CYBERSECURITY RISK ASSESSMENT

ACME Business Consulting, Inc.

Table of Contents

Executive Summary 3

Assessment Scope & Context 4

- Risk Assessment Scope 4
- Risk Management Overview 4
- Enterprise Risk Management Alignment 5
- Integrated & Organization-Wide Risk Management 5

Natural & Man-Made Threats 6

- Risk Threshold for Natural & Man-Made Risk 6
- Summary of Unweighted Natural & Man-Made Threats 7
- Summary of Weighted Natural & Man-Made Threats 7
- Breakdown of Natural Threats & Associated Risks 8
- Breakdown of Man-Made Threats & Associated Risks 13

Cybersecurity Risk Assessment Findings & Recommendations 16

- Defining Appropriate Controls for Assessing Cybersecurity Risk 16
- Risk Threshold for Cybersecurity Risk 16
- Breakdown of Cybersecurity Risks 17

IT Security Program Maturity Assessment Findings & Recommendations 34

- Cybersecurity Maturity Ranking 34
- Findings-Based Recommendations 35
- Future Maturity Projection 35

Glossary: Acronyms & Definitions 36

Appendix A: Natural & Manmade Risk Assessment Matrix 37

Appendix B: Cybersecurity Risk Assessment Matrix 38

EXECUTIVE SUMMARY

The purpose of this risk assessment is to provide a holistic summary of the risks that impact the confidentiality, integrity and availability information systems and data that ACME Business Consulting, Inc. (ACME) relies upon to operate.

This assessment addresses the three most important factors in determining "information risk" that affects the confidentiality, integrity and availability of systems and data:

- An evaluation of natural & man-made threats;
- The existence and operational state of reasonably-expected cybersecurity controls; and
- The overall maturity of the IT security program that focuses on the current capabilities of people, processes and technologies relied upon to protect ACME.

Assessment of Natural & Man-Made Threats

When taking compensating factors into account, ACME's exposure to natural & man-made threats would earn a MODERATE risk rating.

Assessment of Cybersecurity Controls

When taking compensating factors into account, ACME's implementation of reasonably-expected cybersecurity controls would earn a MODERATE risk rating.

Assessment of IT Security Program Maturity

ACME would earn a technology capability maturity rating of Level 2, based on the composite score for maturity of the assessed cybersecurity controls utilized in this assessment.

In summary, taking into account the assessed factors that are covered in this report, ACME's overall IT security capabilities are in the early stages of maturity, which exposes ACME to a moderate level of risk. This is based on the existing people, processes and technologies in place to protect the confidentiality, integrity and availability of ACME's data and systems.

Assessment Scope & Context

Risk Assessment Scope

Assessed Entity	ACME Business Consulting, Inc. (ACME) Address City, State ZIP, VA 20176 Telephone: 888-555-XXXX Fax: 888-555-XXXX
Contact(s)	John Doe
Date of Report	5 January 2016
Type of Assessment	Internal team performed the assessment
Geographic Scope	Single location
Number of Employees	16
Authoritative Sources	**NIST SP 800-30** *Risk Management Guide for Information Technology Systems* **NIST SP 800-37** *Guide for Applying the Risk Management Framework to Federal Information Systems* **NIST SP 800-39** *Managing Information Security Risk*
Risk Analysis Scope	The scope of this risk assessment encompasses the potential risks and vulnerabilities to the confidentiality, availability and integrity of all systems and data that ACME creates, receives, maintains, or transmits.

Risk Management Overview

In simple terms, risk management is about validating that protective measures are operational and appropriate to protect an organization's assets:

