Assignment 2

The objective of a ***risk assessment*** is to understand the existing system and environment, and identify risks through analysis of the information/data collected.

This assignment provides an opportunity to perform an Information Technology (IT) risk assessment following Using NIST SP 800-30 Guide for Conducting Risk Assessments.

The purpose of this assignment is to:

a) Provide awareness of an industry standard framework to assist in performing IT risk assessments
b) Enable critical thinking and analysis given a business context with imminent IT risks
c) Learn to navigate and holistically comprehend the essence of guidance documents!

Question 1 (100 points):

Step 1: Please read the "**ITMM IT Audit University" case study** uploaded in Canvas under **Assignment 2** (modified courtesy of Otero, 2019)

Step 2: review the NIST SP 800-30 Guide for Conducting Risk Assessments.

Step 3: Following Chapter 3 ('THE PROCESS') of the NIST Guide, conduct a risk assessment following the logical steps in Figure 3 of the Guide. *You may need to refer to other sections of the guide to gain additional insights e.g. chapter 2.4*

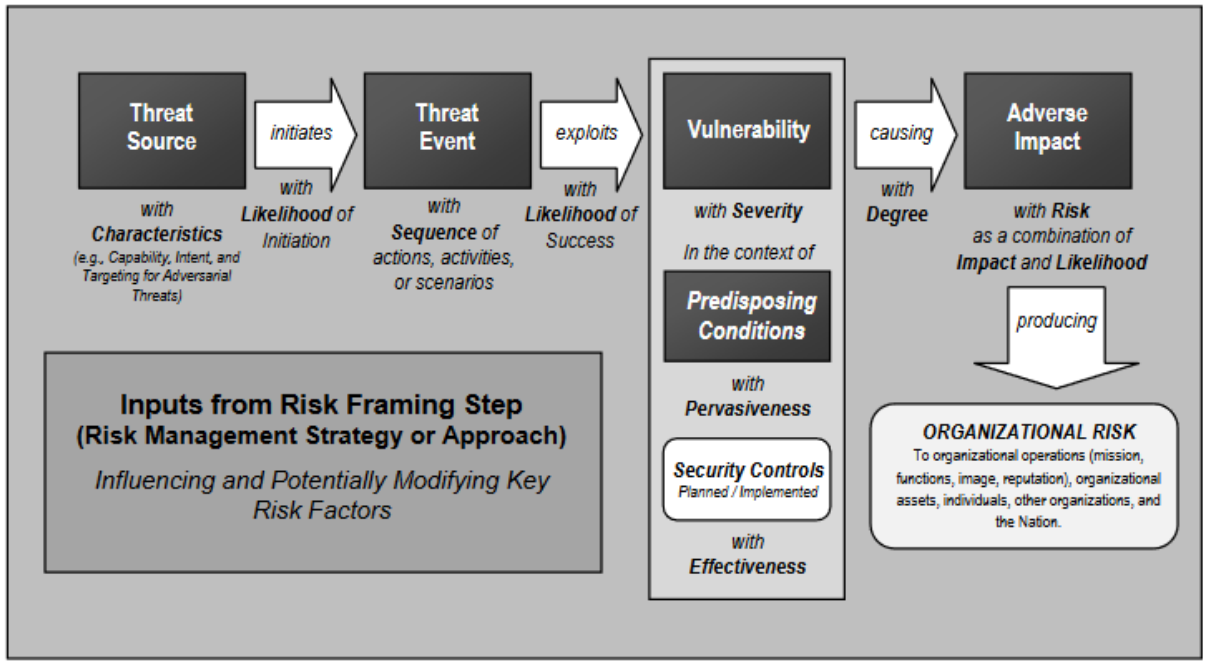

FIGURE 3: GENERIC RISK MODEL WITH KEY RISK FACTORS

Step 4: Submit a **risk assessment report** in a Word document. You may refer to Appendix K however **ONLY the following information is required for your submission:**

