

George Mason University

Cyber security Engineering (CYSE) 492/493 Two-Semester Senior Design Capstone

Sponsor Handbook

Rev 1

March 2021

**Table of Contents**

[1](#_gjdgxs) Executive Summary 1

[2](#_30j0zll) Statement of Objectives 1

[3](#_1fob9te) Customer Provided Materials and Information 1

[4](#_3znysh7) Project Deliverables 2

[5](#_2et92p0) Terms and Conditions 3

[5.1](#_tyjcwt) Work Location 3

[5.2](#_3dy6vkm) Best Effort Basis 3

[5.3](#_1t3h5sf) Handling of Restricted Data 3

[6](#_4d34og8) Proposal Guidelines and Requirements 3

[6.1](#_2s8eyo1) Section 1: Executive Summary 4

[6.2](#_17dp8vu) Section 2: Description of the Problem 4

[6.3](#_3rdcrjn) Section 3: Objectives 4

[6.4](#_26in1rg) Section 4: Technical Approach 4

[6.4.1](#_lnxbz9) Section 4.1: Requirements 4

[6.4.2](#_35nkun2) Section 4.2: Risks 4

[6.4.3](#_1ksv4uv) Section 4.3: Design Constraints 5

[6.4.4](#_44sinio) Section 4.4: CONOPS 5

[6.4.5](#_2jxsxqh) Section 4.5: Architecture 5

[6.4.6](#_z337ya) Section 4.6: Data Model 5

[6.4.7](#_3j2qqm3) Section 4.7: Verification Method 5

[6.4.8](#_1y810tw) Section 4.8: Expected Results 6

[6.4.9](#_4i7ojhp) Section 4.9: Tasks 6

[6.5](#_2xcytpi) Section 5: Equipment and Facilities 6

[6.6](#_1ci93xb) Section 6: Deliverables 6

[6.7](#_3whwml4) Section 7: Cost and Management Proposal 6

[6.7.1](#_2bn6wsx) Section 7.1: Organization Chart and Qualifications 6

[6.7.2](#_qsh70q) Section 7.2: Work Breakdown Structure (WBS) 7

[6.7.3](#_3as4poj) Section 7.3: Project Schedule Example 8

[6.7.4](#_1pxezwc) Section 7.4: Project Cost 9

[Appendix A: Customer’s Technical Specifications 11](#_49x2ik5)

# Executive Summary

Lockheed Martin (LM) Space, the Sponsor, provides large scale and complex systems to the US Government and other customers. In the course of these activities the management and security of extensive enterprise networks and IT solutions is frequently a task. As such, Cybersecurity risks to the supply chain and other critical systems are a significant concern of ours and our customers.

Recent research has shown that Microsoft’s Cortana product has been “caught” listening to, recording and even transmitting sounds and conversations in the vicinity of devices where is it installed. The Sponsor is interested in understanding the potential security risks and extent of the attack surface/vulnerabilities regarding this issue.

This project facilitates the exploration and assessment/vulnerability research with regard to Cortana and systems to which it is deployed. Additionally, the project also enables the development of methods to secure/mitigate any concerns regarding the use of Cortana in enterprise network devices. To that end, the Sponsor desires to better understand Cortana’s behavior with a reversing report, including any potential vulnerabilities discovered.

# Statement of Objectives

The Supplier shall utilize reverse engineering, binary analysis, and penetration testing techniques to identify intentional (i.e. backdoor) and/or unintentional (i.e. vulnerable code) security flaws in the software identified. The Supplier shall also utilize software engineering and development practices, skills and techniques to produce a software tool (s), deliverable to LM, which can perform mitigation tactics regarding the operation of Cortana and it’s vulnerabilities.

This project is broken into three phases:

1. Develop the process, tooling, and workflow to enable rapid identification of Cortana files and behaviors, including vulnerabilities.
2. Document findings and vulnerabilities including proof of concept demonstrations of discovered behaviors.
3. Develop a prototype/tool(s) that mitigate a selected subset of the identified vulnerabilities by prevention or rerouting of any audio data collected.

The Supplier shall deliver a document describing their approach, processes, tooling, and workflow for reversing report and vulnerability identification as well as the code developed. Using this approach, the Supplier shall prove its effectiveness through the identification of vulnerabilities.

