Risk Management Policy

Policy Owner: Dotan Simha

Effective Date: Aug 28, 2024

Purpose

To define actions to address Software Products Guilda Ltd. information security risks and opportunities. To define a plan for the achievement of information security and privacy objectives.

Scope

- All Software Products Guilda Ltd. IT systems that process, store or transmit confidential, private, or business-critical data.
- Risks that could affect the medium to long-term goals of Software Products Guilda Ltd. should be considered as well as risks that will be encountered in the day-to-day delivery of services.
- Software Products Guilda Ltd. risk management systems and processes will be targeted to achieve maximum benefit without increasing the bureaucratic burden and ultimately affecting core service delivery to the organization.
- Software Products Guilda Ltd. will therefore consider the materiality of risk in developing systems and processes to manage risk.
- This Policy applies to all employees of Software Products Guilda Ltd. and to all external parties, including but not limited to Software Products Guilda Ltd. consultants and contractors, business partners, vendors, suppliers, outsource service providers, and other third party entities with access to Software Products Guilda Ltd. networks and system resources.

Risk management statement

Inadequate IT risk management exposes Software Products Guilda Ltd. to risks including compromise of Software Products Guilda Ltd. or customer network systems, services and information, cyber-attacks, contractual, or legal issues. Software Products Guilda Ltd. will ensure that risk management plays an integral part in the governance and management of the organization at a strategic and operational level. The purpose of a risk management policy is designed to ensure that it achieves its stated business plan aims and objectives.

Risk management strategy

Software Products Guilda Ltd. has developed processes to identify those risks that will hinder the achievement of its strategic and operational objectives. Software Products Guilda Ltd. will therefore ensure that it has in place the means to identify, analyze, control and monitor the strategic and operational risks it faces using this risk management policy based on best practices.

Software Products Guilda Ltd. will ensure the risk management strategy and policy are reviewed regularly and that internal audit functions are responsible for ensuring:

- The risk management policy is applied to all applicable areas of Software Products Guilda Ltd.
- The risk management policy and its operational application are regularly reviewed
- Non-compliance is reported to appropriate company officers and authorities

Practical application of risk management

Software Products Guilda Ltd. has adopted a standard format for use in the identification of risks, their classification, and evaluation.

The format is based on the following NIST and ISO standards and frameworks:

- ISO 27005
- NIST 800-30
- NIST 800-37

Risks are assessed and ranked according to their impact and their likelihood of occurrence. A formal Risk Assessment, and network penetration tests, will be performed at least annually and shall take into consideration the results of any technical vulnerability management activities performed in accordance with the *Operations Security Policy*.

Risk categories

Software Products Guilda Ltd. will consider and assess risks across the organization. Risk categories that are considered for evaluation include:

- Access control
- Artificial intelligence
- Asset management
- Business continuity and disaster recovery
- Communications security
- Compliance
- Cryptography
- Environmental, social, and governance
- Fraud
- Incident response management
- Information security operations
- Information security policies
- Operations security
- People operations
- Physical and environmental security
- Privacy
- Software development and acquisition
- Trustworthiness
- Vendor relationships

Each risk will be assessed as to its Likelihood and Impact. Likelihood can range from 1 ("Very unlikely") to 5 ("Very likely"). Impact can range from 1 ("Very low impact") to 5 ("Very high impact").

Risk criteria

The criteria for determining risk is the combined likelihood and impact of an event adversely affecting the confidentiality, availability, integrity, or privacy of organizational and customer information, personally identifiable information (PII), or business information systems.

For all risk inputs such as risk assessments, vulnerability scans, penetration test, bug bounty programs, etc., Software Products Guilda Ltd. management shall reserve the right to modify risk rankings based on its assessment of the nature and criticality of the system processing, as well as the nature, criticality and exploitability (or other relevant factors and considerations) of the identified vulnerability.

Risk response, treatment, and tracking

Risk will be prioritized and maintained in a risk register where they will be prioritized and mapped using the approach contained in this policy. The following responses to risk should be employed:

- **Mitigate:** Software Products Guilda Ltd. may take actions or employ strategies to reduce the risk.
- **Accept:** Software Products Guilda Ltd. may decide to accept and monitor the risk at the present time. This may be necessary for some risks that arise from external events.
- **Transfer:** Software Products Guilda Ltd. may decide to pass the risk on to another party. For example contractual terms may be agreed to ensure that the risk is not borne by Software Products Guilda Ltd. or insurance may be appropriate for protection against financial loss.
- **Avoid:** the risk may be such that Software Products Guilda Ltd. could decide to cease the activity or to change it in such a way as to end the risk.

Where Software Products Guilda Ltd. chooses a risk response other than "Accept" or "Avoid" it shall develop a Risk Treatment Plan.

