SYLLABUS

ISA 697 - Special Topics in Information Security
Strategic Thinking for Cybersecurity

1. General Course Information

Course: Strategic Thinking for CyberSec
Course Number (section): ISA 697 – Special Topics in Information Security
Location: Planetary Hall Room 224, Fairfax Campus
Time: Tuesdays as scheduled (normally 19:20 – 22:00) Jan 24, 2017 through May 2, 2017 no class on Spring Break (March 7th)
Course Homepage: Blackboard
Prerequisites: ISA 656, ISA 562

2. Instructor Information

Professor: Richard Guidorizzi
Office: Engineering Building Rm 5332
Tel. 571-225-4983
Email: rguidori@gmu.edu
Office Hours: Mondays and Wednesdays 17:00 – 18:00 (by appointment)

3. Course Descriptions and Objectives

- A primary concern today relates to "cyber security challenges and real-world problems." Computer security courses treat the problem as a technical computer science problem and often ignore the reality of the environment and the non-technical human and political issues. The result is the constant and growing security breaches on systems across the world.
- The course will delve into the specific aspects of the cybersecurity field and attempt to provide a strategic understanding of the source of the current concerns relating to cyber security and potential directions of how to address the core problems that are deeply rooted in our (mis)understanding of how cybersecurity happens in practical scenarios.
- The course will address the problem at a strategic level, while driving down to specific technical details to ground the strategic understanding in technical reality.
- Core to the course is to provide familiarity and working experience of the more common enterprise tool set, lessons learned in deployment, balancing value with cost, the emerging trends, and when technology may not be the only answer.

- Students will
  - Develop an understanding of the cyber security field including current practices and the primary challenges that are bringing focus to the field
  - Compare IT management approaches and gain an understanding of their intended and unintended impact on an organization’s security posture
  - Learn how to evaluate and balance positive security impact with negative operational impact
  - Become familiar with the differences between defensive and offensive cyber
  - Learn how an organization’s perspectives and operational choices can have unintended security consequences and how to avoid this
  - Become able to evaluate cyber security (technology, procedures, and training) in the context of the field and in the context of an organization’s specific needs

- ○ Learn what senior leadership need to know and how to effectively communicate cyber security issues to senior leaders

4. Required Course Materials

- **Textbook**: *Walking Wounded* by Dr. Michael VanPutte © 2016 ISBN-13: 978-1539945611 ISBN-10: 1539945618
- **Readings:** Optional Readings and discussion board topics may be used during the duration of the class. Those will be posted to Blackboard.
  Required reading:
  - *Surviving on a Diet of Poisoned Fruit*, Richard Danzig, July 2014, (36 pages) available at:

    https://www.cnas.org/publications/reports/surviving-on-a-diet-of-poisoned-fruit-reducing-the-national-security-risks-of-americas-cyber-dependencies

    https://www.youtube.com/watch?v=xQmC6q6cTKE
  - *Why The Vasa Sank: 10 Lessons Learned*, by R. Fairley (6 pages) (PDF provided through Blackboard)

    http://faculty.up.edu/lulay/failure/vasacasestudy.pdf
  - *Unmasked,* HBGary case study from arstechnica.com by Dave Girard, authoring by Clint Ecker (49 pages), (PDF provided through Blackboard)

    http://arstechnica.com/tech-policy/2011/03/hbgaryanonymous-special-report/
  - *Deconstructing The Cyber Kill Chain,* Giora Engel, November 2014, (5 pages) available at:

    http://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542 (PDF provided through Blackboard)
  - *Leveraging The Kill Chain For Awesome*, Sean Mason, 2 Dec 2014, (3 pages) available at:

    http://www.darkreading.com/attacks-breaches/leveraging-the-kill-chain-for-awesome/a/d-id/1317810

    (Opinion Piece on Cyber Kill Chain)

