Concepts of Risk Management

By: H. Morgan Jordan

Flatiron School

June 22, 2022

Table of Contents

[Abstract 3](#_Toc106803008)

[M1-1 – Concepts of Risk Management 4](#_Toc106803009)

[M1-2 – Risk Assessments 5](#_Toc106803010)

[M2-1 – Risk Treatment and Methods & Controls 6](#_Toc106803011)

[M2-2 – Risk Management Frameworks 7](#_Toc106803012)

[M3-1 – Risk Communication 8](#_Toc106803013)

[M4-1 – Final Project 9](#_Toc106803014)

[References 10](#_Toc106803015)

# Abstract

There are many different things to consider when speaking about Risk Management. First you must understand what exactly risk is. From there you will discover your tolerance for certain risks and which framework you would like to utilize in order to perform risk assessments. Once risk assessments are completed, your company will have to decide how to handle the risks that were uncovered through these evaluations. There are many Risk Management Frameworks (RMFs) that can assist you with all aspects of risk management and allow you to utilize risk registers or POA&Ms (Plan of Action and Milestones) to effectively communicate resolved and current risks company wide.

# M1-1 – Concepts of Risk Management

Risk is generally described as “exposure to the chance of injury or loss”. When we apply risk to compliance the meaning changes slightly and is geared more toward an organization’s potential vulnerabilities to legal penalties as well as financial and material loss by neglecting to be in accordance with industry laws and regulations, internal policies or recommended best practices. This could also be seen as an “integrity risk”.

Enterprise risk management (ERM) is a comprehensive, disciplined approach to revealing, addressing, and managing the risks of an organization. ERM takes a look at risk management from a strategic organization-wide viewpoint, making it a ‘top-down’ methodology. This type of methodology makes it necessary for leadership to evaluate teams and set their expectations accordingly instead of the responsibility falling on individual departments like the ‘silo approach’ of traditional risk management. ERM, therefore, presents as a more comprehensive method, encouraging communication throughout the company and ensuring that every risk is accounted for.

Risk tolerance, appetite, and aversion help express the level of risk a company is prepared to accept in order to accomplish its strategic objectives. Creating risk appetite frameworks helps management comprehend the organization’s risk profile, find the most favorable balance between risk and return and create a healthy risk culture within the company. These frameworks need to be both quantitative and qualitative by incorporating business strategies and goals with solid levels or risk tolerance and limits. Without these evaluations, inherent and residual risk becomes significantly more likely.

In 2009, the International Organization for Standardization (ISO) created an international standard named ‘ISO 31000’. This standard was intended to serve as a model for the construction, application and maintenance of risk management. It describes an organized and methodical process, during which companies manage risk by revealing it, evaluating, and analyzing whether the risk should be altered by risk treatment to comply with their risk criteria. Risk management can be used by an entire company, at many different levels and departments, anytime, as well as being applied to specific operations, projects and ventures.

# M1-2 – Risk Assessments

ISO 27006 delineates requirements and supplies guidance for any entity providing audits and certification of an information security management system (ISMS). It is mostly meant to support the accreditation of certification entities supplying ISMS certification. The requirements within this International Standard need to be demonstrated in terms of capability and dependability by any entity providing ISMS certification and the guidance within this International Standard supplies more interpretations of these requirements. ISO 27006 focuses on audit teams’ responsibilities allowing the assessor to identify areas of risk. Each entity has to create an internal audit team that is independent of incentives to mislead while also being cross-functional in order to prepare for external audit and meet the eventual goal of transparency. The guidance goes even more in-depth to stipulate how to provide a complete report. While this model provides clear guidelines for audits and how to maintain them, it does not account for how a CISO could use this information in an assessment, meaning even a well-performed audit can still leave areas of risk.

NIST SP 800-30 provides guidance for performing risk assessments of federal information systems and institutions, expanding the guidance in SP 800-39. Risk evaluations, completed in all three tiers of the risk management hierarchy, are a component of an overall risk management process. This provides senior leaders and executives with the information necessary to determine suitable COAs in reaction to established risks. NIST provides a holistic approach and is applicable to both mature and immature entities, but it requires an information gatekeeper or team to apply the guidelines beyond an acceptable level. Given that this is not mandatory to follow, the increase in cost to adopt these guidelines has to be evaluated by the entity itself.

