

CyberSecurity Essentials Semester Project

Instructor: William A Loring

Table of Contents

CyberSecurity Essentials Semester Project	3
Week 6 Milestone: Team Process	4
Week 7 Milestone: Network Baseline	6
Week 8 Milestone: Outline.....	10
Week 9 Milestone: Network Documentation	12
Week 10 Milestone: Risk Assessment Matrix	14
Week 11 Milestone: Risk Prevention & Mitigation.....	15
Week 12 Milestone: Rough Draft	16
Week 13 Milestone: Security Policies	17
Week 14: Milestone: Project Presentation.....	18
Week 16: Discussion on Project Presentation	20
Finals Week: Project Final Report Submission	20

CyberSecurity Essentials Semester Project

This is a case-based project. It is designed to be open-ended; you will have to do some research to figure out what to do. When you aren't sure what is expected, you should communicate with the instructor (customer). This type of project is designed to simulate real world conditions and problem solving. In the real world, you don't always have clear directions and expectations.

This is a group/team/final project. Experienced students will be paired with inexperienced students.

Each team will be working on the Final Report one assignment at a time over the course of the semester.

Don't Wait! This project is a major part of your grade, get started now!

Rationale for the project: Work in IT is rarely done alone. It is almost always done as part of a team. Presenting or selling an idea or plan is an important part of being in IT. An IT person is always persuading someone that change is good, the project or idea will benefit them, the change to the network will help productivity, make the network more secure, etc. Give reasons why this project will benefit the customer. This real-world project will help you synthesize and consolidate what you are learning in class and the lab activities.

Outlook Groups

An Outlook Group will be created for each Guild. This can be used to share documents, send email, and work collaboratively.

Outlook Group email is a requirement of this project. How professionally, how responsive, and how often you communicate is part of your individual evaluation throughout the semester project.

Please address all Semester Project asynchronous communication to the Outlook Group Email address shown in your Outlook Group. There is no need to include separate email addresses. Everyone's wncc.edu email address is already in the Group Email address.

Each Team has a similar Outlook Group Email address. The last number is the only thing that is different.

For example, if you are in Group 1: Loring-Networking-Group1

Using this address archives a copy of all email in the Groups feature in Outlook. You should see this group under Groups in Outlook. You can create new email messages from the Group.

Here is a video on how to use Outlook Groups. <https://youtu.be/DDG5n0QdvUg>

[How to Work with Word in Outlook Groups](#)

Assignments

Turn in your assignment early! This is meant to be an iterative process. Submit, feedback, improve assignment, repeat. All projects are works in progress; they are adjusted as the project moves forward. The instructor is your customer contact; part of your project is to find out what the customer wants. Communicate with the customer.

Assignment Submission: Each group assignment may be submitted 2 times, provided each submission is prior to the due date. It can be improved and resubmitted based on feedback from the instructor. That week's group leader is responsible for submitting the group assignment.

IT Project Components

IT projects typically have three main components:

- Where we are now?
- Where we want to be?
- How do we get there?

Minimum Requirements

Think of this document as setting out the minimum requirements for the project. As long as the minimum requirements are met in your assignments, you have license to be creative and go further than the assignments request.

Week 6 Milestone: Team Process

100 points

Time required: 60 minutes

1. **Read:** Creating Productive Teams
2. **Read:** Elements of a High Performing Team

3. **Read:** Team Charter

Do: Determine how your team will handle the following items.

1. Communication
 - a. Synchronous
 - i. Skype
 - ii. Zoom
 - iii. Video conference software of your choice
 - b. Asynchronous
 - i. Outlook Group Email
2. Collaboration on documents
 - a. Outlook Group (The instructor will create the group)
3. The team will create a list of the skills needed for the project.
 - a. Team skills
 - b. Computer skills
4. Each member will create a list of the skills they bring to the project.
 - a. Team skills
 - b. Computer skills
5. Team leader for the week
 - a. The team leader is not responsible for doing all the work, only organizing or getting everyone together.
 - b. Rotate between each member for team leader of the week.
 - c. A recommended practice is to set a schedule for team leader rotation at the beginning of the project.
 - d. The team leader is responsible for submitting the project assignment for that week.
6. Expectations for Team Members
 - a. Set your shared expectations for the Team