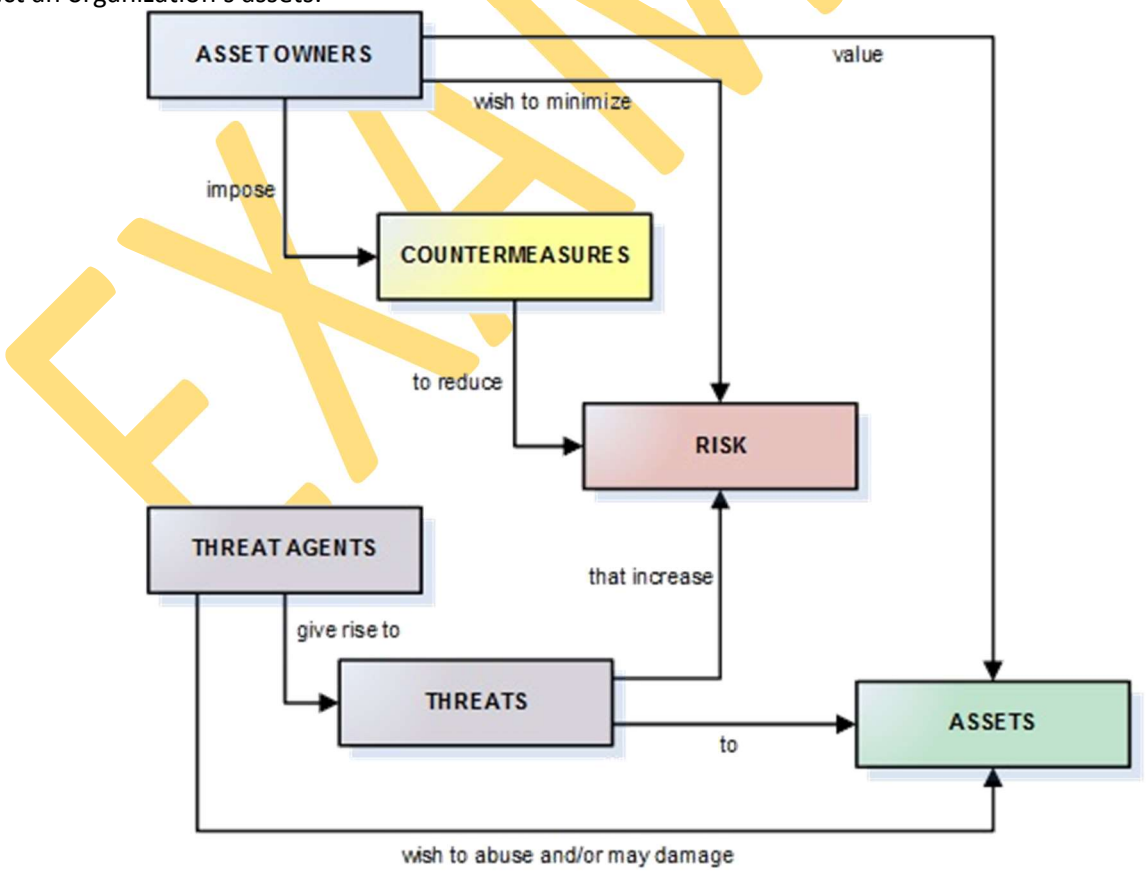

Figure 1: Risk management process flow.

Enterprise Risk Management Alignment

Enterprise Risk Management (ERM) is a process, led by an organization's management and other personnel, that is applied in strategic setting and across the organization and it is designed to identify potential events that may affect the organization, manage risks to be within the "risk appetite," and to provide reasonable assurance regarding the achievement of the organization's objectives.

The underlying premise of ERM is that every organization exists to provide value for its stakeholders. All organizations face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value.

The overall strategic ERM model used by ACME is the 2013 version of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework. Specific to information risk, the framework used for this risk assessment utilizes National Institute of Standards and Technology (NIST) best practices.

Integrated & Organization-Wide Risk Management

At ACME, managing information-related security risks is a complex, multifaceted undertaking that requires the involvement of the entire organization—from senior leaders providing the strategic vision and top-level goals and objectives for the organization, to mid-level leaders planning and managing projects, to individuals on the front lines developing, implementing, and operating the systems supporting the organization's core missions and business processes.

Information risk management can be viewed as a holistic activity that is fully integrated into every aspect of the organization. Figure 1 illustrates a three-tiered approach to risk management that addresses risk-related concerns at:

- Strategic Risk: Tier 1 addresses risk from an organizational perspective with the development of a comprehensive governance structure and organization-wide risk management strategy
- Operational Risk: Tier 2 addresses risk from a mission and business process perspective and is guided by the risk decisions at Tier 1.
- Tactical Risk: Tier 3 addresses risk from an information system perspective and is guided by the risk decisions at Tiers 1 and 2. Risk decisions at Tiers 1 and 2 impact the ultimate selection and deployment of needed safeguards and countermeasures (e.g., security controls) at the information system level.

