for timekeeping. Resource allocation for each deliverable is determined in the Resource, Staffing and cost section of the project proposal template. These sections describe the assignment of resources between the different EH8 team members and their specific tasks ensuring appropriate distribution of support for each project deliverable.

After the development of these proposal template sections, the team will review the relevant information such as the work breakdown structure, Gantt Chart, precedence network overview and resource allocation and all agree on the current state of said sections. If in disagreement the team will work out a resolution to implement that works for all team members of EH8 and any relevant further parties impacted such as Abertay University or PA Consulting Group.

The responsibility for the project planning will be with the project manager along with consultation from the team members to ensure team working in an effort to create the project schedule including resources, project timelines, and milestones. The project manager will then validate the project plan with all parties involved((Team EH8, Abertay University and PA consulting Group).

The project team EH8 as a whole must contribute to the work related to the project planning and a review from all team members of the of the proposed schedule and resource allocation. The project team as a whole must review and validate the proposed project plan after initial agreement and approval from all parties involved(Team EH8, Abertay University and PA consulting Group).

Project Stakeholders(Team EH8, Abertay University and PA consulting Group) will be involved with the approval and reviewal of the project plan proposals.
Project Team members EH8 will be involved with the approval and reviewal of the project plan proposals.
Project Milestones so far are the following

- Planning Start
- Project PowerPoint presentation completion
- Project proposal template completion
- Signing of IP/NDA agreements
- Completion of Risk Assessment for security testing
- Equipment setup
- Project Planning completion
- Project Security testing Start
- Security testing report start
- Security testing report finish
- Project delivery

These project milestones are important points for the parties involved(Team EH8, Abertay University and PA consulting Group) to track progress and ensure appropriate delivery and standard of the project work. These milestones mark significant completion of the project deliverables in which the team EH8 can take the option to review their work related to said milestone. This approach helps to ensure proper management of time for the project deliverables and helping to catch-up with work in the event of delays by seeing how far along the team is in the roadmap.

19.Quality Management Plan

<This section discusses how quality management will be used to ensure that the deliverables for the project meet a formally established standard of acceptance. All project deliverables should be defined in order to provide a foundation and understanding of the tasks at hand and what work must be planned. Quality management is the process by which the organization not only completes the work but completes the work to an acceptable standard. Without a thorough Quality Management Plan, work may be completed in a substandard or unacceptable manner.>

The quality management plan is an essential tool that is used to assign standards to the project work and deliverables. All standards should be agreed upon by all parties (Team EH8, Abertay University, PA Consulting Group). All standards should provide a clear understanding of what is required for each project task and deliverables.

Quality Management is an essential responsibility shared by every team member of EH8 for the LoRaWAN project for their own individual work and the agreement of the teams work prior to submission and or delivery. This responsibility involves the development, agreement, maintenance to keep it relevant and execution of said quality management plan. This responsibility for all team members of EH8 ensures a collaborative review of the project work, tasks and deliverables this approach also helps to ensure that the project delivery is kept at a high level of quality. Every team member of EH8 is responsible for the agreement of the quality management plan. This collaborative approach ensures that quality management is kept up to the previously agreed upon standards.

The project parties(Team EH8, Abertay University, and PA Consulting Group) are responsible for the approval of quality standards for the project work, tasks, deliverables and project delivery to ensure compliance with their own set quality standards and the set of quality standards agreed upon within the project and its parties(Team EH8, Abertay University, PA Consulting Group). Not only this but they are also responsible for the final signing off of the project delivery ensuring the delivered project is of appropriate standard.

The project manager is responsible for the overseeing of the team's own quality management and their quality management of their fellow teammates to ensure an extra final quality check ensuring every piece of work meets the standard. The project manager is also responsible for the communication of said quality standards between team members and stakeholders. The project manager must work closely with team members to ensure the appropriate standards for the relevant work.

The team members are responsible for upholding the quality standards for their own work related to the LoRaWAN project. The team members are responsible for ensuring agreement upon the standard of work whether individual or group related before submission or delivery. Team members are responsible for ensuring the tools and methods used for each piece of work are relevant and uphold the agreed upon quality standard.

Both team members, Project manager, and stakeholders are responsible for the final agreement and approval of quality standards ensuring that these standards are met for all project deliverables.

This quality Management plan ensures that all tools, methods, project work and project delivery is upheld to the agreed upon and approved standards of quality which ensure appropriate, comprehensive and completed project deliverables. This quality management plan also ensures that all tools, methods, project work and project delivery are legally compliant with the scope of the security test and any relevant legislation such as the GDPR. This is ensured by all parties involved that being the team members, project managers and stakeholders upholds the standard for their own work and then having this work reviewed by the appropriate person such as a team members work being reviewed by the project manager. This quality management plan also ensures full agreement with the teams work from every member of EH8 through individual work review project management review of said work followed by a group review of project delivery.
The quality management plan overall establishes a process for agreement of standards across all project deliverables. This done through individual reviewal of work, team EH8 group reviewal of work and a project manager reviewal of work. This ensures that all work and project reviews provides an accurate and true representation of project quality. By involving all parties(Team EH8, Abertay University, PA Consulting Group) involved in the LoRaWAN project this quality management plan ensures that a high standard for every piece of project work including the proposal template and other project tasks, work, and final deliverables.

