netwrix

Understanding Cybersecurity Risk Assessment

Table of contents

Cybersecurity threats are becoming more common and sophisticated — and breaches are increasingly costly. Indeed, the average global cost of a data breach reached $4.45 million, in 2023, an increase of 15% increase in just three years.

Regular cybersecurity risk assessments can help your organization protect its data — and its business. Read this guide to learn about the benefits of cybersecurity risk assessments, the types of assessments and their key components. Then download the free information security risk assessment templates we provide to get you started with assessments for HIPAA and GDPR complianc.

Understanding Cybersecurity Risk Assessments

A cybersecurity risk assessment evaluates an organization's ability to identify, defend against and prioritize threats to its data and systems. The assessment involves identifying information security risks — threats that can potentially exploit your assets' vulnerabilities.

Every organization, regardless of size or sector, should conduct regular cybersecurity and IT risk assessments. The information you glean can help you implement an effective security policy and appropriately allocate resources to improve your security. This can include remediating vulnerabilities like overprovisioned user accounts and misconfigurations, as well as improving threat detection and response capabilities to ensure better defense against password-guessing, phishing, ransomware and other attacks. By strengthening cybersecurity, you reduce your risk of data loss, financial losses, lawsuits and lasting reputational damage.

Moreover, cybersecurity risk assessments are invaluable for achieving and maintaining compliance with regulations such as HIPAA and GDPR, so you can avoid steep fines and other penalties. The templates provided at the link below provide frameworks for performing risk assessments to help with HIPAA and GDPR compliance.

Overview of the Cybersecurity Risk Assessment Process

At a high level, the cybersecurity risk assessment process includes the following steps:

1. Locate all valuable assets in your organization that could be hurt by threats. Examples include websites, servers, trade secrets and partner documents.

2. Identify the potential consequences if each asset is damaged, including financial losses, legal costs, data loss and system downtime.

3. Identify threats and their level. Threats are any event that can cause harm to your assets and your company's security posture. Examples include system failures, natural disasters, malicious human actions and human errors.

4. Identify vulnerabilities and evaluate the likelihood that third parties will exploit them. Vulnerabilities are weaknesses that could allow a third party to breach your security and harm your assets.

5. Assess risks. Risks are the chances that a given threat will exploit the environment's vulnerabilities and cause harm to one or more assets, leading to monetary damages. Risk levels can be assigned either qualitative categories (such as high, moderate and low) or numerical values. Smaller organizations may opt for a qualitative approach, at least initially, because it's simpler to execute, but quantitative assessments are more helpful for detailed cost-benefit analyses.

6. Create a risk management plan with the collected data. Here is an example in table form:

Threat	Vulnerability	Asset and consequences	Risk	Solution

7. Create an IT infrastructure enhancement strategy to mitigate the most important vulnerabilities and get a final sign-off from management.

8. Define mitigation processes. This will help you prevent cybersecurity incidents from happening in the future or, if they do happen, make them less harmful.

Cybersecurity Risk Assessment Methods

Organizations can choose from several cybersecurity risk assessment methods, including the following:

- **Generic risk assessments** follow a template and are used for a wide range of cases. They usually ask generic questions to offer visibility into risks, such as "Do you use firewalls?" and "Do you use end-to-end encryption?" This is a basic type of risk assessment that should be supplemented by more complex tools.

- **Site-specific risk assessments** typically focus on certain use cases, people, environments or locations. They're usually associated with a geographic location, such as a specific office. Therefore, they aren't particularly useful if your company has a hyper-connected ecosystem in which risks can quickly spread from one branch or area to another.

- **Dynamic risk assessments** provide continuous tracking and responses. This method empowers teams to constantly monitor for emerging risks in real time and mitigate them as soon as possible.

Resources for Cybersecurity Risk Assessments

To conduct cybersecurity risk assessments, organizations, regardless of size or sector, can reference the following resources.