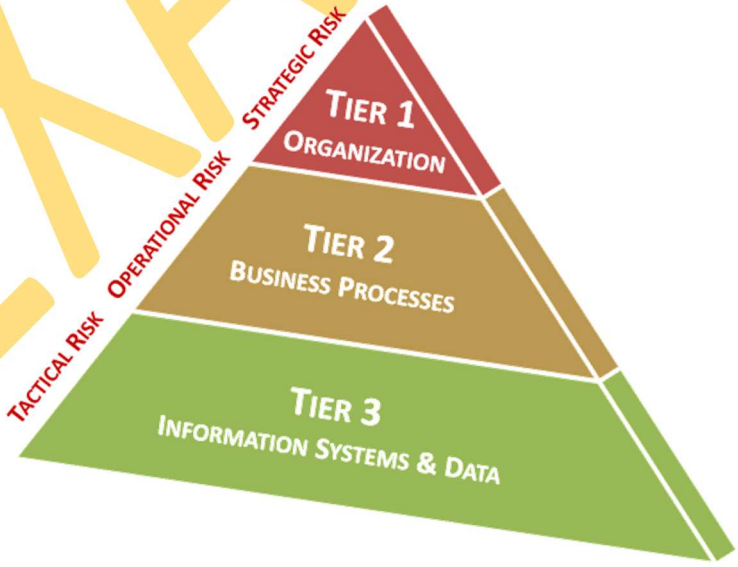

Figure 2: Risk hierarchy flow.

NATURAL & MAN-MADE THREATS

RISK THRESHOLD FOR NATURAL & MAN-MADE RISK

Based on management's guidance, ACME's risk tolerance threshold for natural and man-made threats is moderate risk.

Based on natural and manmade threats, cyber-crime and earthquakes pose the greatest risk to ACME operations. Therefore, an initiative should be launched to evaluate measures that could further reduce the risk associated with these events.

While the natural and man-made risks were averaged to earn a **MODERATE** risk assessment, there are still several threats that are individually considered **HIGH** risk and require management attention.

Reference the ***App B – Control Worksheet*** for the detailed breakdown of the risk assessment criteria and individual scoring.

Natural & Man-Made Risk Matrix		Occurrence Likelihood					
		Remote [<1% chance of occurrence]	Highly Unlikely [1% to 10% chance of occurrence]	Unlikely [10% to 25% chance of occurrence]	Possible [25% to 70% chance of occurrence]	Likely [70% to 99% chance of occurrence]	Almost Certain [>99% chance of occurrence]
Impact Effect	Catastrophic	6	12	18	24	30	36
	Critical	5	10	15	20	25	30
	Major	4	8	12	16	20	24
	Moderate	3	6	9	12	15	18
	Minor	2	4	6	8	10	12
	Insignificant	1	2	3	4	5	6

Risk Tolerance Threshold (*Moderate Risk*)

INITIAL RISK ASSESSMENT - UNWEIGHTED & AVERAGED - Risk Scoring Range (1 to 36)				
LOW (1-4)	MODERATE (5-11)	HIGH (12-19)	SEVERE (20-29)	EXTREME (30-36)

*Compensating Controls & Control Weighting Convert Risk Score To

FINAL RISK ASSESSMENT - WEIGHTED & AVERAGED - Risk Scoring Range (1 to 180)				
LOW (1-22)	MODERATE (22.1-57)	HIGH (57.1-97)	SEVERE (97.1-147)	EXTREME (147.1-180)

NATURAL & MAN-MADE RISK SUMMARY	Initial Risk Assessment	Compensating Factors	Final Risk Assessment
	HIGH 13 Raw Value	→	MODERATE 41 Weighted Value

Figure 3: Natural & Man-Made Risk Matrix

SUMMARY OF UNWEIGHTED NATURAL & MAN-MADE THREATS

Based on unweighted risk scores, the threats from earthquakes and hacking pose the most significant risk to ACME.

