Risk Management Primer

Concepts • Terminology • Tactics

By Joel Parker Henderson

Version 1.0

Contents

Risk management (RM)

Risk management is the process of identifying, assessing, and controlling potential risks in a business, project, or other endeavor. It is an essential part of any business strategy and involves analyzing potential risks, determining the likelihood and severity of each risk, and taking measures to reduce or mitigate the risks.

The goal of risk management is to minimize the negative impact of risks on an organization's goals and objectives, while maximizing opportunities for success. There are several steps involved in the risk management process:

- Risk identification: This involves identifying potential risks that may impact the organization or project. This can be done through brainstorming sessions, historical data analysis, and risk assessments.
- Risk assessment: Once the risks are identified, the next step is to assess the likelihood and potential impact of each risk. This involves analyzing the risk in terms of its likelihood of occurring, its potential impact, and the cost of mitigation.
- Risk mitigation: Based on the assessment, steps can be taken to mitigate the identified risks. This can include risk avoidance (eliminating the activity or process that poses the risk), risk reduction (implementing measures to reduce the likelihood or impact of the risk), risk sharing (transferring the risk to another party, such as an insurance company), or risk acceptance (accepting the risk and implementing a plan to minimize its impact).
- Risk monitoring and review: The final step in the risk management process is to monitor and review the effectiveness of the risk management plan. This involves regularly reviewing the risks, assessing their likelihood and potential impact, and making adjustments to the risk management plan as necessary.

Risk appetite

Risk appetite refers to the level of risk that an organization or individual is willing to accept or tolerate in pursuit of their objectives. It represents the willingness to take on risk in order to achieve desired outcomes while considering potential losses or negative consequences.

Risk appetite is subjective and varies from one organization or individual to another based on factors such as their goals, values, risk tolerance, and risk management strategies. It is an essential component of effective risk management as it helps set boundaries and guides decision-making regarding risk-taking. Understanding risk appetite enables organizations and individuals to make informed decisions regarding risk management, resource allocation, and strategic planning.

Key points...

Risk Appetite Statement: Organizations often articulate their risk appetite in the form of a risk appetite statement or policy. This statement outlines the organization's approach to risk and provides guidance to decision-makers on the acceptable level of risk exposure in various areas of operation.

Risk Tolerance: This is the level of risk that an organization or individual can withstand without compromising their objectives or well-being. This is influenced by factors such as financial resources, industry regulations, legal requirements, stakeholder expectations, and the entity's overall risk management capacity.

Risk Management Framework: Risk appetite serves as a critical input for developing a robust risk management framework. It helps shape risk identification, assessment, mitigation, and monitoring strategies to align with the entity's risk tolerance and desired risk profile.

Alignment with Objectives: Risk appetite should be aligned with an organization's overall objectives and strategic goals. It should consider factors such as financial objectives, growth targets, regulatory compliance, reputation management, and stakeholder expectations.

Risk management department

The Risk management department aims to identify, assess, and mitigate risks that may affect an organization's ability to achieve its objectives.

Key functions often include:

- Risk Identification: Identify various risks associated with the company's operations, including financial, operational, legal, regulatory, and reputational risks.
- Risk Assessment: Analyze the probability and potential impact of each identified risk and categorizes them based on their severity.
- Risk Mitigation: Based on the assessment, develop strategies to mitigate or manage the identified risks. This includes developing risk mitigation plans, risk transfer strategies, or contingency plans.
- Compliance: Ensure that the company adheres to all applicable laws and regulations, industry standards, and internal policies.
- Insurance Management: Manage the company's insurance policies and coordinates with insurers to ensure that the company has adequate coverage for potential risks.
- Crisis Management: Develop and implement a crisis management plan in the event of a major risk event, such as a natural disaster, cyber attack, or reputational crisis.
- Training and Education: Conduct training and education sessions for employees to increase awareness of risks and best practices for risk management.

Inherent risk

Inherent risk, also known as inherent risk exposure, refers to the level of risk or vulnerability that exists in a process, activity, or business environment before any control measures are implemented. It represents the risk inherent in a particular situation or operation, assuming there are no mitigating controls or risk management measures in place.

Key points...

Nature of Risk: Consider factors such as the complexity of the process, the sensitivity of the information involved, the potential impact of the risk event, and the likelihood of its occurrence.

Control Absence: Represent the risk level before considering any controls that may be implemented to reduce or mitigate the risk. Understand the magnitude of the risk exposure and the potential consequences.

Risk Assessment: Identify and prioritize risks based on their inherent characteristics. Provide a foundation for implementing appropriate control measures to mitigate or manage the identified risks.

Risk Evaluation: Analyzing the potential impact and likelihood of risks to determine their significance and prioritize risk management efforts. Focus on risks that pose the most significant threats.

Risk Management: Determine the appropriate level of controls and risk mitigation strategies necessary to reduce the inherent risk to an acceptable level. Implement targeted risk management actions.

Dynamic Nature: Monitor inherent risk over time, because factors such as environmental changes, new technologies, regulatory developments, or market shifts can alter risks and organizational risk appetite.

Control assessment

Control assessment refers to the process of evaluating and assessing the effectiveness of internal controls within an organization. Internal controls are policies, procedures, and mechanisms put in place to mitigate risks, ensure compliance with regulations, safeguard assets, and achieve organizational objectives.

Key aspects...

Objectives and Criteria: Control assessment is performed against specific objectives and criteria established by the organization, such as for finance, operations, IS/IT, and compliance.

Control Evaluation Methods: Control assessment can be conducted through various methods, including interviews, documentation review, walkthroughs, testing, and data analysis.