Risk management procedures

The procedure for managing risk will meet the following criteria

1. Software Products Guilda Ltd. will maintain a Risk Register and Treatment Plan.
2. Risks are ranked by ‘likelihood' and ‘severity/impact' as critical, high, medium, low, and negligible.
3. Overall risk shall be determined through a combination of likelihood and impact.
4. Risks may be evaluated to estimate potential monetary loss where possible.
5. Software Products Guilda Ltd. will respond to risks in a prioritized fashion. Remediation priority will consider the risk likelihood and impact, cost, work effort, and availability of resources. Multiple remediations may be undertaken simultaneously
6. Regular reports will be made to the senior leadership of Software Products Guilda Ltd. to ensure risks are being mitigated appropriately, and in accordance with business priorities and objectives.

Information security in project management

Software Products Guilda Ltd. shall consider information security risk as a part of all projects that are technical in nature or which can pose a risk to the company, regardless of size, duration, or domain. From the initial planning, through completion of a project, appropriate assessment and mitigation of information security risks is essential, involving:

- initial information security risk assessments,
- early identification and addressing of information security requirements, and
- ongoing assessment and management of risks, especially concerning internal and external project communications.

Roles and responsibilities

The following table outlines the specific risk management activities and responsibilities associated with each role.

Role	Responsibility
CEO	Ultimately responsible for the acceptance and/or treatment of any risks to the organization.
CTO	Can approve the avoidance, remediation, transference, or acceptance of any risk cited in the Risk Register.
IT Manager / Systems Engineer	Shall be responsible for the identification and treatment plan development of all Information Security related risks. This person shall be responsible for communicating risks to top management and adopting risk treatments in accordance with executive direction.

Version history

Version	Date	Description	Author	Approver
1.0	Aug 28, 2024	Version 1.0	Dotan Simha	Dotan Simha

APPENDIX A - Risk assessment process

The following is a high-level overview of the process used by Software Products Guilda Ltd. to assess and manage information security related risks.

The process discussed below is based on NIST 800-30 and provides guidance to Software Products Guilda Ltd. on how to:

- Prepare and conduct an effective risk assessment.
- Communicate and share the assessment results and risk-related information.
- Manage and maintain risks on an ongoing basis.

The risk assessment process is comprised of the following steps:

1. Prepare for the assessment
2. Conduct the assessment
3. Communicate the assessment
4. Maintain the assessment

Step 1: Prepare for the Assessment

In this step, the objective is to establish context for the risk assessment. This can be accomplished by performing the following:

- Identify the purpose of the assessment
    - Determine the information that the assessment is intended to produce and the decisions the assessment is intended to support.
- Identify the scope of the assessment
    - Determine the organizational function or process that is applicable, the associated time frame and any applicable architectural or technological considerations.
- Identify any assumptions or constraints associated with the assessment
    - Determine assumptions in key areas relevant to the risk assessment including:
        - Organizational priorities
        - Business objectives
        - Resource availability
        - Skills and expertise of risk assessment team
- Identify sources of information
    - Architectural / technological diagrams and system configurations
    - Legal and regulatory requirements
    - Threat Sources
    - Threat Events
    - Vulnerabilities and influencing conditions
    - Potential Impacts
    - Existing Controls

Step 2: Conduct the Assessment

In this step, the objective is to produce a list of information security related risks that can be prioritized by risk level and used to inform risk response decisions. This can be accomplished by performing the following:

- Identify Threat Sources
    - Determine and characterize threat sources relevant to and of concern to Software Products Guilda Ltd., including but not limited to:
        - Human (Intentional or Unintentional / Internal or External)
        - Environmental
        - Natural
        - System or Equipment
    - Consider the following when identifying threat sources:

            - Capability
            - Motive / Intent
            - Intentionally targeted people, processes, and/or technologies
            - Unintentionally targeted people, processes, and/or technologies
- Identify Threat Events
    - Determine what threat events could be produced by the identified threat sources that have potential to impact Software Products Guilda Ltd..
    - Consider the relevance of the events and the sources that could initiate the events.
- Identify Vulnerabilities
    - Determine the vulnerabilities associated to people, process and/or technologies that could be exploited by the identified threat sources and threat events.
    - Consider any influencing conditions that could affect and aid in successful exploitation.
- Determine Likelihood
    - Determine the likelihood that the identified threat sources would initiate the identified threat events and could successfully exploit any identified vulnerabilities.
    - Consider the following when determining the likelihood:
        - Characteristics of the threat sources that could initiate the events.
            - Capability
            - Motive/Intent
            - Opportunity
        - The vulnerabilities and/or influencing conditions identified
        - Software Products Guilda Ltd.'s exposure based on any safeguards/countermeasures planned or implemented to prevent or mitigate such events.
- Determine Impact
    - Determine the impact to Software Products Guilda Ltd.'s business objectives, operations, assets, individuals, customers, and/or other organizations by considering the following:
        - Business / Operational Impacts
        - Financial Damage
        - Reputation Damage
        - Legal or Regulatory Issues
    - When determining impact, also take into consideration any safeguards/countermeasures planned or implemented by Software Products Guilda Ltd. that would mitigate or lessen the impact.
- Determine Risk
    - Determine the overall information security related risks to Software Products Guilda Ltd. by combining the following:
        - The likelihood of the event occurring.
        - The impact that would result from the event.
    - The risk to Software Products Guilda Ltd. is proportional to the likelihood and impact of an event.
        - Higher Risk Event: Is more likely to occur and the resulting impact will be greater.
        - Lower Risk Event: Is less likely to occur and the resulting impact will be minimal if any.