- b. Responsiveness
 - i. What are the expectations for response to communication?
- c. This is a collaborative team project.
 - i. It is not ok to say to the rest of the team: plan this week without me and let me know what I am supposed to do.
 - ii. Collaboration means each team member contributes equally.
- d. Deadlines for individual assignments
- e. Deadline for team assignments
- f. If these expectations are not met, ask the team member why
- g. If there is no response, move on without them
- h. Give an honest evaluation of individual performance with the evaluation

Assignment Submission

1. **Team Charter:** The Team leader submits the completed Team Charter in Blackboard.
2. **Team Individual Evaluation:** Each team member submits a Guild Individual Evaluation in Blackboard.

Week 7 Milestone: Network Baseline

Time required: 60 minutes

NOTE: Each person contributing to the document:

1. Highlight your text in a different color.
2. Put your name by the parts you worked on.

Business Case Scenario

Your team is a security consulting company. You have been hired to do a security audit for the West Mountain Logistics Company. You will gather the information needed to secure this network.

Company Scenario

This is a scenario you can work with. You can add to this scenario or create your own.

The West Mountain Logistics company is responsible for maintaining the level of small toys at many retail businesses. There are currently 25 employees, with expected growth to 50 in the next 2 years. They are also looking at adding large toys to their portfolio of services. Their network infrastructure is currently:

- Peer-to-peer network
- No backup
- None or shared passwords
- Consumer firewall
- No security awareness or training

In the past year, an employee lost 6 months of work because their computer failed and there were no backups. Another employee clicked on a phishing link in an email. Fortunately, only that employee's computer was compromised. The computer had to be cleaned and reinstalled. Again, no backups, 12 months of work was lost.

As the company has grown, management of their network has become more time-consuming and much harder to secure. The employees don't always know where their files are, and much work is duplicated. Anti-virus software is installed and managed individually on each workstation.

This assignment is an inventory of everything currently at the business. This is where the business is now. Insert information and/or screenshots into your main document as necessary. A table would be a good way to organize the information. This is an audit and evaluation of the security posture of this company.

What do they currently have?

Asset Inventory

1. You might want to use Excel for this.
2. How many, specific makes, models, specifications, date of purchase, OS, Service Pack level, Firmware, etc. of workstations, servers, switches, routers, security cams, copiers, wireless access points, anything connected to the network, etc.

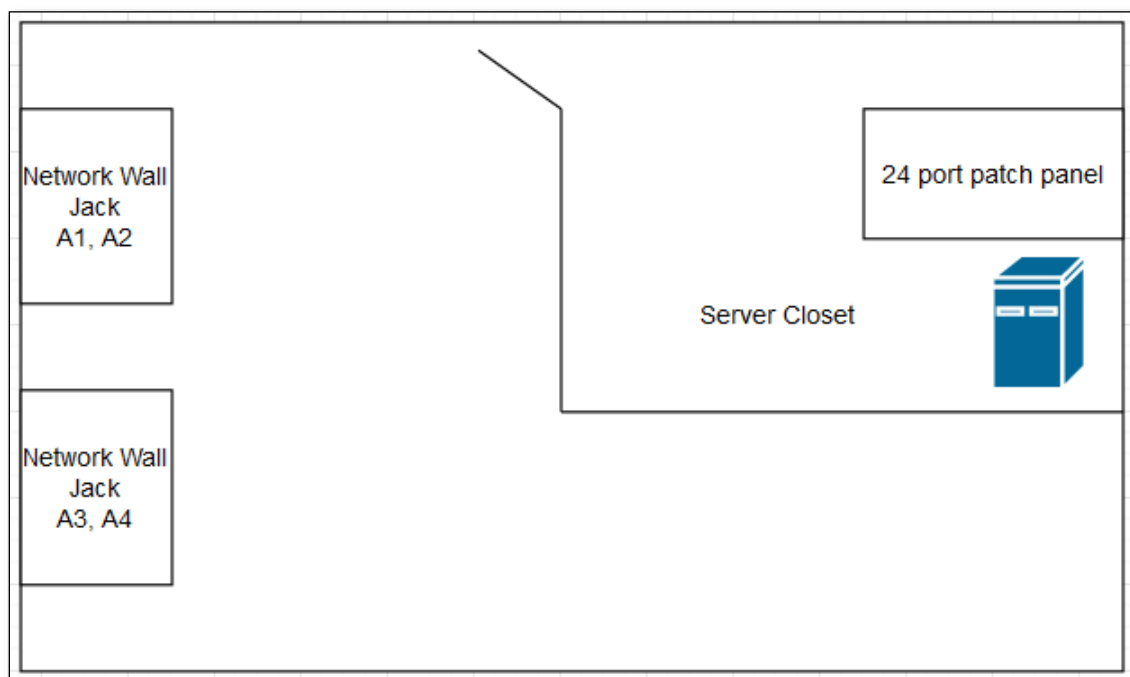
Qty	Item	Description	
-----	------	-------------	--

