APPENDIX A: CYBERSECURITY RISK ASSESSMENT PROJECT TEMPLATE

Organization Name

Risk Assessment Title
Prepared By:
Date:

Table of Contents

1. Executive Summary

Provide a high level summary of the work performed and significant findings of the risk assessment. The summary should be no more than 500-600 words (about ¾ page long) but must clearly describe the most significant risks identified in the assessment as well as a recommended response to those risks (A table would probably be a good strategy for succinctly summarizing the top risks). This section should be written last.

2. Introduction

2.1. Purpose

Describes the overall purpose of the risk assessment and how this assessment fits into the strategy, goals, and mission of the organization

2.2. Scope

Describes the boundaries of this assessment. What specifically was evaluated? What was purposely left out?

2.3. Document Structure

Provide a high level summary of what the remaining sections of this assessment will cover.

3. Risk Assessment Approach/Methodology

3.1. Assessment Resources

Provide a list of all documents (standards, policies, meeting minutes, etc.) used in the preparation of this report. For each item listed, provide a brief explanation of how it was used to prepare the assessment

3.2. Risk Assessment Execution

Provide a brief overview of the process that was followed to complete this assessment. Be sure to document the names of all individuals who were interviewed to collect information from and all steps taken to receive feedback on your assessment.

3.3. Assumptions and Constraints

Describe any assumptions that were made in the compiling of this assessment. In the absence of concrete evidence, did you need to make any judgement calls or inferences on the state or description of certain things contained in the report? Also note any things that constrained your ability to perform a complete and more detailed assessment of this organization.

4. Asset Summary

Brief description of the importance of asset identification for the purposes of performing a risk assessment.

4.1. Personnel

List all key personnel involved in organizing and maintaining physical and logical assets belonging to the organization. For each person, provide a job title and short description of responsibilities.

4.2. Physical Assets

Provide a list of key physical assets (similar assets can be grouped together, e.g. 32 Dell desktop workstations and monitors). For each asset, provide a contact person who is in charge of maintaining the physical asset.

4.3. Information Assets

Provide a list of key information assets, including intellectual property, websites, databases, etc. For each asset, provide a contact person who is in charge of maintaining the information asset.

5. Threat Summary

Provide a summary of the threats identified during the risk assessment. The table below provides a template for recording the threats. Be sure to define the different classifications and categories prior to presenting the table (use definitions derived from class notes and discussions).

Threat sources are the underlying initiator of a loss event or the location in which a loss event can occur. Classification will be either external or internal. Category will be either natural, human, or environmental. Threat agents are specific instantiations of a threat source. One example has been provided to you in the table. This threat may or may not be present for your organization, be sure to modify it as you see fit. Add new rows to the table for each additional threat you identify.

Threat Source	Classification	Category	Threat Agents
Natural Threat Sources	External	Natural	Hurricane, tornado, flood, ice storm/winter storm, electrical storm/thunderstorm

6. Vulnerability Summary

Define vulnerability and provide a brief description of how vulnerabilities were identified. Provide a list of identified vulnerabilities with a brief description of each vulnerability (bulleted list is fine). No assessment of impact or likelihood is necessary in this section.

7. Risk Assessment Results

7.1. Risk Analysis Methodology

Provide a description of the methodology used to classify risks. The methodology must involve some assessment of impact and likelihood and all risks must be given a composite score or classification. This section should clearly describe the different classifications applied to risks

and how composite scores/classifications were derived. Reference any relevant standards and/or class materials to support your methodology.

7.2. Risks Identified

For each risk identified, provide the following information (if applicable…not all risks will require every piece of information to be documented): vulnerability, standard reference (if applicable), threat source(s), assets affected, existing controls, impact, likelihood, and composite score. For ease of cross-referencing risks in other sections of the report, uniquely identify each risk with a specific number or meaningful identifier. These identifiers could include a prefix to designate a specific category of risk. In the example below, "IT-1" is used to denote this is the first IT-related risk. Another risk could be given the identifier "Ops-1" to designate that it is an operational risk.

An example of one risk summary is provided below:

Risk IT-1 – Outdated anti-malware definitions can result in an infection of networked computing devices rendering them unusable for classroom instruction.	
Vulnerability	Webserver is not automatically receiving malware definition updates on a daily basis
ISO 27001 Reference	Objective A.12.2.1
Affected Assets	Organization's webserver and website
Threat Source(s)	External human users, internal human users
Existing Controls	Malware protection is actively running on the webserver, but definitions are only updated on a weekly basis
Impact	6 – A malware infection could easily spread through the network and affect many employee and client devices. Malware could result in a decreased processing capacity and would require the webserver to be quarantined and cleaned before returning it to a normal operating state. This can have a reasonable impact on the organization to generate revenue and it can lead to harming the organization's reputation and trust.
Likelihood	.3 – Existing controls provide a reasonable level of protection in that definitions are updated weekly webserver before definitions are updated.
Composite Score	1.8 (Low)

8. Risk Management Plan

Provide a short description of your criteria for prioritizing risks and determining an appropriate response

8.1. Risk Response Strategies

For each risk identified, outline your proposed response. Draw on the four common responses to risk (avoidance, modification, transfer, and acceptance) as a guide for preparing your responses. For all responses except acceptance, be sure to provide an overview of what should be done to implement this response (acceptance requires no change in operating procedure/behavior thus there is no recommended change).

