INFORMATION SECURITY RISK ASSESSMENT

ACME Technologies, LLC

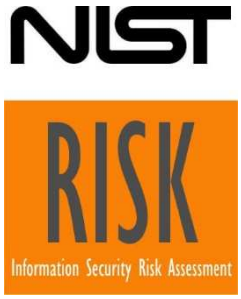

Table of Contents

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:

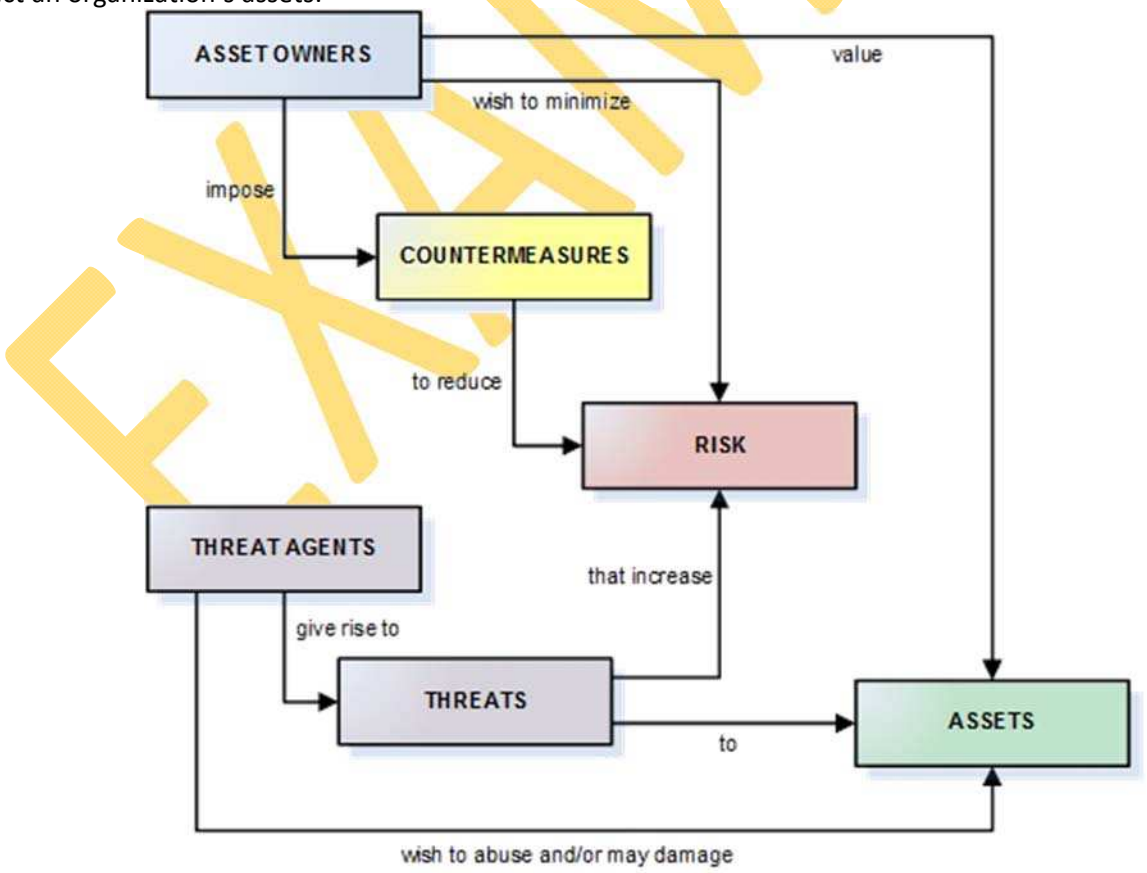

Figure 1: Risk management process flow.

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.