Both guides allow for more comprehensive qualitative data. Some areas of these frameworks focus in on the qualitative assessment of assessing the risk level itself. Neither provide guidance on what is an acceptable measure of that quality and leave the quantitative assessment relatively bare, leaving the quantitative structure for the organization to decide on which poses a risk that can be calculated with a risk aversion or bias.

# M2-1 – Risk Treatment and Methods & Controls

There are four risk treatment methods: Mitigate, Accept, Avoid/Eliminate, and Transfer. To mitigate risk means that you try to reduce the likelihood or impact that specific risk can have on your organization. Accepting risk implies that you acknowledge and choose not to resolve, transfer or mitigate the risk at hand. In order transfer a risk you would need to assign or move the risk to a third-party. And finally, avoiding/eliminating a risk translates to completely eliminating or foregoing that risk by whatever means necessary.

ISO 27002 provides best-practice guidance on applying the controls listed in ISO 27001 while NIST 800-53 defines the minimum baseline of security control for all U.S. federal information security as long they don’t relate to national security. NIST 800-53 has 20 families of controls and ISO 27002 contains 14 control sets. From ISO 27002 is the control set ‘A.7 Human Resource Security’ which states that employees and contractor should be mindful of their part in protecting the organization’s information prior to and during employment, making the risk *transfer* to the employees or contractors. As far as mitigating data, most other families and control sets apply to that effort. There is also a term called compensating controls that is essentially a kind of internal control that allows the organization to adopt an alternative method to obtain the same outcome. These tend to be used when there is a technical or professional restriction that prevents obtaining the established goal and is a method to mitigate the risk of the original requirement.

Both ISO 27002 and 27003 do not allow you to get certified, but they each give valuable help to organizations attempting to reach ISO 27001 requirements. ISO 27002 focuses its instruction on “determining and implementing controls for information security risk treatment in and information security management system (ISMS) based on ISO 27001”. Meanwhile, ISO 27003 is geared more toward a broad overview of the requirements for an ISMS, based on ISO 27001. So, one could see how combining both ISO 27002 and 27003 could help organizations comprehend, classify, and implement the described standards from ISO 27001. In regard to NIST 800-53A, it is simply an extension to NIST 800-53 that gives supplementary instruction on how to conduct an assessment of controls, making it more comprehensible.

# M2-2 – Risk Management Frameworks

Risk Management Frameworks (RMFs) generate an effective means in assisting organizations in selecting the necessary security controls deemed essential to protect the organization, its team members, and all operations and assets they possess. By design, this allows access to each layer of an organization, further comprehending the goals of every project and observing all operating systems to determine and evaluate all potential risks. RMFs supply key security information in order to build successful risk management and mitigation strategies for an organization. As such, there are many frameworks out there for organizations to choose from.

ISO 31000, as previously described, is an organized and methodical process, during which companies manage risk by revealing it, evaluating, and analyzing whether the risk should be altered by risk treatment to comply with their risk criteria. There is also ISO 27005 which is the international standard describing how to administer an information security risk evaluation in accordance with the requirements listed in ISO 27001. COBIT was first released in 1996 by ISACA and assists organizations in creating, arranging, and establishing strategies in regard to information management and governance. The NIST RMF gives organizations a method that incorporates security, privacy and cyber supply chain risk management tasks into the system development life cycle. ITIL is not necessarily a defined process but provides a framework with the main objectives of discovering, assessing, and controlling risks that have been identified using a risk matrix. TARA is an engineering methodology utilized to recognize and evaluate cyber vulnerabilities and choose countermeasures adequate at reducing those vulnerabilities. Factor Analysis of Information Risk (FAIR) is a framework that summarizes and monetizes risk, essentially breaking down risk by identifying and characterizing the building blocks that comprise risk and their relationship to one another. The final framework is Operationally Critical Threat, Asset and Vulnerability Evaluation. OCTAVE develops qualitative risk evaluation criteria that describes the organization’s operational risk tolerances, identifies assets (with their corresponding vulnerabilities and threats) important to the mission, determines and evaluates the potential consequences of those threats, and initiates continuous improvements for risk mitigation.