Control Frameworks: Control assessments often rely on established control frameworks or standards, such as the COSO (Committee of Sponsoring Organizations of the Treadway Commission) Internal Control Framework or ISO (International Organization for Standardization) standards.

Risk-Based Approach: Control assessment typically takes a risk-based approach, focusing on controls that are critical or high-risk areas for the organization. This helps identify and address control deficiencies that pose the greatest risk to the organization's objectives.

Control Remediation: This involves developing and implementing corrective actions or enhancements to address identified issues, such as process improvements, policy revisions, system enhancements, additional training, or strengthening of control monitoring activities.

Reporting and Communication: A control assessment report communicates the identified control deficiencies, potential impact on the organization, and recommendations for improvement. The report is shared with management, stakeholders, and, in some cases, external auditors or regulatory bodies.

Coordinated disclosure

Coordinated disclosure is a process of reporting security vulnerabilities or bugs found in systems to the systems' owners. Coordinated disclosure is important because it allows security vulnerabilities to be addressed and fixed before they can be exploited by malicious actors. This helps protect users, data, and systems from potential harm.

Key steps...

1. Discovery: The first step is discovering a security vulnerability or bug. For example, security researchers can identify potential vulnerabilities in software or hardware systems.
2. Notification: The discoverer notifies the owner of the product or system. This is done privately and securely to prevent the vulnerability from being known to others.
3. Verification: The owner verifies the issue and determines its severity. This can involve testing the system and analyzing the potential impact of the vulnerability on users.
4. Fix and Release: The owner develops a patch or fix for the issue, then releases it to users as soon as possible, along with instructions on how to install and use it.
5. Disclosure: After the fix, the discoverer and owner can disclose the issue publicly. This allows other people to learn about issue, and take steps to protect themselves from similar issues in the future.

Key Risk Indicators (KRIs)

Key Risk Indicators (KRIs) are metrics that assesses the level of risk of processes. KRIs provide an early warning of potential risks and help to identify trends that could have a negative impact on the organization. KRIs are usually specific to an organization or industry and are used to monitor and manage risks on an ongoing basis.

KRIs are used to measure risks in a way that is easy to understand and communicate. They are typically used by senior management to monitor the overall risk profile of an organization. KRIs can be used to measure both financial and non-financial risks, such as operational, strategic, regulatory, and reputational risks.

There are several characteristics of good KRIs, including:

- They are measurable and quantifiable: KRIs should be easy to measure and provide a clear indication of the level of risk.
- They are specific: KRIs should be tailored to the organization or industry they are being used for, and should measure risks that are relevant to the organization.
- They are actionable: KRIs should provide insight into how risks can be mitigated, so that action can be taken to reduce the level of risk.
- They are timely: KRIs should be monitored on an ongoing basis, so that early warning signs of potential risks can be identified and addressed in a timely manner.
- They are aligned with business objectives: KRIs should be aligned with the overall objectives of the organization, so that risks can be managed in a way that supports the organization's goals.

KRIs are often used in conjunction with Key Performance Indicators (KPIs), which measure the performance of an organization against specific goals or targets. Together, KRIs and KPIs provide a comprehensive view of an organization's performance, risk, and health.

Key Performance Indicators (KPIs)

Key Performance Indicators (KPIs) are a set of quantifiable metrics that are used to evaluate the performance of an organization, team, or individual against their strategic objectives. KPIs are typically used in business, but they can also be used in other fields such as healthcare, education, and sports.

KPIs are chosen based on the organization's goals and objectives, and they should be specific, measurable, achievable, relevant, and time-bound. Here are some examples of KPIs:

1. Revenue: the amount of money generated by the organization over a specific period of time.
2. Customer satisfaction: how satisfied customers are with the organization's products or services. It can be measured using surveys, feedback forms, or other methods.
3. Employee engagement: how engaged and motivated employees are. It can be measured using surveys, feedback forms, or other methods.
4. Conversion rate: the percentage of visitors to a website or landing page who take a specific action, such as making a purchase or filling out a form.
5. Cost per acquisition: the cost of acquiring a new customer.

KPIs can be used to monitor and evaluate the performance of an organization, team, or individual over time. They can also be used to identify areas for improvement and make data-driven decisions.

It's important to choose KPIs carefully and not rely on them exclusively. KPIs should be used in conjunction with other measures, such as qualitative feedback and expert judgment. KPIs must be reviewed regularly to ensure that they remain relevant and aligned with the organization's objectives.

Critical Success Factors (CSF)

Critical Success Factors (CSF) are the key factors or elements that determine the success or failure of an organization or a project. They are the few essential areas where a business must excel to achieve its mission, goals, and objectives. CSFs are what organizations must focus on to make their business strategies successful.

CSFs are derived from the company's goals, objectives, and mission and are the key performance areas that need to be monitored and managed to achieve the desired results. These factors can depend on the industry, business model, target market, competition, and so on.

Examples of CSFs can include factors such as:

- Customer satisfaction: The level of customer satisfaction is a CSF for many businesses, especially those in the service industry.
- Quality: Delivering quality products or services can be a CSF for businesses that want to compete on quality rather than price.
- Innovation: Companies that innovate and develop new products or services can gain a competitive advantage in their industry.
- Employee well-being: Employee satisfaction and engagement are CSFs for businesses that rely on a highly skilled and motivated workforce.
- Cost efficiency: For businesses that compete on price, cost efficiency is a CSF.
- Brand reputation: Building a strong brand reputation can be a CSF for businesses that rely on brand recognition and loyalty.

