Your Logo
Will Be
Placed Here

CYBERSECURITY
RISK MANAGEMENT PROGRAM

ACME Business Consulting, LLC

RMP
Risk Management Program

Table of Contents

FOREWORD

Every organization faces a variety of cyber risks from external and internal sources. Cyber risks must be evaluated against the possibility that an event will occur and adversely affect the achievement of ACME's objectives.

While the results of the risk assessment will ultimately drive the allocation of entity resources against control activities which prevent, detect, and manage cyber risk, investments must also be directed at the risk assessment process itself. ACME has finite resources and its decisions to invest in control activities must be based on relevant, quality information that prioritizes funding to the information systems that are the most critical to the entity.

In addition to natural threats that affect ACME, we also have to be prepared to address man-made threats. Malicious actors, especially those motivated by financial gain, tend to operate on a cost/reward basis. The perpetrators of cyber-attacks, and the motivations behind their attacks, generally fall into the following broad categories:

- **Nation States**
  - Hostile foreign nations who seek intellectual property and trade secrets for military and competitive advantage.
  - Those that seek to steal national security secrets.

- **Organized Criminals**
  - Perpetrators that use sophisticated tools to steal money or private and sensitive information about an entity's consumers (e.g., identity theft).

- **Terrorists**
  - Terrorist groups or individuals who look to use the Internet to launch cyber-attacks against critical infrastructure, including financial institutions.

- **Hacktivists**
  - Individuals or groups that want to make a social or political statement by stealing or publishing an organization's sensitive information.
  - Individuals or groups that want to make a social or political statement by rendering an organization's resources unusable.

- **Insiders**
  - Trusted individuals, who are inside the organization, who sell or share the organization's sensitive information.

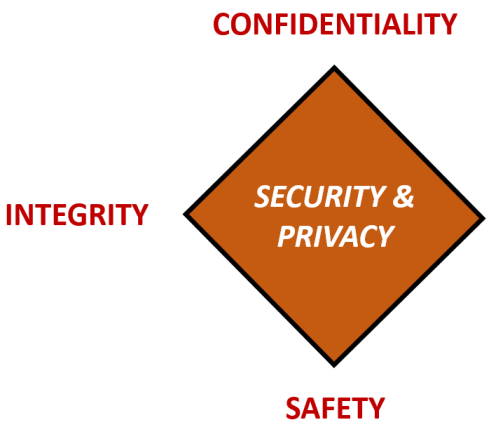
Cybersecurity risk assessments influence management decisions about control activities deployed against information systems that support ACME's objectives. Therefore, it is important that senior management and other critical stakeholders drive the risk assessment process to identify what must be protected in alignment with ACME's objectives.

ACME's cybersecurity risk assessments must begin first by understanding what systems, applications and services are valuable to the organization. The value should be measured against the potential impact to ACME's business objectives.

The Risk Management Program (RMP) provides definitive guidance on the prescribed measures used to manage cybersecurity-related risk at ACME Business Consulting, LLC (ACME).

ACME is committed to protecting its employees, partners, clients and ACME from damaging acts that are intentional or unintentional. An effective cybersecurity program is a team effort involving the participation and support of every ACME user who interacts with data and systems. Therefore, it is the responsibility of every user to conduct their activities accordingly to reduce risk across the enterprise.

Security and privacy are a byproduct of Confidentiality, Integrity, Availability and Safety (CIAS) measures. Consequently, the security of ACME's data must include controls and safeguards to offset possible threats to ACME's systems, applications and services.

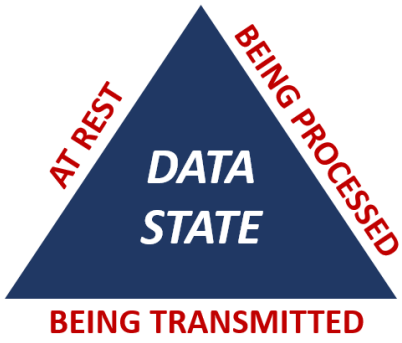


- **CONFIDENTIALITY** – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.
- **INTEGRITY** – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- **AVAILABILITY** – Availability addresses ensuring timely and reliable access to and use of information.
- **SAFETY** – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated by nefarious actors.

Commensurate with risk, CIAS measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes protection against accidental loss or destruction, regardless of what state data is in.

At any given time, data can be viewed as being in only one (1) of the following states:

- Data is at rest;
- Data is being processed; or
- Data is being transmitted.



Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes protecting data and systems from accidental loss or destruction.

What Is Risk?

One important concept to understand is that risk is variable - it is able to be changed and is not static. This is important to keep in mind, since the "risk rating" is subject to change as the risk environment changes.

What is important to understand is that risk represents the potential exposure to harm or loss. This is commonly quantified as a combination of potential impact, likelihood and control effectiveness. Appendix A – Types of Information & Technology Risk provides examples of specific types of risk associated with information and technology.

What Is Meant By Managing Risk?

Risk management is the coordinated activities which optimize the management of potential opportunities and adverse effects. The alternative to risk management is crisis management. Risk management provides a way of realizing potential opportunities without exposing ACME to unnecessary peril.

Risk Management Activities

Risk management activities are logical and systematic processes that can be used when making decisions to improve the effectiveness and efficiency of performance. The activities have these characteristics:

- Should be integrated into everyday work;
- Identifies and helps prepare for what might happen;
- Involves taking action to avoid or reduce unwanted exposures;
- Involves taking action to maximize opportunities identified;
- Encourages proactive management, rather than reactive management; and
- Identifies opportunities to improve performance.