The objectives for this project can be enumerated as follows:

* Phase 1 Objectives:
  + Develop an end-to-end workflow to enable rapid identification of new vulnerabilities. Automation is encouraged as long as it is repeatable across a broad array of test devices. The developed vulnerability research workflow should leverage industry standard free and open source software (e.g. Ghidra, GDB, Wireshark, etc.) to the greatest extent possible. New tools, wrappers, and glue-code scripts may be developed to support automation.
  + The workflow tooling should include both static and dynamic tools in support of reverse engineering the System Under Test (SUT).
  + The team will be provided with the previous teams notes and deliverables and are expected to utilize them catch up and then advance understanding of Cortana.
* Phase 2 Objectives:
  + Identify vulnerabilities within the SUT(s) selected by the Sponsor and develop proof of concept source code/scripts to demonstrate behaviors and vulnerabilities..
  + All vulnerabilities found should be documented with at least the following information:
    - Summary description of identified vulnerability
    - Vulnerability Type (e.g. Denial of Service, static password, authentication bypass, arbitrary code execution, unauthenticated open port, etc.)
    - Impact statement categorizing the risk associated with the vulnerability
    - Affected OS Versions/Platforms
    - Recommended mitigation
    - Vulnerability details. Include hex dumps, assembly code, screenshots, PCAP extracts, etc. that walk the reader through the details of what the vulnerability is, how it was identified, and how it manifests
    - Test Plan – including test environment diagram, dependencies, test tools, and any caveats.
    - Test Procedures/Exploitation methodology – Describing step-by-step the proof of concept exploitation of the vulnerability. Include script extracts, screenshots, and commands used to enable exploitation.
  + Desired: Vulnerabilities should be new and not previously disclosed (i.e. 0-day vulnerabilities)
* Phase 3 Objectives:
  + Identify/Down-select a subset of behaviors and potential vulnerabilities from preceding phases

Design and develop prototype code leveraging the selected vulnerabilities which allows a user optional prevention or rerouting of any audio data collected by Cortana.

# Customer Provided Materials and Information

There are no unique hardware, software or data needs for this project. All software to support development activities should be available open source. Technical skills needed for this project include software development (C/C++ programming). The Sponsor will provide materials from the last team in effort to accelerate progress.

# Project Deliverables

The student team shall generate a project plan and associated deliverables that are appropriate for the project. The following deliverables are required for this project. Each deliverable is identified by their Contract Line Item Number (CLIN).

1. CYSE 492/493 Deliverables

| CLIN | Deliverable | Due Date |
| --- | --- | --- |
| CLIN-1 | Customer Reporting “Quad Pack” (Monthly Report) | Monthly |
| CLIN-2 | Weekly Activity / Time Sheet (Weekly Report) | Weekly |
| CLIN-3 | Technical Approach: Color Team Briefing | Early-Fall |
| CLIN-4 | Proposal (Response to this RFP) | Mid-Fall |
| CLIN-5 | Design Review Briefing | Late-Fall |
| CLIN-6 | Sage Article | Mid-Spring |
| CLIN-7 | Poster | Mid-Spring |
| CLIN-8 | Team Sage and Sponsor Presentation | Late Spring |

1. Sponsor Project-Specific Deliverables

| CLIN | Deliverable | Due Date |
| --- | --- | --- |
| CLIN-9 | Reversing Process for Systems Used | Mid Fall |
| CLIN-10 | Reversing report including vulnerabilities. | Late-Fall |
| CLIN-11 | Source Code and Completed/Compiled Tool | Early Spring |
| CLIN-12 | Final Report and Team Presentation | Late Spring |
| CLIN-13 | Final Product Specifications (hardware, software) | Late Spring |

# Terms and Conditions

This section covers the terms and conditions between the Sponsor Company and the University and its faculty / students.

## Work Location

Projects will be performed at George Mason University, Fairfax, VA, unless other arrangements have been negotiated. This includes virtual project work performed in remote student locations in accordance with current George Mason University policies and guidance.

## Best Effort Basis

This work scope is to be performed on a best effort basis.

## Handling of Restricted Data

Students, faculty, and administration are prohibited from signing any Intellectual Property agreements or Non-Disclosure agreements. These are University policies and there are no exceptions. No project work may include elements that are deemed For Official Use Only, Proprietary, Sensitive, or Classified. Posters will be publicly displayed and Project Notebooks will be publicly available. The Sponsor has the right to specify that their project team be comprised of US citizens; however, this does not imply allowance of Import/Export restricted information flow. Students nor faculty nor administration can receive ITAR restricted information or data. Should a company require approval of the Poster or other materials before public display, it is the responsibility of the Sponsor to ensure that such approval is secured in a proper and timely fashion and according to the requirements of the Sponsor's firm. Sponsoring companies must assume widespread discrimination of provided technical and project information. This includes other students, faculty, administration and even competitors in the marketplace as this is a totally open project. In any event, GMU shall be held harmless for the public display of project materials.