  Optional reading:
  - *Why the Vasa Sank: 10 Problems and Some Antidotes for Software Project* by Richard E. Fairley, Oregon Health and Sciences University and Mary Jane Willshire, University of Portland, IEEE Software March/April 2003 issue

    https://pdfs.semanticscholar.org/4947/cd77938c850ca27bea61e3588146b97f8d46.pdf
  - *2016 Verizon Data Breach Investigations Report*, Verizon (authors not provided), available at:

    www.verizonenterprise.com/DBIR/ (PDF provided through Blackboard)
  - *Leveraging The Kill Chain For Awesome*, Dave Aitel, 31 Oct 2016, (1 page) available at:

https://cybersecpolitics.blogspot.com/2016/10/the-cyber-kill-chain-has-killed-your.html (Opinion Piece on Cyber Kill Chain)

- Ten Simple Rules for Making Good Oral Presentations - Philip E Bourne (NIH) (shot page) http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1857815/
- Martonosi, B. (2008). How to give a good Presentation. Retrieved from Princeton: https://www.princeton.edu/~archss/webpdfs08/BaharMartonosi.pdf [1]

- **Audio Visual Resources**
  - *Cyber Analytic Framework* Speaker: Peiter "Mudge" Zatko, DARPA, the Defense Advance Research Project Agency, directs billions of dollars towards research. One of these research areas is Cyber. This is a keynote delivered at 2011 "ShmooCon" www.youtube.com/watch?v=xo1YUEn49WA. (if this link does not work, then copy and paste the following into your browser:
    http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0CDAQtwIwAw&url=http%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3Dxo1YUEn49WA&ei=qZwIVJrVLpOjyASbvoCwDQ&usg=AFQjCNF1vp3h2N5kOiDh5obSH0ClrfAmTA

- *#5 Surviving on a Diet of Poisoned Fruit: Reducing the Risks of America's Cyber Dependencies* Speaker: Richard Danzig, Johns Hopkins University Applied Physics Laboratory speaking at NYU Poly
  https://www.youtube.com/watch?v=xQmC6q6cTKE

- **Blackboard**: This course will use Blackboard to deliver course materials such as lecture notes, announcements, online discussions, and assignments, etc. Additional materials beyond the textbook may also be posted on Blackboard. It is important for you to visit Blackboard (http://mymason.gmu.edu) regularly for course materials and announcements.

[1] 2008 Meeting Agenda for event, Retrieved from Princeton: https://www.princeton.edu/~archss/agenda.htm

5. Course Details

5.1 Tentative Course Schedule

Class 1: **Jan 24, 2017**	What is the current state of Cyber Security and associated challenges? • An overview of the main cyber security field with a discussion on Cyber Security, Information Assurance, and Information Technology, their meaning and their relationships • Learn what the current research challenges are and the difference is between the goals of IT Operations and Cyber Security, how they relate and how they conflict (from the CIO/CISO perspective). Being secure and being usable/operational has become untenable and students will be exposed to different alternatives to overcome that dilemma.
Assignments:	#1 Presentation (Research): Find an article discussing the state of cyber in an industry that illustrates a concern in the field; create and present a single slide describing how this article demonstrates the issue/concern you have chosen Due before Class 13 #2 Paper(2p): The author suggests little attention is paid to security in the development of technology? Is the core issue a flaw in the technology itself? Select a position (agree or disagree) and defend your position in a paper not to exceed 2 pages Due Class 2 #3 Group Presentation: Develop a method of how to objectively evaluate risk in the field of cyber security and provide an example of the relative risk in two scenarios Due Class 4 Reading #1: *Walking Wounded* Chapter 1, 2 complete by Class 2 Reading #2: Surviving on a Diet of Poisoned Fruit, pages 1-18* complete by Class 2 Reading #3: Surviving on a Diet of Poisoned Fruit, pages 19-36* complete by Class 9 Page numbers are listed with the page numbered, so the page labeled 18 is the 18th page, this does not count the pages in the PDF
Class 2: **Jan X, 2017**	Cyber Security in Practice • Gain an understanding of the current state of cyber within the private and public sectors • Discuss the weaknesses built into the system • Understand the breakdown and relevance of the 14 competency areas within DHS's Essential Body of Knowledge for Cyber Security and why it is relevant to you as a cyber practitioner
Assignments:	#4 Paper(2p): Given the case of Buckshot Yankee, (described in Chapter 3. Ground Hogs Day section: Thumbdrives, Viruses, and Lies, Oh My) what circumstances might motivate so many soldiers to go against known security policy? Due Class 3 #5 Paper(2p): Choose **one of the 4 questions** below and provide a response that is no more than 2 pages 1) Many believe cryptography (methods to send and receive messages securely) and strong authentication (methods to verifying the identity of a user or device) will provide "sufficient" confidence or trust for remote communications. How do the variable security policies and enforcement across agencies or corporations hinder these goals, and how can hackers