Risk Management Benefits

The benefits of comprehensive risk management include:

- Improves transparency in decision making because criteria are made explicit;
- Reduces costly surprises, since undesirable risks are identified and managed;
- Establishes a more rigorous basis for strategic planning as a result of a structured consideration of the key elements of risk;
- Allows for better identification and exploitation of opportunities; and
- Improves effectiveness and efficiency in compliance with applicable statutory, regulatory and contractual requirements.

Corporate Governance

Corporate governance refers to the way in which ACME is directed and controlled in order to achieve its strategic goals and operational objectives. It involves governance of ACME to ensure the control environment makes the organization reliable in achieving its goals and objectives within an acceptable degree of risk.

Essential to corporate governance and compliance are management and staff knowledge of:

- Statutory, regulatory and contractual requirements;
- ACME's internal policies, standards and procedures;
- Impact of changes; and
- Consequences of non-compliance.

When Should Risk Be Managed?

Risk must be managed continuously. All business decisions involve the management of some kind of risk. That is true whether the decisions affect everyday operations (e.g., deciding work priorities, making budget or staffing decisions) or decisions about policies, strategies or projects.

It is desirable to develop a mindset of a conscious approach to managing the risks inherent in every decision. Many decisions have to be made quickly and are often based on intuition, but it is nevertheless important to think about the risks involved. The formal step-by-step process is to be applied to decision making at all levels throughout ACME. The risk management process involves establishing the context, identification, analysis, evaluation, treatment, monitoring and review of risks. Effective communication and consultation with stakeholders is required throughout the risk management process, as well.

Risks can arise from both internal and external sources. While it is not possible to have a totally risk-free environment, it may be possible to treat risk by avoiding, reducing, transferring, or accepting the risks.

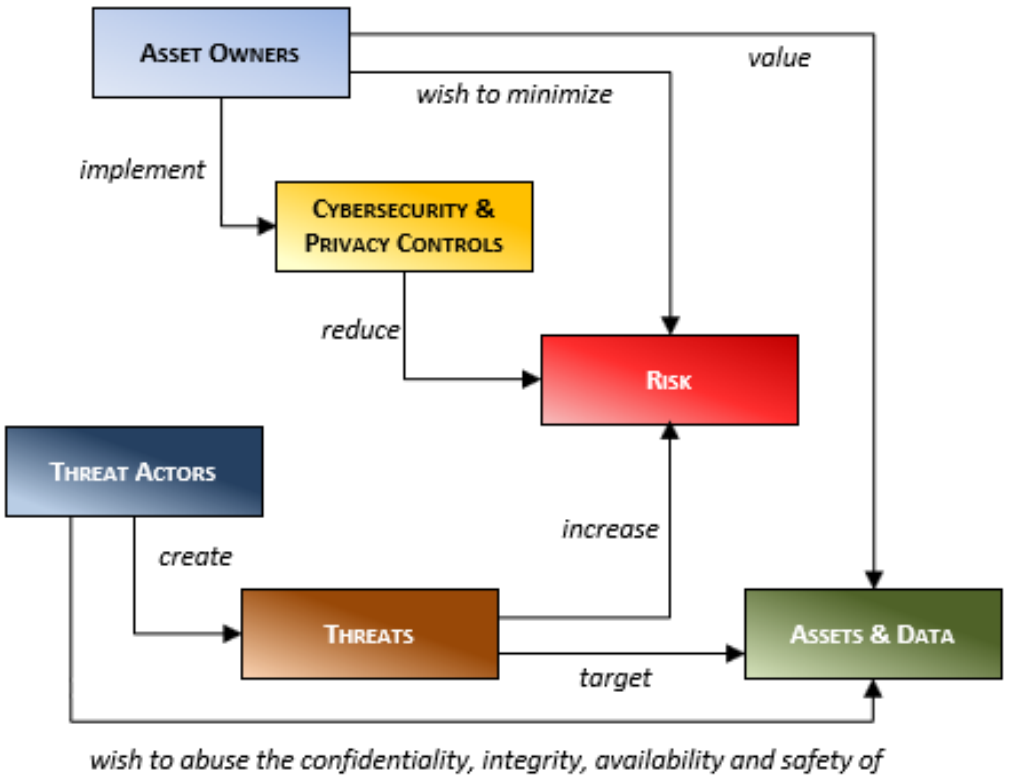


Figure 1: Understanding connected nature of managing risk.

Who Has The Authority To Manage Risk?

Determining how to handle risk is always a management decision. Appendix B – Risk Roles & Responsibilities provides more granular guidance on risk-related roles and responsibilities.

It is important to keep in mind that risk management is far more than a "technology issue," and it requires the direct involvement of business process owners, IT personnel, and cybersecurity. Each has a role to play in risk management operations:

Business Unit

- The Business Unit (BU) that requires the technology to be in place and function ultimately "owns" the risk associated with ongoing operation of systems.
- Business Process Owners (BPOs) are individuals within BUs who are the central point of contact for IT and cybersecurity to work with on risk management decisions.

Information Technology (IT)

- IT has a shared responsibility with the BUs to securely operate and maintain systems.
- IT executes vulnerability management tasks.

Cybersecurity

- Cybersecurity operates as a facilitator of vulnerability and patch management decisions.
- Cybersecurity focuses on providing expert guidance and support to both IT and the Business Unit.