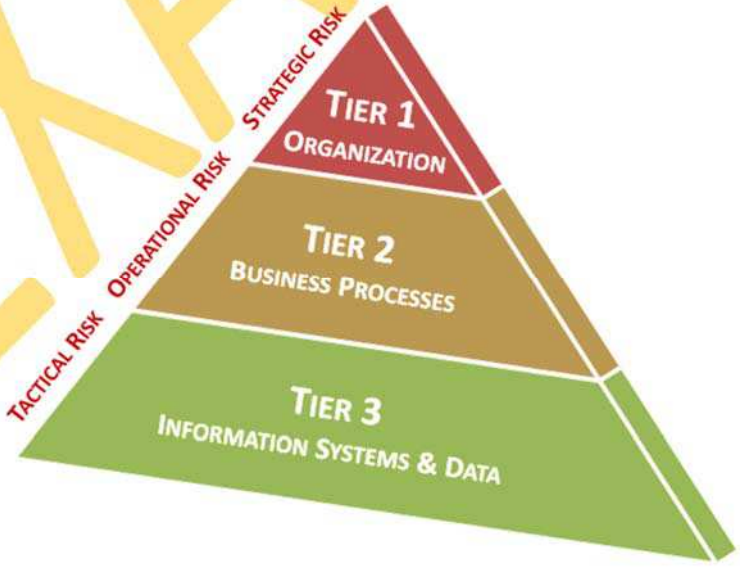

Figure 2: Risk hierarchy flow.

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		Impact Effect				
		1 *Insignificant*	2 *Minor*	3 *Moderate*	4 *Major*	5 *Catastrophic*
Occurrence Likelihood	5 *Expected*	5	10	15	20	25
	4 *Likely*	4	8	12	16	20
	3 *Reasonably Possible*	3	6	9	12	15
	2 *Unlikely*	2	4	6	8	10
	1 *Improbable*	1	2	3	4	5

Risk Tolerance Threshold *(Moderate Risk)*

Initial Risk Assessment
HIGH
12
Raw Value

INITIAL RISK ASSESSMENT - UNWEIGHTED & AVERAGED - Scoring Range (1 to 25)			
LOW (1-5)	MODERATE (6-11)	HIGH (12-19)	EXTREME (20-25)

Final Risk Assessment*
MODERATE
38
Averaged Value

*Compensating Controls & Control Weighting Convert Risk Score To

FINAL RISK ASSESSMENT - WEIGHTED & AVERAGED - Scoring Range (1 to 125)			
LOW (1-27)	MODERATE (28-60)	HIGH (61-99)	EXTREME (100-125)

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.