<you also need to list the standards you need to meet, e.g., legal and ISO, accessibility, usability standards, GDPR etc. and who is responsible for meeting those.>

20. Risk Management Plan

<This section provides a general description for the approach taken to identify and manage the risks associated with the project. It should be a short paragraph or two summarizing the approach to risk management on this project. There is a detailed risk assessment template as well as risk matrix provided in Appendix C>.

To facilitate PA Consulting Group efficiently, deploying a LoRaWAN network will involve a structured approach to identifying and managing a variety of risks, through evaluating technical, operational, environmental and security factors specific to its business. The primary challenges include using suitable equipment, ensuring correct placement of IoT devices, and adhering to relevant regulations and protocols. Addressing these risks with strategic mitigation measures is essential for a successful deployment. These proactive measures will ensure a reliable, scalable, and legally compliant LoRaWAN network tailored to PA Consulting Group's needs and objectives.

We will also use a vulnerability scanner Nessus to rank and evaluate vulnerabilities exposed through penetration testing. This scanner takes into account various categories of exploitation techniques and with scores them from 1 (low impact) through to 10 (high impact). The highest probability and highest impact risks will be added to the project schedule and Isaac Potts will assign the appropriate team member(s) to implement the mitigation response at the appropriate time. Allocated managers will provide status updates on their assigned risks in the bi-weekly project team meetings, when such meetings include the risk's planned timeframe.

The three main anticipated risks in the project and their mitigation strategies entail:

- Risk: Suitable Equipment
  - The effectiveness of a LoRaWAN deployment hinges on the selection of appropriate hardware, including gateways and IoT devices. Using equipment that is incompatible with the business's needs or the environment can lead to network failures, increased maintenance costs, and inefficiencies. The IoT devices have been supplied to the Project by PA Consulting Group.
    Mitigation Strategies:
    - Ensure the devices are (i) LoRa Alliance-certified to ensure compatibility with the LoRaWAN protocol; and (ii) comply with the UK IoT Code of Practice.
    - Use Nessus to rank and evaluate vulnerabilities exposed through penetration testing taking into account various categories of exploitation techniques and scoring them from low impact through to critical impact.
    - Research to assist PA Consulting Group to only use reputable suppliers offering warranties and after-sale support to ensure replacements and repairs if needed.
- Risk: Correct Placement of IoT Devices
  - Proper placement of gateways and IoT devices is critical for ensuring consistent network coverage, reliable data transmission, and optimal performance. Misplacement can lead to signal obstructions, coverage gaps, data loss and increased costs for corrective measures.
    Mitigation Strategies:
    - Survey the deployment area, to assess signal strength, potential obstructions, and coverage zones.
    - Use simulation tools to design an optimised network layout before deployment, ensuring sufficient coverage and minimal dead zones.
    - Overlap coverage areas where possible to prevent single points of failure and ensure reliable connectivity even if one gateway malfunctions.

- Risk: Compliance with Relevant Regulations and Protocols
    - LoRaWAN operates [within the 868 MHz ISM band in Scotland] and [PA Consulting Group] must comply with Ofcom's rules for power limits and duty cycles. Additionally, data management must adhere to GDPR to ensure data security and privacy. Non-compliance can result in fines, legal action, or reputational damage.

      Mitigation Strategies:
        - Stay updated on Ofcom regulations, including frequency usage, transmission power, and duty cycle limits, and ensure all IoT devices meet these requirements [together with the LoRaWAN Protocol and UK IoT Code of Practice].
        - Have encryption and device authentication to protect network data and prevent unauthorised access.
        - Keep the data within the university facility, to ensure GDPR regulations are followed for the project.
        - PA Consulting Group employees to be trained on GDPR requirements and company policies for data collection, storage, and sharing.
        - Have regular compliance audits to ensure adherence to legal and regulatory standards.

Further details are set out in the risk assessment in Appendix C.

21.Staffing, Resource and Cost

<Discuss how you plan to staff the project. This section should include discussion on matrixed or projected organizational structure depending on which is being used for this project. This section should also include how resources will be procured and managed as well as the key resources needed for the project. Remember to justify your costs. You can make up staff costs – check websites etc. what you would expect to earn as a recent graduate, for example, working for a specific period. Be mindful that – for your academic project – you need to make sure that all teammates have a roughly equal workload across the term, that is, do not overtax the project manager.>

Deploying and penetration testing LoRaWAN in PA Consulting Group's business will involve utilising a combination of hardware, software, infrastructure, and compliance resources. These components are essential for creating a secure, reliable and efficient IoT network capable of meeting PA Consulting Group's business objectives.