# Proposal Guidelines and Requirements

Provide a detailed description of the project requirements, technical approach, and deliverables. Use tables and figures to demonstrate your understanding and describe the approach. Teams are encouraged to incorporate iterative, agile lifecycle approaches especially in cases where exact outcomes are difficult to define at the beginning of the project. Examples are shown in the subsequent sections. Student teams must include the types of information shown but may modify format and add details as desired.

The student team shall provide a response to this RFP using the outline specified below. **Refer to the example template posted with the Blackboard Assignment.** The student team shall deliver the proposal response in a PowerPoint format with the following recommendations:

* Title Slide should include Project Name, Sponsor Company, Team Name with each student name listed
* Font should be easily readable; at least 12-point (Times New Roman) or 11-point (Calibri) or 10-point (Arial)
* Each slide should be numbered (except for the Title Slide)
* Each slide should include the name of the student who authored the specific slide

## Section 1: Executive Summary

**[1 Slide]** Describes your entire project, why it is important, and the approach/solution.

## Section 2: Description of the Problem

**[1 Slide]** In your own words, describe the problem the Sponsor has asked you to solve. Explain WHY the problem is a concern and what critical impacts it will have if unresolved. Answer WHY the solution is important to the Sponsor.

## Section 3: Objectives

**[1 Slide]** List 3-5 project objectives (or goals). Consider the objectives to be the criteria or goals of success and not a list of activities or tasks. Objectives should be SMART:

* **Specific.** Enough detail to be meaningful (e.g., identify 100% of known vulnerabilities vs. identify majority of vulnerabilities).
* **Measurable.** Can we verify that we met the goal through testing, demonstration, reporting, etc.?
* **Acceptable.** Does the sponsor support the goal? Does it align with the RFP?
* **Realistic.** Can the team feasibly accomplish the goal?
* **Timebound.** When will the goal be completed?

## Section 4: Technical Approach

This is the heart of the proposal: you must convince the sponsor that your technical approach is credible. Make an extra effort to make it easy for your Sponsor to to evaluate your response against their requirements point by point. This section must include:

### Section 4.1: Requirements

**[1 Slide]** Requirements are usually “shall” or “user story” format. Requirements are the key drivers or characteristics of the project and do not detail a specific solution or technology. Provide the top 5-10 project requirements.

### Section 4.2: Risks

**[1 Slide]** Identify top 3-5 risks for your project and define:

* + **Likelihood:** What is the chance the risk will occur?
  + **Impact:** What is the severity or damage to the project if the risk does occur?
  + **Mitigation:** What will be done to either reduce the risk or mitigate the risk if it occurs?

Risks should be worded as “If/Then” statements (e.g., IF X occurs, THEN Y will be the effect).

### Section 4.3: Design Constraints

**[1 Slide]** Identify the major design constraints for your project and keep them in mind as you develop your solution. Design constraints are not the same as requirements. Design constraints can specify technologies, locations, and methodologies/implementations. Some design constraints are negotiable.

### Section 4.4: CONOPS

**[1-2 Slides]** According to the Institute of Electrical and Electronics Engineers (IEEE), the Concept of Operations (CONOPS) is a user-oriented document describing system characteristics for the proposed system from the user(s) perspective. Examples of users are cyber analysts, penetration testers, auditors, medical staff, warfighters, executives, etc. In 1 or 2 slides, show the primary user(s) and how they interact with the system. This can be described in steps, in a diagram, or a combination. It is important to clearly show how the user will use the system or the solution you are proposing.

### Section 4.5: Architecture

**[1-3 Slides]** In 1 or 2 diagrams, show the system elements and how they interact. Your architecture should include:

* **Elements** (boxes on your diagram): Tools, components, functions/modules, data sources, external systems
* **Interfaces** (lines on your diagram): Physical connections, network connections, logical connections, information exchanges
* **Description of your interfaces:** What is flowing (data type, size)? Is it bidirectional (one or two way)? What periodicity (how often)?
* **Security:** Ensure that you show how your system is secured. Examples include scanners, filters (FW/IDS/IPS), protocols, analytics, etc.