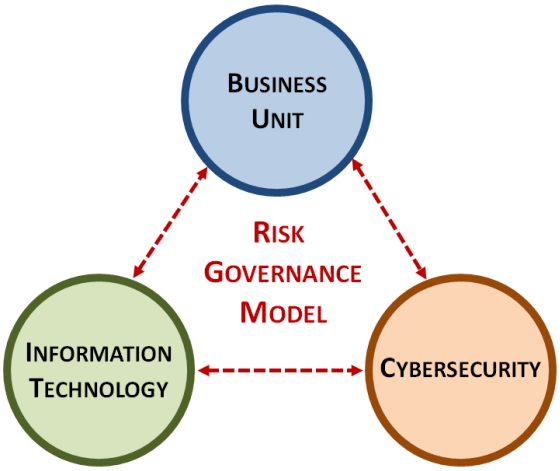


Figure 2: Risk governance model.

HOW ARE RISK MANAGEMENT DECISIONS ESCALATED?

To empower management at the lowest level, four (4) tiers are established that allow for escalation. These tiers provide ACME with the appropriate level of management oversight, based on the level of risk:

TIER 1 – LINE MANAGEMENT

Line Management is authorized to decide on risk treatment options for **LOW** risks and:

- May decide on a risk treatment plan or decide to accept the risk.
- Should develop a plan to incorporate remediation actions within a reasonable period of time.

TIER 2 – SENIOR MANAGEMENT

Senior Management is authorized to decide on risk treatment options for **MEDIUM** risks and:

- May decide on a risk treatment plan or decide to accept the risk.
- Should develop a plan to incorporate remediation actions within a reasonable period of time.

TIER 3 – EXECUTIVE MANAGEMENT

Executive Management is authorized to decide on risk treatment options for **HIGH** risks and:

- May decide on a risk treatment plan or decide to accept up to HIGH risk.
- Must develop a plan to incorporate remediation actions within a reasonable period of time.

TIER 4 – BOARD OF DIRECTORS

The Board of Directors (or a designated risk steering committee) is authorized to decide on risk treatment options for both **SEVERE** and **EXTREME** risks and:

- Must decide on a risk treatment plan.
- Must develop a reasonable plan to proactively address risk treatment actions in a timely manner.

The intent of a tiered approach is for a repeatable, scalable process that manages risk at the lowest possible level of management. Once the risk is identified and evaluated, the appropriate level of management will be approached for a decision on risk treatment options.

