CYBERSECURITY RISK ASSESSMENT

ACME Technologies, LLC

Table of Contents

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 Technologies, LLC (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 Technologies, LLC (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:

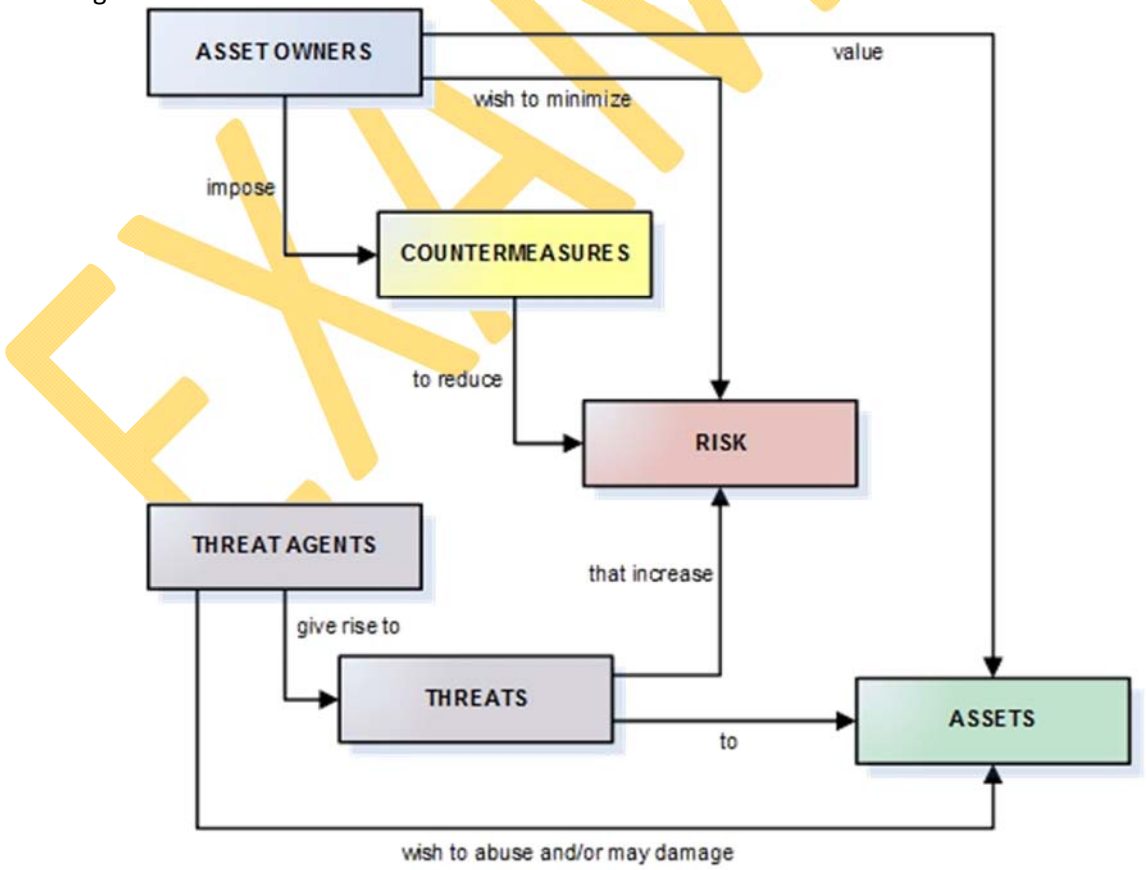

Figure 1: Risk management process flow.

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.