# M3-1 – Risk Communication

A common tool used in risk management is a risk register. This tool identifies potential risks for an organization whether it be for regulation compliance or to minimize potential issues that may impact business operations. By ensuring one location for all risks to be registered, this allows teams to see precisely what each risk is, who it is assigned to, and the current plan of action to address it. These registers typically contain descriptions of the risk/threat, how they occurred and the vulnerable department that they apply to. The remaining delimiters are regarded as more of a risk status by being marked as high, moderate, or low depending on the amount of risk they could potentially hold.

Another tool used to mitigate and assess risks is a POA&M (Plan of Actions and Milestones). This tool is a high-structured, version-controlled, and sensitive document mostly used within military and defense working environments. POA&Ms identify tasks needing to be completed, detailing the resources required to accomplish the items within the plan, any necessary milestones to complete the tasks, and scheduled completion dates for each milestone.

Both of these tools help the user attain the same goal, one location where authorized personnel can review current identified risks and how they will be addressed should they occur. What makes them different is the fact that one is more verbose than the other, which is a typical occurrence with military and defense information. One downside to the POA&M that I have noticed is that there is no real delineation of priority regarding these tasks like with risk registers and their high, moderate, and low ratings. Risk registers are also slightly lacking in information regardless of the ratings themselves though. Altogether I think they are both valuable tools to be used depending on the environment that they are being applied to and how much detail is required.

# M4-1 – Final Project

Leviton Financial Corporation (LFC) is currently bound by many external governance requirements. In California, they are regulated by the Department of Financial Protection and Innovation (DFPI) along with the California Consumer Privacy Act (CCPA) which is similar to the EU’s GDPR. DFPI supplies protections to consumers and services to companies involved in financial dealings. LFC is also bound by the FDIC (Federal Deposit Insurance Corporation), the Gramm-Leach-Bliley Act (GLBA), and the Fair Credit Reporting Act (FCRA). The FDIC has regulations regarding anti-money laundering, consumer identification, and reporting, just to name a few. The GLBA governs the gathering of PII by banks and financial institutions and FCRA regulated the collection and utilization of credit information.

In order to successfully conduct business in Singapore, LFC will have to follow the rules and regulations listed in the Banking Act 1970 and the Monetary Authority of Singapore Act 1970. The United Kingdom has a primary framework legislation governing the regulation or banking and financial services known as FSMA (Financial Services and Markets Act 2000). Although that may be the primary framework there is also the EU-derived legislation (including GDPR), which set minimum requirements for banks and bank services through various laws following the UK’s departure from the European Union in 2020. Financial regulations in Argentina are provided by the Financial Entities Law (21,526) with the Central Bank of the Republic of Argentina sitting as the regulating authority, providing communications that have been incorporated to consolidated regulations. To operate a banking institution in France, LFC must follow EU law (to include GDPR), French legislation, and other regulatory authority regulations (European Central Bank, Prudential and Resolution Control Authority, the AMF).

The computing environment for the new LFC data center should be considered a high priority given that LFC is wanting to have very high availability and provide complete redundancy. By utilizing the NIST risk management framework steps we can identify and categorize LFC’s organizational systems, create security controls to protect confidentiality, integrity, and availability, implement those security controls, conduct assessments, determine permitted risks, and continuously monitor to maintain LFC’s regulatory compliance.

All of the control families that NIST provides apply in some way to every organization, but there are a few that stand out to me more than others when it comes to LFC’s new data center. Access control regarding PII is a major security issue. This controls who has access to which assets and reporting capabilities such as account management, system privileges, and remote access. Configuration management (CM) will also be a large component. CM involves a baseline configuration to operate as the foundation for potential builds or modifications to information systems. There will need to be a contingency plan in place as well in case a cybersecurity event occurs. This involves contingency plan testing, updating, training, backups, and system reconstitution. Identification and authentication for organizational and non-organizational users will need to be made a priority as well. There is also the matter of physical and environmental (PE) protection to consider. PE would contain controls such as physical access authorizations, monitoring, visitor records, power, lighting, fire protection, etc. System and Information Integrity (SI) would protect the new LFC data center from potential malicious code or spam along with monitoring the information system, providing security alerts, and maintaining software and firmware integrity.