Critical to quality (CTQ)

Critical to quality (CTQ) is a term used in Six Sigma methodology, which is a data-driven approach to process improvement. CTQ is a metric that captures customer requirements in a measurable and quantifiable way. It is used to identify areas where the organization's processes fall short of customer expectations and can be improved to achieve better customer satisfaction.

CTQs are critical features of a product or service that are essential to meeting customer expectations. They can be defined as specific measurable characteristics of a product or service that determine customer satisfaction. CTQs can be both internal (for example, manufacturing processes) and external (for example, customer requirements). They are determined by analyzing customer feedback, market research, and the organization's quality management data.

Once the CTQs are identified, the next step is to measure them, which requires establishing performance targets for each CTQ. The targets should be set in a way that ensures the CTQs are met consistently over time. The organization can then analyze the data to determine whether the CTQs are being met and identify areas where improvements can be made.

CTQs are important because they help the organization focus on the most important aspects of its products or services. By identifying and measuring the CTQs, the organization can ensure that it is meeting customer expectations and can prioritize process improvements to address areas where customer expectations are not being met. The end result is better customer satisfaction and loyalty, increased sales, and improved profitability.

Risks, Actions, Issues, Decisions (RAID)

Risks, Actions, Issues, Decisions (RAID) is a project management abbreviation. A RAID log is a document that lists a project's known RAID items, and provides a way to monitor RAID progress and ensure that RAID items addressed.

Each element of a RAID log serves a specific purpose:

- Risks are potential events that could have a negative impact. The RAID log lists each risk, the likelihood of it occurring, the potential impact of it, and the steps that will be taken to mitigate it or manage it.
- Actions are tasks that need to be completed to keep the project on track. The RAID log lists each action, who is responsible for it, the target date for completion, and the status of it.
- Issues are problems that arise during the project that need to be addressed. The RAID log lists each issue, the impact of it on the project, who is responsible for addressing it, and the status of it.
- Decisions are choices made by the project team that impact the direction of the project. The RAID log lists each decision that has been made, who made it, the date it was made, and the impact of it on the project.

By using a RAID log, project managers can proactively identify potential risks and take steps to mitigate or manage them before they become major issues. It also provides a central location for tracking all important information related to the project, ensuring that nothing falls through the cracks. The RAID log can be used as a tool for communication with stakeholders to keep them informed about the project's progress and any potential concerns.

Governance

Governance in a business context refers to the system of rules, processes, and practices through which a company is directed and controlled. It involves the structures and mechanisms that determine how decisions are made, how authority is exercised, and how accountability happens.

Key aspects...

Board of Directors: The board of directors oversees the company's management and strategy, makes major decisions, appoints executives, and ensures the company operates in the best interest of shareholders.

Shareholder Rights: Governance provides shareholders with the information necessary to make informed decisions, facilitates their participation in corporate decisions, and safeguarding their rights.

Ethical Standards: Governance establishes codes of conduct, policies, and procedures that guide the behavior of individuals within the company, such as for integrity and fairness in business practices.

Risk Management: Governance establishes processes for monitoring and mitigating risks that could impact the company's performance, reputation, or compliance with regulations.

Financial Reporting: Governance establishes systems for internal control, financial auditing, and disclosure of relevant information.

Compliance: Governance ensures compliance with laws, regulations, and industry standards. It establishes procedures for monitoring compliance, addressing non-compliance, and maintaining the company's legal and regulatory obligations.

Stakeholder Engagement: Effective governance involves engaging and considering the interests of various stakeholders, including employees, customers, suppliers, and the local community.

Performance Evaluation: Governance establishes processes for setting goals, monitoring progress, assessing outcomes, and evaluating the performance of the board, management, and the organization.

Compliance

Compliance refers to the act of adhering to rules, regulations, and standards that are set by a governing body or authority. It is a critical component of any organization, as non-compliance can lead to legal, financial, and reputational risks.

Some common compliance examples include:

- Regulatory compliance: This refers to the adherence to laws and regulations that are set by government bodies, such as environmental regulations, labor laws, data protection laws, and financial regulations.
- Industry-specific compliance: This refers to adherence to standards and regulations that are specific to a particular industry, such as healthcare, banking, or aviation. For example, healthcare organizations must comply with the Health Insurance Portability and Accountability Act (HIPAA) regulations.
- Internal compliance: This refers to adherence to policies, procedures, and standards that are set by the organization itself, such as codes of conduct, employee handbooks, and internal controls.

Compliance can be achieved through various means, such as training programs, internal audits, risk assessments, and monitoring and reporting mechanisms. Compliance is not a one-time event but an ongoing process that requires continuous effort and vigilance.

Benefits of compliance include reduced legal and financial risks, improved reputation and brand image, enhanced trust and confidence from customers and stakeholders, and increased operational efficiency and effectiveness. For comparison, non-compliance can result in penalties, fines, legal actions, loss of business opportunities, and damage to reputation and brand image.

International Standard on Assurance Engagements 3000 (ISAE 3000)

International Standard on Assurance Engagements 3000 (ISAE 3000) is a global standard developed by the International Auditing and Assurance Standards Board (IAASB) that provides guidelines and requirements for conducting assurance engagements that are not audits or reviews of financial statements. These engagements may include providing assurance on internal controls, sustainability reporting, or other non-financial information.

It includes the following key elements:

- Engagement acceptance and planning: The auditor must plan the engagement and assess the risks associated with the engagement to ensure that the appropriate level of assurance can be provided.
- Performance of the engagement: The auditor must perform procedures to gather evidence to support the conclusion that is to be reported.
- Reporting: The auditor must report on the results of the engagement and provide a conclusion that is supported by the evidence gathered during the engagement.