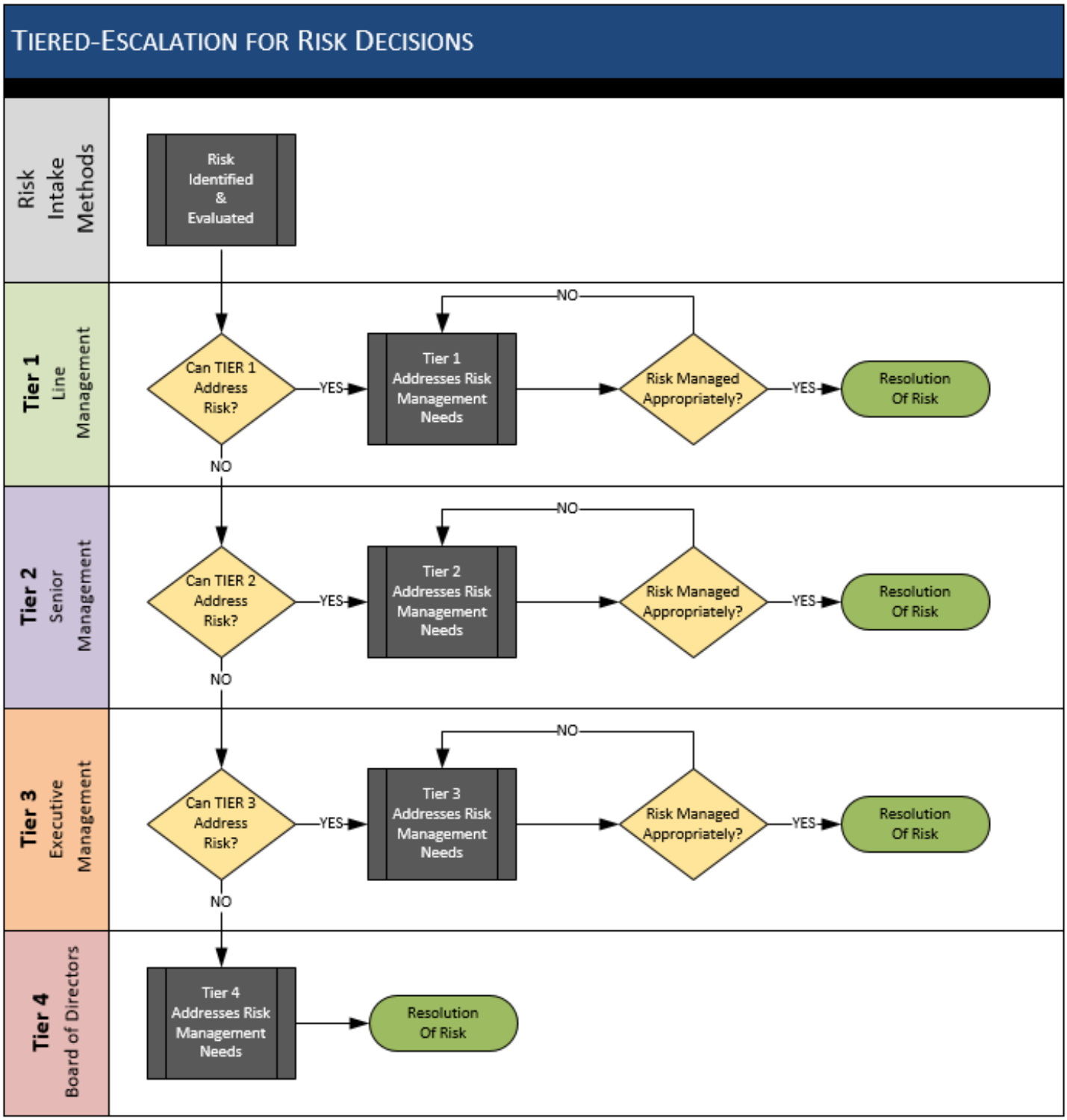


Figure 3: Governance of Risk Decisions

How Do We Categorize Risk?

The following five (5) categories establish the risk taxonomy for ACME. These categories range from "low" to "extreme" risk and allow for a more granular understanding of risk. The intent of standardizing risk terminology for categories is so that all ACME personnel can speak the same "risk language" across the enterprise. Categorization also allows management to compare and prioritize risks.

Based on the degree of exposure, these risk categories help enable ACME's leadership to have informed decisions at the appropriate level of management oversight. See the Threat & Risk Assessment (TRA) Methodology section for more details on calculating risk categories.

Low Risk

Insignificant damage could occur from a low risk:

- Financial impact is negligible (less than $[DEFINE MODERATE RISK VALUE]).
- Impact would not be damaging to ACME's reputation or impede business operations.
- There are no violations of contractual, statutory or regulatory requirements.

Medium Risk

Minimal damage could occur from a medium risk:

- Financial impact is potentially between $[DEFINE MODERATE RISK VALUE] and $[DEFINE MAJOR RISK VALUE].
- Impact would not be damaging to ACME's reputation or impede business operations.
- Impact could impede Business Core (CL3) or Business Supporting (CL4) systems or business operations.
- This may involve a violation of contractual requirements.
- There are no violations of statutory or regulatory requirements.

High Risk

Moderate damage could occur from a high risk:

- Impact could include damage to ACME's reputation.
- Impact could impede Business Essential (CL2) systems or business operations.
- This may involve a violation of contractual, statutory and/or regulatory requirements.
- Financial impact is potentially between $[DEFINE MAJOR RISK VALUE] and $[DEFINE CRITICAL RISK VALUE].
- ACME's stock price could be negatively affected (<5% negative deviation).

Severe Risk

Significant financial and brand damage could occur from a severe risk.

- Impact could include significant damage to ACME's reputation.
- Impact could impede Mission Critical (CL1), and below, systems or business operations.
- Impact could negatively affect ACME's short-term competitive position.
- This may involve a violation of contractual, statutory and/or regulatory requirements.
- Financial impact is potentially between $[DEFINE CRITICAL RISK VALUE] and $[DEFINE CATASTROPHIC RISK VALUE].
- ACME's stock price could be moderately affected (>5% negative deviation).

Extreme Risk

Extensive financial and long-term brand damage could occur from a critical risk:

- Impact could include extensive damage to ACME's reputation.
- Impact could impede Mission Critical (CL1) systems or business operations.
- Impact could negatively affect ACME's long-term competitive position.
- Risk scenarios involving potential physical harm or fatality are included in this category.
- Financial impact is potentially over $[DEFINE CATASTROPHIC RISK VALUE].
- ACME's stock price could be significantly affected (>10% negative deviation).

CONTEXT OF RISK MANAGEMENT

Managers need to identify their role in contributing to ACME's wider goals, objectives, values, policies and strategies when making decisions about risk. This assists with establishing the criteria that determines whether a risk is tolerable or not.

Questions to clarify for context about risk include, but are not limited to:

- What are ACME's strengths and weaknesses?
- What are the major outcomes expected?
- What are the major threats and opportunities presented?
- What are the significant factors that impact ACME's internal and external environment?
- What is the policy, program, process or activity to which the risk management process is being applied?
- What problems were identified in previous reviews?
- What risk criteria should be established?
- Who are the stakeholders?

RISK MANAGEMENT MATURITY LEVELS

The Risk Maturity Model (RMM) provides standardized criteria by which organizations can benchmark risk management strategies to identify program maturity levels, strengths and weaknesses, and next steps in the evolution of an Enterprise Risk Management (ERM) program.[1] Appendix C – Risk Maturity Model provides additional information on this topic, with specifics about which characteristics exist for each maturity level.

The RMM maturity levels are organized progressively from "ad hoc" to "leadership" and depict corresponding levels of risk management competency. The seven drivers for the systematic progression of levels are termed as "Attributes" and include variables such as Process Management, Risk Appetite Management, Uncovering Risks, and Business Resiliency and Sustainability.

The RMM helps the leadership team define a roadmap to the successful adoption of an ERM. An ERM should be designed to view risks across all areas of the business to identify strategic opportunities and reduce uncertainty. A unique feature of the RMM is its applicability regardless of the frameworks and standards that are used.

RISK MANAGEMENT MODEL (RMM)

There are six (6) distinct levels of the RMM:

Figure 5: Risk maturity levels.