When considering a location to build a new data center, there are quite a few factors to consider. The first factor being the ease of building. Comparatively, San Francisco (SF) is much more difficult to build in versus Salt Lake City (SLC) and Oklahoma City (OC). Another factor would be the weather conditions seeing as a humid, wet climate, such as that in SF, would not be beneficial to electronic equipment. Also, the propensity for natural disasters, such as tornadoes and earthquakes, is more likely to occur in OC. These types of natural disasters could cause a lot of damage to the data center and all the equipment contained within. Thirdly, a corporation looking to build a new data center would need to look at electricity costs, stability, and availability. SF regularly faces the threat of rolling blackouts along with their high electricity costs while OC and SLC have lower costs. Finally, there are tax exemptions regarding data centers available for both SLC and OC. Based off of only these above listed factors, I would have to advise LFC to build a data center in Salt Lake City seeing as it possesses the best traits when compared to Oklahoma City and San Francisco.

Once a final location is decided upon for the new data center it would be wise to consider creating a business continuity and disaster recovery plan (BCDR). BCDRs are a combination of strategies, policies, and procedures about what an organization should do in order to effectively respond or adapt to potential threats or disruptive events while minimizing the overall impact those threats would have to the company. This will allow LFC to reduce overall risk, resume operations after an outage or disruption, and help mitigate the risk of data loss and safeguard against reputational damage. For a data center, a couple risky scenarios that stand out to me first would be power outages or malware attacks. By addressing these and many other potential disasters with the appropriate communications, we can ensure that routine business continues smoothly with minimal to no downtime or data loss. The use of a risk register or POA&M (Plan of Actions and Milestones) can effectively communicate current and ongoing threats to LFCs new data center. Seeing as LFC is a financial institution, I would greatly consider the more detailed POA&M. Through proper upkeep, this type of document will keep all employees up to date on what potential or current risks there are to LFC and how to handle them should they occur.

In order to come up with a sound Data Loss Prevention (DLP) solution, we must first know what information we are wanting to protect. In the financial industry there are many pieces of PII that are needed, which include, but is not limited to: legal names, credit card numbers, account numbers, social security numbers, addresses, etc. By using a regular expression pattern among other various methods, DLP can detect sensitive data and analyze content for common patterns such as a 16-digit card number or a 9-digit social security number. Operating much like a SIEM or intrusion prevention system (IPS), a DLP would send alerts regarding any detected suspicious movement and notify IT teams of the potential breach. In event of a violation, DLP can encrypt data and perform other actions preventing users from accidentally or maliciously sharing sensitive information. DLP additionally provides reports, adhering to compliance and auditing requirements while also allowing the company to identify areas of weakness.