Project LoRaWAN will proceed on the basis of a projected organisational structure with interaction and support from the client, PA Consulting Group. All penetration testing and

reporting work will be performed internally at Abertay University, i.e., none of the project will be outsourced.
[NOTE DOUBLE CHECK THESE ROLES WITH SOMEONE]
The staffing requirements for Project LoRaWAN comprises the following:

1. Project Manager (Isaac Potts) – Team Activities Coordination and Main Contact Point
2. Developer (Ben Poulton) – Technology and Setup Management
3. Evaluator (Annie Place) – Strategy Consultancy
4. Coder (Joey Hall) – Tools and Software Management
5. Evaluator (Ryan Petrie) – Strategy Consultancy
6. Quality Assurance Tester (Mattia Pulvirenti) – Testing and Delivery Control

In addition, the client will provide a point of contact (Client POC) for the project manager (and team members as necessary) to liaise within undertaking and completing the project. The first such Client POC shall be Andy Bridden [Andy Bridden was our first client right?].

The main additional resources and associated costs for Project LoRaWAN are:

1. Infrastructure and Hardware

1.1 Gateways – LoRaWAN gateways connect IoT devices to the network. Costs: Nil (given how it's being provided by PA Consulting Group).

1.2 IoT Devices

Device
LHT65N -- LoRaWAN Temperature & Humidity Sensor
LSE01 -- LoRaWAN Soil Moisture & EC Sensor
LPS8v2 -- Indoor LoRaWAN Gateway
LDDS20 LoRaWAN Liquid Level Sensor

Costs: Nil as provided to project by PA Consulting Group.

1.3

Connectivity – Gateway(s) require connectivity to a network server. Costs: Nil as utilising Abertay facilities and ethernet cables (connections) for Project LoRaWAN.

2. Software Resources

2.1 Network Server Software – LoRaWAN servers manage data flow between devices and applications. Cost: Nil as utilise a free open-source platform.

2.2 Application Software (WHAT WAS IT THAT WE WERE USING AGAIN??) Applications process and visualise data for end users.

2.3 Data Storage – Storing collected data. Costs: Nil as project using Abertay facilities

3. Deployment

3.1 Installation – Deploying gateways and devices involves site surveys, labour, and setup. Costs: Nil

3.2 Maintenance – Regular maintenance ensures the network's longevity. Costs: Assume nil given limited 12-week duration of LoRaWAN project.

4. Compliance and Security

4.1 Regulatory Compliance – In Scotland, businesses must comply with Ofcom regulations and GDPR for frequency use and data protection. Costs: Nil as regulatory and GDPR training undertaken inhouse.

4.2 Security Measures – Securing the network is essential to prevent unauthorised access. Costs: Nil for penetration testing through using Kali Linux software. Kali Linux tools which include Wireshark, Aircrack, Metasploit, Nmap, and Nessus applications to be used namely.

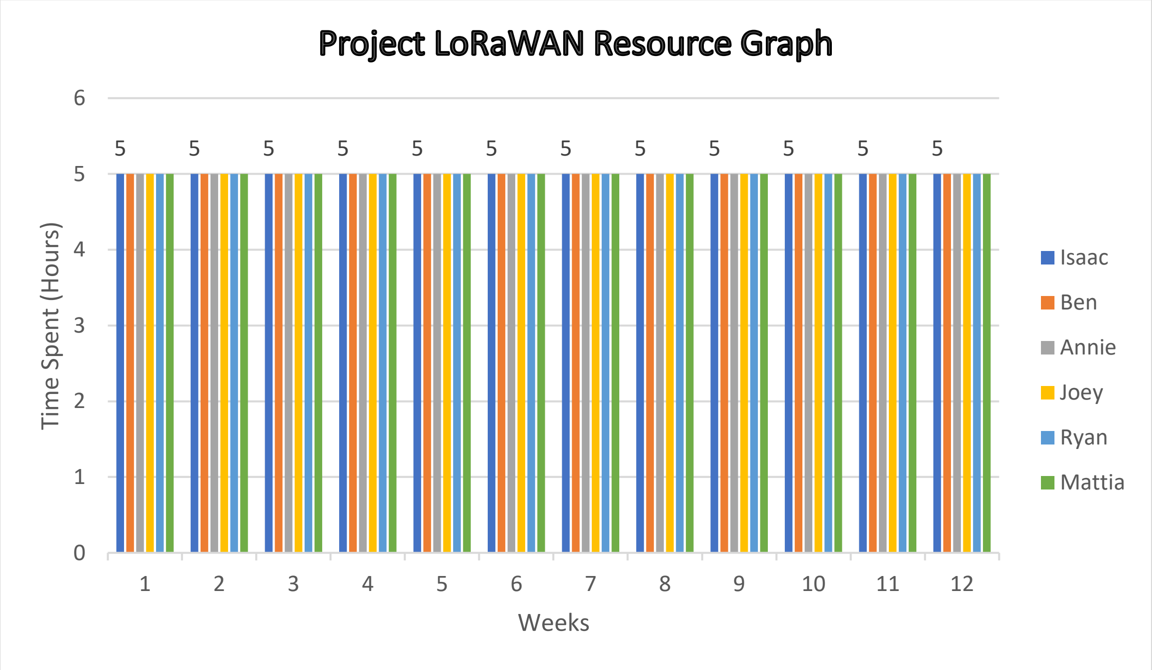
- Wireshark – Used to analyse network traffic and perform packet sniffing, helping to detect potential intrusions and anomalies in the network as well as testing data transmission security against possible attacks such as Man in the Middle.
- Aircrack - Used to analyse and exploit wireless networks, allowing testers to assess the security strength of WIFI connections.
- Metasploit - A vulnerability framework to check for and exploit weaknesses in devices running LoRaWAN firmware.
- Nmap – A scanning tool to identify the different devices connected to the network helping understand topology and where weak points lie.
- Nessus – A tool used to find vulnerabilities that hackers could exploit. It scans ports and reports results as well as determines the severity of said exploits.