TARGET MATURITY LEVEL

As part of ACME's multi-year strategy to reduce risk, the target is to achieve at least a Level 3 (Repeatable) maturity level.

DEFINING THE RISK APPETITE

ACME is committed to the management of risk as an integral part of its operations, focusing on strategies to minimize risks to ACME's mission and objectives. Staff must consider the risk appetite in strategic and operational decision-making.

To achieve its objectives, ACME must undertake activities that carry risks. To that end, ACME's risk appetite will often be different at an operational level from that at a strategic level.

[1] Risk Management Society - https://www.rims.org/resources/ERM/Pages/RiskMaturityModelFAQ.aspx

MAINTAINING FLEXIBILITY – HYBRID APPROACH TO RISK MANAGEMENT

There is no single "best practice" to managing risk, and risk assessments may require a multidisciplinary approach since risks may cover a wide range of causes and consequences. Therefore, ACME is adopting a "best in class" or hybrid approach to implementing its risk management methodology. This will allow ACME to be flexible in how it assesses risk.

Since every organization is managed by different people, who have unique skills and experiences that drive their professional judgments, one organization's accepted method for internal control will not equally apply to other organizations. As it pertains to ACME, while the COSO framework provides principles and points of focus that direct ACME towards well-designed control activities, COSO was not intended to dictate the specific controls that should be implemented. Therefore, ACME must also rely upon additional frameworks to provide granularity in evaluating risks in order for ACME to be secure, vigilant, and resilient.

ACME will use guidance from the following best practice frameworks to manage risk, according to which framework is most applicable:

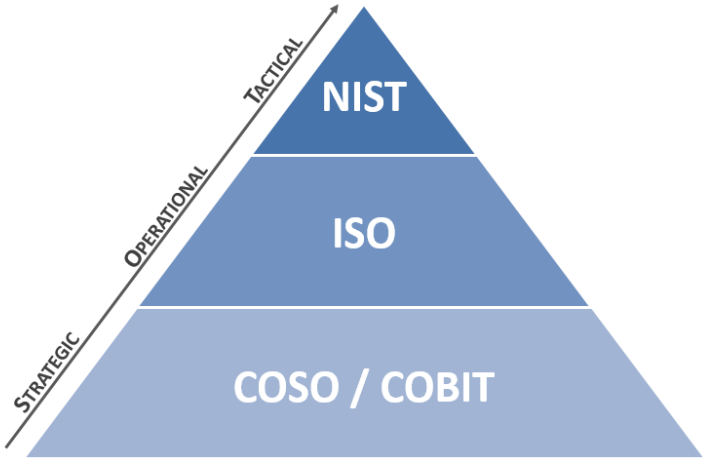


Figure 6: Hierarchical risk frameworks.

COSO / COBIT – STRATEGIC APPROACH TO RISK MANAGEMENT

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative and is dedicated to providing thought leadership through the development of frameworks and guidance on Enterprise Risk Management (ERM), internal control and fraud deterrence.
- The 2013 version of the COSO framework establishes the enterprise-level model used to manage risk.[2]
- Control Objectives for Information and Related Technology (COBIT) establishes a control base to help implement COSO.

ISO – OPERATIONAL APPROACH TO RISK MANAGEMENT

- The International Organization for Standardization (ISO) 31010 establishes a framework for managing the risk that builds on existing ISO standards, guidelines, and practices to guide organizations to reduce the potential impacts of cyber risks.[3]
- ISO 31010 guidance establishes the initiative/program-level model used to manage risk since it provides a higher-level model for evaluating and managing risk.

NIST – TACTICAL APPROACH TO RISK MANAGEMENT

- The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce publishes cybersecurity guidance for the public and private sectors.
- NIST Special Publication 800-37 establishes a framework for managing the risk that builds on existing NIST standards, guidelines, and practices to guide organizations to reduce the potential impacts of cyber risks.[4]
- NIST SP 800-37 guidance establishes the system/application/service-level model used to manage risk since it provides a granular model for evaluating and managing risk throughout the lifecycle of an asset or project.

[2] COSO - http://www.coso.org/
[3] ISO 31010 - http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51073
[4] NIST 800-37 - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

Enterprise Level – Strategic Approach to Risk Management

When a company manages cyber risk through a COSO lens, it enables the board of directors and senior executives to better communicate their business objectives, their definition of critical information systems, and related risk tolerance levels. This enables others within the organization, including IT personnel, to perform a detailed cyber risk analysis by evaluating the information systems that are most likely to be targeted by attackers, the likely attack methods, and the points of intended exploitation. In turn, appropriate control activities can be put in place to address such risks.

Ultimately, ACME needs to identify its systems/applications/services, determine their value, and protect them against cyber-attacks. This is accomplished through the deployment of control activities that are commensurate with the value of the assets. To achieve these results, business and IT stakeholders must initially arrive at a common understanding of the structure of the business, including outsourced service providers, and the related business objectives and sub-objectives that are important to ACME. While this concept is easy to grasp, it is important to formally document this approach. Documenting the business structure will help ensure that processes and controls can be executed consistently with relevant, quality information, in a manner that allows continuous refinement as people, process, and technology evolves along with ACME's objectives.