24	Dell Optiplex 1400 Window 7 Home edition	10 years old	
1	Old Netgear 100 MB switch		

Physical network wiring map

Create a diagram, overhead floor plan view of the building or room with data closet, servers, networking devices, and wall jacks located and labeled. You do not have to put in the client machine's physical locations.

<https://app.diagrams.net> was used for these drawings. These are simple example ideas to get you started.

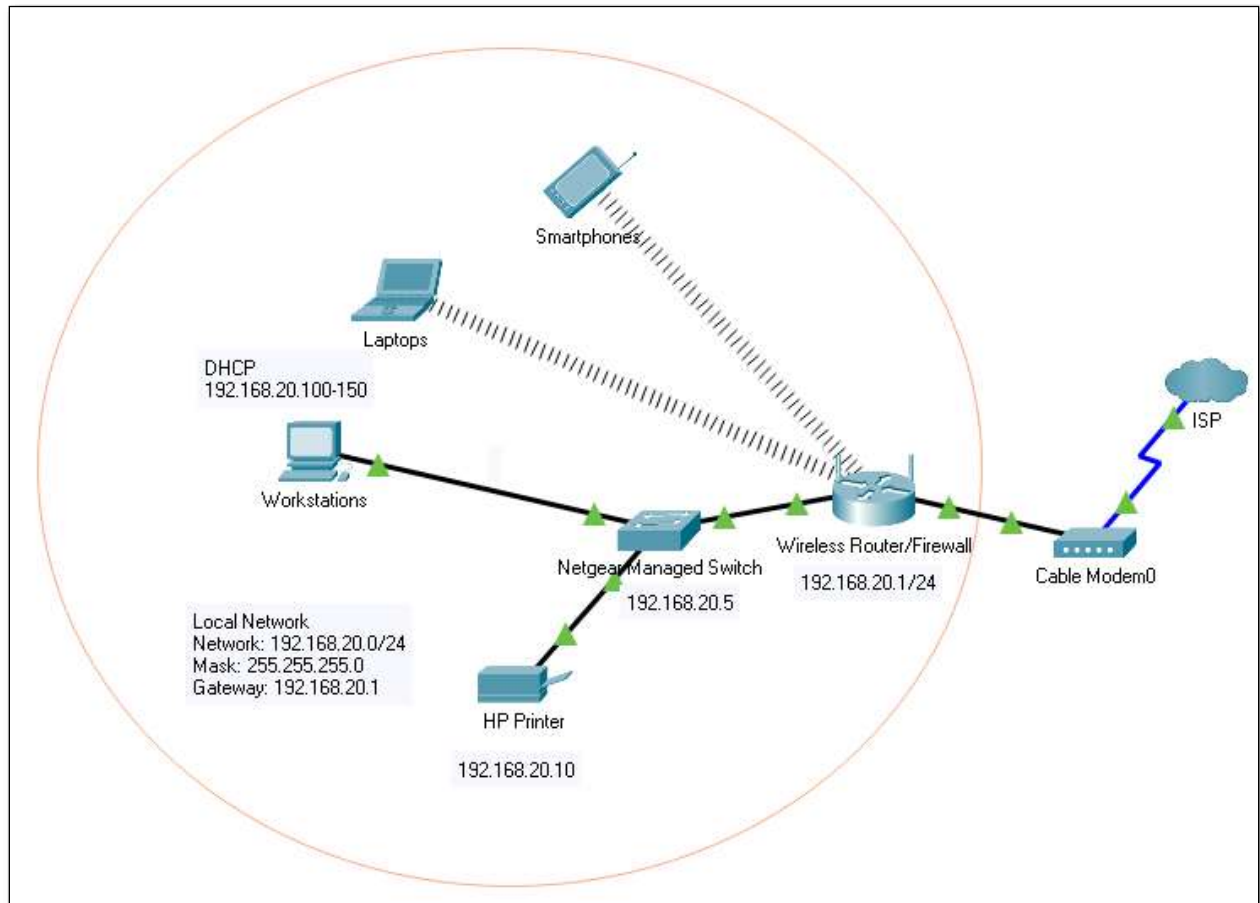


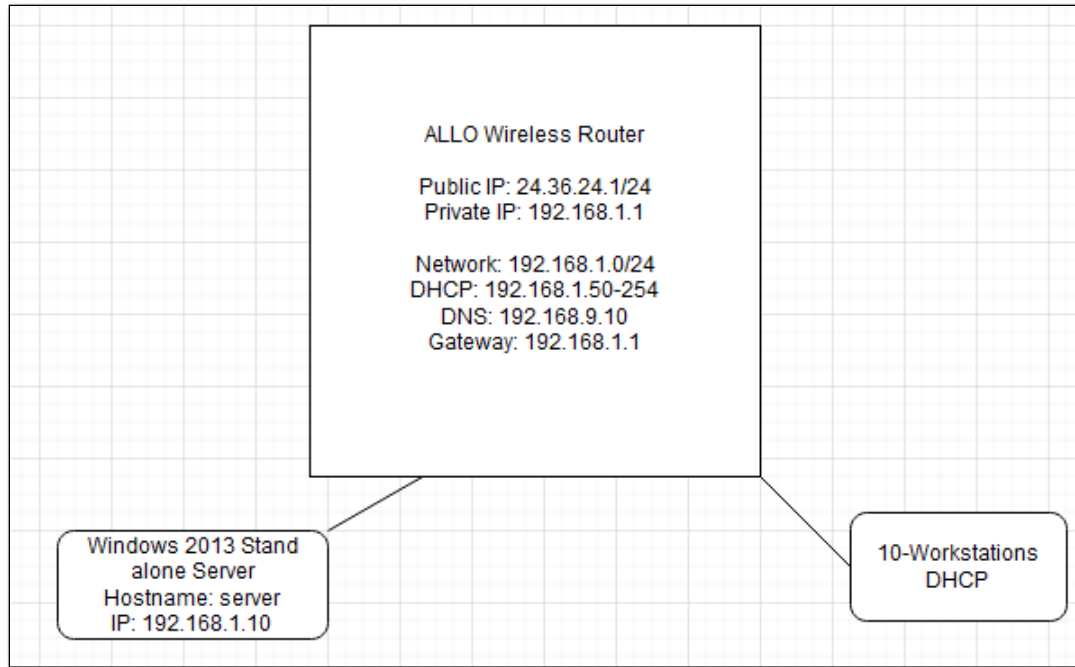
Logical Network Diagram

Packet Tracer would be a good choice to diagram the network settings. www.lucidchart.com has a free option for diagram software. You can also use yEd Graph Editor, Google Draw www.draw.io, SmartDraw Free, SmartArt in Word or any other diagramming software.

This includes a logical network diagram (Packet Tracer) that includes the switches, routers, servers, workstations, wireless access points, printers and IP addresses. You are not designing a new network; you are documenting it as it currently exists.

This example was done in Packet Tracer. It is missing the outside IP address.





1. Security software or hardware
 - a. Anti Malware, Anti Virus, firewall, Bitlocker, etc.
2. Security policies and procedures
 - a. A policy says what we do.
 - b. A procedure says how we do it.
 - c. Policies and procedures are managerial controls. They are guides to manage how people behave and interact with technology.
3. [Nmap](#), [Zenmap](#), or [Advanced IP Scanner](#) scan.

You can scan D1 if you wish. You can also scan your local network at home. Only scan a network that you have permission to scan.

Week 8 Milestone: Outline

100 points

Time required: 60 minutes

NOTE: Each person contributing to the document:

1. Highlight your text in a different color.
2. Put your name by the parts you worked on.

This week's milestone is creating an outline for your entire project. After this assignment is submitted, you can start filling in what you have completed. You should continue working on this document as this will turn into your rough draft. Your rough draft will turn into your final presentation.