Resource:

<Include a Resource Calendar as part of your project plan. The resource calendar identifies key resources needed for the project and the times/durations they'll be needed. Some resources may be needed for the entire length of the project while others may only be required for a portion of the project. This information must be agreed to by the Project Sponsor and Functional Managers prior to beginning the project. As before, be mindful not to overburden the project manager.>

<you will probably have to amend this graph by week (across 12 weeks project duration), rather than month as depicted below. Make sure it is realistic (e.g., you would not be expected to work 40 hours a week). Also consider a roughly even distribution of work across the team members.

Project LoRaWAN will require all 6 project team members to be engaged during the entire 12-week duration of the project although the levels of effort will vary as the project progresses. The below resource calender shows how many hours for each week during the 12-week duration of implementation of Project LoRaWAN, each team member estimates they will be working on the project.



[Each team member has a colour. For each week, chart will indicate how many hours each team member will be working on the project - we need to assume team members broadly work similar total hours].

<This section contains the cost baseline for the project upon which cost management will be based. The project will use earned value metrics – later more on that - to track and manage costs and the cost baseline provides the basis for the tracking, reporting, and management of costs. You should make up 'reasonable', i.e., realistic costs. Estimate and try to get an idea of how you can estimate costs (do some online research and put the references in the reference section and in the body of the text here). Justify your costs.>

The total cost of undertaking a comprehensive security assessment of LoRaWAN technology to be deployed in PA Consulting Group in accordance with Project LoRaWAN will therefore be the labour cost of the Team. Based on the estimated time for the 12 week implementation programme as per the Resource Calendar above together with a market hourly rate of [36 pounds per hour], total spent would be 5760 pounds per person.

Project Activity	Budgeted Game	Comments
Equipment set up and initial Client Meetings		Includes work hours for all project team members for work on
Reconnaissance and Scanning		Includes all work hours for
Vulnerability Assessment and Exploitation		Includes all work hours for
Post Exploitation and Reporting		Includes all work hours for
Security Report Refinement and Project Delivery		Includes all work hours for

<Also include whether you need any particular equipment, workstations, and who used it in which week etc. This could also mean that, for example, equipment is used throughout the entire duration of the project.>

22.Quality Baseline

<This section should include the quality baseline for the project. You are essentially also describing key performance indicators. The purpose of this baseline is to provide a basis for ensuring that quality can be measured to determine if acceptable quality levels have been achieved. It is important for all projects to clearly define and communicate quality standards and the quality baseline serves this purpose.>

Project LoRaWAN must meet the quality standards set out in the quality baseline described in the table below. The Quality Performance Baseline is the baseline, i.e., in effect key performance indicators (KPI's), which provides the acceptable quality levels of Project LoraWAN. The pen tests on a LoRaWAN deployed with PA Consulting Group must meet the baseline values in order to achieve success. The KPIs provide a structured framework to the Team to evaluate security performance, manage risks, and identify areas for improvement.
A quality baseline establishes the minimum standards for performing penetration tests on LoRaWAN networks. It should be aligned with industry best practices, regulatory requirements, and the specific operational context of Scottish businesses. Key aspects include:
· Protocol Compliance: Ensuring adherence to the latest LoRaWAN protocol specifications, including secure device provisioning, and [robust encryption (e.g., AES-128)].
· Regulatory Compliance: Verifying that data transmission, storage, and handling meet UK GDPR and other relevant data protection laws.

· Threat Surface Analysis: Comprehensive identification of all potential attack vectors, from physical devices to application layers.
A detailed quality metric is provided in Appendix D.

Each key component of the Quality Baseline and its associated KPIs are set out in the Table below:
Adopting KPI-driven penetration testing provides:

- Ability to measure the effectiveness of security efforts.
- Identification and mitigation of vulnerabilities before exploitation.
- Confidence in compliance with legal and industry standards.
- Strengthened ability to withstand and recover from potential attacks.