	defeat or bypass these tools? 2) Compare and contrast the effectiveness of cryptography with security by obscurity. 3) In the section Defense in Depth in Chapter 4 the author highlights issues with the implementation of security controls, but NIST (and the Federal Government) continues to focus on compliance with security controls. Discuss the value of each perspective. Which do you feel has a stronger case and why? Defend your perspective 4) In the section Stupid Users in Chapter 4, what is the issue the author is highlighting relating to users and security controls/training? Explain your perspective Due Class 5 (2 papers) Reading #4: *Walking Wounded* Chapter 3 complete by Class 3 Reading #5: *Why The Vasa Sank: 10 Lessons Learned* complete by Class 3
Class 3: **Jan X, 2017**	What makes management of IT and IT security ("cyber") so challenging? • Discussion of the complicated technologies and processes that make up IT operations and the inherent challenges • A discussion of the challenges presented to software developers and how their primary incentivizes increases the overall complexity of software and reduces security posture
Assignments:	#6 Presentation: Define the comparative value of two similar products, explaining which is a better value for the money spent Due Class 5 **#7 Mid-Term** – Individual Presentation: XXX Due Class 6 Reading #6: *Walking Wounded* Chapter 4 complete by Class 5
Class 4: **Jan X, 2017**	What is "Risk" in the terms of Cyber Security? • Gain an understanding of why traditional risk evaluation methods fail when applied to Cyber Security • Discussion of valuable methods of how to evaluate risk in Cyber Security • Discussion risks, threats, and vulnerabilities • Understand how to manage risks in an environment where all the necessary information is not available Cost of Security vs the Value of Security • Discussion of the costs of security technology, the actual and hidden • Understand how to evaluate TCO and ROI on security improvements • Discussion of the actual value security provides
Assignments:	#8 **Mid-Term** – Group Presentation: (based results of the individual assignment). Due Class 6 #9 Presentation: Define the "Cyber Kill Chain" – how adversaries work, using reading assignments #10 and #11 as well as any available open source materials Due Class 7 #10 Presentation: The "Cyber Kill Chain" describes the defender's perception of how the adversary attacks –describes the business process that is behind the attack, that aligns with the "Cyber Kill Chain" but still makes sense from how the business perspective Due Class 7 Note: In class 7, half the students will present assignment #9, and half assignment #10, but all will turn in both assignments for credit