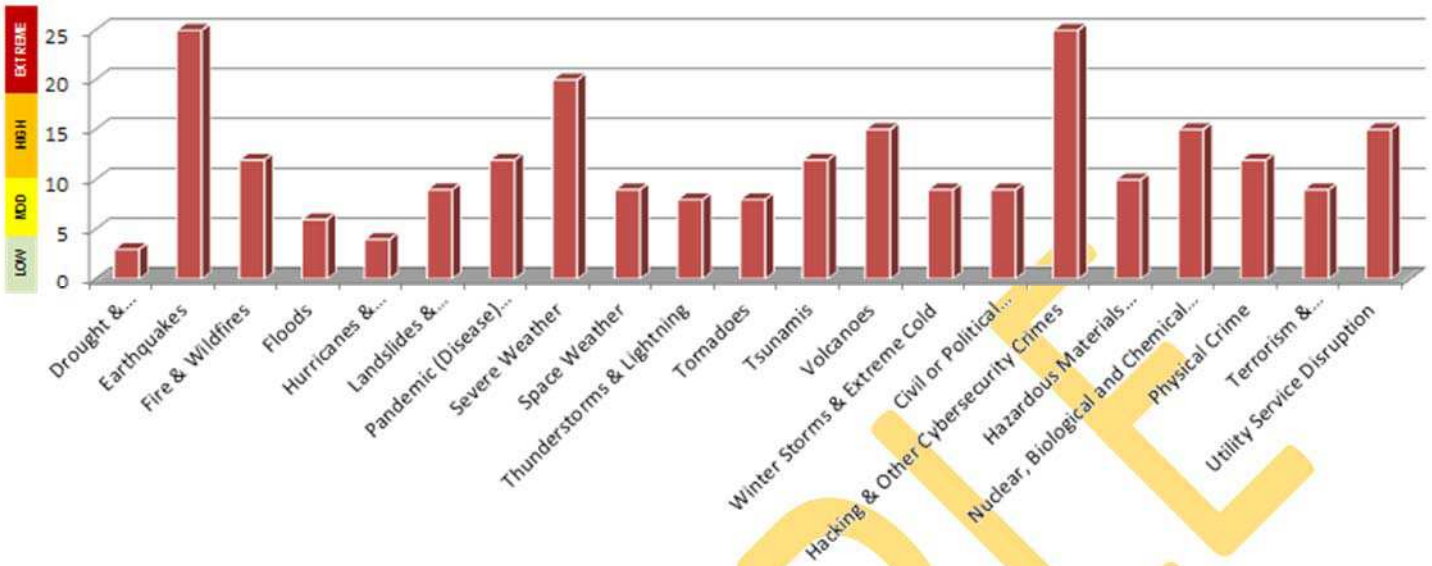

Figure 4: Unweighted Natural & Man-Made Risks

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.