9. Information Security Policy 1

Include your first information security policy here. Please keep in mind what makes a good policy, what your client needs, and how the policy can be enforced.

10. Information Security Policy 2

Include your second information security policy here. Please keep in mind what makes a good policy, what your client needs, and how the policy can be enforced.

Appendix A

Include any meeting minutes or additional information you have gathered for this project.

Meeting Minutes

This form will be used to document any meetings between your team and the start-up you'll be working with. You'll have to fill it out every time you meet with your client. The minutes can help you later remember what you talked about and what you agreed upon. Your notes could be in the form of bullet points and/or essay text. They should be clear and concise. Make sure you include actionable items and individuals responsible for each one. The meeting minutes are an important part of your project documentation so please keep all minutes until the end of the semester. **All attendees must agree and sign the meeting minutes.** One form is needed for every meeting and your team should submit them as appendices at the end of the risk assessment document.

Date: _____

Time: _____

Location: _____

Name	Signature
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

Comments:

_____
_____
_____
_____
_____
_____
_____

APPENDIX B: INQUIRY PROJECT AND PRESENTATION RUBRICS

Inquiry Project Paper Rubric:

Dimension	Incomplete	Does not meet expectations		Meets expectations		Exceeds Expectations
Score	**0**	**1**	**2**	**3**	**4**	**5**
Introduction	Position and Organization missing	Position is vague. Organization of argument is missing, vague, or not consistently maintained. (Below 15 Points)		Position is clearly stated. Organization of argument is clear in parts or only partially described and mostly implemented.		Position and exceptions, if any, are clearly stated. Organization of the argument is completely and clearly outlined and implemented.
Research	Research selection is unclear, not identified; components are missing. Theory behind work not completed	Research selected is not relevant to the argument or is vague. Components inaccurate or unclear. Theory is not relevant or only relevant for some aspects; theory is not clearly articulated and/or has incorrect components. Relationship between theory and research is unclear or inaccurate, major errors in the logic are present.		Research is relevant to the argument and is mostly accurate and complete – there are some unclear components or some minor errors in the method, results or implications. Theory is relevant and accurately described; some components may not be present or are unclear. Connection to theory is mostly clear and complete, or has some minor errors.		Research selected is highly relevant to the argument, is presented accurately and completely – the method, results, and implications are all presented accurately; Theory is relevant, accurately described and all relevant components are included; relationship between research and theory is clearly articulated and accurate.

Conclusions	Conclusion is missing	Conclusion may not be clear and the connections to the research are incorrect or unclear or just a repetition of the findings without explanation. Underlying logic has major flaws; connection to position is not clear.		Conclusion is clearly stated and connections to research and position are mostly clear, some aspects may not be connected or minor errors in logic are present.		Conclusion is clearly stated and connections to the research and position are clear and relevant. The underlying logic is explicit.
Writing	No attempt at proper grammar or clarity.	Paper is poorly organized and difficult to read – does not flow logically from one part to another. There are several spelling and/or grammatical errors; technical terms may not be defined or are poorly defined. Writing lacks clarity and conciseness.		Paper is generally well organized and most of the argument is easy to follow. There is only a few minor spelling or grammatical errors, or terms are not clearly defined. Writing is mostly clear but may lack conciseness.		Paper is coherently organized and the logic is easy to follow. There is no spelling or grammatical errors and terminology is clearly defined. Writing is clear and concise and persuasive.
Formatting	No attempt at discipline-appropriate formatting used	Paper is poorly formatted. There are several areas where formatting is inaccurate/misused, or missing.		Paper is generally formatted well. There are a few minor errors or only 1-2 larger formatting issues.		Paper format is very well done. There are less than 2 minor errors and no major errors in formatting style.

Inquiry Project Presentation Rubric:

Dimension	Incomplete	Does not meet expectations		Meets expectations		Exceeds Expectations
Score	0	1	2	3	4	5
Organization	No logical sequence present	Presentation jumps around, but has some sense of sequence		Information is presented in logical sequence that audience can follow.		Logical and interesting ordering
Content (grammar, graphics)	Presentation has more than 5 errors; words are difficult to read and excessive on most slides; graphics are used in excess and ineffective	Presentation has between 3 and 5 errors; words are easy to read and clear on some slides, but crammed on others; graphics, if used, do not have clear connection to topic		Presentation has no more than 2 errors (e.g., misspellings, grammar usage); words on slides are easy to read; graphics, if used, are interesting and appropriately related to topic		No errors; text on slides is clear and concise; Graphics, if used, are informative and explain and reinforce topic
Delivery	Voice is mumbled and so low that majority of audience struggles to hear	Voice is low and lacks clarity; audience alternates between being able to hear and not		Voice is clear, words are mostly pronounced appropriately, audience can hear presentation majority of presentation		Voice is clear, pronunciation is appropriate, and all audience can hear entire presentation
Eye Contact	Reads directly from notes, head down most of the presentation	Uses notes frequently, makes minimal attempt at eye contact		Student uses notes only, but keeps consistent eye contact, talking somewhat freely, with audience		Student uses notes sparingly and maintains eye contact throughout presentation
Sources	Information comes completely from websites, no use of peer-reviewed journal articles	Information comes mostly from websites, minimal use of peer-reviewed journal articles		Information comes mostly from peer-reviewed journal articles, minimal reliance on websites		Information comes completely from peer-reviewed journal articles, no use of websites