In order to manage cyber risks, ACME needs to view its cyber risk profile through the components of internal control. This includes, but is not limited to:

- Control Environment
  - Does the board of directors understand ACME's cyber risk profile and are they informed of how the organization is managing the evolving cyber risks management faces?
- Risk Assessment
  - Has ACME and its critical stakeholders evaluated its operations, reporting, and compliance objectives and gathered information to understand how cyber risk could impact such objectives?
- Control Activities
  - Has ACME developed control activities, including general control activities over technology, that enable ACME to manage cyber risk within the level of tolerance acceptable to the organization?
  - Have such control activities been deployed through formalized policies and procedures?
- Information and Communication
  - Has ACME identified information requirements to manage internal control over cyber risk?
  - Has ACME defined internal and external communication channels and protocols that support the functioning of internal control?
  - How will ACME respond to, manage, and communicate a cyber risk event?
- Monitoring Activities
  - How will ACME select, develop, and perform evaluations to ascertain the design and operating effectiveness of internal controls that address cyber risks?
  - When deficiencies are identified how are these deficiencies communicated and prioritized for corrective action?
  - What is ACME doing to monitor their cyber risk profile?

COSO 2013 Internal Control Components

Principles 6 through 9 of the COSO 2013 framework focus on risk assessment.

COSO 2013 Internal Control Components				
Control Environment	**Risk Assessment**	**Control Activities**	**Information & Communication**	**Monitoring Activities**
1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibilities 3. Establishes structure, authority, and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures	13. Uses relevant, quality information 14. Communicates internally 15. Communicates externally	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Figure 7: COSO 2013 risk management components.

Risk Assessments for Assets / Projects (Tactical Focus)

At the project / asset-level, ACME's management must ensure that risk assessments are conducted to understand and document risks from security failures that may cause loss of confidentiality, integrity, or availability. Risk assessments should:

- Take into account the potential adverse impact on ACME's reputation, operations, and assets; and
- Be conducted by personnel associated with the activities subject to assessment.

Risk assessments should be conducted on any system or project internal or external to ACME, including applications, servers, networks, and any process or procedure by which these systems are administered and/or maintained. ACME encourages periodic risk assessments for determining areas of vulnerability and to initiate appropriate remediation.

The execution, development, and implementation of remediation programs are the responsibility of ACME's management. Users are expected to cooperate fully with any risk assessments being conducted on systems for which they are held accountable.

See the Threat & Risk Assessment (TRA) Methodology section for guidance on determining potential impacts, potential likelihood, and system criticality levels.

Cybersecurity Control Selection for Projects / Assets (Tactical Focus)

For the evaluation of cybersecurity controls for projects or assets, the following frameworks will be leveraged to determine the appropriate control set, based on applicability and appropriateness:

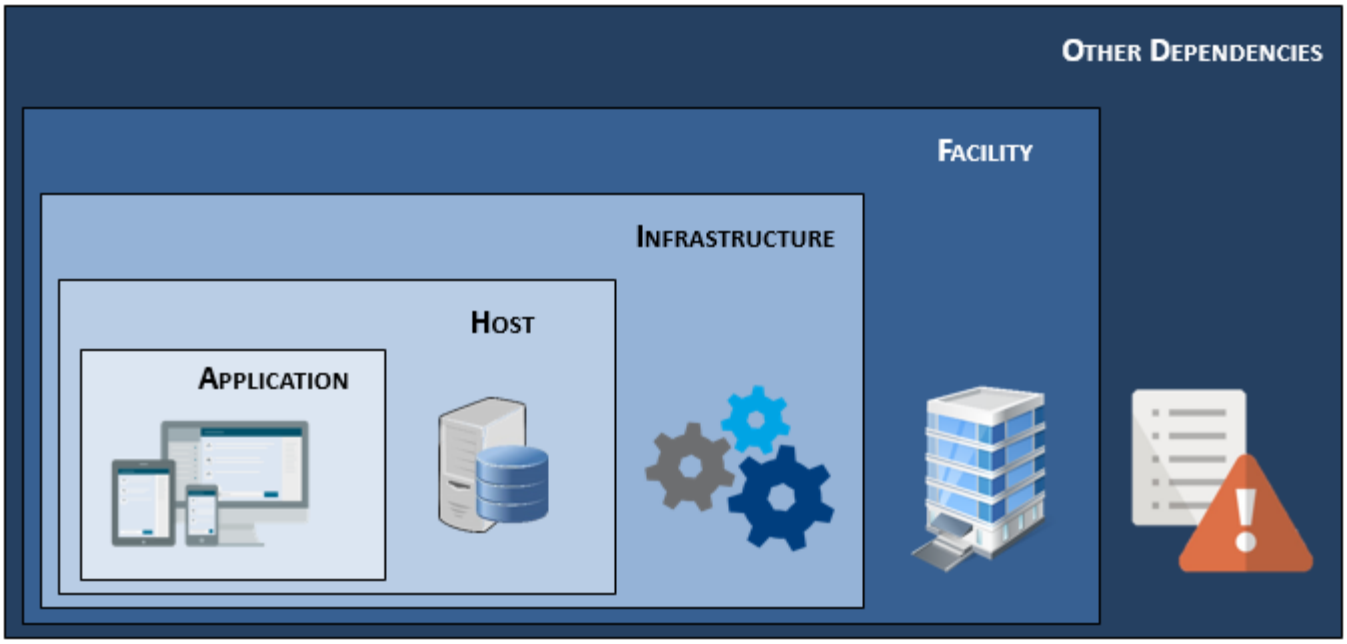
- ISO 27002:2013 – *Code of Practice for Information Security Management*[12]
- NIST Special Publication 800-53 Revision 4 – *Security and Privacy Controls for Federal Information Systems and Organizations*[13]
- NIST Cybersecurity Framework – *Framework for Improving Critical Infrastructure Cybersecurity*[14]

Deviations from using a complete framework are acceptable. However, a business justification needs to be documented that describes why controls were used, as well as why certain controls or groups of controls were excluded.

