Prevention First

A strategic blueprint for proactive risk assessment and data security

ESET®

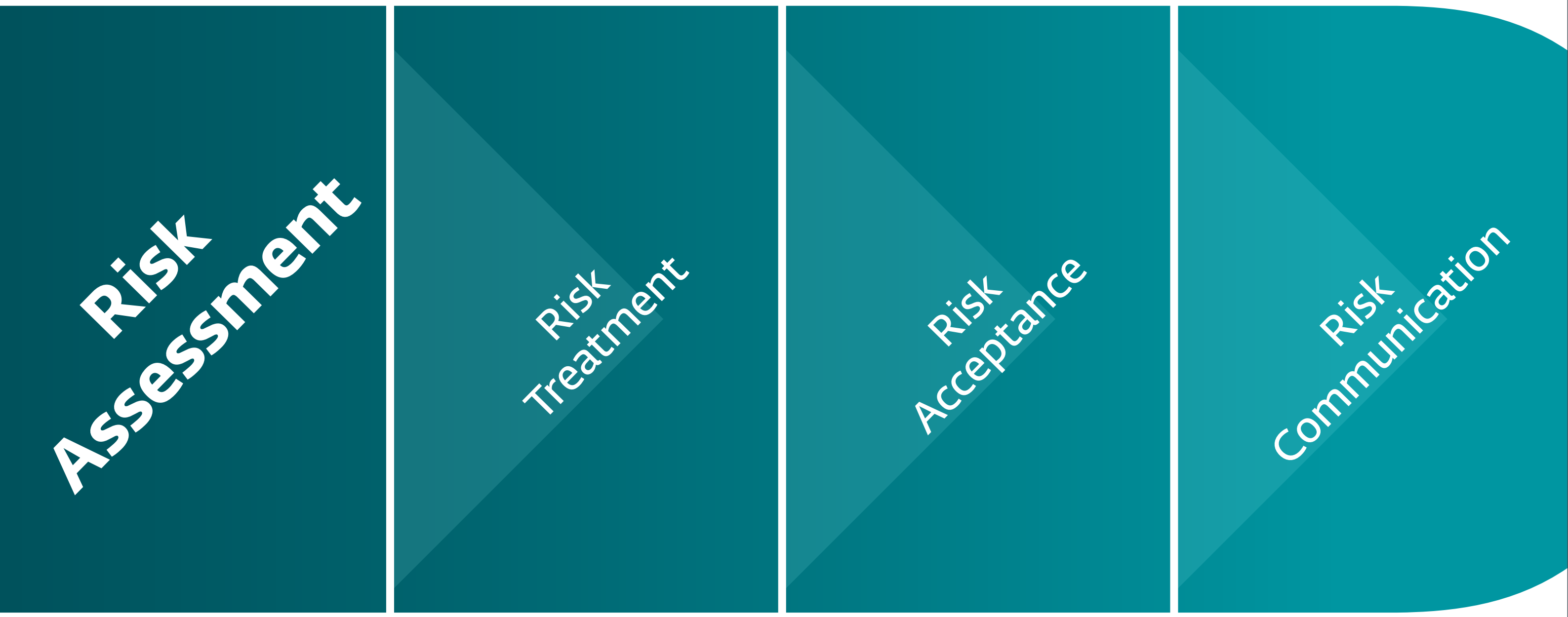
Digital Security
Progress. Protected.

A risk-based approach not only empowers organizations to implement suitable controls tailored to specific threats but also emphasizes **the importance of prevention as a strategic priority**. By integrating preventive measures into the initial phase of security risk management, **organizations can proactively address vulnerabilities and mitigate potential threats**.

The risk assessment process involves a thorough **identification of assets, analysis of threats, and assessment of vulnerabilities** to establish a comprehensive understanding of potential risks. This foundational step is crucial in guiding IT professionals to make informed decisions regarding risk mitigation, assignment, avoidance, or acceptance. It also necessitates clear communication with stakeholders about their proactive roles in managing and preventing these risks.

Understanding the nuances of data security risks, particularly through the identification of data processing operations and evaluation of potential business impacts, is crucial. It sets the stage for determining the likelihood of threats and **evaluating risks to ensure that data is safeguarded effectively**, leveraging both organizational and technical controls in a cohesive security management strategy.

The four key phases of security risk management



Risk Assessment

Risk Treatment

Risk Acceptance

Risk Communication

Phase 1: Risk Assessment

The first phase, the one we cover in this paper, is Risk assessment. There are many risk assessment methodologies with varying levels of cost and complexity. The basic process consists of:

- **Asset identification:** Identify all the organization's assets (both tangible and intangible) that require protection, including the asset's quantitative (such as cost or contribution to revenue) and/or qualitative (such as relative importance) value.
- **Threat analysis:** Define possible adverse natural and/or manmade circumstances or events, the potential impact or consequences, and the likelihood and frequency of occurrence.
- **Vulnerability assessment:** Determine what safeguards and/or controls are absent or weak in an asset, thereby making a threat potentially more harmful, costly, likely, or frequent.

Other key phases

Risk treatment: After assessing risks, IT admins have several options:

- **Risk mitigation**, which reduces the threat's impact or likelihood through policies and controls;
- **Risk assignment**, where the risk is transferred to a third party like an insurer;
- **Risk avoidance**, which involves eliminating the risk entirely by upgrading, disposing of the asset, or stopping the activity that introduces the risk.