	Reading #7: *Unmasked - HBGary* case study (p1-16, 26-59) complete by Class 9 Reading #8: *Walking Wounded* Chapter 7, 12, 13, 14 complete by Class 9 Reading #9: *Walking Wounded* Chapter 5, 9, 10 complete by Class 8 Reading #10: *Deconstructing the Cyber Kill Chain* complete by Class 8 Reading #11: *Leveraging The Kill Chain For Awesome* complete by Class 8
Class 5: **XXX X, 2017**	Cyber Defense • Review the aspects of IT Operations that make up the cyber defensive • Discussion defense as it related to the mission and activities performed by a cyber-adversary • Develop an understanding of the challenges of the defense that are creating the issues we are seeing in industry
Assignments:	#11 Paper(2p): How do the steps defined in the text (Walking Wounded) compare with the steps defined in the "Cyber Kill Chain"? Due Class 7 #12 Presentation: Understanding the CIO/CISO priorities, define the type of threat vectors that offer the greatest opportunities for the adversary Due Class 9 #13 Presentation: Starting with a known attack, and define a major threat vector in cyber that would make use of that attack Due Class 9 Note: In class 9, half the students will present assignment #12, and half assignment #13, but all will turn in both assignments for credit
Class 6: **XXX X, 2017**	Mid-Term Exam: Present Cyber Security Research Research/Operations agenda
Class 7: **XXX X, 2017**	Cyber Offense • Review the aspects of Cyber Offense as it relates to business • Discussion of the actual mission and activities performed by a cyber-adversary and how they relate to the impact on Cyber Defense • Discussion of the different types of adversaries, and what risks and threats they each bring • Develop an understanding of the interrelationship between offense and defense and the tradeoffs that are made
Assignments:	Reading #12: *Walking Wounded* Chapter 6 complete by Class 8
Class 8: **XXX X, 2017**	Attribution and Anonymity • Discuss how attribution is performed in cyber • Understand the limitations of attribution, and why perfect attribution is not possible • Discuss methods defenders attempt to get attribution of adversaries
Assignments:	**#14 Final-Exam:** Group Presentation: Due Class 13 #15 Paper(2p): Choose one of the 3 questions below and provide a response that is no more than 2 pages, Due Class 9 1) Government bureaucrats like to say the U.S. should reengineer the cyber environment. However, cyberspace is no longer a military or even

	government environment. It’s built and managed by private enterprise and required for trillions of dollars of national and international commerce. How could we reengineer cyberspace to prevent malicious activities but preserve its positive features? 2) Would perfect and complete attribution be desirable? Would we want an oppressive regime to have perfect attribution? Would we want to suppress expressing ideas? Don’t we want to protect personal privacy? Would we want our espionage activities attributed by our adversaries? 3) Governments may want their intelligence and/or law enforcement agencies to have the ability to track anyone responsible for malicious cyber actions. However, these same agencies don’t want to be tracked by anyone else. Does this make sense? What are the implications? #16 Paper(2p): Perform an open source analysis of person of interest. The analysis cannot be a family member; think a peer or celebrity. Present a detailed analysis of the person to include their background, interests, genealogy, real-estate tax records, social groups, contact information, and social media. Present an analysis of this information (max 2 pages) Due Class 11 #17 Paper(2p): After performing Task #16 above, perform the same analysis of someone from the person’s next layer of friends, contacts, and organizations (max 2 pages) Due Class 11 Reading #13: *Walking Wounded* Chapter 8 complete by Class 10
Class 9: **XXX X, 2017**	Cyber Threats • Discuss the spread of information due to technology • Discuss the likelihood of a cyber "Pearl Harbor" and the reasons this subject continues to be discussed • Discuss vulnerabilities, the vulnerability equity program, and secrecy • Discuss the most significant threat vectors in Cyber • Discuss security classification, Intellectual Property, and False Flag Operations • A detailed discussion of what makes up an “Advanced Persistent Threat” • An evaluation of potential threat vectors, as compared to the most expeditious threat vectors, and potential new threat vectors • Discuss the level of risk that comes from "cyber terrorists" • Detailed discussion of the cyber-attack process, and why the “cyber kill chain” offers a limited understanding on reality
Assignments:	#18 Group Presentation: Compare the impact of the hack at Aramco with impact of Hurricane Katrina. What was the difference between the cyber disaster and the natural disaster? (max 2 pages) Due Class 12
Class 10: **XXX X, 2017**	How do equities impact cyber defense and policy? • Discussion the steps security professionals can take to improve security • Comparative evaluation of how the value of security technology and processes as varies when compared to organization’s size and scale • Understand how the security answer for a small organization is not the same as for a large organization
Assignments:	#19 Paper: Choose one of the 2 questions below and provide a response that is no more than 2 pages, Due Class 11