### Section 4.6: Data Model

**[1-2 Slides]** Show 1 diagram that shows the project information elements (structure, relationships external information sources). The intent is to show how information elements are structured and defines a relationship between information elements.

### Section 4.7: Verification Method

**[1 Slide]** Describe what verification methods the team intends to implement to prove that the solution meets the requirements. Describe if multiple verification events are planned (e.g., internal test in December, demonstrations in January and March) and who will be involved.

### Section 4.8: Expected Results

**[1 Slide]** Create a short list (3-5 items) that describe the major engineering outputs. What is considered success and what will be delivered?

### Section 4.9: Tasks

**[1 Slide]** List and describe the major tasks or phases your team will execute to complete the project. Tasks must align to the WBS and Schedule.

## Section 5: Equipment and Facilities

**[1 Slide]** Identify needs equipment and/or facilities required to perform your tasks. For example, if you require specific hardware, software, licenses, etc., they should be listed here along with the rationale why. If costs are associated with these needs, those should be detailed in *6.7.4 Section 7.4: Project Cost*.

## Section 6: Deliverables

**[1 Slide]** Identify and describe the deliverables you will deliver throughout the project lifecycle.

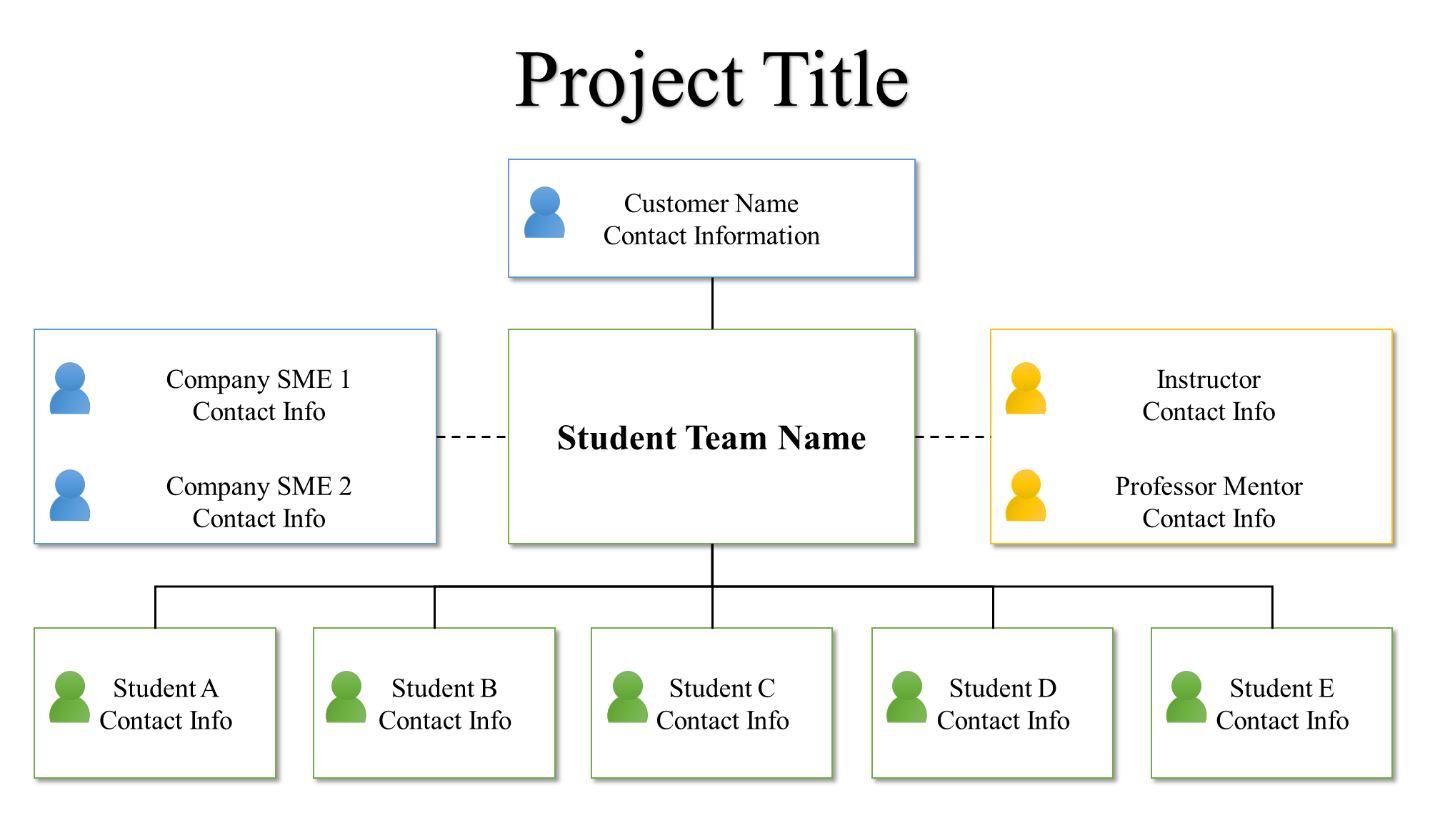
## Section 7: Cost and Management Proposal