ISAE 3000 also requires that the auditor obtain an understanding of the entity's internal controls, and design and perform procedures that are appropriate in the circumstances. The auditor must communicate with the entity's management and those charged with governance, to obtain relevant information and ensure that the engagement is properly planned and executed.

ISAE 3000 is applicable to a wide range of assurance engagements, such as for sustainability, social responsibility, information security, risk management, compliance, and corporate governance practices.

Service Organization Control 2 (SOC 2)

Service Organization Control 2 (SOC 2) is a set of auditing standards developed by the American Institute of Certified Public Accountants (AICPA) for assessing the effectiveness of a service organization's information security and privacy policies, procedures, and controls. SOC 2 audits are conducted by independent auditors to provide assurance to stakeholders that the organization is protecting sensitive information.

The SOC 2 framework is based on the Trust Services Criteria (TSC) developed by the AICPA, which include the following five categories:

- Security: The service organization's system is protected against unauthorized access, both physical and logical.
- Availability: The service organization's system is available for operation and use as committed or agreed to.
- Processing integrity: System processing is complete, accurate, timely, and authorized.
- Confidentiality: Information designated as confidential is protected as committed or agreed to.
- Privacy: Personal information is collected, used, retained, and disclosed in conformity with the commitments in the entity's privacy notice.

SOC 2 reports can be of two types: Type I and Type II. A Type I report assesses the design of the controls at a point in time, while a Type II report assesses both the design and operating effectiveness of the controls over a period of time (usually 6-12 months).

To get a SOC 2 report, an organization engages an independent auditor to examine the controls. The auditor provides opinions on whether the controls are suitably designed and operating effectively to meet TSC criteria. The auditor's report provides assurances that the controls are appropriate.

Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley Act (SOX) is a United States (U.S.) federal law designed to increase corporate accountability and transparency, and to protect investors by improving the accuracy and reliability of corporate disclosures. SOX applies to all U.S. publicly traded companies, and to foreign companies that are registered with the Securities and Exchange Commission (SEC) and have securities listed on U.S. exchanges.

Key provisions:

- Corporate governance: SOX requires that public companies have an independent board of directors and establish audit committees composed of independent members. The CEO and CFO are required to certify the accuracy of financial statements.
- Financial reporting: SOX requires that public companies disclose all material information in their financial reports, and that their financial statements are accurate and complete.
- Internal controls: SOX requires that public companies establish and maintain internal controls over financial reporting to ensure the accuracy and reliability of financial statements.
- Whistleblower protections: SOX provides protections for employees who report accounting fraud, securities violations, or other types of misconduct.
- Penalties: SOX imposes severe penalties on companies and executives who engage in financial fraud or other types of misconduct, including fines and imprisonment.

SOX has had a significant impact on corporate governance in the U.S. SOX led to increased transparency and accountability, and helped restore investor confidence. However, SOX has been criticized for being burdensome and costly for companies, particularly smaller ones, and for creating a compliance-focused culture that distracts from more-important priorities.

General Data Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) is a comprehensive data privacy regulation by the European Union (EU). GDPR is intended to harmonize data protection laws across the EU, and to provide individuals with greater control over their personal data.

The GDPR applies to all organizations, regardless of their location, that process the personal data of individuals within the EU. Personal data is defined as any information that can be used to directly or indirectly identify an individual, such as a name, email address, or IP address.

Key areas of the GDPR:

- Obtaining consent: Organizations must obtain explicit and informed consent from individuals before collecting and processing their personal data.
- Transparency: Organizations must provide individuals with clear concise information about how their data is being processed.
- Data portability: Individuals have the right to receive a copy of their personal data and to transfer it to another organization.
- Right to erasure: Individuals have the right to request that their personal data be erased.
- Data breach notification: Organizations must notify individuals and the relevant authorities of any data breaches that may affect their personal data.
- Accountability: Organizations must be able to demonstrate compliance with the GDPR and implement appropriate technical and organizational measures to protect personal data.

The GDPR also includes strict penalties for non-compliance, with fines of up to €20 million or 4% of a company's global annual revenue.

UK Data Protection Act (DPA)

The UK Data Protection Act (DPA) 2018 is a comprehensive data protection legislation that governs the processing of personal data in the United Kingdom. It incorporates the requirements of the European Union's General Data Protection Regulation (GDPR) into UK law.

Key provisions and principles...

Data Protection Principles: Includes fairness, lawfulness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality.

Lawful Basis for Processing: Includes consent, contract performance, legal obligations, vital interests, public task, legitimate interests, and explicit consent for special categories of personal data.

Rights of Data Subjects: Includes the right to be informed, right of access, right to rectification, right to erasure, right to restrict processing, right to data portability, right to object, and rights related to automated decision-making and profiling.

Accountability and Governance: Requires organizations to demonstrate compliance with data protection principles, and requires appointment of a Data Protection Officer (DPO) for certain processing.

International Data Transfers: Allows the transfer of personal data to countries outside the UK or the European Economic Area (EEA) only with appropriate safeguards, and derogations in specific circumstances.

Data Breach Notification: Requires timely notification to the Information Commissioner's Office (ICO) of any personal data breach that is likely to result in a risk to the rights and freedoms of individuals.

Enforcement and Penalties: Grants the Information Commissioner's Office (ICO) the authority to enforce data protection regulations and impose fines for non-compliance.