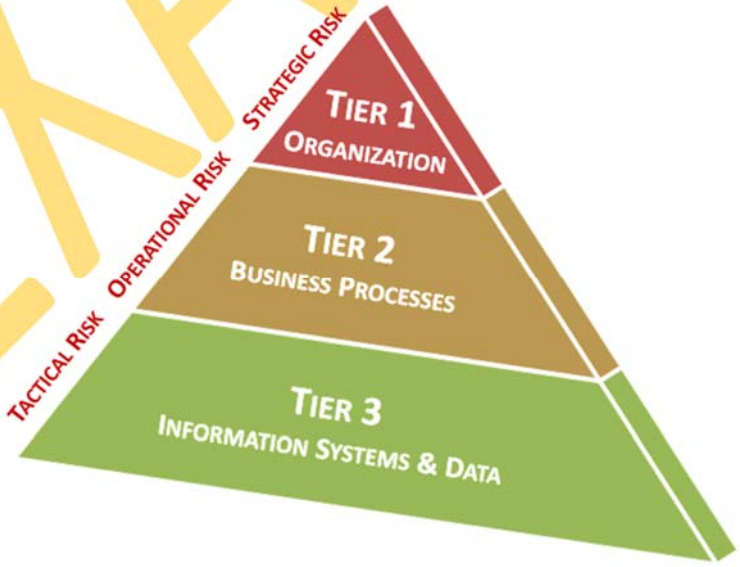

Figure 2: Risk hierarchy flow.

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		MODERATE
	13		*41*
	Raw Value		*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.

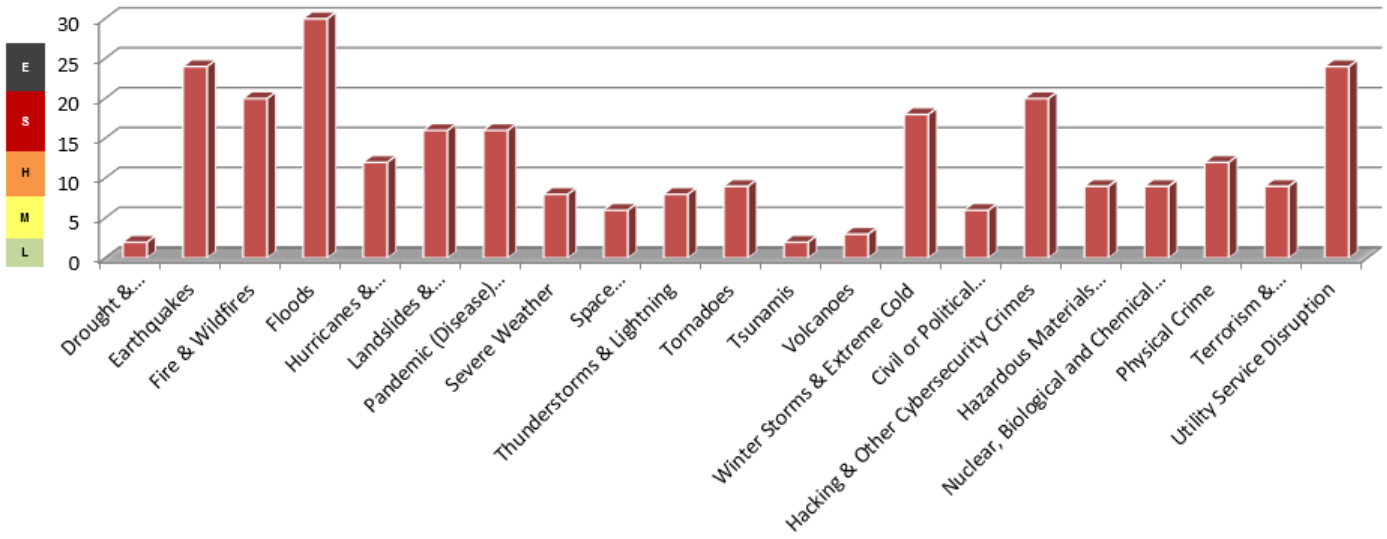

Figure 4: Unweighted Natural & Man-Made Risks

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.

