Project Teams

Section 001

Name	emal	Team
Steven Lin	tuk88604@temple.edu	1
Daniel Akoto-Bamfo	tus07807@temple.edu	1
Clement Tetteh Kpakpah	tut34684@temple.edu	1
Tony Zhang	tun39122@temple.edu	2
Justin Chen	tut41639@temple.edu	2
Yash Mane	tup81957@temple.edu	2
Elias Johnston	tun66471@temple.edu	3
Sara Sawant	tuu06857@temple.edu	3
Parth Tyagi	tut51841@temple.edu	3
Aaroush Bhanot	tup01547@temple.edu	4
Charles Lemon	tug92478@temple.edu	4
Jocque Sims	tus67218@temple.edu	4
Sarah Maher	tup81957@temple.edu	5
Lili Zhang	tut45086@temple.edu	5
Lily Li	tun56865@temple.edu	5
Rohith Murageppa	tuu06992@temple.edu	5

Section 701

Name	Email	Team
Neel Patel	tuq14910@temple.edu	1
Christopher Williams	tub56587@temple.edu	1
Nelson Ezeatuegwu	tut29015@temple.edu	1
Andrea Baum	tuq70745@temple.edu	2
Eric Mariscal	tug99004@temple.edu	2
James Nyamokoh	tus13050@temple.edu	2
Vincenzo Macolino	tut49384@temple.edu	3
Aisha Ings	tuu18812@temple.edu	3
GB Afolabi	tuu12483@temple.edu	4
Dawn E Foreman	tuu12483@temple.edu	4
Benjamin Rooks	tuu22848@temple.edu	4
Cyrena Haynes	tur40731@temple.edu	5
Tache Johnson	tuf57322@temple.edu	5
Brittany Pomish	tut97225@temple.edu	5

Team Project

Context

- You and your team have volunteered to participate in a free community information security clinic (“ITACS Clinic”) and provide support to an under-served small local business
- In a prior meeting your team was introduced to a number of small businesses and community support organizations
  - At that meeting you did a great job introducing yourself and the service you are offering through the clinic
  - One organization that attended the meeting has taken you up on your offer, and signed up to meet with you and receive intensive help from your team
- You will conduct your next meeting with your client during your Team Presentation
  - Your client knows who you are and there is no need to reintroduce your team during your Team Presentation

Team Project Presentation

Your assignment is to deliver a presentation to your client (Prof. Lanter will act as the owner/manager of the business.)

During your 15-minute presentation your team is responsible for explaining the following:

1. **Information & Information System Security**
   - Introduce them to the information security objectives we learned in this MIS 5206 class
   - Explain how the objectives and impacts of breaches are relevant to a small business like theirs

2. **Cyber Security Process**
   - Describe the process you will guide them through to help them decide how to secure their information and computer systems
   - Explain that they are in the first step in the process, and how their data inventory and categorization homework assignment you are giving them fits in the process

3. **Homework Assignment** – Explain how your client should get started, what they need to work on, and what they need to bring with them to your next meeting
   i. **Provide motivation** – Explain why they need to do their homework and what is in it for them?
   ii. **Provide details of their homework assignment using a worked-out example or template** – So they know how to do their homework

Deliverables

Your team will deliver your presentation during either Unit #13 or #14.

By end of Unit #14 each student should submit to Canvas in PDF format the following:

1. Team project PowerPoint slide presentation
   - Be sure to identify: your client, your Team, and all members of your team in deliverables for both 1 &2

2. Homework materials your team prepared for your client
   - Worked out example &/or template for your client to use in doing their homework