Risk Assessment Layers

Dependencies are of critical importance when assessing assets, since risk can have a cascading effect.

Ideally, a risk assessment for a specific application or host should leverage existing risk assessments that address "upstream" risks. For example, a well-designed and securely coded application could be compromised if the host system it is running on is insecure. Similarly, the application could be made unavailable if the datacenter lacks measures to ensure uptime against natural or man-made threats.



[12] ISO 27002:2013 - http://www.iso.org/iso/catalogue_detail?csnumber=54533
[13] NIST 800-53 rev4 - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[14] NIST Cybersecurity Framework - http://www.nist.gov/cyberframework/

Figure 10: Layers of Risk

As part of overall risk management, ACME should perform several formal risk assessments, which are meant to be used as references for more detailed project-specific risk assessments. At a minimum, standing risk assessments should exist for:

- Datacenters (including infrastructure risks)
- Secure configurations for hosts and major applications (e.g., databases, email, Intranet)

By being able to leverage those existing risk assessments, it will allow for more efficient assessments of applications.

Applications

Risks associated with applications include, but are not limited to:

- Insecure code (developers did not follow secure coding practices)
- Default/weak credentials
- Weak encryption
- Passwords/sensitive data stored in clear text
- Poor permissions management
- Missing software patches
- Logging/monitoring not being performed

Host

Risks associated with hosts include, but are not limited to:

- Lack of system hardening
- Default/weak credentials
- Lack of encryption at rest
- Role-Based Access Control (RBAC) improperly managed
- Missing software patches
- Logging/monitoring not being performed
- Backups not being performed

Infrastructure

Risks associated with infrastructure include, but are not limited to:

- Improper equipment (e.g., consumer-grade networking hardware vs. business/enterprise-grade)
- Lack of system hardening
- Default/weak credentials
- Lack of encryption in transit
- Role-Based Access Control (RBAC) improperly managed
- Missing software patches
- Logging/monitoring not being performed

Facility

Risks associated with facilities include, but are not limited to the lack of:

- Physical access controls
- Environmental controls
- Redundant utilities
- Trained personnel (disaster recovery plan)

Other Dependencies

Risks associated with other dependencies include, but are not limited to:

- Software escrow agreements
- Developer/vendor management
- International trans-border data transfers

Estimating Probability

Three (3) general approaches are commonly employed to estimate probability:

- Relevant historical data;
- Probability forecasts; and
- Expert opinion.

These approaches may be used individually or jointly.

Relevant Historical Data

The use of relevant historical data to identify events or situations which have occurred in the past can be extrapolated to estimate the probability of their occurrence in the future.

- The data used should be relevant to the type of system, facility, organization or activity being considered and to the operational standards of the organization involved.
- If historically there is a very low frequency of occurrence, then any estimate of probability will be very uncertain.
- This applies especially for zero occurrences when one cannot assume the event, situation or circumstance will not occur in the future.

Probability Forecasts

Probability forecasts use predictive techniques such as fault tree analysis and event tree analysis. When historical data are unavailable or inadequate, it is necessary to derive probability by analysis of the system, activity, equipment or organization and its associated failure or success states. Numerical data for equipment, personnel, organizations and systems from operational experience or published data sources are then combined to produce an estimate of the probability of the top event.

- When using predictive techniques, it is important to ensure that due allowance has been made in the analysis for the possibility of common mode failures involving the coincidental failure of multiple different parts or components of the system arising from the same cause.
- Simulation techniques may be required to generate the probability of equipment and structural failures due to aging and other degradation processes.

Expert Opinion

Expert opinion can be used in a systematic and structured process to estimate probability.

- Expert judgments should draw upon all relevant available information including historical, system-specific, organizational-specific, experimental, design, etc.
- There are several formal methods for eliciting expert judgment which provide aid to the formulation of appropriate questions.
- The methods available include the Delphi approach, paired comparisons, category rating, and absolute probability judgments.

Defining Criticality Levels (CL) for Assets / Systems / Data

One component of assessing risk is to understand the criticality of systems and data. By having a clear understanding of the Criticality Level (CL) for an asset, system, application, service or data, determining potential impact will be more accurate.

There are four (4) criticality levels:

- Mission Critical (CL1);
- Business Essential (CL2);
- Business Core (CL3); and
- Business Supporting (CL4).

Mission Critical (CL1)

Mission Critical systems handle information that is determined to be vital to the operations or mission effectiveness of ACME.

The impact of a CL1 system, or its data, being unavailable includes, but is not limited to:

- Enterprise-wide business stoppage with significant revenue impact – can be anything that creates a significant impact on ACME's ability to perform its mission;
- Public, wide-spread damage to ACME's reputation;
- Direct, negative & long-term impact on customer satisfaction; and
- Risk to human health or the environment.

Examples of CL1 systems include, but are not limited to:

- *Enterprise Resource Management (ERM) system (e.g., SAP)*
- *Active Directory (AD)*
- *Ability to process Point of Sale (PoS) or eCommerce payments*

BUSINESS ESSENTIAL (CL2)

Business Essential systems handle information that is important to the support of ACME's primary operations.