This outline will include all the components of your project, whether you have completed that section or not. An outline just contains the high-level views and placeholders for future information.

An outline is just that, an outline. Don't start writing sentences, this is not a rough draft. Yet.

1. Research the components needed for a Security Assessment or Security Audit.
 - a. www.sans.org is a good place to start researching.
 - b. This pdf has some good information. <http://www.sans.org/reading-room/whitepapers/auditing/base-security-assessment-methodology-1587>
 - c. This web page has a good list of items to check in your assessment. <http://www.gfi.com/blog/the-ultimate-network-security-checklist/>
 - d. Google for security audit, security assessment, or assessment checklist.
2. Outline your Security Assessment.
 - e. How to outline. https://owl.purdue.edu/owl/general_writing/the_writing_process/developing_an_outline/types_of_outlines.html
3. Use the Project Final Report Outline section at the end of this document as a general guide.

Sample outline

This is a rough idea of the format an outline can have:

I. Main idea

A. Secondary or supporting idea to main idea I

B. Secondary or supporting idea to main idea I

1. Secondary idea to B

2. Secondary idea to B

a. Secondary idea to 2

b. Secondary idea to 2

II. Main idea

A. Secondary or supporting idea to main idea II

B. Secondary or supporting idea to main idea II

C. Secondary or supporting idea to main idea II

III. Main idea

4. Submit the assignment.

Week 9 Milestone: Network Documentation

100 points

Time required: 60 minutes

NOTE: Each person contributing to the document:

1. Highlight your text in a different color.
2. Put your name by the parts you worked on.

Network Documentation Template**WAN/Internet Settings**

WAN IP	
Subnet Mask	
Gateway	
DNS	
SMTP	
POP3	
IMAP	

LAN Settings

Domain	
Network	
Subnet Mask	
Gateway	
DNS	

IP Address Ranges

Routers	
Switches	
Servers	
Printers	
WAP	
Static Devices	
DHCP Range	

Static IP Devices

IP Address	Host Name	Description	Location
192.168.100.1			
192.168.100.2			
192.168.100.3			
192.168.100.4			
192.168.100.5			
192.168.100.6			
192.168.100.7			
192.168.100.8			
192.168.100.9			
192.168.100.100	DHCP		
192.168.100.149			

Router Configuration

External IP Address:	
Trusted IP Address:	
Optional/DMZ:	
DNS:	
Status Passphrase:	
Configuration Passphrase:	

1. Submit the assignment.

Week 10 Milestone: Risk Assessment Matrix

100 points

Time required: 60 minutes

NOTE: Each person contributing to the document:

1. Highlight your text in a different color.
2. Put your name by the parts you worked on.

This is the current state of security of the organization. This can be assessed by using a scale of 1-5 showing which areas are the most vulnerable.

- There should be a minimum of 10 risk items.
- Each item should be in one of the following three categories.
- These items should correspond with what you have discovered so far.

1. Managerial

- a. Nonexistent or poorly written policies and procedures.
- b. No end user security training.

2. Technical

- a. Out of date firewall firmware.
- b. Firewall improperly configured.

3. Operational

- a. Server room doesn't have a locked door.

	Risk Assessment Matrix Example	Low ----- High				
Risk	Description	1	2	3	4	5
Managerial	Nonexistent or poorly written policies and procedures				X	
Managerial	No end user security training					X
Technical	Out of date firewall firmware			X		
Technical	Improperly configured firewall					X

Operational	Server room doesn't have a locked door						X
-------------	--	--	--	--	--	--	---

Week 11 Milestone: Risk Prevention & Mitigation

100 points

Time required: 60 minutes

NOTE: Each person contributing to the document:

1. Highlight your text in a different color.
2. Put your name by the parts you worked on.

How do you propose to solve their problems and improve their security?

For each risk in your risk assessment matrix, there should be a specific prevention or mitigation strategy. You will want to align this assignment with your risk assessment matrix.

This would be a rough draft of these items.

1. Managerial

- a. Whether or not these policies are in your Risk Matrix, you will research and locate examples of these policies. You don't have to create them yet, just do the research and find examples.