Center for Internet Security Risk Assessment Method (CIS RAM)

Organizations can use CIS RAM to assess their cybersecurity posture against the CIS Critical Security Controls, a set of best practices for improving cybersecurity. CIS RAM can be used in several ways:

- **Risk analysts** can use CIS RAM to simulate foreseeable threats.
- **Experienced cybersecurity experts** can use CIS RAM instructions to model threats against assets and determine the appropriate configuration for protecting data assets.
- **Cyber risk experts** can use CIS RAM to analyze risks based on attack paths.

NIST SP 800-30

NIST SP 800-30 also provides guidance on conducting risk assessments. While it is aimed at federal information systems and organizations, it can be used by any organization interested in improving cybersecurity and risk management.

It explores how risk assessments can be applied across three risk management tiers:

- **Tier 1** — Organization
- **Tier 2** — Mission/business process
- **Tier 3** — Information system

These tiers inform the scope of the risk assessment and affect its impacts.

ISO/IEC 27000

ISO/IEC 27000 is an international family of standards for information security risk management. It includes:

- **ISO/IEC 27000** addresses security for any kind of information technology.
- **ISO/IEC 27001** outlines how organizations can improve information security, cybersecurity and privacy protection using an information security management system (ISMS).
- **ISO/IEC 27002** builds on ISO/IEC 27001 by providing guidance on choosing appropriate security controls as part of ISMS deployment.

NIST Risk Management Framework

The NIST Risk Management Framework helps organizations determine whether their risk management controls have been implemented correctly, are working as intended, and are producing the desired outcome in regard to meeting their security and privacy requirements.

The NIST Risk Management Framework helps organizations with the following:

- Selecting risk assessors and assessment teams
- Developing a plan of action and milestones for risk assessments
- Developing security and privacy assessment reports
- Ensuring control assessments are conducted according to assessment plans
- Updating privacy and security plans to reflect control implementation changes based on remediation actions and assessments

Key Components of a Cybersecurity Risk Assessment

A robust cybersecurity risk assessment should have the following key components:

- **Introduction** — Explain how and why the company has handled the assessment process. Include a description of the systems and software reviewed and specify who was responsible for gathering, providing, and assessing information.

- **Purpose** — Explain why the risk assessment is being performed.

- **Scope** — Define the scope of the IT system assessment. Describe the users, system components and other details to be considered in the cybersecurity risk assessment.

- **System description** — List the hardware, systems, interfaces, software and data that were examined, as well as what was out of the assessment's scope.

- **Participants** — List names and roles of all participants, including the risk assessment team, the asset owners, and the IT and security teams.

- **Assessment approach** — Explain the techniques and methodology used for the risk assessment.

- **Risk identification and assessment** — Compile the assessment results.

- **Data inventory** — Identify all of the valuable assets in scope, including regulated data, critical data, servers and other types of data whose exposure would have a significant impact on business operations.

- **System users** — Detail who uses the systems, including their level of access and location.

- **Threats** — Catalog threats, such as system failures, natural disasters, malicious human actions and human errors.
- **Vulnerabilities** — Identify weaknesses and security gaps that could allow threats to violate your security. For example, a lack of a disaster recovery plan could lead to the loss of important data in case of disaster.
- **Risk determination** — Assess the possibility that vulnerabilities will lead to damage. Make sure to perform risk probability determination, impact analysis and risk-level evaluation.
- **Risk assessment results** — List vulnerabilities and threats, assess the risk of each, and provide recommendations for implementing controls.

Risk Assessment Templates

The templates provided in this document are designed to offer guidance for developing a risk assessment process that helps your organization assess its compliance with HIPAA and GDPR. They are not meant to be used as-is for formal risk assessments.

HIPAA: Risk Assessment Template

Section	Comments
Introduction: Explain why this document exists.	
Purpose: Explain why you need a risk assessment.	
Scope: Document your company's electronic protected health information (ePHI) flow. List and describe all system components, field site locations, elements, users, and other relevant details.	
Approach: Explain the methods used to perform the risk assessment.	
Participants: Identify the participants responsible for interacting with ePHI. Include their names and roles.	