This section translates the technical approach into an executable plan. This section must include:

### Section 7.1: Organization Chart and Qualifications

Student teams should provide:

1. **[1 Slide]** A visual Organization Chart (as shown in the example below)
2. **[1 Slide]** A short bio for each team member



**Figure 1: Organization Chart Example**

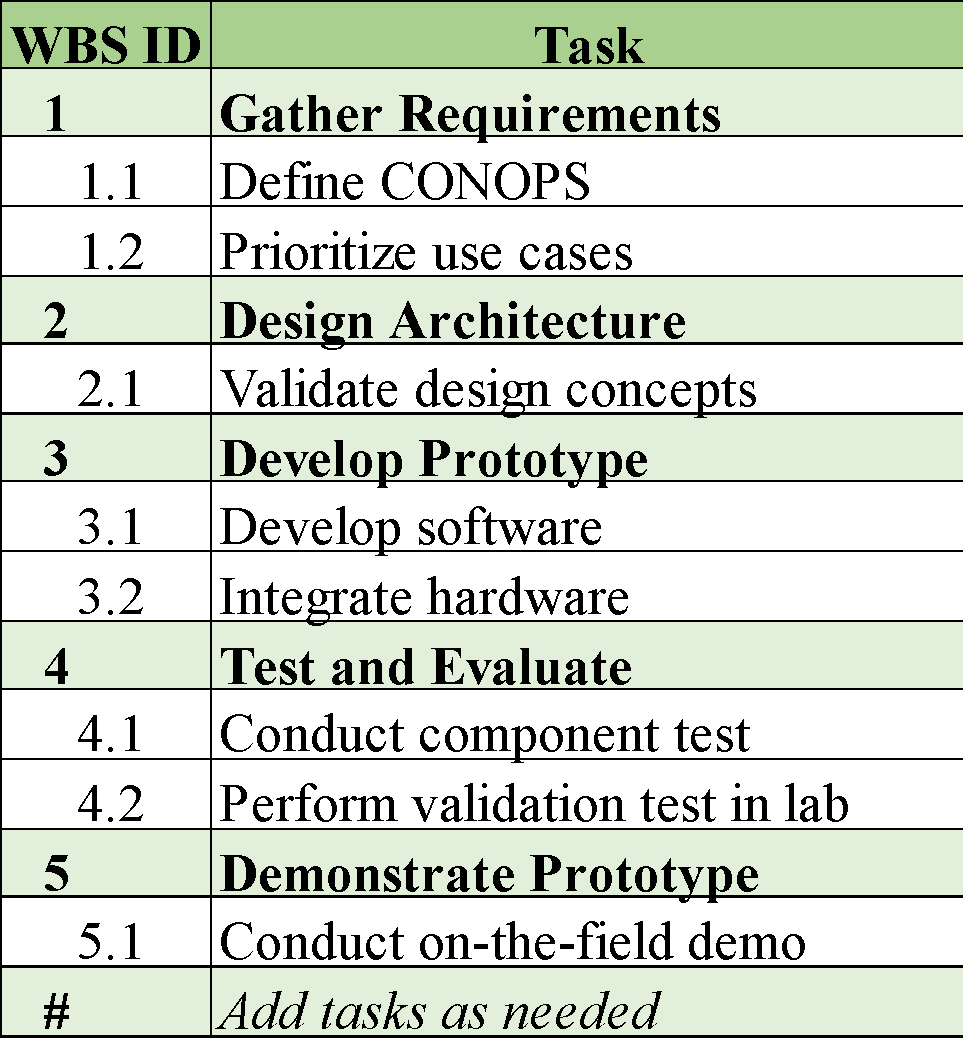
Student Bios: Provide a “bio” for each team member. Limit student bios to a short paragraph, summarizing skills and achievements. Include information such as current student grade (i.e., Junior or Senior), anticipated graduation date, prior cybersecurity experience, and aspirations / interesting facts. Also indicate the weeks each student will serve as team leader.