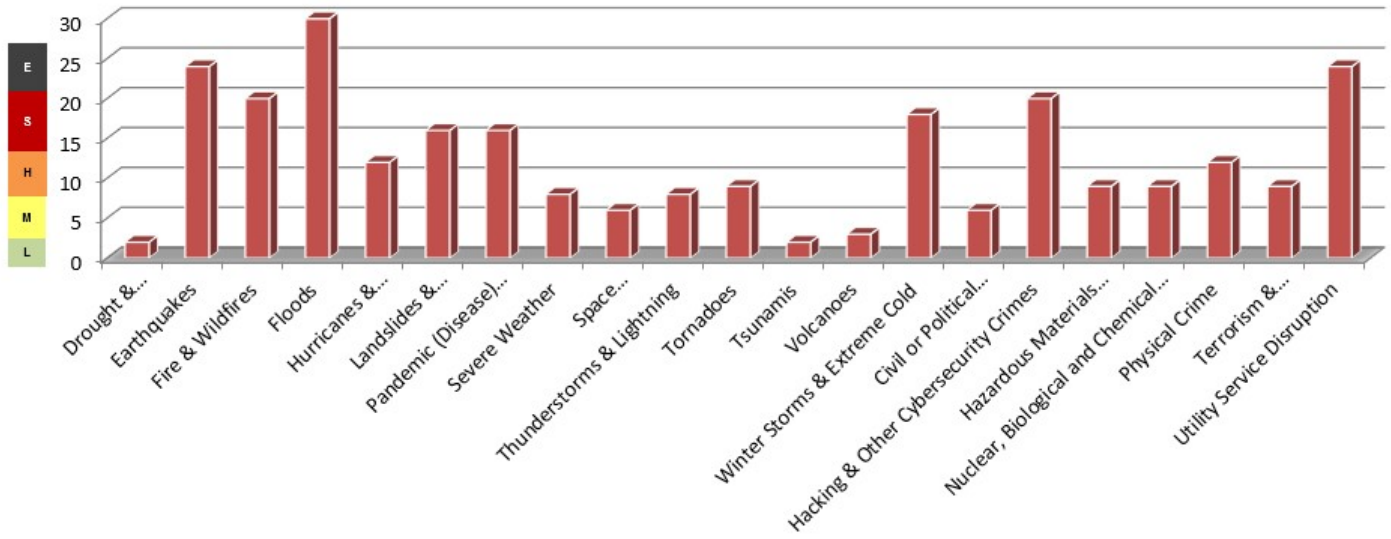

Figure 4: Unweighted Natural & Man-Made Risks

SUMMARY OF WEIGHTED NATURAL & MAN-MADE THREATS

Based on weighted risk scores that address compensating measures, the threats from earthquakes and hacking still pose the most significant risk to ACME. However, utility service disruption also factors in as a high risk to ACME.