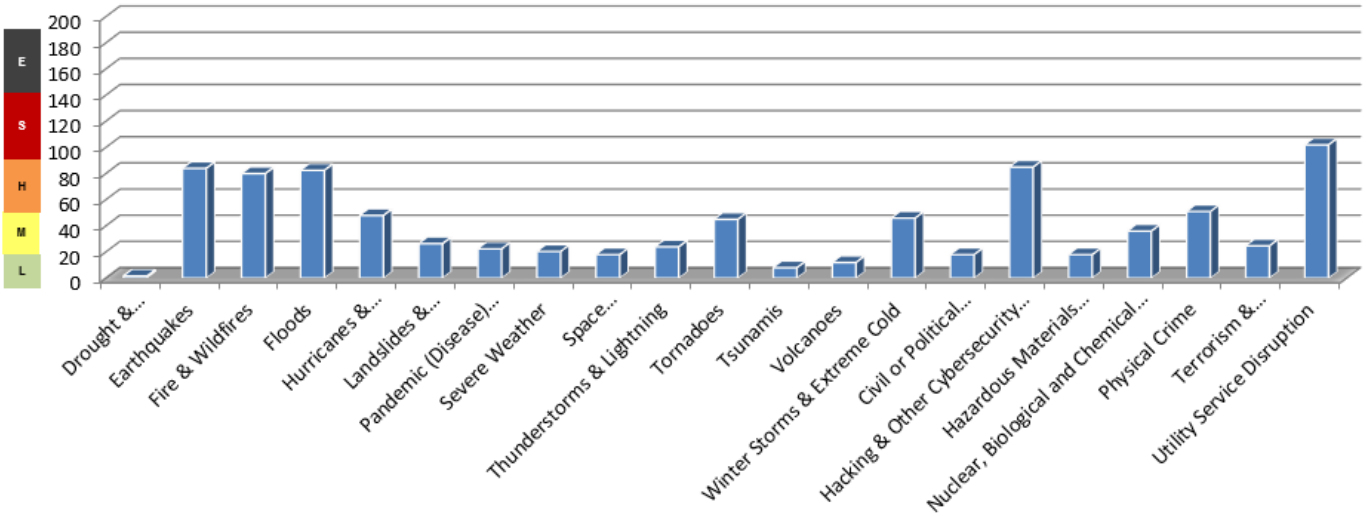

Figure 5: Weighted Natural & Man-Made Risks

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 occurance
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 equiped with a fire suppression system and all backups are replicated off-site daily.

DEFINING APPROPRIATE CONTROLS FOR ASSESSING CYBERSECURITY RISK

The controls used to assess cybersecurity risk are from NIST Special Publication 800-171, *Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organization*. This document can be referenced at - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf. Within NIST 800-171, Tables D-1 through D-14 (Appendix D) provide an informal mapping of the CUI security requirements to the relevant security controls in NIST 800-53 and ISO 27001/27002.

This set of information security best practices was used for the simple reason that that portion of security controls were determined by NIST to be relevant to the security of sensitive information in private industry.

RISK THRESHOLD FOR CYBERSECURITY RISK

Based on management's guidance, ACME's risk tolerance threshold for cybersecurity threats is moderate risk.

While the cybersecurity risks were averaged to earn a **MODERATE** risk assessment, there are still numerous cybersecurity controls that are individually considered **HIGH** risk and require immediate attention.

Reference the ***App C – 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)

CYBERSECURITY RISK SUMMARY

Initial Risk Assessment: MODERATE, 5 (Raw Value)

Compensating Factors

Final Risk Assessment: LOW, 13 (Weighted Value)

Figure 8: Cybersecurity Risk Matrix

BREAKDOWN OF CYBERSECURITY RISKS

Control Description	Likelihood of Control NOT Operating Properly	Potential Impact of Control NOT Operating Properly	Compensating Factors *(see Risk Assessment Notes)*	Assessed Level of Maturity for the Capability (Process / Technology)	Risk Assessment Notes *(Explanation of compensating factors to justify reduction in risk)*
Access to information system is limited to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Improbable	Major	None Available	High level of maturity - capabilities, processes & documentation are robust and comprehensive.	
Information system access is limited to the types of transactions and functions that authorized users are permitted to execute.	Improbable	Moderate	Moderate Impact Reduction	High level of maturity - capabilities, processes & documentation are robust and comprehensive.	Least access necessary principle deployed.
The flow of sensitive data is controlled in accordance with approved authorizations.	Improbable	Major	Significant Impact Reduction	High level of maturity - capabilities, processes & documentation are robust and comprehensive.	Encryption Vault deployed
Separation the duties for individuals is implemented to reduce the risk of malevolent activity without collusion.	Highly Unlikely	Moderate	Moderate Impact Reduction	High level of maturity - capabilities, processes & documentation are robust and comprehensive.	
The principle of least privilege is employed, including for specific security functions and privileged accounts.	Improbable	Moderate	None Available	Moderate level of maturity - capabilities, processes & documentation are informal or not comprehensive.	

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.