### Section 7.2: Work Breakdown Structure (WBS)

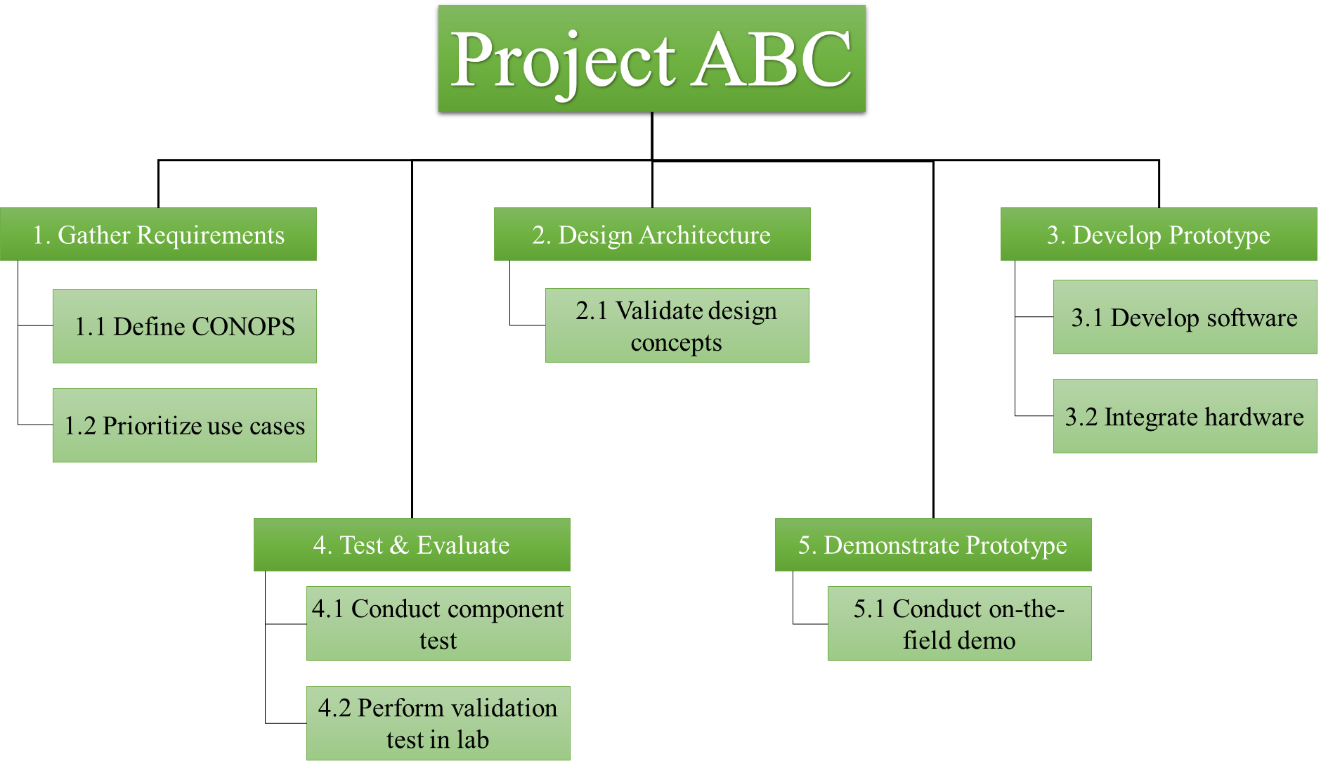
**[1 Slide]** The WBS should show the tasks the team will execute to implement your design. Add additional levels of detail (sub-tasks) to fully define the project plan. Elements in the WBS should include:

1. **WBS ID / Level:** Indicate main tasks and sub-tasks
2. **Tasks:** Major activities / phases of your project

The WBS can be visually displayed in different formats as shown in the examples below.