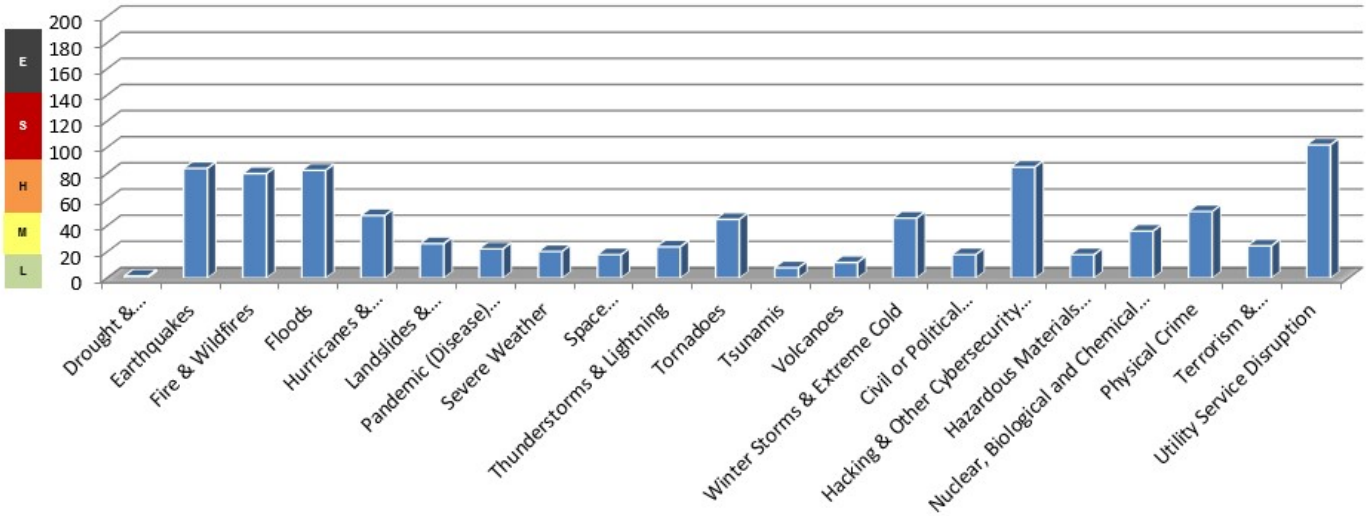

Figure 5: Weighted Natural & Man-Made Risks

BREAKDOWN OF NATURAL THREATS & ASSOCIATED RISKS

Threat Type	Threat Description	Occurrence Likelihood	Potential Impact	Compensating Factors	Risk Assessment Notes *(Justification for compensating controls or other factors that need to be explained)*
Drought & Water Shortage	Regardless of geographic location, periods of reduced rainfall are expected. For non-agricultural industries, drought may not be impactful to operations until it reaches the extent of water rationing.	Improbable	Minor	Minimal Impact Reduction	Located in heavily populated area with no history of water shortages.
Earthquakes	Earthquakes are sudden rolling or shaking events caused by movement under the earth's surface. Although earthquakes usually last less than one minute, the scope of devastation can be widespread and have long-lasting impact.	Almost Certain	Major	Moderate Impact Reduction	No history of occurrence
Fire & Wildfires	Regardless of geographic location or even building material, fire is a concern for every business. When thinking of a fire in a building, envision a total loss to all technology hardware, including backup tapes, and all paper files being consumed in the fire.	Possible	Critical	None Available	Server room is equipped with a fire suppression system and all backups are replicated off-site daily.

Risk can be assessed by measuring the current maturity level of an organization against an industry best practice or standard. Essentially, the lesser maturity an organization has with its management of its technical capabilities, the greater overall risk it accepts. As governance is refined through policies, standards and procedures, risk is diminished through the implementation of risk avoidance and/or risk mitigation measures.

This risk assessment is based upon representation from ACME as to the accuracy and completeness of information provided in the risk assessment questionnaire and the procedures performed.

CYBERSECURITY MATURITY RANKING

Technology capability maturity is assessed, based on the following 0 through 5 point criteria from the International Standards Organization (ISO) 21827 standards for ranking technological capability maturity. This rating is an indicator of an organization's ability to protect information in a sustainable manner:

ACME would earn a technology capability maturity rating of Level 2, based on the composite score for assessed maturity of the cybersecurity controls utilized in this assessment.

- **Level 0 – Non-existent.**
  - Gaps in policy do not identify requirements/standards to be met.
  - Base practices do not exist.
  - Technology is ad hoc and/or chaotic.
- **Level 1 – Initial / Ad Hoc.**
  - Policies are used to enforce requirements/standards.
  - Base practices are poorly defined, informal and/or undocumented.
  - Technology is ad hoc and/or chaotic.
- **Level 2 – Repeatable.**
  - Policies and procedures are used to enforce requirements/standards.
  - Base practices are defined and documented enough to be repeatable.
  - Technology project success is a result of individual efforts.
- **Level 3 – Defined.**
  - Policies, procedures and technologies are relied upon to enforce requirements/standards.
  - Base practices are documented, standardized and integrated.
  - Management of technology is planned and structured.
- **Level 4 – Managed.**
  - Policies, procedures and technologies are consistently used to enforce requirements/standards.
  - Base practices are managed and quantitatively measured.
  - Managers employ statistical process control techniques to achieve and maintain high levels of quality.
- **Level 5 – Optimized (world-class)**.
  - Policies, procedures and technologies are consistently used to enforce requirements/standards.
  - Base practices are proactively managed for continuous improvement.
  - Quantitative management techniques enable continuous improvement of processes and innovation.

