KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY,

KUMASI

INFORMATION SECURITY AND TECHNOLOGY ASSURANCE DIVISION, UITS

RISK ASSESSMENT AND RISK TREATMENT METHODOLOGY

Document ID :	Doc 000002
Version:	1.0
Date of version:	1st September 2023
Created by:	Mr. Phanuel Seli. K. Asense
Approved by:	Mr. Emmanuel N.O. Afful
Confidentiality level:	low

Change history

Date	Version	Created by	Description of change

1. Purpose, scope and users

This document defines the methodology for assessment and treatment of information technology (IT) risks in Kwame Nkrumah University of Science and Technology (KNUST) and the acceptable level of risk according to the 1S0/IEC 27001 standard. Risk assessment and risk treatment are applied to the entire scope of the Information Security Management System (ISMS) i.e., to all assets used within the organization, or which could impact information security within the ISMS. Users of this document are all employees of KNUST who take part in risk assessment and risk treatment.

2. Reference documents

1. 1S0/IEC 27001 standard. clauses 6.1.2, 6.1.3, 8.2, and 8.3
2. ISO 22301 standard clauses 8.2.1, 8.2.3 and 8.3.2
3. Information Security Policy of KNUST ICT policy
4. All Legal, Regulatory, Contractual, and Other related documents
5. Statement of Applicability
6. Data Protection Act, 2012 (Act 843)
7. www.techtarget.com/searchsecurity/tip/How-to-perform-a-cybersecurity-risk-assessment-step-by-step
8. www.cybersaint.io/blog/cyber-security-risk-assessment-templates
9. drata.com/blog/iso-27001-risk-assessment
10. www.cybersaint.io/blog/risk-assessment-tips-based-on-nist-800-30
11. nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

3. Definitions

- 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.

- Data Protection Act, 2012 -The Data Protection Act, 2012 (Act 843) sets out the rules and principles governing the collection, use, disclosure and care for your personal data or information by a data controller or processor. It recognizes a person's right (data subject rights) to protect their personal data or information by mandating a data controller or processor to process (collect, use, disclose, erase, etc.) such personal data or information in accordance with the individual's rights. The Act also established the Data Protection Commission as an independent statutory body to ensure and enforce compliance.

- Information security management system (ISMS): This is a set of policies and procedures for systematically managing an organization's sensitive data.

4. Risk Assessment and Risk Treatment (Mitigation) Methodology

4.1 Risk assessment

4.1.1. The process

Risk assessment is implemented through the Risk Assessment Table (appendix a). The Deputy Director, Information Security and Technology Assurance (ISTAD) coordinates the risk assessment process, asset owners' knowledge is essential in performing identification of threats and vulnerabilities, and the security team and risk owners perform the assessment of impacts and likelihood.

This is the prime means for including the data about threats, vulnerabilities, consequences, and likelihood in the Risk Assessment Table.

4.1.2. Assets, vulnerabilities and threats

The first step in risk assessment is the identification of all assets in the ISMS scope by the organizational unit responsible for each asset. The next step is for the asset owners, risk owners and security team to collaborate to identify all threats and vulnerabilities associated

with each asset. Threats and vulnerabilities are identified using the catalogues included in the Risk Assessment.

4.1.2.1. Asset identification

Assets could be anything of value to an organization. In the context of this document, assets include the people, processes, and technologies that are involved in the processing, storage, transmission, and protection of information. 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. See Appendix B.

4.1.2.2. Threat identification

Identification of all threat assets in the scope – i.e., of all assets that may affect confidentiality, integrity, and availability of information, for example 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. See Appendix C.

4.1.2.3. 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. See Appendix B.

The table 1 below shows the category and characteristics for risk assessment

No.	***Category***	***Characteristics***
1	*Assets*	● *Asset type (primary or supporting asset, information or business process, hardware or software, etc.)* ● *Asset Value*
2	*Threat*	● *Threat Properties (insider or outsider, accidental or deliberate, physical or network, etc.)* ● *Threat likelihood/probability*
3	*Vulnerabilities*	● *Vulnerability description* ● *Level of Vulnerability*
4	*Risk*	*Risk score is a function of:* ● *Asset value* ● *Likelihood of threat, and* ● *Level of vulnerability*

Table 1.