****

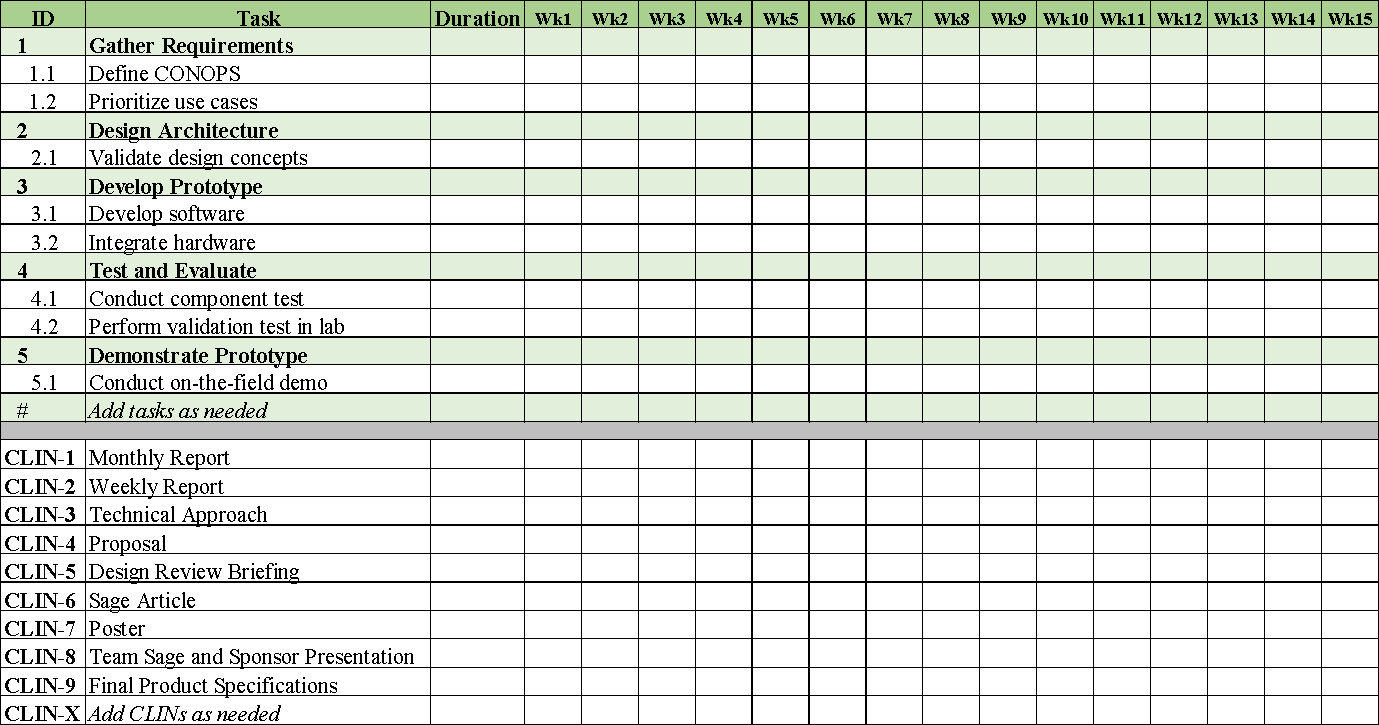
**Figure 2: Project WBS Example 1**



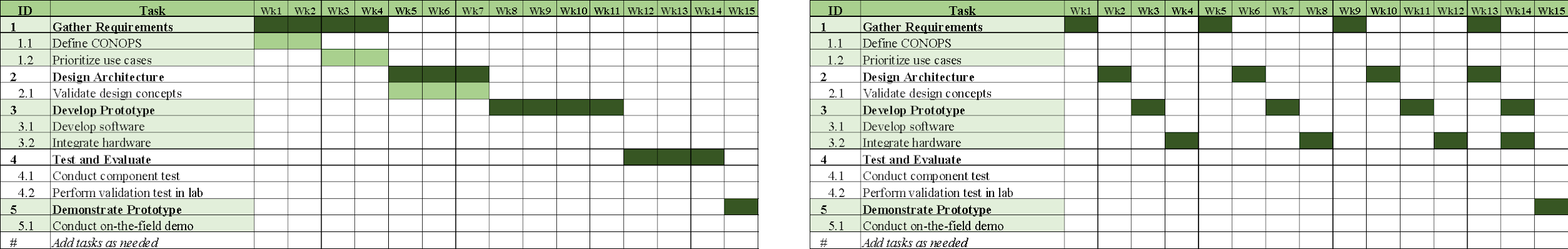
**Figure 3: Project WBS Example 2**

### Section 7.3: Project Schedule Example

**[1 Slide]** Project schedules should align to the WBS. In other words, the activities defined in the WBS should be the same in the schedule and map to a delivery date. Note that the schedule will need to span across both Fall and Spring Semesters. If the team is implementing an, iterative process, show the iterations in the schedule. See schedule examples below.