Americans with Disabilities Act (ADA)

The Americans with Disabilities Act (ADA) is a United States federal law that protects the rights of individuals with disabilities. The ADA prohibits discrimination against individuals with disabilities in areas such as employment, public accommodations, transportation, telecommunications, and government services.

The ADA defines a disability as a physical or mental impairment that substantially limits one or more major life activities, such as walking, seeing, hearing, speaking, breathing, or learning. The definition also includes individuals who have a history of such an impairment, or who are perceived as having such an impairment.

Under the ADA, employers with 15 or more employees are required to provide reasonable accommodations to individuals with disabilities, as long as the accommodations do not create an undue hardship for the employer. Reasonable accommodations may include changes to job duties, work schedules, or physical work environments, or the provision of auxiliary aids and services, such as sign language interpreters or assistive technology.

Public accommodations, such as restaurants, hotels, and stores, are required to provide equal access to individuals with disabilities. This may include providing accessible entrances, parking spaces, and restrooms, or providing auxiliary aids and services, such as braille menus or wheelchair ramps.

Telecommunications companies are required to provide relay services for individuals with hearing or speech impairments.

State and local governments are required to provide equal access to government services and programs.

The ADA has had a significant impact in improving the lives of individuals with disabilities and increasing their participation in society. However, challenges and barriers still exist, and ongoing efforts are needed to ensure full compliance.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. federal law that was enacted in 1996. It was introduced to improve the portability and continuity of health insurance coverage, as well as to safeguard the privacy and security of individuals' health information.

The HIPAA law has several key provisions, including:

- Privacy rule: This rule establishes national standards for the protection of individually identifiable health information, known as protected health information (PHI). Covered entities, such as healthcare providers, health plans, and healthcare clearinghouses, are required to safeguard PHI and obtain individuals' authorization before disclosing their information.
- Security rule: This rule sets standards for the security of electronic PHI (ePHI) and requires covered entities to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI.
- Breach notification rule: This rule requires covered entities to notify affected individuals, the Department of Health and Human Services (HHS), and, in some cases, the media, if there is a breach of unsecured PHI.
- Enforcement rule: This rule outlines the procedures for investigating and enforcing HIPAA violations and imposes penalties for non-compliance.

HIPAA applies to covered entities, which include healthcare providers, health plans, and healthcare clearinghouses, as well as their business associates, such as third-party vendors and contractors that handle PHI. HIPAA violations can result in significant financial penalties, reputational damage, and legal liability.

Family Educational Rights and Privacy Act (FERPA)

Family Educational Rights and Privacy Act (FERPA) is a United States federal law that was enacted in 1974. It applies to educational institutions that receive federal funding, including elementary and secondary schools, colleges, and universities. The purpose is to protect the privacy of students' education records and to give them certain rights with respect to those records.

Under FERPA, educational institutions are required to:

- Obtain written consent from students or their parents before disclosing any personally identifiable information from education records, with certain exceptions.
- Allow students or their parents to inspect and review their education records within 45 days of the request.
- Correct any inaccurate or misleading information in their education records.
- Limit access to education records to only those who have a legitimate educational interest in them.

FERPA defines education records as any records that are directly related to a student and maintained by an educational institution or its representatives. Examples: grades, transcripts, records, and financial information.

FERPA provides exceptions to the consent requirement. For example, educational institutions may disclose education records without consent to some officials and authorities, if they have a legitimate interest.

FERPA violations can result in the loss of federal funding for an educational institution, as well as reputational damage and legal liability.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards established by major credit card companies, to ensure that merchants and service providers who handle cardholder data are protecting it in a secure manner. PCI DSS applies to any organization that accepts, processes, stores, or transmits credit card data.

The standard includes 12 requirements:

- Use a firewall configuration to protect cardholder data.
- Do not use default passwords and security parameters provided by the vendors.
- Protect stored cardholder data.
- Encrypt transmission of cardholder data.
- Use and regularly update anti-virus software.
- Develop and maintain secure systems and applications.
- Restrict access to cardholder data to need-to-know.
- Assign a unique ID to each person with computer access.
- Restrict physical access to cardholder data.
- Monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.
- Maintain a policy that addresses information security.

PCI DSS compliance can be achieved through self-assessment or via a qualified security assessor (QSA) formal audit. Failure to comply can result in fines and bans. Additionally, data breaches resulting from non-compliance can cause damage to the reputation of the affected organization and result in legal action by customers and regulatory authorities.

Authentication, Authorization, Accounting, Auditing (AAAA)

Authentication, Authorization, Accounting, Auditing (AAAA) are four essential components of information security and access control that ensure secure and reliable access to resources within an organization's IT environment.

- Authentication: Authentication is the process of verifying the identity of an individual or system attempting to access a resource. This process is used to ensure that only authorized users are allowed to access the system. Common authentication methods include username and password, biometrics (such as fingerprint or face recognition), smart cards, or tokens.
- Authorization: Authorization is the process of granting or denying access to specific resources based on a user's authenticated identity and their level of privilege. This process ensures that authenticated users have only the necessary permissions to perform their job duties and access the resources required to perform those duties. For example, a software developer may need access to the source code of an application, but a marketing executive may not.
- Accounting: Accounting involves tracking the usage of resources by authorized users, including the amount of time spent accessing a resource and the actions performed while accessing it. This information is used to monitor system activity, ensure compliance with organizational policies, and identify potential security breaches.
- Auditing: Auditing involves the regular review and analysis of system activity logs to ensure that security policies and procedures are being followed, and to identify potential security breaches or unauthorized access. Auditing also helps to maintain compliance with regulatory requirements.

