Coralogix

RISK ASSESSMENT METHODOLOGY

Version 6.0

Version Control

Version	Developed by	Changes	Approved by	Date
1.0	Oded David	Initial Version		
2.0	BDO	Annual Review		30/05/2020
3.0	Shiran Wolfman	Annual Review		18/01/2022
4.0	Shiran Wolfman	Annual Review	Oded David	17/01/2023
5.0	Shiran Wolfman	Annual Review	Oded David	17/01/2024
6.0	Shiran Wolfman	Added vulnerability sources in vulnerability identification section	Oded David	13/08/2024

Table of Contents

Purpose, scope and users

The purpose of this document is to define the methodology for assessment and treatment of information risks in Coralogix, and to define the acceptable level of risk according to security laws, regulations and standards including ISO 27001, 27701, HIPAA and PCI-DSS.

Risk assessment are applied to the entire scope of all assets which are used within the organization or which could have an impact on information security within the company.

Coraogix will perform a yearly risk analysis, which will provide an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of PII/ePHI and credit card information.

Users of this document are all employees of Coralogix who take part in risk assessment.

Reference documents

- HIPAA
- PCI-DSS
- Information Security Policy
- Risk assessment

Definitions

- **HIPAA** - HIPAA (Health Insurance Portability and Accountability Act of 1996) is United States legislation that provides data privacy and security provisions for safeguarding medical information.
- **PCI-DSS** - The Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards from the major card schemes.

- **PHI** - Protected Health Information, including demographic information collected from an individual and created or received by a health provider, health plan, employer or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of any individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, and that identifies an individual or there is a reasonable basis to believe the information can be used to identify the individual and that is transmitted or maintained by electronic media or any other form or medium.
    - **ePHI** - Electronic protected health information is protected health information (PHI) that is produced, saved, transferred or received in an electronic form.

Risk Assessment, Risk Mitigation and Work plan

Risk assessment

The process

Risk assessment is implemented through the Risk Assessment Table. The CISO coordinates the risk assessment process, asset owners perform identification of threats and vulnerabilities, and risk owners perform the assessment of impacts and likelihood.

System Characterization

Define the scope of the effort by identifying where ePHI and credit card information is received, processed or transmitted.

Asset identification

Assets could be anything of value to an organization. In the context of PCI DSS, assets include the people, processes, and technologies that are involved in the processing, storage, transmission, and protection of subjects.

Each asset may be identified to an asset owner who will then be responsible for adequately protecting the asset. The asset may also be assigned an asset value based on its importance and criticality.

Threat identification

Identification of all threat assets in the scope – i.e. of all assets that may affect confidentiality, integrity, and availability of PII/ePHI and credit card information in the organization. Assets may include documents in paper or electronic form, applications, and databases, people, IT equipment, infrastructure, and external services\outsourced processes. When identifying assets, it is also necessary to identify their owners – the person or organizational unit responsible for each asset.

Vulnerability identification

Identify all vulnerabilities associated with each asset. A vulnerability is a weakness that can be exploited by a threat and may originate from technology, the organization, the environment, or a business process. In a risk assessment, all vulnerabilities should be considered. Every asset may be associated with several threats, and every threat may be associated with several vulnerabilities.

Vulnerabilities are identified through several sources and are labeled, tracked and assessed. External internal penetration tests are conducted on a semi-annual basis by authorized expert 3rd party assessors, including re-tests to verify remediation of vulnerabilities within industry standard SLA's. Internal penetration tests are conducted by our security researchers with a defined scope and under the guidance of the Coralogix CISO. Network vulnerability scans are conducted regularly. Various other scanning tools are used to cover the entire depth of our systems and lifecycles. A bug-bounty program is established and available to external security researchers.

The table below shows the category and characteristics for risk assessment

Category	Characteristics
Assets	• Asset type (primary or supporting asset, information or business process, hardware or software, etc.) • Asset Value
Threat	• Threat Properties (insider or outsider, accidental or deliberate, physical or network, etc.) • Threat likelihood/probability
Vulnerabilities	• Vulnerability description • Level of Vulnerability
Risk	Risk score is a function of: • Asset value • Likelihood of threat, and • Level of vulnerability

Determining the risk owners

For each risk, a risk owner has to be identified – the person or organizational unit responsible for each risk. This person may or may not be the same as the asset owner.

Control Analysis

Document and assess the effectiveness of technical and non-technical security controls that have been or will be implemented by the Coralogix to reduce the likelihood of a threat source exploiting a system vulnerability.

Impact and likelihood

Once risk owners have been identified, it is necessary to assess impacts for each combination of threats and vulnerabilities for an individual asset if such a risk materializes:

Impact	Level	Description
Low	1	Loss of confidentiality, availability or integrity does not affect the organization's cash flow, legal or contractual obligations, or its reputation.
Medium	2	Loss of confidentiality, availability or integrity incurs costs and has a low or moderate impact on legal or contractual obligations, of the organization's reputation.
High	3	Loss of confidentiality, availability or integrity has considerable and/or immediate impact on the organization's cash flow, operations, legal or contractual obligations, or its reputation.

After the assessment of impacts, it is necessary to assess the likelihood of occurrence of such a risk, i.e. the probability that a threat will exploit the vulnerability of the respective asset:

Impact	Level	Description
Low	1	Existing security controls are strong and have so far provided an adequate level of protection. No new incidents are expected in the future.