Step 3: Communicate and Share the Risk Assessment Results

In this step, the objective is to ensure that decision makers across the Software Products Guilda Ltd. and executive leadership have the appropriate risk-related information needed to inform and guide risk decisions.

- Communicate the Results
    - Communicate the risk assessment results to Software Products Guilda Ltd. decision maker and executive leadership to help drive risk based decisions and obtain the necessary support for the risk response.
    - Share the risk assessment and risk-related information with the appropriate personnel at Software Products Guilda Ltd. to help support the risk response efforts.

Step 4: Maintain the Assessment

In this step, the objective is to keep current, the specific knowledge related to the risks that Software Products Guilda Ltd. incurs. The results of the assessments inform, and drive risk based decisions and guide ongoing risk responses efforts.

- Monitor Risk Factors
  - Conduct ongoing monitoring of the risk factors that contribute to changes in risk to Software Products Guilda Ltd.'s business objectives, operations, assets, individuals, customers, and/or other organizations.
- Maintain and Update the Assessment
  - Update existing risk assessments using the results from ongoing monitoring of risk factors and by conducting additional assessments, at minimum annually.

APPENDIX B - Risk assessment matrix and description key

Each risk will be assessed as to its Likelihood and Impact. Likelihood can range from 1 ("Very unlikely") to 5 ("Very likely"). Impact can range from 1 ("Very low impact") to 5 ("Very high impact").

		Likelihood				
		Very unlikely: 1	**Unlikely: 2**	**Somewhat likely: 3**	**Likely: 4**	**Very likely: 5**
Impact	**Very high impact: 5**	5	10	15	20	25
	High impact: 4	4	8	12	16	20
	Medium impact: 3	3	6	9	12	15
	Low impact: 2	2	4	6	8	10
	Very low impact: 1	1	2	3	4	5

Risk level	**Description**
Low (1 - 4)	A threat event could be expected to have a limited adverse effect on organizational operations, mission capabilities, assets, individuals, customers, or other organizations.
Med (5 - 14)	A threat event could be expected to have a serious adverse effect on organizational operations, mission capabilities, assets, individuals, customers, or other organizations.
High (15 - 25)	A threat event could be expected to have a severe adverse effect on organizational operations, mission capabilities, assets, individuals, customers, or other organizations.

Impact	**Description**	**Score**
Very low impact (1)	A threat event could be expected to have almost no adverse effect on organizational operations, mission capabilities, assets, individuals, customers, or other organizations.	1
Low impact (2)	A threat event could be expected to have a limited adverse effect, meaning: degradation of mission capability yet primary functions can still be performed; minor damage; minor financial loss; or range of effects is limited to some cyber resources but no critical resources.	2
Medium impact (3)	A threat event could be expected to have a serious adverse effect, meaning: significant degradation of mission capability yet primary functions can still be performed at a reduced capacity; minor damage; minor financial loss; or range of effects is significant to some cyber resources and some critical resources.	3
High impact (4)	A threat event could be expected to have a severe or catastrophic adverse effect, meaning: severe degradation or loss of mission capability and one or more primary functions cannot be performed; major damage; major financial loss; or range of effects is extensive to most cyber resources and most critical resources.	4
Very high impact (5)	A threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, assets, individuals, or other organizations. Range of effects is sweeping, involving almost all cyber resources.	5

Likelihood	**Description**	**Score**

Very unlikely (1)	A threat event is so unlikely that it can be assumed that its occurrence may not be experienced. A threat source is not motivated or has no capability, or controls are in place to prevent or significantly impede the vulnerability from being exploited.	1
Unlikely (2)	A threat event is unlikely, but there is a slight possibility that its occurrence may be experienced. A threat source lacks sufficient motivation or capability, or controls are in place to prevent or impede the vulnerability from being exploited.	2
Somewhat likely (3)	A threat event is likely, and it can be assumed that its occurrence may be experienced. A threat source is motivated or poses the capability, but controls are in place that may significantly reduce or impede the successful exploitation of the vulnerability.	3
Likely (4)	A threat event is likely, and it can be assumed that its occurrence will be experienced. A threat source is highly motivated or poses sufficient capability and resources, but some controls are in place that may reduce or impede the successful exploitation of the vulnerability.	4
Very likely (5)	A threat event is highly likely, and it can be assumed that its occurrence will be experienced. A threat source is highly motivated or poses sufficient capability or resources, but no controls are in place or controls that are in place are ineffective and do not prevent or impede the successful exploitation of the vulnerability.	5