Authentication

Authentication is the process of verifying the identity of an entity, such as a user or a device, before allowing access to a system or service. In computing, authentication is typically performed using a combination of something the entity knows (such as a password or PIN), something the entity has (such as a smart card or token), or something the entity is (such as a biometric feature like a fingerprint or iris scan).

There are several types of authentication methods, including:

- Password-based authentication: This is the most common form of authentication, in which a user enters a username and password to access a system or service. However, this method is vulnerable to attacks like password guessing or phishing.
- Multi-factor authentication (MFA): This method requires the user to provide two or more forms of identification before granting access. For example, a user might enter a password and then receive a one-time code via text message or mobile app.
- Biometric authentication: This method uses a physical characteristic of the user, such as a fingerprint or facial recognition, to verify their identity.
- Certificate-based authentication: This method uses digital certificates to authenticate users, devices, or applications.
- Token-based authentication: This method uses a physical token, such as a smart card or USB drive, to authenticate users.

Authentication is often used in conjunction with authorization, which is the process of granting or denying access to resources based on the authenticated user's privileges or permissions. Together, authentication and authorization are critical components of access control in information security.

Authorization

Authorization is the process of determining whether a user or system has the necessary permissions to access a particular resource or perform a particular action. In computer security, authorization is often used in conjunction with authentication, which is the process of verifying the identity of a user or system.

Authorization typically involves the use of access control mechanisms, such as permissions, roles, or other attributes, to restrict or grant access to specific resources or operations. These access control mechanisms may be implemented at various levels, such as operating system, application, or network.

One common approach to authorization is role-based access control (RBAC), which involves assigning users to specific roles and then defining the permissions associated with each role. Another approach is attribute-based access control (ABAC), which uses various attributes, such as user identity, location, time of day, and other factors, to determine access.

Authorization is an important aspect of security, as it helps ensure that sensitive resources and operations are only accessible to authorized users or systems. It is often implemented using a combination of technical controls, such as access control lists and firewalls, as well as administrative controls, such as policies and procedures for managing user access.

Accounting for information systems

In the context of AAAA (Authentication, Authorization, Accounting, and Auditing) information systems, accounting refers to the process of recording and tracking user activities and system events. It involves capturing relevant data related to user logins, actions performed, resources accessed, and other system events for the purpose of monitoring, analysis, and auditing.

Key areas...

Auditing and Forensics: Provide an audit trail that can be used for forensic analysis and investigations. It helps trace the sequence of events and identify any suspicious or unauthorized activities within the system.

Compliance and Governance: Provide evidence of adherence to security policies and practices. It helps organizations demonstrate their compliance efforts and respond to regulatory inquiries or audits effectively.

Incident Response: Help identify the affected systems, determine the extent of the compromise, the potential root causes and origins, and facilitate remediation efforts.

Monitoring and Alerting: Detect abnormal activities or potential security threats. Continuously analyze data to identify patterns, anomalies, or deviations from expected behaviors, then trigger alerts.

Performance and Usage Analysis: Analyze system performance, resource utilization, and user behavior. Identify areas of improvement, optimize resource allocation, track system usage trends, aid in capacity planning, and enhance overall efficiency.

Auditing

Auditing involves the regular review and analysis of system activity logs to detect any unauthorized access or suspicious activity that may compromise the integrity, confidentiality, or availability of sensitive information.

In the context of information security, auditing helps ensure that access to sensitive data is properly controlled, monitored, and recorded.

Auditing involves collecting and analyzing data from various sources, including system logs, network traffic, and user activity. This data is used to identify patterns, trends, and anomalies that may indicate security incidents or policy violations. Auditing may also involve reviewing policies, procedures, and controls to ensure they are effective and up-to-date.

Auditing can be conducted manually or through automated tools, such as intrusion detection systems (IDS) or security information and event management (SIEM) systems. Automated auditing tools can provide real-time alerts and notifications, enabling security teams to quickly respond to potential threats.

Regular auditing is essential for maintaining the security and integrity of sensitive data, as well as for demonstrating compliance with legal and regulatory requirements. Auditing should be conducted on a regular basis, with results documented and reported to management and stakeholders.

Company leadership roles

There are several company leadership roles that play a critical role in the success of an organization. Here are some of the most common leadership roles and their responsibilities:

- Chief Executive Officer (CEO): The CEO is the highest-ranking executive in the company and is responsible for setting the overall strategy and vision for the organization.
- Chief Technology Officer (CTO): The CTO is responsible for overseeing the company's technology strategy and ensuring that the company has the technology resources it needs to achieve its objectives.
- Chief Operating Officer (COO): The COO is responsible for overseeing the day-to-day operations of the company. They ensure that the company's business processes are efficient and effective, and are responsible for managing the company's resources.
- Chief Financial Officer (CFO): The CFO is responsible for managing the company's finances, including financial planning, budgeting, and financial reporting.
- Chief Marketing Officer (CMO): The CMO is responsible for developing and executing the company's marketing strategy. They are responsible for promoting the company's products or services, building the brand, and generating leads.
- Chief Human Resources Officer (CHRO): The CHRO is responsible for managing the company's human resources, including hiring, training, employee satisfaction, and employee benefits.
- Chief Legal Officer (CLO): The CLO is responsible for managing the company's legal affairs. They are responsible for ensuring that the company is complying with all applicable laws and regulations and for managing legal risks.

Board of directors (BOD)

The board of directors (BOD) is a group of individuals who oversee the management and direction of a company or organization. They are responsible for ensuring that the company is being run in a way that maximizes value and minimizes risk. They are elected or appointed by the shareholders or members of the organization.