Techniques: List the methods for identifying and inventorying ePHI data, processes, physical devices and procedures.		
Risk documentation: Explain when the company performs risk assessments, how risks are determined, and the risk classification system (qualitative levels or numerical scale).		
System description: Talk about the boundaries of the IT system under consideration and the information and resources that make up the system.		
System-related information: Include relevant information and a summary of the processing environment.	**System name**	
	System owner	
	Physical location	
	Major business function	
	Description and components	
	Interfaces and boundaries	
	Data sensitivity	
	Overall IT sensitivity rating and classification	
System users: Explain who uses the system.	**System name**	
	User category	
	Access level	
	Number of users	
	System owner	
	Physical location	

Data inventory: Document all data and where it is received, stored, transmitted or maintained. Examples include ePHI, test results, billing data and medical procedures.	**Type of data**	**Description**	**Level of sensitivity**
	ePHI	Electronic protected health information	High
	Test results		
	Billing data		
	Medical procedures		
Threats: Create a catalog of anticipated threats. Prioritize human threats from criminals, patients, ex-employees, and others who have access to and knowledge of the system or motivation to harm your company.			
Vulnerabilities: List all non-technical and technical vulnerabilities that potential threats could exploit or trigger.			
Security measures: Assess and document the effectiveness of all non-technical and technical controls that have been or will be implemented for risk mitigation.			
Risk assessment results: Talk about the vulnerabilities and the threats that can exploit them, measure each risk, and provide recommendations for corrective action or control implementation. Consider presenting detailed results in a separate spreadsheet or appendix.			
Revision history: Track changes to your HIPAA risk assessment.	**Version**	**Published**	**Author**
	1.0		
	1.1		
	1.2		

GDPR: Data Protection Impact Assessment (DPIA) Template

Section	Comments			
Identify the need for a data protection impact assessment (DPIA). Document its nature, scope, context and purpose.	**Section**	**Section**	**Section**	**Section**
Explain the data processing operations and their purposes.	How is data being collected and used?			
	Where and how is data being stored?			
	Where are you collecting the data from?			
	How much data is being collected? How many data subjects have been affected?			
	Where are the data processing activities occurring?			
	What are the data retention requirements?			