GLOSSARY: ACRONYMS & DEFINITIONS

ACRONYMS

ACL	Access Control List.
AD	Active Directory.
AP	Access Point.
DHCP	Dynamic Host Configuration Protocol.
DNS	Directory Naming Service.
GPO	Group Policy Object.
HTML	Hypertext Markup Language.
IRP	Incident Response Plan.
ISP	Internet Service Provider.
LAN	Local Area Network.
PSK	Pre-Shared Key.
SSH	Secure Shell.
SSL	Secure Sockets Layer.
VLAN	Virtual Local Area Network.
VPN	Virtual Private Network.
WAP	Wireless Access Point.
WPA	Wi-Fi Protected Access.
WPA2	Wi-Fi Protected Access version 2.
WISP	Written Information Security Program.

DEFINITIONS

The National Institute of Standards and Technology (NIST) IR 7298, Revision 1, *Glossary of Key Information Security Terms*, is the approved reference document used to define common IT security terms. [1]

[1] NIST IR 7298 - http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf

APPENDIX A: COSO PRINCIPLES

The COSO 2013 principles are focused on the proper governance of an organization, which includes the proper identification and management of associated risks to the business.

Components of Internal Control	#	COSO Principles	How COSO Principles Apply To Our Company
Control Environment	**1**	Demonstrates commitment to integrity and ethical values.	Our company demonstrates a commitment to integrity and ethical values.
	2	Exercises oversight responsibility	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
	3	Establishes structure, authority and responsibility	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
	4	Demonstrates commitment to competence	Our company demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
	5	Enforces accountability	Our company holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
Risk Assessment	**6**	Specifies suitable objectives	Our company specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

	7	Identifies and analyzes risk	Our company identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
	8	Assesses fraud risk	Our company considers he potential for fraud in assessing risks to the achievement of objectives.
	9	Identifies and analyzes significant change	Our company identifies and assesses changes that could significantly impact the system of internal control.
Control Activities	**10**	Selects and develops control activities	Our company selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
	11	Selects and develops general controls over technology	Our company selects and develops general control activities over technology to support the achievement of objectives.
	12	Deploys through policies and procedures	Our company deploys control activities through policies that establish what is expected and procedures that put policies into place.
Information & Communication	**13**	Uses relevant information	Our company obtains or generates and uses relevant, quality information to support the functioning of internal control.
	14	Communicates internally	Our company internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
	15	Communicates externally	Our company communicates with external parties regarding matters affecting the functioning of internal control.
Monitoring Activates	**16**	Conducts ongoing and/or separate evaluations	Our company selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
	17	Evaluates and communicates deficiencies	Our company evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

COSO 2013 Principle 1: The organization demonstrates a commitment to integrity and ethical values.

The following points of focus highlight important characteristics relating to this principle:

- **Sets the Tone at the Top**—The board of directors and management at all levels of the entity demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.
- **Establishes Standards of Conduct**—The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the organization and by outsourced service providers and business partners.
- **Evaluates Adherence to Standards of Conduct**—Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.
- **Addresses Deviations in a Timely Manner**—Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.

COSO 2013 Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

The following points of focus highlight important characteristics relating to this principle:

- **Establishes Oversight Responsibilities**—The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.
- **Applies Relevant Expertise**—The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate actions.
- **Operates Independently**—The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.
- **Provides Oversight for the System of Internal Control**—The board of directors retains oversight responsibility for management's design, implementation, and conduct of internal control:
  - *Control Environment*—Establishing integrity and ethical values, oversight structures, authority and responsibility, expectations of competence, and accountability to the board.
  - *Risk Assessment*—Overseeing management's assessment of risks to the achievement of objectives, including the potential impact of significant changes, fraud, and management override of internal control.
  - *Control Activities*—Providing oversight to senior management in the development and performance of control activities.
  - *Information and Communication*—Analyzing and discussing information relating to the entity's achievement of objectives.
  - *Monitoring Activities*—Assessing and overseeing the nature and scope of monitoring activities and management's evaluation and remediation of deficiencies.

COSO 2013 Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

The following points of focus highlight important characteristics relating to this principle:

- **Considers All Structures of the Entity**—Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.
- **Establishes Reporting Lines**—Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.
- **Defines, Assigns, and Limits Authorities and Responsibilities**—Management and the board of directors delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization:
  - *Board of Directors*—Retains authority over significant decisions and reviews management's assignments and limitations of authorities and responsibilities
  - *Senior Management*—Establishes directives, guidance, and control to enable management and other personnel to understand and carry out their internal control responsibilities