The BOD has a number of key responsibilities, including:

- Setting company strategy: The board is responsible for establishing the overall direction of the company and approving major strategic decisions, such as mergers and acquisitions or entering new markets.
- Selecting and overseeing the CEO: The board hires and evaluates the CEO, who is responsible for running the day-to-day operations of the company.
- Providing financial oversight: The board ensures that the company is managing its finances responsibly and is in compliance with all relevant laws and regulations.
- Approving major expenditures: The board approves major capital expenditures, such as investments in new technology or equipment.
- Ensuring compliance: The board ensures that the company is complying with all relevant laws and regulations, including those related to financial reporting, labor practices, and environmental and social responsibility.
- Protecting shareholders' interests: The board represents the interests of shareholders and ensures that the company is being run in a way that maximizes shareholder value.

The BOD typically meets several times a year, with additional meetings called as needed. Board members are expected to attend all meetings and actively participate in discussions and decision-making.

Chief Executive Officer (CEO)

The Chief Executive Officer (CEO) is the highest-ranking executive officer in a company or organization responsible for overseeing the overall operations and strategy of the organization. The CEO typically reports to the board of directors and is accountable for the company's performance and growth.

The primary responsibilities of a CEO may include setting the company's strategy and vision, building and leading the executive team, allocating resources and budget, making major corporate decisions, developing and implementing policies, overseeing day-to-day operations, and managing relationships with key stakeholders such as investors, customers, and partners.

The CEO must also possess strong leadership and management skills, be able to communicate effectively, have a deep understanding of the industry and market trends, and possess the ability to make strategic decisions in a timely and effective manner.

CEOs can come from a variety of backgrounds and possess a range of educational qualifications. Many CEOs have a strong background in business, finance, or management, and often have extensive experience in senior leadership roles within the organization or the industry. Some CEOs may also have a background in technology, engineering, or other technical fields, particularly in companies focused on innovation and technology.

Overall, the CEO plays a critical role in the success of an organization, providing leadership, guidance, and strategic vision to drive growth and ensure long-term sustainability.

Chief Risk Officer (CRO)

A Chief Risk Officer (CRO) is a corporate executive responsible for identifying, analyzing, and managing the risks that a business or organization may face. The CRO is typically responsible for developing and implementing risk management policies, procedures, and strategies to mitigate the negative impact of potential risks on the organization.

The primary role of a CRO is to help organizations identify and understand the risks they face and take steps to minimize those risks. This involves analyzing the company's operations, processes, and systems to identify potential risks, such as financial, legal, operational, and reputational risks. Once identified, the CRO works with other senior leaders to develop and implement risk management strategies that will minimize the impact of those risks on the organization.

In addition to identifying and managing risks, the CRO is also responsible for ensuring that the organization is compliant with relevant regulations and standards. This involves working closely with legal and compliance teams to ensure that the organization is adhering to relevant laws, regulations, and industry standards.

To be successful in this role, a CRO must have a strong understanding of risk management principles and techniques, as well as the ability to analyze complex data and make informed decisions based on that analysis. They should also have excellent communication and interpersonal skills, as they will need to work closely with other senior leaders, stakeholders, and regulatory bodies.

Chief Legal Officer (CLO)

A Chief Legal Officer (CLO) is a top-level executive who is responsible for overseeing a company's legal affairs. They are typically part of the senior management team and report directly to the CEO or board of directors.

A CLO generally has key responsibilities that may include:

- Provide legal advice and guidance to the company's leadership team and board of directors.
- Ensure that the company's business practices are in compliance with all relevant laws and regulations.
- Negotiate contracts and other legal documents on behalf of the company.
- Manage the company's relationships with outside legal counsel.
- Oversee the company's litigation and dispute resolution strategies.
- Manage the company's intellectual property portfolio and ensuring that the company's intellectual property rights are protected.
- Provide training and guidance to other employees on legal issues that may impact the company.
- Provide input on issues such as mergers and acquisitions, risk management, and corporate governance.
- Stay current on changes in laws and regulations that may impact the company, and adapt the company's legal strategy accordingly.

Chief Security Officer (CSO)

A Chief Security Officer (CSO) is a high-level executive in an organization who is responsible for developing and implementing strategies to protect the organization's physical and digital assets, including personnel, facilities, and data. The role of the CSO has become increasingly important in recent years as companies face a growing number of security threats, ranging from cyber-attacks to physical security breaches.

The CSO is responsible for creating and overseeing the organization's security policies and procedures, as well as managing its security personnel and resources. This includes identifying potential security risks and vulnerabilities, developing strategies to mitigate those risks, and establishing procedures for responding to security incidents.

The CSO may also work closely with other departments, such as IT and legal, to ensure that the organization is in compliance with all relevant regulations and standards. In addition, the CSO may be responsible for managing relationships with law enforcement agencies and other external partners, such as security consultants and vendors.

To be successful in this role, a CSO must have a deep understanding of the organization's business operations and the risks it faces, as well as strong leadership and communication skills. They must also stay up to date on the latest security threats and trends, and be able to adapt their strategies accordingly.

Chief Human Resources Officer (CHRO)

The Chief Human Resources Officer (CHRO) is a high-ranking executive in an organization who is responsible for managing and overseeing all aspects of the company's human resources functions. The CHRO typically reports directly to the CEO or COO.