By establishing robust quality baselines and tracking KPIs, PA Consulting Group deploying LoRaWAN can safeguard their network, ensure compliance, and build
trust in their IoT-enabled operation. Each key component of the Quality Baseline and its associated KPIs are set out in the Table below:

<Replace Table Content with your own content.>

Item	Acceptable Level	Comments
1: Network Connectivity – The network must provide consistent connectivity across the targeted deployment are.	**1: Signal Strength:** • **Minimum Receive Signal Strength Indicator (RSSI): >= 120 dBm.** • **Signal-to-Noise Ratio (SNR): >= 8dB for uplink communications** **2: Network Uptime:** • **Gateways must achieve >= 99.5% uptime per month, allowing for no more than 3.6 hours of downtime.**	**Use site surveys and RF propagation tools to design optimal gateway placement. Conduct real time monitoring of signal metrics and network performance.**
2: Data Transmission and Performance – The LoRaWAN network must ensure reliable data	**Data Throughput:** • **Minimum uplink throughput: 100**	**Use Adaptive Data Rate (ADR) to optimize transmission and reduce interference.**

transmission between IoT devices and the network server.	bytes per second per device. - Minimum downlink throughput: 50 bytes per second for firmware updates or commands	
3: Scalability - The network must support the anticipated number of IoT devices and have the flexibility to accommodate future growth without performance degradation.	Allow a 33% increase in device count without significant performance loss.	Simulate load scenarios during deployment testing to ensure scalability.
4: Regulatory Compliance - The network must comply with Scottish regulations, including Ofcom's frequency Usage guidelines and GDPR for data protection.	1. 100% adherence to Ofcom's guidelines for the 868 MHz ISM band, including power limits and duty cycle restrictions. 2. 100% data encryption compliance using AES-128 encryption for all transmissions. 3. Ensure data minimization, lawful processing, and transparency in line with GDPR requirements.	1.Consult with regulatory authorities. 2. Implement encryption protocols and secure authentication for all devices and gateways.
5: Scope Coverage: Percentage of network components included in the pen test (e.g., gateways, end devices, network servers, and applications).	Target: 100% inclusion of critical infrastructure in the test scope.	Target: 100% inclusion of critical infrastructure in the test scope.
6: Threat Modelling Completeness: Number of potentials attack vectors identified	Comprehensive mapping of physical, network, and application-layer threats.	Requires ongoing monitoring of laws, regulations and protocols.

and incorporated into the testing plan.		
7: Compliance Preparation: Verification readiness against regulatory and industry standards (e.g., LoRa Alliance specifications, OWASP IoT Top 10).	100% alignment with applicable standards.	
8: Testing Efficiency: Percentage of planned tests executed within the allotted time frame.	Completion of all planned tests on schedule.	
9: Tool Utilization Rate: Effectiveness of specialized tools like RF analysers, packet sniffers, and vulnerability scanners in detecting issues	Detection of all vulnerabilities with minimal false positives.	
10: Exploit Success Rate: Percentage of identified vulnerabilities successfully exploited during ethical testing.	Exploit all critical vulnerabilities without disrupting business operations	
11: Critical Vulnerabilities Identified: Number and severity of vulnerabilities uncovered in areas like encryption and authentication.	Zero high-severity vulnerabilities post-mitigation	
12: False Positive Rate - Less than [5%] false positives. Ratio of reported vulnerabilities that are not actual threats.	Less than [5%] false positives.	
13: Time-to-Detection: Average time taken to detect vulnerabilities during testing.	Rapid detection, within the first half of	

14: Remediation Guidance Quality: Clarity and practicality of recommendations provided for mitigating vulnerabilities.	Actionable, detailed remediation steps for 100% of identified issues.	
15: Risk Mitigation Timeline - Time required to address and resolve vulnerabilities after the pen test.	All critical issues resolved within [one week] of reporting.	
16: Client Engagement: Level of collaboration with business stakeholders to ensure clear communication of risks and remediation plans.	High engagement and full understanding of reports by stakeholders.	

SPONSOR ACCEPTANCE

Approved by the Project Sponsor **<You can also use the client(s) instead of the sponsor, or one of the module team. Get your signatures in time – whoever signs this form has to have a chance to read the document before providing a signature. Change the title below if necessary, so it is clear who signed the form. It is important that you get a digital or real signature from the client or an external stakeholder of your project. Do NOT fake a signature.>**:

P.Be

____

Date: November 26th, 2024
Bennett, P.
PA Consulting

APPENDIX A: WORK BREAKDOWN STRUCTURE

INTRODUCTION

<The WBS is a view into the project which shows what work the project encompasses. It is a tool which helps to easily communicate the work and processes involved to execute the project. The Project Manager and project team use the WBS to develop the project schedule, resource requirements and costs. There are many ways you can present the WBS for your project; this template provides many of the most popular layouts from which you can choose. Depending on where in the Project Plan you're putting the WBS a different layout may be more suitable for you. For instance, many Project Managers include a high level WBS within the project plan, then a detailed version as an appendix to the plan. You may find that you prefer one layout for a high level WBS and a different one for a detailed WBS.