- i. Acceptable Use Policy
- ii. Computer Use Policy
- iii. Password Policy
- iv. Email Policy
- v. Ethics Policy
- vi. Remote Access Policy
- vii. BYOD Policy

2. Technical

- a. Update the firmware on the firewall
- b. Configure the firewall in a secure manner
- c. Implement new password policies on the server
<https://technet.microsoft.com/en-us/magazine/ff741764.aspx>

3. Operational

- a. Put in a new lock on the server room door.

Week 12 Milestone: Rough Draft

150 points

Time required: 120 minutes

NOTE: Each person contributing to the document:

1. Highlight your text in a different color.
2. Put your name by the parts you worked on.

Use the Final Project Submission Minimum Requirements at the end of this document to create a rough draft.

Create these minimum recommended policies. These policies can be in one document. Templates can be located on the internet as examples.

- a. Acceptable Use Policy
- b. Computer Use Policy
- c. Password Policy
- d. Email Policy
- e. Ethics Policy
- f. Remote Access Policy
- g. BYOD Policy

Connect the scenario to the issues/risks to the solution/mitigation to the benefits. Here is an example.

Scenario: Lack centralized and regularly scheduled backup.

Issue: Data could be lost forever.

Solution: Migrate all data to a central server. Schedule nightly backup using Windows Server Backup. Use a scheduled rotation of portable hard drives on and offsite. Test backup on a regular basis.

Benefits: Reliable backup will avoid catastrophic data loss.

1. Put enough detail in each section to give the general idea of the project.
2. Write to a person without a technical background. No acronyms. If there are any acronyms, explain them.
3. Your rough draft should be in Microsoft Word. This assignment is an example of what it should look like.
4. Include a real table of contents with headings and page numbering.
5. Rough out all the parts of your project report.
6. All past milestones will be included, either in the report, or as a supporting separate document.
7. You may have to change some of your past work to align with the rough draft. We want a consistent project and document.
8. Complete a rough draft of your report.

Helpful Hint: This is a business document, don't use first person words like I. Example: (First person) I think I will install Microsoft Windows Server 2019. Better: Install Microsoft Windows Server 2019 from USB media.

This is a professional business document.

- Write clearly and concisely.
- Use short and to the point sentences. Less is more.
- Bullet points and numbered lists are appropriate.

Week 13 Milestone: Security Policies

100 points

Time required: 60 minutes

NOTE: Each person contributing to the document:

1. Highlight your text in a different color.
2. Put your name by the parts you worked on.

Use the examples of policies you found on the internet to write your own policies. Please modify the policies you choose for your organization. These policies can be in a single separate document referenced from the main document.

<https://www.sans.org/information-security-policy> is a good place to get started. You will also want to do some Googling.

Policies are management controls for the users.

At the minimum, please include the following policies:

- Acceptable use
- Access control
- Mobile device security
- Physical security
- Computer security
- Network security
- User Training
- On boarding and off boarding employees
- Any other policies you think are necessary for this business.

Week 14: Milestone: Project Presentation

200 points

Time required: 60 minutes

You are pitching your proposal to upper management. Sell them on the tangible benefits of your proposal. Be specific.

Fluff: This project will benefit your employees by helping them to be more efficient.

Specific and Tangible: A nightly backup of all data on the server with rotating media, a nightly cloud backup, and a physical copy offsite weekly, monthly, and yearly will reduce the possibility of data loss. Recreating data that is lost could cost your company \$2,000 or more in lost time.

1. Each member of the team should be heard equally in the presentation.
2. Please have the speaker showing in a thumbnail, like a screencast recording.
3. Use PowerPoint, www.prezi.com or your choice of presentation software.
4. Submit the url of the recording.

Presentation Helpful Hints

- Don't put too much detail in the presentation, use it as a guide to help tell the story.
- Use the 6x6 rule, no more than 6 bullet points and 6 words per bullet point.
- Use pictures and diagrams. Use as little text as possible.
- The presentation should follow your final project Word document. Use the same headings in the presentation as the Word document. The Table of Contents can be used as a guide.
- Practice the presentation, preferably for an audience.
- Practice the presentation until it feels comfortable. Minimize the uh's, um's, or hesitations. Be enthusiastic, sell the project!
- Target an audience that doesn't know anything about the subject. Explain any technical terms used.