**Figure 4: Project Schedule Example**

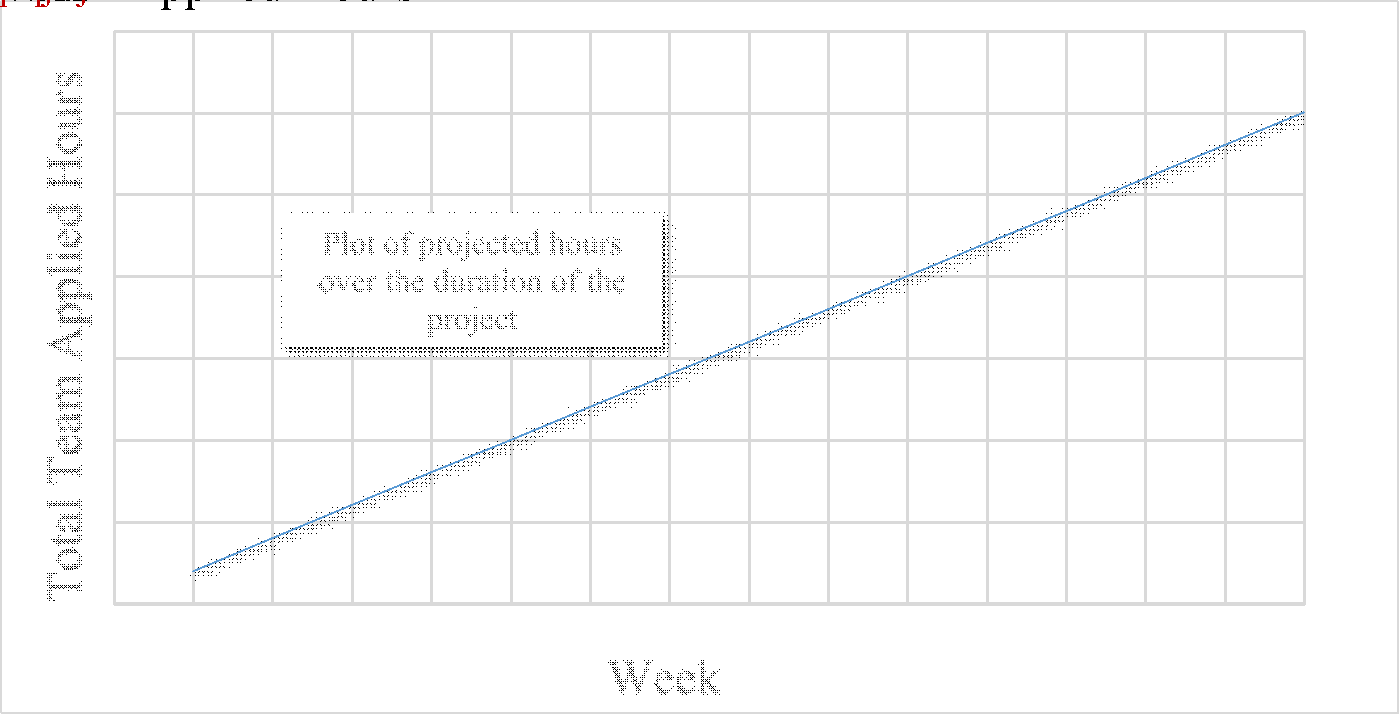


**Figure 5: Waterfall vs Agile Schedule View Example**

### Section 7.4: Project Cost

Student teams should provide the following:

1. **[1 Slide]** Weekly projected applied hours (see example graph)
2. **[1 Slide]** If applicable, provide estimated non-labor cost items separately. This includes any software, cloud computing resources, or other non-labor items.



**Figure 6: Project Cost Example – Applied Hours**

Provide a description of the cost as shown in the example below. If you listed a special item in *6.5 Section 5: Equipment and Facilities* it should also appear here if it requires a cost.

**Table 1: Example Non-Labor Project Costs**

| Item | Model | Cost | Vendor | Purchased by |
| --- | --- | --- | --- | --- |
| Azure Windows Server 2019 VM | F8s v2 CPUs 8 RAM 16 GiB | $250 / month | Microsoft | GMU |
| Azure Windows Server 2019 VM | Standard D2s v3 - 2 vcpus 8 GiB | $72 / month | Microsoft | GMU |
| CanaKit Raspberry Pi 4 | 4GB RAM | $100 | Amazon | GMU |

# Appendix A: Customer’s Technical Specifications

Insert any additional technical specifications required.