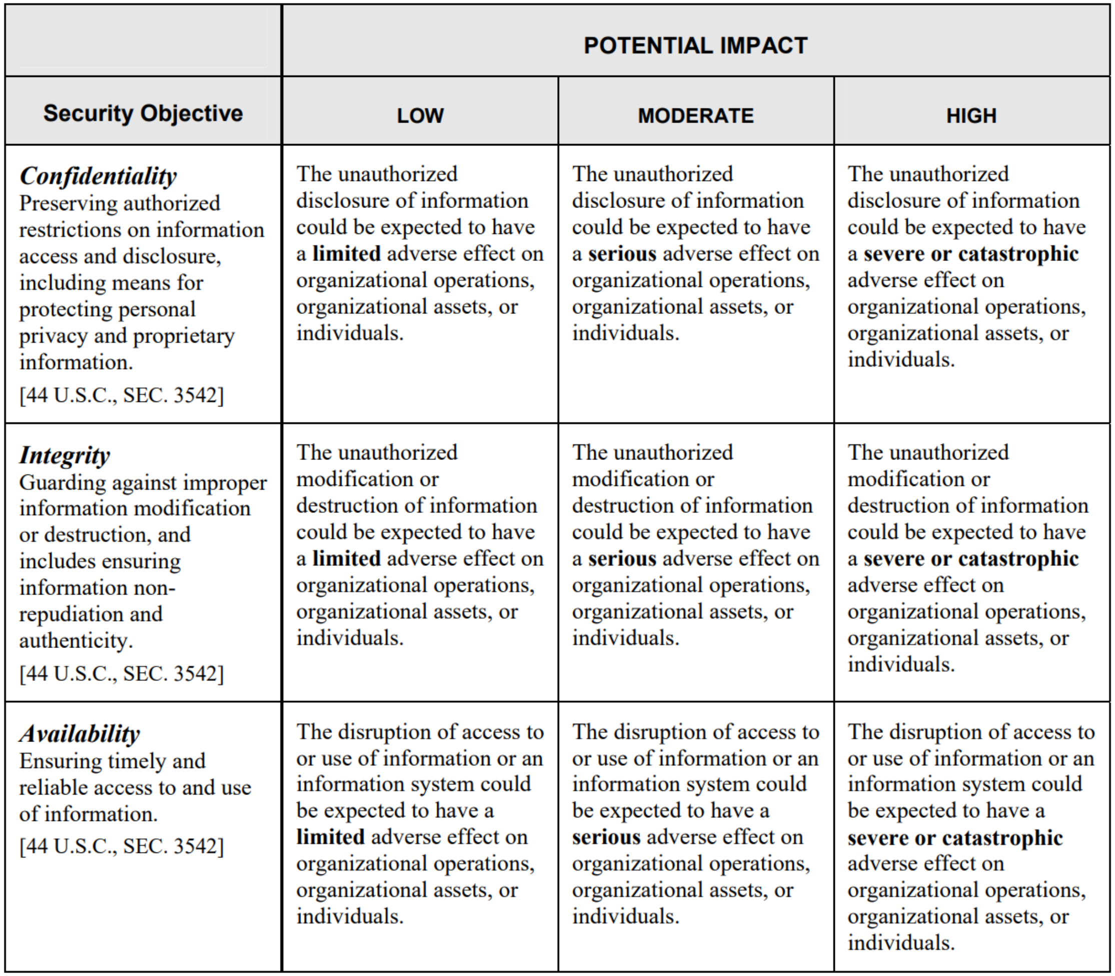
3. Your 360-degree review, answering the questions:
   - What you contributed to your team's project?
   - What each other member of the team contributed to the project?

The teams not presenting are responsible for:

A. Listening to each presentation made by other teams

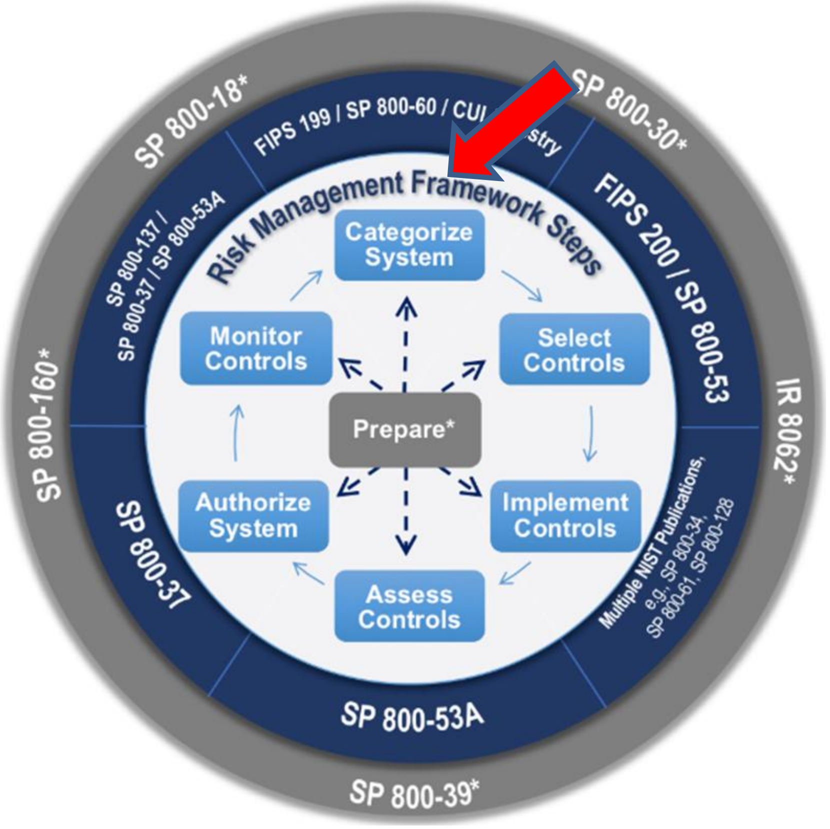
B. Asking clarifying questions of the presenting teams to identify any gaps, inconsistencies or issues in the presentation – in the 10 minutes after the presentation is over