Length: The presentation should be a minimum of 5 minutes long.

Presentation Example

When you record the presentation, don't read it line by line. Use it as a guide to tell the story of how your company's plan can benefit the customer. Sell the audience, not with fluff like guaranteed service, but with tangible benefits. For instance:

This is what you might say:

Increasing the internet bandwidth will benefit the faculty in the following ways:

- More than just a few faculty at a time can do research or work on their online classes.
- The faculty will spend much less time uploading and downloading videos and other educational media.
- Two way communication such using technologies such as Zoom or Skype is now possible with the students, faculty, and other campuses

For the presentation, cut the verbiage down to enough to remind you of what you wanted to say.

This is what might be in the presentation:

Faculty benefit with increased bandwidth:

- Increased faculty efficiency
- Decrease time spent online
- Video conferencing is now possible

Now you are selling the project with tangible, measurable benefits.

Week 16: Discussion on Project Presentation

Time required: 30 minutes

Use this discussion to analyze another team's presentation. Please be constructive. We are here to learn and look at all objective feedback. This is one of the ways we learn.

- All feedback is good.
- What did the team do well?
- What could have been improved?

Finals Week: Project Final Report Submission

300 points

Time required: 3 hours

NOTE: Each person contributing to the document:

1. Highlight your text in a different color.
2. Put your name by the parts you worked on.

Submission

1. Submit the project early. There will be feedback and adjustments, just like a real project.
2. Attach written report to the assignment
 - a. Final Report in Word
 - b. Presentation file or URL
 - c. All supporting documents and drawings

Final Report Requirements

TIP: Use Track Changes in Word to work on the Final Report. That will allow whoever is working on the document at the time to see the other changes that have been made. When the document is complete, turn off track changes to finalize the document.

The final report should be formatted like a research paper, this document is an example. References are not necessary. This is a professional presentation to sell the proposal to a business or internally to management.

Audience

The audience for the final report are non-technical people. Explain any acronyms or technical concepts. The supporting documents are for technical or detail people who want more detail.

Technical Writing Tips

- Short sentences
- Short paragraphs
- Concise
- Less is more
- The best writing is re writing
- Text at least 1.5 or double spaced

Final Report Outline

The following is an outline of the minimum necessary requirements.

1. **Title Page**
2. **Table of Contents**
 - a. Construct a Word Table of Contents linked to styles.
 - b. Headers and/or footers with document information after the table of contents page.
 - c. The header or footer should contain the project name and page numbers.
3. **Scenario**
 - a. General information about the company and future growth.
4. **Issues**

- a. What were the security issues that prompted them to request this security audit?
- b. What was the specific incident that prompted this audit?

5. Asset Identification

- a. What does the business currently have for technology infrastructure?
- b. This is a supporting document.
- c. Provide a summary in the main document.

6. Network Documentation

- a. Document the network as it is currently.
- b. Document the IP addressing in a logical diagram.
- c. Document the physical wiring in a layout diagram.
- d. This is a supporting document.
- e. Provide a summary in the main document.

7. Risk Assessment Matrix

- a. This is a list of the security risks and how they rank.
- b. This should include the issues raised earlier.
- c. Please refer to the book for an example.

8. Risk Mitigation & Prevention

- a. How do you propose the business handle the risks you have identified?
- b. Align this with your Risk Assessment Matrix.

9. Security Policies

- a. A summary of the security policies you are proposing.
- b. How do you propose the business implement these policies?
- c. The specific policies will be a supporting document.
- d. Provide a summary in the main document.

10. Supporting Documents

Refer to the supporting documents in the main report. Give a short summary, then refer the reader to the supporting documents.

The following items are supporting documents.

- i. Asset identification
- ii. Network documentation
- iii. Security policies

Supporting documents also include:

- a. Include any diagrams or other supporting documents that will help describe the project.
- b. Provide an appendix to these documents.
- c. Reference the appendix items in the main document text.

11. Benefits

- a. How will your solution benefit the company?
- b. How will this project save money and/or time?
- c. Be tangible and specific.
- d. Align this with your Risk Mitigation & Prevention.

12. Executive Summary

- a. Summarize the project.
- b. Include the next steps in the process.