	1) Compare the impact of the hack at Aramco with impact of Hurricane Katrina. What was the difference between the cyber disaster and the natural disaster? 2) The author suggests there is an asymmetry in cyber that gives the advantage to the terrorist, are there actions that can be taken that limit that advantage? Defend your position Reading #14: *Walking Wounded* Chapter 11 complete by Class 11
Class 11: **XXX X, 2017**	What actions can we take to make things better? • Discussion on the strategies used in cyber now, where they come from and how effective they have been • Discussion the goal of cyber defense, and how we are currently trying to reach that goal • Discussion the steps security professionals can take to improve security • Comparative evaluation of the value of security technology and processes as compared to organization's size and scale • Understand how the security answer for a small organization is not the same as for a large organization
Assignments:	#20 Presentation: How might a defender shift the asymmetric advantage from the attacker to the defender? (max 2 pages) Due Class 12
Class 12: **XXX X, 2017**	Do I need to communicate differently to senior leaders (C-level executives)? Why is Communication such a challenge in the field of Cyber? • Discuss what senior leadership requires in communications • Evaluation of the challenges facing communicating technological issues to senior management • Discussion of how to communicate technical security issues with non-technical people • Learn how to communicate effectively with senior leadership to get to the "yes"
Assignments:	#21 Presentation: Public American military strategy comes from the perspective that the US forces are technologically advanced over our adversaries. The author notes that the current military has reduced its size with "smaller, highly mobile forces supported by stealth aircraft, precision artillery, satellites and drones" – creating a greater reliance on our technology. However, the author suggests (and offers examples) that our technology is very vulnerable to attack from our adversaries. How should this alter our current policies and plans? Due Class 14 Reading #15: *Walking Wounded* Chapter 15, 16 complete by Class 14
Class 13: **XXX X, 2017**	Final Exam: Group Project Presentation
Class 14: **XXX X, 2017**	Cyber Security from the Strategic Perspective • Discuss what the purpose of cyberware is likely to be • Draw conclusions from the subject areas addressed throughout the class to understand the primary issues and concerns presented in the field of cyber security
Assignments:	None

5.2 Reading Assignments

Reading		Assigned		Due		#
		Class	Date	Class	Date	Pages
1.0	*Walking Wounded* Chapter 1,2	1	24-Jan	2	31-Jan	17
2.0	Surviving on a Diet of Poisoned Fruit (1-18)	1	24-Jan	2	31-Jan	18
3.0	Surviving on a Diet of Poisoned Fruit (19-36)	1	24-Jan	9	28-Mar	18
4.0	*Walking Wounded* Chapter 3	2	31-Jan	3	7-Feb	12
5.0	Why The Vasa Sank: 10 Lessons Learned	2	31-Jan	3	7-Feb	6
6.0	*Walking Wounded* Chapter 4	2	31-Jan	5	21-Feb	13
7.0	Unmasked - HBGary case study (p1-16, 26-59)	4	14-Feb	9	28-Mar	49
8.0	*Walking Wounded* Chapter 7, 12, 13, 14	4	14-Feb	9	28-Mar	46
9.0	*Walking Wounded* Chapter 5, 9, 10	4	14-Feb	8	21-Mar	29
10.0	Deconstructing the Cyber Kill Chain	4	14-Feb	8	21-Mar	5
11.0	Leveraging The Kill Chain For Awesome	4	14-Feb	8	21-Mar	3
12.0	*Walking Wounded* Chapter 6	7	7-Mar	8	21-Mar	10
13.0	*Walking Wounded* Chapter 8	8	21-Mar	10	4-Apr	13
14.0	*Walking Wounded* Chapter 11	10	4-Apr	11	11-Apr	13
15.0	*Walking Wounded* Chapter 15, 16	12	18-Apr	14	2-May	15

5.3 Writing Assignments

(P) = Presentation, (D) = Written Document, (#) = maximum number of pages for written document
(#m) = number of minutes maximum for presentation duration

Ex:

(P,I,5m)	= Presentation, Individual, no more than 5 minutes in duration
(D,2)	= Written document no longer than 2 pages in length