Medium	2	Existing security controls are moderate and have mostly provide an adequate level of protection. New incidents are possible, but not highly likely.
High	3	Existing security controls are low or ineffective. Such incidents have a high likelihood of occurring in the future.

By entering the values of impact and likelihood into the Risk Assessment Table, the level of risk is calculated automatically by adding up the two values. Existing security controls are to be entered in the last column of the Risk Assessment Table.

Risk acceptance criteria

Values 1,2 and 3 are acceptable risks, while values 4,6 and 9 are unacceptable risks. Unacceptable risks must be treated.

Risk Mitigation

Risk mitigation involves prioritizing, evaluating and implementing the appropriate risk reducing security controls recommended from the risk assessment process to ensure the confidentiality, integrity and availability of PII/ePHI and credit card information. Determination of appropriate security controls to reduce risk is dependent upon the risk tolerance of the covered entity consistent with its goals and mission. Consistency of risk mitigation methods among departments and over time is helpful and encouraged and while there are a variety of methods suitable for HIPAA risk mitigation. Coralogix will implement measures to reduce computer risks and vulnerabilities, including identifying and documenting potential risks and vulnerabilities that could impact systems processing PII/ePHI and/or credit card information; performing annual technical security assessments of systems processing PII/ePHI and/or credit card information in order to identify and remedy detected security vulnerabilities.

Prioritize Action and select control

Preparation a list of threats\vulnerabilities that may occur in accordance with the level of the existing risks and presentation of the actions are required to implement the risk reduction method. In addition determines the appropriate security controls for reducing risks to the information systems and to the confidentiality, integrity and availability of PII/ePHI and credit card information.

Assign Responsibility

Identify the individual(s) or team with the skills necessary to implement each of the specific security controls listed in the previous step and assign their responsibilities. Identify the equipment, training and other resources (e.g. time, equipment, and budget) needed for the successful implementation of security controls.

Work plan

The work plan is based on the Risk Assessment, by copying all risks identified as unacceptable from the Risk Assessment. The CISO will conduct the work plan. One or more treatment options must be selected for risks valued 4, 6 and 9:

1. Selection of security control or controls from ISO 27001, 27701, HIPAA\PCI-DSS.
2. Transferring the risks to a third party – e.g. by purchasing an insurance policy or signing a contract with suppliers or partners.
3. Avoiding the risk by discontinuing a business activity that causes such risk.
4. Accepting the risk – this option is allowed only if the selection of other work plan options would cost more than the potential impact should such risk materialize.

The selection of options is implemented through the Work plan. Usually, option 1 is selected: selection of one or more security controls. When several security controls are selected for a risk, then additional rows are inserted into the table immediately below the row specifying the risk.

The treatment of risks related to outsourced processes must be addressed through the contracts with responsible third parties, as specified in Supplier Security Policy.

In the case of option 1 (selection of security controls), it is necessary to assess the new value of impact and likelihood in the work plan, in order to evaluate the effectiveness of planned controls.

Regular reviews of risk assessment and work plan

Risk owners must review existing risks and update the Risk Assessment and Work plan in line with newly identified risks. The review is conducted at least once a year, or more frequently in the case of significant organizational changes, significant change in technology, change of business objectives, changes in the business environment, etc.

Statement of Applicability and work plan

The CISO must document the following in the Statement of Applicability: which security controls from ISO 27001, 27701, HIPAA\PCI-DSS standard are applicable and which are not, the justification for such decisions, and whether they are implemented or not.

On behalf of the risk owners, top management will accept all residual risks through the Statement of Applicability.

The CISO will reduce and treat the risks from the risk assessment in the work. On behalf of the risk owners, CEO will approve the Work plan.

Risk Management Schedule

The two (2) principle components of the risk management process (risk assessment and risk mitigation) will be carried out according to the following schedule to ensure the continued adequacy and improvement of the department's information security program.

Throughout a System's Development Life Cycle

From the time that a need for a new information system is identified until the time they system is disposed of, ongoing assessments of the potential threats to a system and its vulnerabilities should be undertaken as a part of the system's maintenance.

Reporting

CISO will document the results of risk assessment and work plan, and all of the subsequent reviews, in the Risk Assessment and Work plan.

CISO will monitor the progress of implementation of the work plan and report the results to the CEO.

Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Risk Assessment Table	CISO	CISO	Only CISO has the right to make entries into and changes to the Risk Assessment Table	Data is stored permanently
Work plan	CISO	CISO	Only CISO has the right to make entries	Data is stored permanently.

			into and changes to the work plan.	
Risk Assessment and Work plan (electronic form)	CISO	CISO	The Report is prepared in read-only PDF format.	The Report is stored for a period of 3 years.
Statement of Applicability (electronic form)	CISO	CISO	Only CISO has the right to make entries into and changes to the Statement of Applicability.	Older versions of SOA are stored for a period of 3 years.

Only **CEO** can grant other employees access to any of the above mentioned documents.

Validity and document management

This document is valid as of Coralogix.

The owner of this document is the CISO who must check and, if necessary, update the document at least once a year, before the regular review of existing risk assessment.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- The number of incidents which occurred, but were not included in risk assessment.
- The number of risks which were not treated adequately.

- The number of errors in the risk assessment process because of unclear definition of roles and responsibilities.