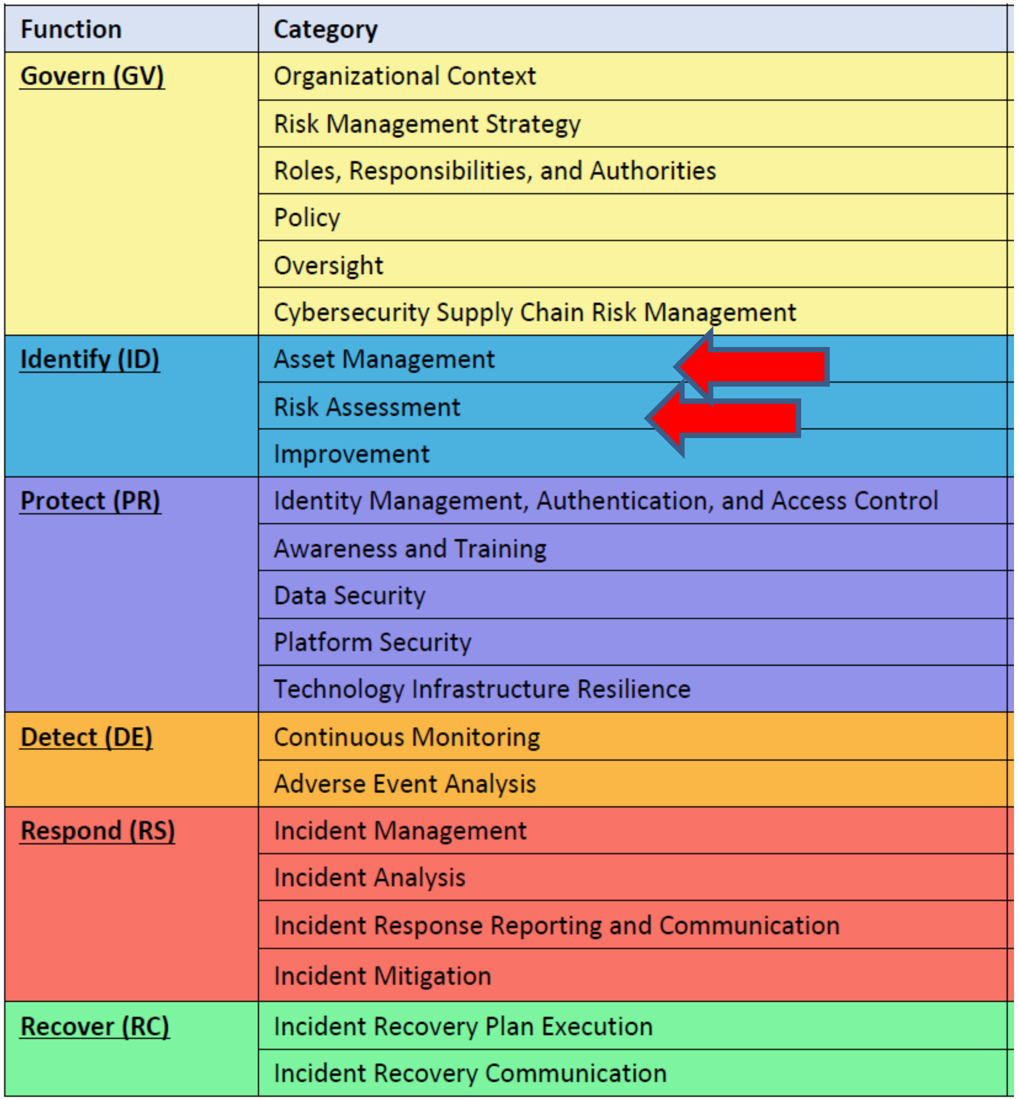
Security Objectives & Categorizations



	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Cybersecurity processes





Function	Category
Govern (GV)	Organizational Context
	Risk Management Strategy
	Roles, Responsibilities, and Authorities
	Policy
	Oversight
	Cybersecurity Supply Chain Risk Management
Identify (ID)	Asset Management
	Risk Assessment
	Improvement
Protect (PR)	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience
Detect (DE)	Continuous Monitoring
	Adverse Event Analysis
Respond (RS)	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	Incident Mitigation
Recover (RC)	Incident Recovery Plan Execution
	Incident Recovery Communication

Homework

- Data Asset Inventory
- Data Asset Security Categorization