In order to save space in this template we only developed the WBS examples down to the third level and you do not need to exceed this. In a 'real' project you may want to develop the WBS down to a much more detailed level using the 8 to 80 rule, where appropriate (where the WBS is broken down to where a work package contains between 8 and 80 hours of work to complete). It is likely that you reach the 8 hours of work with 3 levels. Provide two different presentations of your WBS, one of them MUST be a tree structure. You are free to select the other presentation of your WBS (e.g., outline, hierarchical or tabular – see below). Remove the presentation formats below that you are not using. Also fill in the WBS Glossary of Terms as appropriate.

Replace the provided content for the WBSs with your own content.>

The Work Breakdown Structure presented here represents all the work required to complete this project.

The Work Breakdown Structure (WBS) represents all work required to complete this project, divided into sections containing smaller tasks, refereed to as "work packages."

OUTLINE VIEW

<The outline view presents an easy to view and understand layout for the WBS. It is also a good layout to use when developing the WBS because you can easily make changes, especially since the Microsoft Word auto numbering feature updates the WBS Code automatically. >

Tabular View

Level 1	Level 2	Level 3
1 Penetration Test	1.1 Planning and Setup	1.1.1 Initial meet with client 1.1.2 Confirm stakeholder expectations 1.1.3 Develop Project Plan + Charter 1.1.4 Plan schedule for Bi-Weekly sprints 1.1.5 Create outline of project 1.1.6 Set up LoRaWAN project
	1.2 Methodology	1.2.1 Processing Units 1.2.2 Memory 1.2.3 Firmware 1.2.4 Data Exchange Service 1.2.5 Internal Interfaces 1.2.6 Physical Interfaces 1.2.7 Wireless Interfaces 1.2.8 User interfaces
2 Deliverables	2.1 Continuous deliverables	2.1.1 RAID log 2.1.2 Activity Log
	2.2 Deliverables	2.2.1 1-hour presentation 2.2.2 Tentative presentation 2.2.3 Academic report 2.2.4 Vulnerability disclosure report

Glossary of Terms

Level of Effort: Level of Effort (LOE) is how much work is required to complete a task.

WBS Code: A unique identifier assigned to each element in a Work Breakdown Structure for the purpose of designating the elements hierarchical location within the WBS.

Work Package: A Work Package is a deliverable or work component at the lowest level of its WBS branch.

WBS Component: A component of a WBS which is located at any level. It can be a Work Package or a WBS Element as there's no restriction on what a WBS Component is.

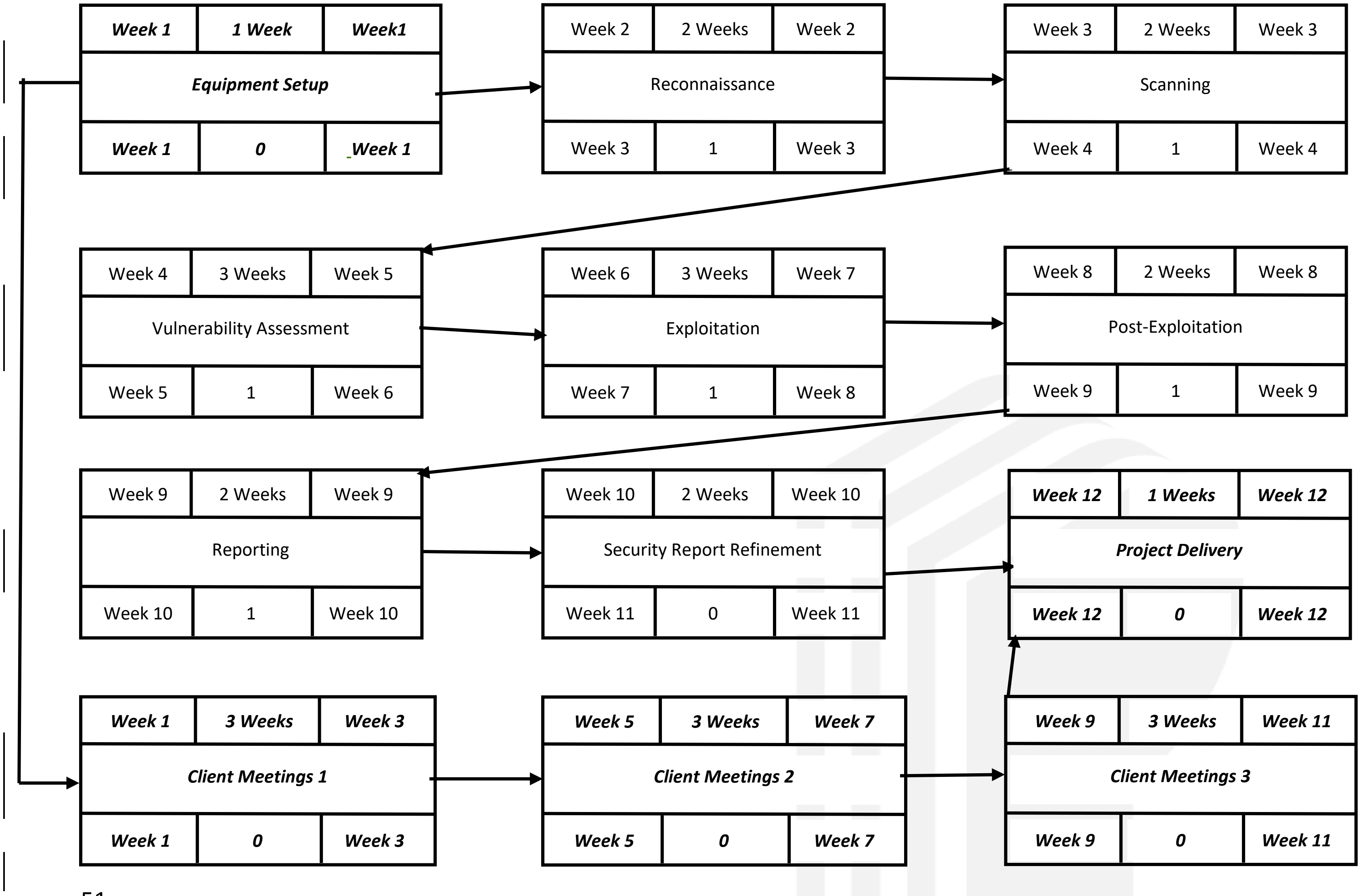
WBS Element: A WBS Element is a single WBS component and its associated attributes located anywhere within a WBS. A WBS Element can contain work, or it can contain other WBS Elements or Work Packages.