Risk Assessment Report Executive Summary Report

- List the date of the risk assessment.
- Summarize the purpose of the risk assessment.
- Describe the scope of the risk assessment.
- **For Tier 1 and Tier 2 risk assessments,** identify: organizational governance structures or processes associated with the assessment (e.g., risk executive [function], budget process, acquisition process, systems engineering process, enterprise architecture, information security architecture, organizational missions/business functions, mission/business processes, information systems supporting the mission/business processes).
- **For Tier 3 risk assessments**, identify: the information system name and location(s), security categorization, and information system (i.e., authorization) boundary.
- Describe the overall level of risk (e.g., Very Low, Low, Moderate, High, or Very High).
- List the number of risks identified for each level of risk (e.g., Very Low, Low, Moderate, High, or Very High)
- **Appendix**:
    - **All** tables you will be creating to support your assessment. This is described next
    - **Assumptions:** list any assumptions you may have made in creating the assessment report, based on the case study

Grading Rubric

Executive Summary Report Item	Grade
Report contains date of risk assessment	5%
Purpose of risk assessment is presented in at least 150 words	10%
Scope of risk assessment is presented in at least 150 words	10%
Risk assessment contains *at least* one Tier 1, one Tier 2, and one Tier 3 risk	15%
Report provides a risk statement describing overall level of risk (e.g., Very Low, Low, Moderate, High, or Very High).	5%
Report lists the number of risks identified for each level of risk (e.g., Very Low, Low, Moderate, High, or Very High)	5%
Appendix contains tables with information you have identified from conducting the risk assessment following the NIST SP 800-30 Guide for Conducting Risk Assessments **Table D-7** **Table D-8** **Table E-5** **Table F-3** **Table F-6** **Table H-4** **Table I-5** **Table I-7**	40%
Appendix lists any assumptions made in creating the report, based on the case study	5%
Report is presented in a professional manner suitable for senior leadership consumption	5%
Total	**100%**

Supporting Tables Required for Submission:

Table D-7: Identification of Adversarial Threat Sources

Identifier	Threat Source	Source of Information	In Scope	Capability	Intent	Targeting
1						
2						
…						

Table D-8: Identification of Non-Adversarial Threat Sources

Identifier	Threat Source	Threat Source Type	In Scope	Range of Effects
1				
2 …				

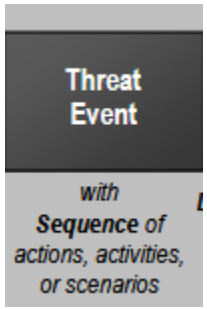

Table E-5: Identification of Threat Events for Adversarial Risk

Identifier	Threat Event	Source of Information	Threat Source	Relevance
1				
2				
…				

Table E-5: Identification of Threat Events for Non-Adversarial Risk

Identifier	Threat Event	Source of Information	Threat Source	Relevance
1				
2 …				

TABLE F-3: TEMPLATE – IDENTIFICATION OF VULNERABILITIES

Identifier	Vulnerability	Vulnerability Severity
1		
2 …		

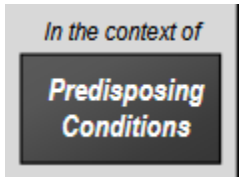

TABLE F-6: TEMPLATE – IDENTIFICATION OF PREDISPOSING CONDITIONS

Identifier	Predisposing Condition	Pervasiveness of Condition
1		
2 …		

TABLE H-4: IDENTIFICATION OF ADVERSE IMPACTS

Type of Impact	Impact	Affected Asset	Maximum Impact
Financial			
Operational			
Reputational			
Legal/Compliance			
Data Integrity			
Privacy			
Service Availability			
Environmental			

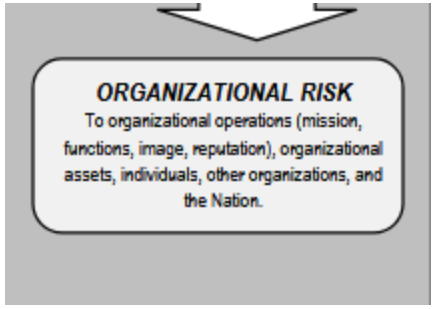

TABLE I-5: ADVERSARIAL RISK

Identifier	1	2	3	4	5	6	7	8
	Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions
			Capability	Intent	Targeting			
1								
2								
…								

9	10	11	12	13
Severity and Pervasiveness	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**
…				

Table I-7: Template – Non-Adversarial Risk

Identifier	1	2	3	4	5	6
	Threat Event	**Threat Sources**	**Range of Effects**	**Relevance**	**Likelihood of Event Occurring**	**Vulnerabilities and Predisposing Conditions**
1						
2						

7	8	9	10	11
Severity and Pervasiveness	**Likelihood Event Results in Adverse Impact**	**Overall Likelihood**	**Level of Impact**	**Risk**