FINDINGS-BASED RECOMMENDATIONS

Based on the assessed findings, the following recommendations are proposed:

- IT Security Documentation.
  - Formalize information security documentation to progress from an ad hoc state to a more mature, structured state for managing IT and information security.
  - Generate current network diagrams.
- Log Management.
  - Enable logging on all information systems and network devices.
  - Centrally collect logs so that log management can be performed.
  - Develop and implement processes to routinely review logs.

FUTURE MATURITY PROJECTION

The "sweet spot" for growing businesses with a dedicated IT staff is a capability maturity level in the 2-3 range. By implementing the findings-based recommendations, it should advance ACME's practice to a level 3 maturity level. This will allow for future process improvement and goal setting to find ways to reach a level 3 maturity level.

The benefits that come with a higher maturity level include, but are not limited to:

- Decreased malware/spyware outbreaks
- Decreased downtime from hardware failures
- Decreased downtime from data loss events
- Increased productivity
- More efficient and effective compliance with requirements

- **Level 2 – Repeatable.**
  - Policies and procedures are used to enforce requirements/standards.
  - Base practices are defined and documented enough to be repeatable.
  - Technology project success is a result of individual efforts.
- **Level 3 – Defined.**
  - Policies, procedures and technologies are relied upon to enforce requirements/standards.
  - Base practices are documented, standardized and integrated.
  - Management of technology is planned and structured.

APPENDIX A: NATURAL & MANMADE RISK ASSESSMENT MATRIX

The calculation of natural and manmade risk is performed via the below NIST 800-30-influenced risk matrix model:

Natural & Man-Made Risk Matrix		Occurrence Likelihood					
		Remote *[<1% chance of occurrence]*	Highly Unlikely *[1% to 10% chance of occurrence]*	Unlikely [10% to 25% chance of occurrence]	Possible [25% to 70% chance of occurrence]	Likely [70% to 99% chance of occurrence]	Almost Certain [>99% chance of occurrence]
Impact Effect	Catastrophic	6	12	18	24	30	36
	Critical	5	10	15	20	25	30
	Major	4	8	12	16	20	24
	Moderate	3	6	9	12	15	18
	Minor	2	4	6	8	10	12
	Insignificant	1	2	3	4	5	6

Risk Tolerance Threshold (*Moderate Risk*)

INITIAL RISK ASSESSMENT - UNWEIGHTED & AVERAGED - Risk Scoring Range (1 to 36)				
LOW (1-4)	MODERATE (5-11)	HIGH (12-19)	SEVERE (20-29)	EXTREME (30-36)

*Compensating Controls & Control Weighting Convert Risk Score To

FINAL RISK ASSESSMENT - WEIGHTED & AVERAGED - Risk Scoring Range (1 to 180)				
LOW (1-22)	MODERATE (22.1-57)	HIGH (57.1-97)	SEVERE (97.1-147)	EXTREME (147.1-180)

NATURAL & MAN-MADE RISK SUMMARY

Initial Risk Assessment: HIGH — 13 — *Raw Value*

Compensating Factors →

Final Risk Assessment: MODERATE — 41 — *Weighted Value*

Score	Occurrence Likelihood	Impact Effect
5	**Expected** - Virtual certainty the event will occur at some time, under normal business conditions.	**Catastrophic** - Critical, long-term damage or service impact. Financial and reputational damage could be enough to ruin the business.
4	**Likely** - Likely to expect the event to occur at some time, under normal business conditions.	**Major** - Major damage or service impact. Extensive reputational and financial impact, but not enough to ruin the business.
3	**Reasonably Possible** - Reasonable to expect the event could occur at some time, under normal business conditions.	**Moderate** - Noticeable damage or service impact. Harmful reputational and financial impact, but not enough to ruin the business.
2	**Unlikely** - Unlikely to expect the event to occur at some time, under normal business conditions.	**Minor** - Localized or minimal damage or service impact. Minor reputational and financial impact.
1	**Improbable** - Theoretically possible. May only occur under exceptional circumstances.	**Insignificant** - Little to no damage or service impact. No reputational or financial impact.

Cut & paste a screenshot of APPENDIX C from the Excel spreadsheet called "Information Security Risk Assessment Worksheet" – that contains the information security risk assessment calculations, based on your answers from the controls assessment.