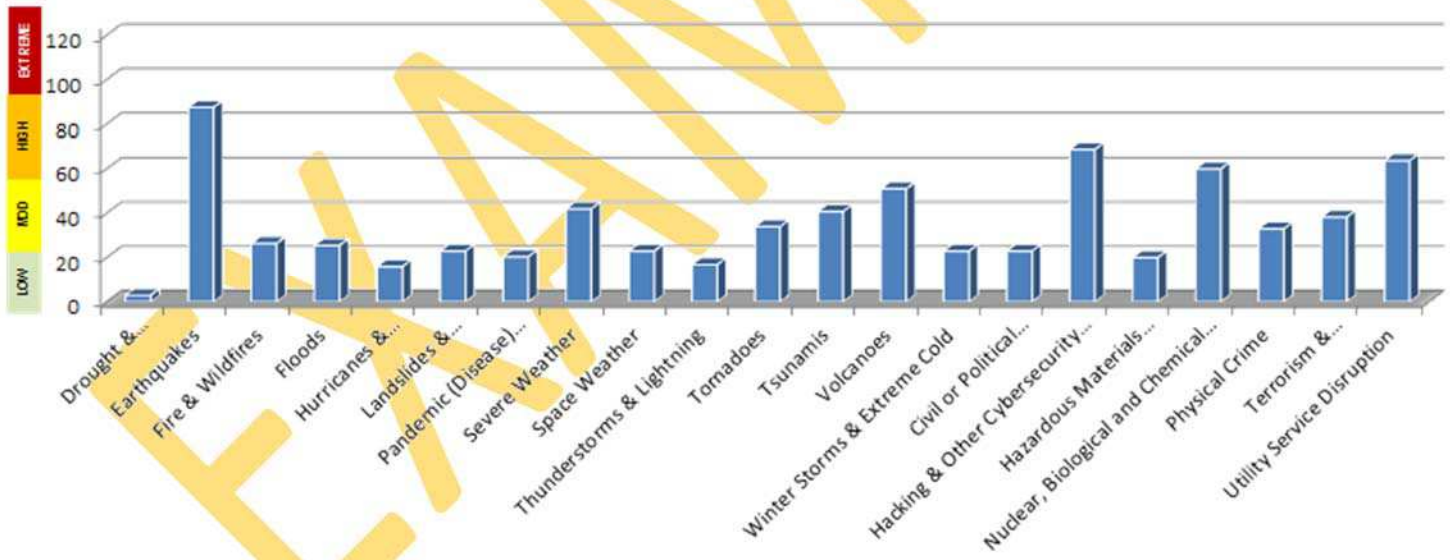

Figure 5: Weighted Natural & Man-Made Risks

BREAKDOWN OF NATURAL THREATS & ASSOCIATED RISKS

Threat Type	Threat Description	Occurrence Likelihood	Potential Impact	Compensating Control(s)	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.	Reasonably Possible	Insignificant	None Available	- Business is in a geographic region affected by this natural threat. However, the business is not in an industry primarily affected by this natural threat. - It would be expected that services the company relies on and the general economy would likely be impacted. - Moderate to long-term service disruption of any utility service would render the facility unusable. - Internet-based / cloud services running core business functions would be unimpacted by local or regional service disruptions.
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 long-lasting.	Expected	Catastrophic	Moderate Impact Reduction	- Business is located in a geographic region not generally affected by this natural threat. - If the facility was damaged, an alternate site would be able to be setup using XYZ Solutions. - Moderate to long-term service disruption of any utility service would render the facility unusable. - Internet-based / cloud services running core business functions would be unimpacted by local or regional service disruptions.
Fire & Wildfires	When thinking of a fire in a building, picture a total loss to data stored on servers or all of the paper files being consumed in the fire.	Reasonably Possible	Major	Significant Impact Reduction	- Business is in a geographic region that is affected by this natural threat. - XYZ Solutions is a hosted solution, so data loss is not a concern. - If the facility was damaged, an alternate site would be able to be setup using XYZ Solutions. - Moderate to long-term service disruption of any utility service would render the facility unusable.

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.

Cybersecurity Risk Matrix		Impact Effect				
		1 *Insignificant*	2 *Minor*	3 *Moderate*	4 *Major*	5 *Catastrophic*
Occurrence Likelihood	5 *Expected*	5	10	15	20	25
	4 *Likely*	4	8	12	16	20
	3 *Reasonably Possible*	3	6	9	12	15
	2 *Unlikely*	2	4	6	8	10
	1 *Improbable*	1	2	3	4	5

Initial Risk Assessment: HIGH 12 *Raw Value*

Final Risk Assessment*: MODERATE 37 *Averaged Value*

■ ■ ■ ■ Risk Tolerance Threshold *(Moderate Risk)*

INITIAL RISK ASSESSMENT - UNWEIGHTED & AVERAGED - Scoring Range (1 to 25)			
LOW (1-5)	MODERATE (6-11)	HIGH (12-19)	EXTREME (20-25)

*Compensating Controls & Control Weighting Convert Risk Score To

FINAL RISK ASSESSMENT - WEIGHTED & AVERAGED - Scoring Range (1 to 125)			
LOW (1-27)	MODERATE (28-60)	HIGH (61-99)	EXTREME (100-125)

Figure 8: Cybersecurity Risk Matrix

BREAKDOWN OF CYBERSECURITY RISKS

Control #	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)*
C-AC-1	Access to information system is limited to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Unlikely	Catastrophic	Significant Impact Reduction	High level of maturity - capabilities, processes & documentation are robust and comprehensive.	- ACME is predominantly a Microsoft environment and Active Directory (AD) is utilized. - Role Based Access Control (RBAC) is implemented in AD to limit access to authorized users.
C-AC-2	Information system access is limited to the types of transactions and functions that authorized users are permitted to execute.	Reasonably Possible	Major	Moderate Impact Reduction	Moderate level of maturity - capabilities, processes & documentation are informal or not comprehensive.	- Vendor recommended best practices are implemented to limit system functionality.
C-AC-3	The flow of sensitive data is controlled in accordance with approved authorizations.	Reasonably Possible	Major	Minimal Impact Reduction	High level of maturity - capabilities, processes & documentation are robust and comprehensive.	- End user training stresses what personnel are expected to do when handling data. - Preventative mechanisms are only administrative and not technical in nature.
C-AC-4	Separation the duties for individuals is implemented to reduce the risk of malevolent activity without collusion.	Likely	Moderate	Minimal Impact Reduction	Low level of maturity - very limited capabilities. Processes are ad hoc & documentation is little to none.	- Managers have discretion to implement separation of duties (SOD), but it is not required by position or role.
C-AC-5	The principle of least privilege is employed, including for specific security functions and privileged accounts.	Reasonably Possible	Catastrophic	Significant Impact Reduction	High level of maturity - capabilities, processes & documentation are robust and comprehensive.	- Vendor recommended best practices are implemented to limit system functionality. - Access rights are reviewed by managers on a regular basis.

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