APPENDIX B: GANTT CHART AND PRECEDENCE NETWORK

GANTT CHART <to change the colour in a given cell, if you wish, right-click in the cell and select the shading icon; then choose the respective colour indicating the team member who is doing the work indicated in the table in the relevant week.>

Time Activity	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Week 10	Week 11	Week 12
Reconnaissance		Annie	Annie									
Scanning			Ben	Ben								
Vulnerability Assessment				Issac	Issac	Issac						
Exploitation						Ryan	Ryan	Ryan				
Post-Exploitation								Joey	Joey			
Reporting									Mattia	Mattia		
Equipment Setup	Full Team											
Client Meetings	Full Team		Full Team		Full Team		Full Team		Full Team		Full Team	
Security Report Refinement										Full Team	Full Team	
Project Delivery												Full Team

Precedence Network with Identification of Critical Path



Week 1	***1 Week***	***Week1***
	Equipment Setup	
Week 1	***0***	***Week 1***

Week 2	2 Weeks	Week 2
	Reconnaissance	
Week 3	1	Week 3

Week 3	2 Weeks	Week 3
	Scanning	
Week 4	1	Week 4

Week 4	3 Weeks	Week 5
	Vulnerability Assessment	
Week 5	1	Week 6

Week 6	3 Weeks	Week 7
	Exploitation	
Week 7	1	Week 8

Week 8	2 Weeks	Week 8
	Post-Exploitation	
Week 9	1	Week 9

Week 9	2 Weeks	Week 9
	Reporting	
Week 10	1	Week 10

Week 10	2 Weeks	Week 10
	Security Report Refinement	
Week 11	0	Week 11

Week 12	***1 Weeks***	***Week 12***
	Project Delivery	
Week 12	***0***	***Week 12***

Week 1	***3 Weeks***	***Week 3***
	Client Meetings 1	
Week 1	***0***	***Week 3***

Week 5	***3 Weeks***	***Week 7***
	Client Meetings 2	
Week 5	***0***	***Week 7***

Week 9	***3 Weeks***	***Week 11***
	Client Meetings 3	
Week 9	***0***	***Week 11***

APPENDIX C: RISK ASSESSMENT

TOP THREE RISKS

<It is important to explicitly state the top three risks to the project. This will make management aware of the top risks for the project and the nature of the risks. You should also address the other risks that you have identified and describe how you address (e.g., how you mitigate, avoid etc.) all risks. Use the Risk Probability Matrix below to calculate the ranking of risks. Replace the risks with your own.>

The top three high probability and high impact risks to this project are:

R1. Risk: Suitable Equipment
Challenges:
The effectiveness of a LoRaWAN deployment hinges on the selection of appropriate hardware, including gateways and IoT devices. Using equipment that is incompatible with the business's needs or the Scottish environment can lead to network failures, increased maintenance costs, and inefficiencies. The IoT devices have been supplied to the Project by PA Consulting Group.
Mitigation Strategies:

- Ensure the devices and gateways are (i) LoRa Alliance-certified to ensure compatible with the LoRaWAN protocol; and (ii) comply with the UK IoTCode of Practice.
- Use CVE3.0 calculator to rank and evaluate vulnerabilities exposed through penetration testing taking into account various categories of exploitation techniques and scoring them from 1 (low impact) through to 10 (high impact).
- Research to assist PA Consulting Group to only use reputable suppliers offering warranties and after-sale support to ensure replacements and repairs if needed.