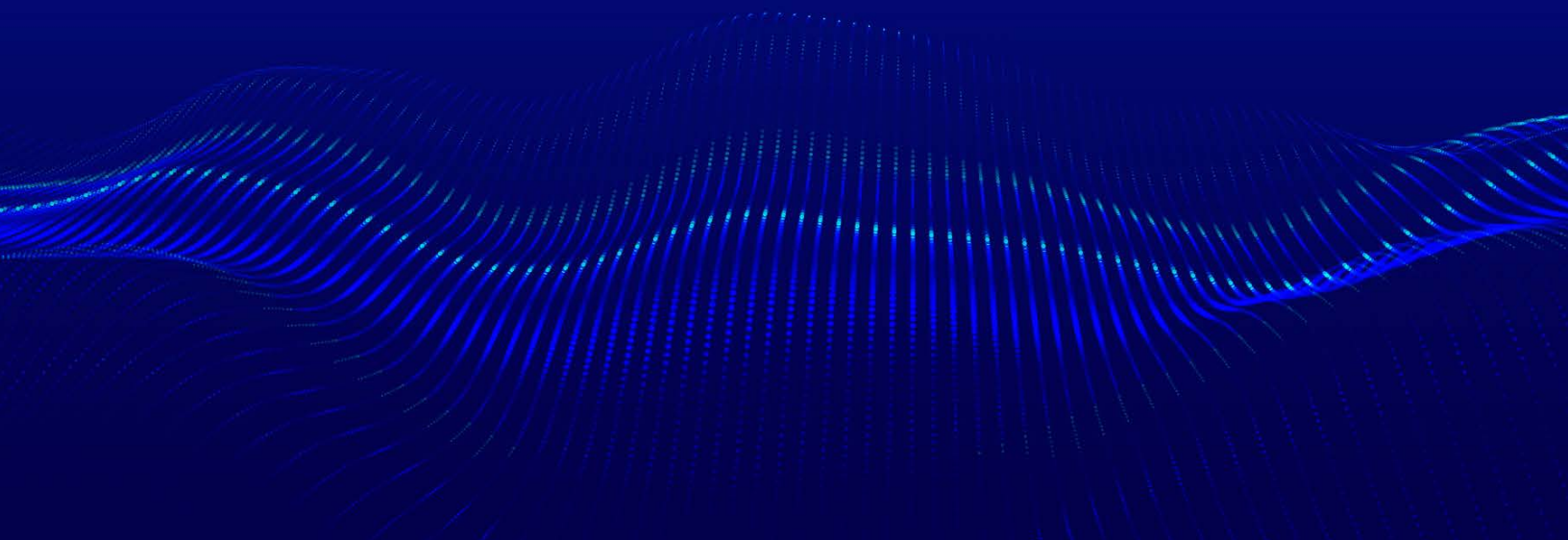
Assess the necessity and proportionality of the data collection and processing.	Is there a legal basis for gathering this data?	
	Does the organization have appropriate consent measures?	
	Were and are vulnerable data subjects involved?	
	Is the data processing necessary to achieve the project's objectives?	
	Are there ways to minimize consumer data usage?	
	Are data subjects' and consumers' rights being upheld?	
	Have previous projects performed similar processing? If so, were cybersecurity flaws spotted and fixed?	
Consult relevant and interested parties throughout the DPIA. These include project stakeholders, outside experts, data protection officers (DPOs), and data subjects and their representatives.	Project stakeholders	
	Outside experts	
	DPOs	
	Data subjects and their representatives	

Spot and evaluate risks to personal data. Create a prioritized list of your company's assets and identify vulnerabilities.			
Identify measures for addressing and mitigating risks. Document which risks each mitigation measure can address and how.			
Get the sign-off from relevant parties, such as the DPO.			
Deploy measures for addressing risks.			
Produce a final DPIA report with the following information: ▪ A detailed explanation of the project and its purpose ▪ An assessment of the data processing scope and needs ▪ An assessment of consumer privacy and data protection risks ▪ An explanation of how the organization will comply with GDPR requirements and mitigate risks			
Revision history: Track changes to your GDPR risk assessment.	**Version**	**Published**	**Author**
	1.0		
	1.1		
	1.2		

Unleash the Power of Risk Assessment with Netwrix Auditor

- Inventory your IT assets, leaving no stone unturned.
- Proactively identify gaps that put those assets at risk and prioritize your remediation efforts.
- Identify sensitive data that is at risk because it is open to everyone.
- Find access permissions that are assigned directly instead of through group membership.
- Get alerts on suspicious activity around sensitive data.
- Have a high-level overview of the current security posture of the IT infrastructure.

Request One-to-One Demo



About Netwrix

Netwrix makes data security easy. Since 2006, Netwrix solutions have been simplifying the lives of security professionals by enabling them to identify and protect sensitive data to reduce the risk of a breach, and to detect, respond to and recover from attacks, limiting their impact. More than 13,000 organizations worldwide rely on Netwrix solutions to strengthen their security and compliance posture across all three primary attack vectors: data, identity and infrastructure.

For more information, visit www.netwrix.com

Next Steps

Netwrix products — Check out the full portfolio of Netwrix products: netwrix.com/products

Live demo — Take a product tour with a Netwrix expert: netwrix.com/livedemo

Request quote — Receive pricing information: netwrix.com/buy

CORPORATE HEADQUARTER:

6160 Warren Parkway, Suite
100 Frisco, TX, US 75034

5 New Street Square, London
EC4A 3TW

PHONES:

1-949-407-5125
Toll-free (USA): 888-638-9749

+44 (0) 203 588 3023

OTHER LOCATIONS:

Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

SOCIAL:

netwrix.com/social