Some of the key responsibilities of the CHRO may include:

- Developing and implementing HR policies and procedures: The CHRO is responsible for creating policies and procedures that align with the company's mission, vision, and goals.
- Talent acquisition and retention: The CHRO must ensure that the company is attracting and retaining top talent, which includes developing an effective recruitment strategy, establishing compensation and benefits programs that attract and retain employees, and creating a culture that fosters employee engagement and retention.
- Employee engagement and retention: The CHRO is responsible for developing and executing employee engagement and retention programs that foster a positive workplace culture and support the company's business objectives.
- Diversity and inclusion: The CHRO plays a critical role in driving diversity and inclusion initiatives throughout the organization, which includes developing and executing strategies that promote diversity, equity, and inclusion.
- Performance management: The CHRO is responsible for developing and implementing performance management systems that align with the company's goals and objectives, as well as providing coaching and support to managers and employees to ensure they are meeting performance expectations.
- Compliance: The CHRO is responsible for ensuring that the company complies with all relevant labor laws, regulations, and ethical standards.

Chief Financial Officer (CFO)

A Chief Financial Officer (CFO) is a top-level executive in a company who is responsible for managing the financial activities of the organization. They oversee financial planning and analysis, accounting, budgeting, forecasting, and reporting to ensure the company's financial health.

Some of the key responsibilities of a CFO include:

- Financial planning and analysis: The CFO is responsible for developing and implementing financial plans, strategies, and policies to ensure the company's financial success. They analyze financial data, identify trends, and forecast future financial performance.
- Accounting and financial reporting: The CFO oversees the company's accounting department, ensuring that all financial transactions are recorded accurately and on time. They are also responsible for preparing and presenting financial reports to the board of directors, investors, and other stakeholders.
- Budgeting and forecasting: The CFO is responsible for creating and managing the company's budget and forecasting future financial performance. They work closely with other department heads to ensure that budgetary goals are met and financial resources are allocated effectively.
- Risk management: The CFO is responsible for identifying and mitigating financial risks, such as credit and market risks. They work with other executives to ensure that the company's financial policies and procedures comply with relevant laws and regulations.
- Fundraising: The CFO is often responsible for managing the company's fundraising activities, including debt and equity offerings. They work with investors and lenders to secure financing for the company's operations and growth.

About the author

I'm Joel Parker Henderson. I'm a software developer and writer.

https://linkedin.com/in/joelparkerhenderson

https://github.com/joelparkerhenderson

Professional

For work, I consult for companies that seek to leverage technology capabilities and business capabilities, such as hands-on coding and growth leadership. Clients range from venture capital startups to Fortune 500 enterprises to nonprofit organziations.

For technology capabilities, I host repositories for developers who work with architecture decision records, functional specifications, system quality attributes, git workflow recommendations, monorepo versus polyrepo guidance, and hands-on code demonstrations.

For business capabilities, I host repostitories for managers who work with objectives and key results (OKRs), key performance indicators (KPIs), strategic balanced scorecards (SBS), value stream mappings (VSMs), statements of work (SOWs), and similar practices.

Personal

I'm a strong believer in free libre open source software (FLOSS). I'm an avid traveler and enjoy getting to know new people, new places, and new cultures. I love music and play guitar.

I advocate for chariable donations to help improve our world. Some of my favorite charities are Apache Software Foundation (ASF), Electronic Frontier Foundation (EFF), Free Software Foundation (FSF), Amnesty International (AI), Center for Environmental Health (CEH), Médecins Sans Frontières (MSF), and Human Rights Watch (HRW).

About the ebook PDF

This ebook PDF is generated from the repository markdown files. The process uses custom book build tools, fonts thanks to Adobe, our open source tools, and the program `pandoc`.

Book build tools

The book build tools are in the repository, in the directory `book/build`. The tools select all the documentation links, merge all the markdown files, then process everything into a PDF file.

Fonts

https://github.com/sixarm/sixarm-fonts

The book fonts are Source Serif Pro, Source Sans Pro, and Source Code Pro. The fonts are by Adobe and free open source. THe book can also be built with Bitstream Vera fonts or Liberation fonts.

markdown-text-to-link-urls

https://github.com/sixarm/markdown-text-to-link-urls

This is a command-line parsing tool that we maintain. The tool reads markdown text, and outputs all markdown link URLs. We use this to parse the top-level file `README.md`, to get all the links. We filter these results to get the links to individual guidepost markdown files, then we merge all these files into one markdown file.

pandoc-from-markdown-to-pdf

https://github.com/sixarm/pandoc-from-markdown-to-pdf

This is a command-line tool that uses our preferred pandoc settings to convert from an input markdown text file to an output PDF file. The tool adds a table of contents, fonts, highlighting, sizing, and more.

About related projects

These projects by the author describe more about startup strategy, tactics, and tools. These are links to git repostories that are free libre open source.

- Architecture Decision Record (ADR)
- Business model canvas (BMC)
- Code of conduct guidelines
- Company culture
- Coordinated disclosure
- Crucial conversations
- Decision Record (DR) template
- Functional specifications tutorial
- Icebreaker questions
- Intent plan
- Key Performance Indicator (KPI)
- Key Risk Indicator (KRI)
- Maturity models (MMs)
- Objectives & Key Results (OKR)
- Oblique strategies for creative thinking
- OODA loop: Observe Orient Decide Act
- Outputs vs. outcomes (OVO)
- Pitch deck quick start
- Queueing theory
- Responsibility assignment matrix (RAM)
- SMART criteria
- Social value orientation (SVO)
- Statement Of Work (SOW) template
- Strategic Balanced Scorecard (SBS)
- System quality attributes (SQAs)
- TEAM FOCUS teamwork framework
- Value Stream Mapping (VSM)
- Ways of Working (WOW)