R2 Fiber Optics Connection Not Completed
Due to construction delays in installing the fiber optic cable between the data center and the headquarters facilities users will not have a high speed connection between their site and the datacenter resulting in slow responses from the application making it unusable. The Project Manager will implement a site to site broadband Ethernet radio network between the data center and headquarters facility.

R3 Network Operations Center (NOC) Not Appropriately Staffed
Due to lead times associated with hiring and training additional staff, the NOC does not have the necessary staff to monitor the additional bandwidth associated with the

project resulting in a delay to the project schedule. The project manager will mitigate this risk by working with the NOC to create an alternate work schedule to compensate for the staffing shortage until additional staff hiring and training is complete.

Other risks identified and how they are addressed are: **< indicate how you address these.>**

R4: Business Continuity
Challenges: Here is an ever-evolving threat landscape. Failure to spot, prevent and deal with threats and risks can cause significant loss to the business and even delay or halt

operations [see section 6 Costs and Benefits Template and Cost Management Presentation Slide].

Mitigation Strategies:

- Redundancy: Deploy multiple gateways with overlapping coverage to ensure uninterrupted service in case of failure.
- Robust Infrastructure: Use reliable and reputable vendors and equipment.
- Monitoring Systems: Implement real-time network monitoring to identify and resolve issues promptly.
- Backup Connectivity: Use dual backhaul options (e.g., cellular and Ethernet) to maintain connectivity during disruptions.
- Training: Introduce an ongoing training and awareness program across the business so staff are vigilant to avoid risks.

R5: Data Loss Prevention

Challenges: LoRaWAN networks transmit sensitive data that may be vulnerable to breaches or transmission errors. Data loss or corruption can compromise operations and lead to regulatory penalties under GDPR.

Mitigation Strategies:

- Encryption: Use AES-128 encryption to protect data during transmission.
- Data Backups: Store data redundantly on secure cloud servers or local systems.
- Access Control: Implement strong authentication protocols to prevent unauthorised access.
- Compliance Audits: Conduct regular audits to ensure adherence to GDPR and security standards.
- Blocking specific information from being copied outside the company.
- Monitoring information being sent outside of the company.
- Encrypting USB devices information so that it can be read on company laptops and desktops only.
- Introducing an escalation process for Data Loss Prevention (DLP) alerts.
- Drafting a playbook for detection and incident response.

Risk Probability-Impact Matrix

Probability of Risk

Probability of Risk	Low	Moderate	High
High		R1	R2
Moderate		R4, R5	R3
Low			

Impact of Risk

APPENDIX D: QUALITY METRICS

Based on the Project Sponsor's requirements, the following metrics have been enacted for the LoRaWAN project. These metrics have been approved by the LoRaWAN team:

a. **Security Metrics**: A list of security measures will be used to measure the quality of the device's verse threat actors. Utilizing a Packet Integrity Rate of at least 99.5% will ensure there are no packet disruptions with the devices. Anything below this threshold could suggest a fault in the machine or a disruption in the security. On top of this, whenever a device is pinged there should be proper ping replay logged to ensure the device is documenting attacks onto it. Finally, ensuring that the device authentication process is properly secure and working with valid credentials will be used as a metric during testing.

b. **Network Performance Metrics**: Due to the importance of networking within LoRaWAN devices a Network Performance metric is of great use to the team. Measuring the Packet Delivery Ratio, the fraction dictating a ratio between sent and received packets, is a good indicator to the health of the system. For this testing purpose, a percentage above 95% would be an acceptable margin for the team to hit on these devices. Other factors involved in the network metric will be the latency of the devices as well as the rate at which the devices throw error messages at the testers.

c. **Compliance Metrics**: The standard at which the team will use to conduct their testing through is the official LoRaWAN standards. These LoRaWAN standards are listed in the official LoRaWAN documentation, linked here.
User Metrics: Lastly, the standard at which the devices function with end users will be tested during the entirety of the team's time allocated with these devices. The alerts that end users are given, as well as their functionality as the testing is conducted will be of utmost importance for the team and thus a user account will be always logged in as the team tests the system.

Metric	**Standard**	**Frequency**	**Report**
Security	>=99.5% PIR	Per device	Monthly Quality Management Review (QMR)

Network Performance	>=95%PDR	Entire Network Average	Monthly QMR
Compliance	Maximum 1 Compliance break	Entire Network	Monthly QMR
User	Maximum 3 User Errors.	Per device	Monthly QMR

REFERENCES

<You can list the references by section, so it is clear which student has used which reference, as a student is working on a defined set of sections. Use Harvard referencing style, and also put your reference in the body of the text (Author, Year). >

References for Section 1. Executive Summary
<list references>

References for Section 2. Business case analysis team and stakeholders
<list references>

Etc….