Task		Form	Assigned		Due	
			Class	Date	Class	Date
1.0	The State of Cyber (with reference)	(P,I,5m)	1	24-Jan	2	31-Jan
2.0	Security in the development of technology	(D,2)	1	24-Jan	2	31-Jan
3.0	Objectively evaluate risk with an example	(P,G,15m)	1	24-Jan	4	14-Feb
4.0	Why do people go against security policy?	(D,2)	2	31-Jan	3	7-Feb
5.0	Choose 1 of 4 (the other 3 are **extra credit**)	(D,2)	2	31-Jan	5	21-Feb
5.1	How Choose the variable security policies hinder cyber security?	(D,2)	2	31-Jan	7	21-Mar
5.2	Compare and contrast *cryptography* with *security by obscurity*	(D,2)	2	31-Jan	7	21-Mar
5.3	Defense in Depth - pick a side and defend	(D,2)	2	31-Jan	7	21-Mar
5.4	Are Users the problem?	(D,2)	2	31-Jan	7	21-Mar
6.0	Measure the comparative value of two products, showing the better value	(P,G,15m)	3	7-Feb	5	21-Feb

7.0	MidTerm:		3	7-Feb	6	28-Feb
8.0	MidTerm:		4	14-Feb	6	28-Feb
9.0	Define the “Cyber Kill Chain”	(P,G,15m)	4	14-Feb	7	7-Mar
10.0	Define the Adversary's business process	(P,G,15m)	4	14-Feb	7	7-Mar
11.0	Compare the text with the "Cyber Kill Chain"	(D,2)	5	21-Feb	7	7-Mar
12.0	Define the type of threat vectors that offer the greatest opportunities for the adversary	(P,G,10m)	5	21-Feb	9	28-Mar
13.0	Define a major threat vector in cyber that would make use of that attack	(P,G,10m)	5	21-Feb	9	28-Mar
14.0	Final		7	7-Mar	13	25-Apr
15.0	Choose 1 of 3 (the other 2 are **extra credit**)	(D,2)	7	7-Mar	9	28-Mar
15.1	How could we reengineer cyberspace to prevent malicious activities but preserve its positive features?	(D,2)	7	7-Mar	12	18-Apr
15.2	Would perfect and complete attribution be desirable?	(D,2)	7	7-Mar	12	18-Apr
15.3	What are the implications of having the ability to track everyone in cyber?	(D,2)	7	7-Mar	12	18-Apr
16.0	Perform an open source analysis of person of interest	(D,2)	8	21-Mar	11	11-Apr
17.0	After performing Task #16 above, on the person’s next layer of friends, contacts, and organizations.	(D,2)	8	21-Mar	11	11-Apr
18.0	What was the difference between the cyber disaster and the natural disaster?	(P,G,10m)	9	28-Mar	11	11-Apr
19.0	Choose 1 of 2 (the other one is **extra credit**)	(D,2)	10	4-Apr	11	11-Apr
19.1	How does the current activities relating to IP thefts relate to the US-UK IP war (1780-1824)?	(D,2)	10	4-Apr	14	2-May
19.2	Can we limit the asymmetry in cyber? Defend your position	(D,2)	10	4-Apr	14	2-May
20.0	How might a defender shift the asymmetric advantage from the attacker to the defender?	(P,I,5m)	11	11-Apr	12	18-Apr
21.0	If we are not the most technologically advanced players in cyber, how should we alter our policies?	(P,I,5m)	12	18-Apr	14	2-May

5.4 Direction for Writing Assignments

Written assignments **must be submitted through Blackboard** to be considered on time.

All written assignments should be provided in Microsoft Word format with the following characteristics:

- Language: English
- Font size no smaller than 11 point Calibri, no larger than 12 point Calibri
- Margins:
  - no smaller than ½ inch and no larger than 1" for left margin
  - no smaller than ½ inch and no larger than 1" right margin
  - no smaller than 7/10" inch and no larger than 1" top margin
  - no smaller than 7/10" inch and no larger than 1" bottom margin
- Page numbers should be located on the bottom of the page with a font size no smaller than 11 point Calibri, no larger than 12 point Calibri
- Line spacing should be set to no less than single (1) and no greater than 1 ½ line spaced (1.5)
- Paragraphs should be separated by a single line
- The first page of the document should note the following:
  - The student's name
  - The course number and title
  - The assignment number and title
- If the assignment required the student to select an option (eg. support or don't support a perspective) or gave multiple choices (eg. choose one of the 3 questions to answer), the choice the student made for this assignment should be listed on the first page below the assignment number and title
- The first page should have **no other content**, and does not count in the page number count (i.e. a document with a cover and two pages of text is considered to be 2 pages long)
- Tables or graphics included in the written document should have a caption describing the table/graphic, and (for those not created by the student) a citation describing the source
- Note: Graphics do not count towards content, (i.e. a document with a cover and two pages of text that included a table or graphic for ½ of a page is considered to be 1.5 pages long)
- Detailed grading information on written assignments is included in the Grading Guidance presentation on Blackboard

5.4 Direction for Presentations

Presentation assignments **must be submitted through Blackboard** to be considered on time.

All presentation assignments should be provided in Microsoft PowerPoint format with the following characteristics:

- Language: English
- Use of Fonts should not include anything smaller than 10 Point Calibri, and no larger than 88 point Calibri
- Page numbers should be located on the bottom of the page with a font size no smaller than 11 point Calibri, no larger than 12 point Calibri (page numbers can be omitted from a title page)
- The first page of the presentation should note the following:
    - The student's name(s)
    - The course number and title
    - The assignment number and title
- Students are not required to use Mason templates, but are encouraged to use one of the Mason templates before choosing no template at all
- If tables or graphics are included that are not created by the student should have a citation noting where/when the table/graphic was taken from. Links are helpful for citations if they also include the date when the link was last seen as active by the student
- Detailed grading information on presentation assignments is included in the Grading Guidance presentation on Blackboard

6. Grading and Assessment

Grading for the course will be based on total points earned by the end of the course. Final course letter grade assignments will be as follows:

- **Grade Percentage**

A	exceptional students that are >98%
A	greater than or equal to 93% but less than 98%
A-	greater than or equal to 88% but less than 93%
B+	greater than or equal to 83% but less than 88%
B	greater than or equal to 78% but less than 83%
B-	greater than or equal to 75% but less than 78%
C+	greater than or equal to 70% but less than 75%
C	greater than or equal to 65% but less than 70%
C-	greater than or equal to 60% but less than 65%
F	less than 60%

- **Peer evaluation. Group may be required to evaluate the quality of effort, work product and general contribution to group assignments by all team members.**

- **Graded Assignments**

Element	Weight	Individual or Group
Participation	15%	I
Assignments (18)	54%	I/G
Mid-Term (Individual Portion)	6%	I
Mid-Term (Group Portion)	5%	G
Final Exam/Project Presentation	20%	G
	100%	

Assignments - To be successful in this course, assignments will be an integral part of learning the course material. It is in the best interest of the student and of student teams to complete each and every individual and group assignment.

Homework will only be accepted through Blackboard submission prior to the start of class. Scanned, hand written work will not be accepted. Homework assignments are pass/fail.

Presentations done in class also must be submitted through Blackboard by the start time of the presentation.

- **Late Assignments**

  Late assignment submissions are subject to penalties:
  - 1 day late (within 24 hours) 30%
  - 2 days late (between 24 hours and 48 hours) 60%
  - penalty after the 3rd day (>48 hours) 100%

Extra Credit – Students will be required to complete 18 of the 21 assignments, they have the option to complete up to 3 additional assignments either as extra credit or to replace assignments with lower grades. If a student opts to make an assignment extra credit they will **need to submit the assignment no later than the due date** for the assignment.

- **Extra Credit assignments submitted after the due date will not be graded and will not alter the student's grade.**
- **Extra Credit assignments must score at least a C+ (70%) to provide additional points to a student's grade.**
- An assignment that does not score at C+ (70%) can be used to replace other assignments with lower score.

An assignment to be used as extra credit will use the same due date as a normal credit assignment.

Specific details on how written documents and presentations are graded are included in the presentation *ISA 797 Grading Guidance* found on Blackboard on the course's site.