The impact of a CL2 system, or its data, being unavailable includes, but is not limited to:

- Enterprise-wide delay or degradation in providing important support services that may seriously impact mission effectiveness or the ability to operate;
- Department-level business stoppage with direct or indirect revenue impact; and
- Direct, negative & short-term impact on customer satisfaction.

Examples of CL2 systems include, but are not limited to:

- *Email (e.g., Exchange)*
- *Payroll systems*
- *Corporate website functionality*
- *Corporate mobile device application functionality*
- *HVAC systems*
- *Customer support / call center functionality*

BUSINESS CORE (CL3)

Business Core systems handle information that is necessary for the conduct of day-to-day business, but they are not mission critical in the short-term.

The impact of a CL3 system, or its data, being unavailable includes, but is not limited to:

- Widespread delays or degradation of services or routine activities;
- Widespread employee productivity degradation;
- Indirect revenue impact; and
- Indirect negative customer satisfaction.

Examples of CL3 systems include, but are not limited to:

- *Test / Development / Staging environment*
- *Security Incident Event Monitor (SIEM) / log collector*
- *Internal / Intranet web functionality*

BUSINESS SUPPORTING (CL4)

Business Supporting systems are the least important category of systems and handle information that is used in the conduct of routine, day-to-day business. CL4 systems are not mission-critical in the short or long term.

The impact of a CL4 system, or its data, being unavailable includes, but is not limited to:

- Localized employee productivity degradation;
- Localized delays or degradation of services or routine activities;
- No revenue impact; and
- No impact on customer satisfaction.

Examples of CL4 systems include, but are not limited to:

- *Team-level metrics reporting*
- *Team-level productivity or reporting tools*

Information & Technology Risks

ACMEhas an increasing dependence on information technology to support its day-to-day operations. Information technology systems are relied upon for communications, transaction processing, record maintenance and security.

A risk to any organization is the confidentiality, availability, and integrity of its information systems and the data they hold. Management should undertake a full review and assessment of the risks associated with recording, capturing, using and storing data.

Information Risks

Matters that should be considered for information risks include, but are not limited to:

- Accuracy of data;
- Access control;
- Data integrity; and
- Insufficient or unskilled resources that impact IT services.

Technology Risks

Matters that should be considered for technology risks include, but are not limited to:

- System failure or unavailability;
- Production changes that impact IT services' stability or availability (e.g., change management);
- Information system and data security;
- Vendor/service provider failure;
- Irretrievable data or delays in retrieving data (e.g., backups);
- Cloud-based service offerings;
- Bring Your Own Device (BYOD);
- Social media;
- Collaborative environments (e.g., SharePoint, wikis, Google Docs or Office 365);
- Legacy applications or systems;
- Uncontrolled network environments; and
- Personal storage devices.

It may not be possible for every internal and external information system to be free of exposure to significant risk. Therefore, in anticipation of possible failures, consideration must be given to how disruptions to normal operations caused by data/information technology issues will be managed to minimize the time needed to resume normal business operations.

Examples

Risk	Description
Resource Constraint	Insufficient or unskilled resources impact IT services.
Change Management	Production changes impact the stability or availability of services.
Data Loss	Data is irretrievable or there are unacceptable delays in retrieving data.
Configuration Management	Configuration management practices create unstable or insecure systems.
Business Continuity	IT recovery objectives for the business are not able to be achieved.
Incident Management	Failure to properly manage incidents impacts IT and business services.
Environmental Exposure	Natural and man-made events expose IT services to damage in environmental conditions.
Physical Security	Insufficient access control allows unauthorized physical access to IT services and data.
Segregation of Duties	Transactions are processed or approved beyond authority level.
Logging & Monitoring	Activities are unable to be traced back to users or source.

Appendix D – Risk Assessment Techniques

The techniques listed below have unique attributes, which make selecting the correct technique for a specific risk assessment very important. While a simple matrix can work for most simple risk assessments, other methods are needed for more complex assessments.

Look Up Methods

TECHNIQUE	TECHNIQUE DESCRIPTION	QUANTITATIVE SOLUTION?	USEFUL FOR RISK IDENTIFICATION?	FACTORS TO CONSIDER			STRENGTH IN EVALUATING RISK	RISK ANALYSIS STRENGTHS		
				REQUIRED SKILLS	DEGREE OF UNCERTAINTY	DEGREE OF COMPLEXITY		CONSEQUENCE	PROBABILITY	LEVEL OF RISK
Consequence & Probability Matrix	The consequence/probability matrix is a means of combining qualitative or semi-quantitative ratings of consequence and probability to produce a level of risk or risk rating. The format of the matrix and the definitions applied to it depend on the context in which it is used, and it is important that an appropriate design is used for the circumstances.	No	Great Choice	Low	Low	Low	OK	Great Choice	Great Choice	Great Choice
Multi-Criteria Decision Analysis (MCDA)	The objective is to use a range of criteria to objectively and transparently assess the overall worthiness of a set of risk treatment options. In general, the overall goal is to produce a preference of order between the available options. The analysis involves the development of a matrix of options and criteria which are ranked and aggregated to provide an overall score for each option.	No	OK	Medium	Medium	Medium	OK	Great Choice	OK	Great Choice
Check Lists	A simple form of risk identification. A technique which provides a listing of typical uncertainties which need to be considered. Users refer to a previously developed list, codes or standards.	No	Great Choice	Low	Low	Low	Weak	Weak	Weak	Weak