# References

1. <https://www.dictionary.com/browse/risk>
2. <https://www.techtarget.com/searchcio/definition/compliance-risk#:~:text=Compliance%20risk%20is%20an%20organization's,also%20known%20as%20integrity%20risk>.
3. <https://reciprocity.com/what-is-enterprise-risk-management-its-importance/>
4. <file:///Users/morganjordan/Downloads/GRC200-M1-1-Slides-Risk%20Management.pdf>
5. <https://www.soa.org/globalassets/assets/Files/Research/Projects/research-risk-app-link-report.pdf>
6. <https://pecb.com/whitepaper/iso-31000-risk-management--principles-and-guidelines#:~:text=ISO%2031000%3A2009%20describes%20a,to%20satisfy%20their%20risk%20criteria>.
7. <https://www.iso.org/standard/62313.html>
8. <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>
9. <https://alexisschottenstein.medium.com/understanding-risk-assessments-nist-sp-800-and-is0-2700-guidelines-e9694c8b890a>
10. <https://www.pivotpointsecurity.com/blog/risk-tolerance-in-business/#:~:text=Avoid%2Fresolve%20the%20risk%20(completely,to%20resolve%2C%20transfer%20or%20mitigate)>
11. <https://www.itgovernanceusa.com/iso27002>
12. <https://blog.netwrix.com/2021/03/03/nist-800-53/#:~:text=NIST%20800%2D53%20is%20a%20regulatory%20standard%20that%20defines%20the,Information%20Processing%20Standard%20(FIPS)>.
13. <https://www.strongdm.com/blog/iso-27001-vs-27002-vs-27003#:~:text=ISO%2027002%20focuses%20its%20guidance,ISMS%2C%20based%20on%20ISO%2027001>.
14. <https://grcmusings.com/a-primer-on-nist-800-53-rev-5-800-53a-and-800-53b/#:~:text=NIST%20800%2D53A%20is%20an,make%20it%20more%20easily%20understandable>.
15. <https://www.securetrust.com/compensating-control-requirements-for-pci/#:~:text=Compensating%20controls%20are%20a%20type,risk%20of%20the%20original%20requirement>.
16. <https://www.invensislearning.com/blog/risk-management-frameworks/#:~:text=A%20risk%20management%20framework%20creates,and%20assets%20of%20the%20organization>.
17. <https://www.itgovernanceusa.com/cyber-security-solutions/iso27001/iso-27005>
18. <https://www.cio.com/article/228151/what-is-cobit-a-framework-for-alignment-and-governance.html#:~:text=COBIT%20is%20an%20IT%20management,around%20information%20management%20and%20governance>.
19. <https://www.itiltraining.com/usa/blog/risk-management#:~:text=The%20main%20objectives%20of%20ITIL's,business's%20vulnerability%20to%20those%20threats>.
20. <https://www.mitre.org/publications/technical-papers/threat-assessment-and-remediation-analysis-tara>
21. <https://www.risklens.com/resource-center/blog/the-fair-model-in-90-seconds#:~:text=FAIR%20%5BFactor%20Analysis%20of%20Information,their%20relationship%20to%20one%20another>.
22. <https://pecb.com/whitepaper/risk-assessment-with-octave#:~:text=OCTAVE%20is%20a%20risk%20assessment,the%20organization's%20operational%20risk%20tolerances>
23. <https://www.projectmanager.com/blog/guide-using-risk-register#:~:text=A%20risk%20register%20is%20a,that%20can%20derail%20intended%20outcomes>.
24. <https://trailhead.salesforce.com/content/learn/modules/project-risk-management-for-partners/monitor-communicate-risk>
25. <https://www.ignyteplatform.com/how-can-poams-help-improve-your-security-budgeting-process/>
26. <https://csrc.nist.gov/glossary/term/plan_of_action_and_milestones#:~:text=Definition(s)%3A,completion%20dates%20for%20the%20milestones>.
27. <https://dfpi.ca.gov/about/>
28. <https://www.mondaq.com/argentina/finance-and-banking/977442/banking-regulation-comparative-guide#:~:text=The%20Financial%20Entities%20Law%20(21%2C526,been%20incorporated%20into%20consolidated%20regulations>.
29. <https://uk.practicallaw.thomsonreuters.com/w-008-0211?transitionType=Default&contextData=(sc.Default)#:~:text=The%20FCA%20is%20responsible%20for,the%20PRA%20and%20the%20FCA>.
30. <https://uk.practicallaw.thomsonreuters.com/w-007-9444?transitionType=Default&contextData=(sc.Default)>
31. <https://uk.practicallaw.thomsonreuters.com/w-007-9978?transitionType=Default&contextData=(sc.Default)#:~:text=Under%20French%20law%2C%20only%20authorised,as%20the%20French%20banking%20monopoly>.
32. <https://www.cybersaint.io/blog/six-steps-of-the-nist-risk-management-framework>
33. <https://info.pcxcorp.com/blog/why-salt-lake-city-is-a-booming-data-center-construction-location>
34. <https://www.datacenterknowledge.com/colocation/exclusive-san-francisco-see-its-first-data-center-build-more-decade>
35. <https://www.datacenterknowledge.com/industry-perspectives/why-salt-lake-city-has-become-top-data-center-location>
36. <https://www.tierpoint.com/data-centers/oklahoma/oklahoma-city/>
37. <https://www.unitrends.com/blog/bcdr-business-continuity-disaster-recovery#:~:text=What%20Is%20a%20BCDR%20Plan,while%20minimizing%20the%20negative%20impacts>.