4.1.3. Determining the risk owners

For each risk, a risk owner must be identified - i.e., the person or organizational unit responsible for each risk. This person may or may not be the same as the asset owner.

4.1.4. Consequences (impact) and likelihood

It is necessary to assess consequences 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.

Table 2.

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:

Likelihood (Probability)	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 provided 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.

Table 3.

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

4.2 Risk acceptance criteria

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

4.3 Risk Mitigation (treatment)

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 information, example 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. The consistency of risk mitigation methods among departments over time are helpful and encouraged, and while there are many methods suitable for risk mitigation. Risk treatment is conducted by the Deputy Director, ISTAD in collaboration with the risk owner.

4.3.1. Prioritize Action and select control

Preparation of 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, determination of the appropriate security controls for reducing risks to the information system's confidentiality, integrity, and availability is required.

4.3.2. 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.

4.4 Work Plan

The Work Plan is based on the Risk Assessment items that are identified as unacceptable. The Deputy Director, ISTAD, 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

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

4.5 Regular reviews of risk assessment and Work Plan

Security team and 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.

4.6 Statement of Applicability and Work Plan

The Deputy Director, ISTAD must document the following in the Statement of Applicability: which security controls from ISO 27001, 27701 standards 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 Deputy Director, ISTAD will reduce and treat the risks from the risk assessment in the work. On behalf of the risk owners, the Director, UITS or Chair of the ICT Management Committee will approve the Work Plan.

4.7 Risk Management Schedule

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

4.8 System's Development Life Cycle maintenance

From the time that a need for a new information system is identified until the time the 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.

4.9 Reporting

Deputy Director, ISTAD will document the results of risk assessment and Work Plan, and all the subsequent reviews, in the Risk Assessment and Work plan.

Deputy Director, ISTAD will monitor the progress of implementation of the Work Plan and report the results to the Director, UITS.

5.0 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	Deputy Director, ISTAD	Deputy Director, ISTAD	Only Deputy Director, ISTAD has the right to make entries into and changes to the Risk Assessment Table. However, this can be delegated	Data is stored permanently
Work plan	Deputy Director, ISTAD	Deputy Director, ISTAD	Only Deputy Director, ISTAD has	Data is stored permanently

			the right to make entries into and changes to the work plan. However, this can be delegated	
Risk Assessment and Work plan (Electronic form)	Deputy Director, ISTAD	Deputy Director, ISTAD	The Report is prepared in read-only PDF format.	The Report is stored for a period of 3 years.
Statement of Applicability (Electronic form)	Deputy Director, ISTAD	Deputy Director, ISTAD	Only Deputy Director, ISTAD has the right to make entries into and changes to the Statement of Applicability. However, this can be delegated	Older versions of SOA are stored for a period of 3 years.

Table 4.

Only the Director, UITS, can grant other employees access to any of the above-mentioned documents.

6.0 Validity and document management

This document is valid as of 1st September 2023. The owner of this document is the Deputy Director, ISTAD, 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.

7.0 Appendices

Appendix A

Risk Assessment Template

RISK ID NO.	*RISK DESCRIPTION*	*PROCESS*	*ISO 27001*	*IMPACT DESCRIPTION*	*IMPACT LEVEL*	*PROBABILITY LEVEL*	*PRIORITY LEVEL*	*Can the following step in the process eliminate the risk?*	*What controls already exist that can address the risk?*	*MITIGATION OR CONTROL STRATEGY*	*OWNER*
	Give a summary of the risk.	*Which process is this risk a part of?*	*Which of the 14 ISO 27001 Information Security Standards steps does this cyber security risk relate to?*	*What will happen if the risk is not mitigated or eliminated?*	*Rate 1 (LOW) to 5 (HIGH)*	*Rate 1 (LOW) to 5 (HIGH)*	*(IMPACT X PROBABILITY) Address the highest first.*	*YES or NO*	*If the risk is eliminated or mitigated by existing processes, list them here.*	*What can be done to lower or eliminate the impact or probability?*	*Who's responsible?*
1.1					2	1	2	YES			
1.2					1	4	4	NO			

Appendix B

Asset and Vulnerability Identification

No.	Asset Name	Asset Owner	Asset Value (Importance/Criticality)	Asset Vulnerabilities

Appendix C

Threat Identification

No.	Asset Name	Asset Owner	Threat(s)