7. Student Responsibilities

Students are expected to attend class each Class and to participate in class discussions and exercises. Students are expected to complete assignments on time. Students are expected to respect their instructor and fellow classmates, both in and out of the classroom environment. Students are expected to turn off or silence their mobile phones during class time.

Attendance Policy:

Attendance in this class is highly recommended in order to be successful in learning the course content. The student is solely responsible for all assignments and material presented in class even if missed due to absence.

8. Email Communication

By policy of the University and to help protect confidentiality, students are must use their official George Mason email accounts for communication with the instructor and other students in the class. All emails from the instructor will be sent to your official George Mason email email addresses.

9. George Mason Standards of Behavior:

The mission of the George Mason University is to create and deliver high-quality educational programs and research. Students, faculty, staff, and alumni who participate in these educational programs contribute to the well-being of society. High-quality educational programs require an environment of trust and mutual respect, free expression and inquiry, and a commitment to truth, excellence, and lifelong learning. Students, program participants, faculty, staff, and alumni accept these principles when they join the School of Business community. In doing so, they agree to abide by the following standards of behavior:

- Respect for the rights, differences, and dignity of others
- Honesty and integrity in dealing with all members of the community
- Accountability for personal behavior

Integrity is an essential ingredient of a successful learning community. Ethical standards of behavior help promote a safe and productive community environment, and ensure every member the opportunity to pursue excellence. To this end, community members have a personal responsibility to integrate these standards into every aspect of their experience. Through our personal commitment to these Community Standards of Behavior, we can create an environment in which all can achieve their full potential.

10. Honor Code Statement:

Honor System and Code: The Honor System and Code adopted by George Mason University will be enforced for this class:

http://oai.gmu.edu/the-mason-honor-code/

In your work on all written assignments, keep in mind that you may not present as your own the words, the work, or the opinions of someone else without proper acknowledgement. You also may not borrow the sequence of ideas, the arrangement of material, or the pattern of thought of someone else without proper acknowledgement. Please note: Faculty are obligated to submit any Honor Code violations or suspected violations to the Honor Committee without exception.

The appropriate version of the School of Business "Recommendations for Honor Code Violations" should be attached.

11. Disability: If you have a disability and you need academic accommodations, please see me and contact the Office of Disability Services (ODS) at 703-993-2474. All academic accommodations must be arranged through the ODS. Please take care of this during the first two weeks of the semester. More information about ODS is available at http://www.gmu.edu/student/drc

12. Religion: Students who will miss class for religious reasons should inform me of their anticipated absences as soon as possible.

13. Counseling center: George Mason University has a counseling center that can provide assistance if you find yourself overwhelmed by life, want training in academic or life skills, or the like. More information is available at http://www.gmu.edu/departments/csdc/

14. Writing Guidelines (if relevant for the course): Unless otherwise specified, all writing assignments should be formatted as follows: double-spaced, Times New Roman, 12-point font, and 1-inch margins. To cite and reference professional or academic sources, please use APA style. Specific instructions for in-text citations and referencing are found in the *Publication Manual of the American Psychological Association, 6th Edition* or at http://owl.english.purdue.edu/owl/resource/560/01/ .

To help manage the citations and seamlessly create reference lists, Mason supports a free software called Zotero. Please go to https://www.zotero.org/

This program offers:

- Centralized bibliography management
- Ability to sync across computers
- Ability for teams to combine contributions to the references
- Word plug-in that allows citation management within MS word

George Mason University has a writing center that can help you improve your English writing skills. More information is available at http://writingcenter.gmu.edu/

15. Inclement weather & campus emergencies: Information regarding weather related changes in the University's schedule (e.g., closing or late opening) will be provided on the GMU website and via MasonAlert. Students sign up for the Mason Alert system to provide emergency information of various sorts at https://alert.gmu.edu.

16. Emergencies: An emergency poster exists in each classroom explaining what to do in the event of crises and that further information about emergency procedures exists on http://www.gmu.edu/service/cert.