Risk acceptance: This is the formal management approval of the risk treatment measures that are implemented, and the acceptance of any residual (or remaining) risk that cannot be further or practically mitigated, assigned, or avoided.

Risk communication: Appropriate stakeholders need to be made aware of any risk treatment and/or risk acceptance decisions that have been made, including their individual roles and responsibilities concerning specific risks.

Understanding the Risk Assessment Process

Risk assessment is the first phase of the risk management process. A risk assessment consists of identifying your assets, analyzing threats, and assessing vulnerabilities.

Assessing specifically data security risks involves:

- Identifying your data processing operations (to determine how and where your data assets are used by your business)
- Determining potential business impact (if your data is compromised)
- Identifying possible threats and evaluating the likelihood (of occurrence, including frequency)
- Evaluating risk (to assess which safeguards or controls should be implemented to protect your data)

Step 1: Identify Your Data Processing Operations

Data within an organization has different risk profiles, not only based on the content of the data but also due to the way data is used within the organization. Thus, it is important to **understand how data is processed within your business** as you begin the risk assessment process. For example, a typical SME might have some or all of the following types of data processing operations:

- **Human resources** such as employee payroll management, recruiting and retention, training records, disciplinary actions, and performance evaluations.
- **Customer management, marketing, and suppliers** such as customer information, purchase and sales orders, invoices, email lists, marketing and advertising data, and vendor contracts.
- **Personnel safety and physical security** such as employee security access logs, visitor logs, and video monitoring.

For each data processing operation, consider the following:

- What personal data is being processed?
- What is the purpose of the process?
- Where does the processing occur?
- Who is responsible for the process?
- Who has access to the data?

Step 2: Determine Potential Business Impact

Next, you need to **determine the potential impact of a data breach or compromise**. A breach or compromise may affect the confidentiality (for example, unauthorized access) of data, the integrity of data (for example, unauthorized modification), or the availability of data (for example, a ransomware attack).

Organizations must protect the confidentiality, integrity, and availability of data. In information security, this is known as the C-I-A triad.

In a typical risk assessment, the potential impact of a given risk is typically expressed in terms of damage to the organization, such as the loss or destruction of a physical asset (for example, a server, a copier machine, or a vehicle).

The impact of a risk to data security on the business is similar to other risk impacts, but the impact may be indirect. In the case of sensitive personal data, the individual whose data is breached or compromised is the direct victim. In such cases, an individual's identity or financial assets may be stolen and/or their privacy may be violated. **The impact on the business is less direct but still very costly** and may include (among others):

- Loss of customers and revenue
- Brand damage and adverse public relations
- Regulatory fines and litigation
- Breach notifications and credit monitoring services
- Forensic analysis and recovery

Business impact can be classified as Low, Medium, or High. However, the actual definition of each of these impact levels will be unique to every business and should involve both objective (quantitative) and subjective (qualitative) measures.

Step 3: Identify Possible Threats and Evaluate Likelihood

A threat can be any event or circumstance, either natural or man-made, that **has the potential to negatively affect the confidentiality, integrity, or availability of personal or sensitive data**. This can include cybersecurity attacks, accidental loss or disclosure, insider threats, fire and flooding, earthquakes and tsunamis, severe weather (such as a hurricane or tornado), civil unrest, labor disputes, and more.

Businesses must identify possible threats to their data processing operations and evaluate the likelihood (including frequency of occurrence) of each possible threat. Ensure that you cover threats in well-defined areas including threats from network and technical resources (software/ hardware) that are used for data processing, threats from related processes and procedures, threats from involved human resources, and threats from scale of processing. For each threat identified, the likelihood can be classified same as the business impact: Low, Medium, or High.

Step 4: Evaluate Risk

Once you've identified all of your data processing operations (and the data being processed), determined the potential business impact of a breach or compromise, and identified possible threats and the likelihood and frequency of occurrence, you can **evaluate the risk associated with each operation** and determine the appropriate protection controls and organizational/process.

According to the risk valuation, organizational and process controls should be implemented to properly secure your businesses and data processing operations using a risk-based approach.

Exploring Organizational and Process Controls

An effective prevention-first approach requires more than technical solutions. You need to establish administrative and organizational controls to ensure that technical controls are properly deployed, configured, and operated in support of a cohesive security management strategy.

Some examples of organizational controls include:

- **Private and sensitive personal data:** Use technical controls like encryption and DLP software with discretion.
- **Data documentation and auditing:** Document why data is collected, how it's used, and how it's protected.
- **Security policies:** Clearly define individual roles and responsibilities related to the protection of personal data.
- **Human resources:** Ensure that personal data collected by human resources is properly protected.
- **Using a security maturity model:** Determine your security capabilities in specific areas and identify any gaps between where you are and where you need to be.
- **Training and testing your employees:** Provide security awareness training and test employees to reinforce learning.
- **Implementing data protection by design and by default:** Implement measures to minimize personal data collection, processing, and storage.

This is ESET

Proactive defense. Our business is to minimize the attack surface.

Stay one step ahead of known and emerging cyber threats with our **prevention-first approach, powered by AI and human expertise**.

Experience best-in-class protection, thanks to our in-house global **cyber threat intelligence**, compiled and examined for over 30 years, which drives our extensive R&D network, led by **industry-acclaimed researcher**s. ESET protects your business so it can unlock the full potential of technology.

EXPLORE

Digital Security
Progress. Protected.