DUS 2209

UGANDA STANDARD

First Edition
2019-12-2

Information Security — Risk Assessment

Reference number
DUS 2209: 2019

Compliance with this standard does not, of itself confer immunity from legal obligations

A Uganda Standard does not purport to include all necessary provisions of a contract. Users are responsible for its correct application

The Executive Director
Uganda National Bureau of Standards
P.O. Box 6329
Kampala
Uganda
Tel: +256 414 333 250/1/2/3
Fax: +256 414 286 123
E-mail: info@unbs.go.ug
Web: www.unbs.go.ug

Contents

Page

Foreword

Uganda National Bureau of Standards (UNBS) is a parastatal under the Ministry of Trade, Industry and Cooperatives established under Cap 327, of the Laws of Uganda, as amended. UNBS is mandated to co-ordinate the elaboration of standards and is:

A member of International Organisation for Standardisation (ISO); and

A contact point for the WHO/FAO Codex Alimentarius Commission on Food Standards, and

The National Enquiry Point on TBT Agreement of the World Trade Organisation (WTO).

The work of preparing Uganda Standards is carried out through Technical Committees. A Technical Committee is established to deliberate on standards in a given field or area and consists of key stakeholders including government, academia, consumer groups, private sector and other interested parties.

Draft Uganda Standards adopted by the Technical Committee (TC) are widely circulated to stakeholders and the general public for comments. The committee reviews the comments before recommending the draft standards for approval and declaration as Uganda Standards by the National Standards Council (NSC).

The committee responsible for this document is Technical Committee UNBS/TC18, Information and Communication Technology

This is the first edition

Introduction

Risk assessment forms part of the risk management activities that occur throughout the lifecycle of an Information and Communications Technology (ICT) system including development, acceptance, operation, decommissioning and disposal. It presents a systematic approach for identifying and evaluating the risks of deliberate and accidental disclosure, interception and modification of information held, stored and processed by a CII. An organisation is able to understand the nature and estimate the level of security risks affecting critical information infrastructure (CII) or protected computers

Risk assessment focuses on three activities namely risk identification, analysis and evaluation. Risk identification aims to establish what, how, where and why events could cause potential loss. Analysis on the other hand, aims to understand the nature and level of risk. Evaluation uses agreed criteria to determine the acceptability of risk and/or its magnitude. Risk assessment combines the steps comprising of:

a) Asset identification;

b) Grouping of assets into security domain;

c) Valuing assets by determining the business impact of a security incident;

d) Identification of threat sources;

e) Determination of threat actors; and

f) Categorisation of threat actors into threat actor types.

It uses the information in the completed steps above to present the approach for creating a list of risks with a Risk Level for each risk.

Risk assessment helps organisations operating CII comply with DUS 2175: 2019 obligation to adopt a formal, consistent and policy-guided approach to prioritise risks by:

a) Ensuring that ICT solution procurements contain security requirements;

b) Ensuring ICT solutions contain APT controls to secure CII capabilities and assets; and

c) Supporting the risk management activities including the development of a Risk Management Accreditation Plan

Information Security — Risk Assessment

1 Scope

This Uganda Standard specifies the requirements that public and private sector organisations that own and/or operate CII shall adhere to in order to identify, quantify or qualitatively describe and prioritise risks against risk evaluation criteria and objectives relevant to them. It addresses risks to the confidentiality, integrity and availability of information that CII hold, store and process.

2 Normative references

The following referenced documents referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

DUS 2175, 2019 *Information Security — Requirements for Security Controls*

US ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

US ISO/IEC 27005*, Information Technology — Security Techniques — Information Security Risk Management*

US IEC 31010*, Risk Management – Risk Assessment Techniques*

ISO Guide 73*, Risk Management — Vocabulary*

US ISO/IEC 27001*, Information Technology — Security Techniques — Information Security Management Systems — Requirements (2nd Edition)*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in US ISO/IEC 27000, US ISO/IEC 27005, DUS 2175:2019, ISO Guide 73 and the following apply. ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
accreditation
process in which certification of competency, authority, or credibility is presented

3.2
accountability
property that enables the unambiguous tying of an action to an entity such as a user, process, system and information asset

3.3
asset
anything that has value to an organisation and which, therefore requires protection

3.4
cryptanalysis
ability to break a code (cipher) and obtain plaintext from cipher text. Cryptography and cryptanalysis are sub-domains of cryptology a branch of Mathematics that deals with the science of information secrecy

3.5
integrity
anything dealing with the safeguarding of the accuracy and completeness of information assets

3.6
risk
effect of uncertainty on objectives

3.7
security Domain (SD)
group of assets that are the focus of risk identification (i.e. finding, recognising and describing) and evaluation activities. Security domains may be a group of IT assets delivering an end-to end business service e.g. remote access. The domain may also refer to network segments, environments, services or units controlled by a single security policy. Domains help to standardise approaches to risk identification and treatment

3.8
threat
potential cause of an unwanted incident, which may result in harm to a system or an organisation. The Standard adopts the list of typical threats identified in Annex A of US ISO/IEC 27005:2018

3.9
threat Actor
entity that actually exploits a security vulnerability to cause harm to a system or an organisation.

3.10
threat Source
entity that seeks to cause an unwanted incident, which may result in harm to a system or an organisation.

3.11
vulnerability
weaknesses in security controls that threat actors may exploit to harm assets or organisations

3.12
zero-day attack
software-related attack that exploits a weakness that a vendor or developer was unaware of

4 Symbols (and abbreviated terms)

APT-Advanced Persistent Threat

C-I-A-Confidentiality, Integrity, Availability

CD- Compact Disc

CII - Critical Information Infrastructures

CIRO- Chief Information Risk Owner

DVD- Digital Versatile Disc

EOI-Expression of Interest

GoU- Government of Uganda

HR- Human Resource

ICT-Information and Communications Technology

IT-Information Technology

ITT-Invitation to Tender

PABX - Private Automated Branch Exchange

SD -security domain

USB- Universal Serial Bus

5 Scoping Risk Assessments

A risk assessment shall have a clear scope and boundary. For consistency, organisations shall consider risk assessment from at least three perspectives namely external, internal and project as illustrated in Figure 1 below.

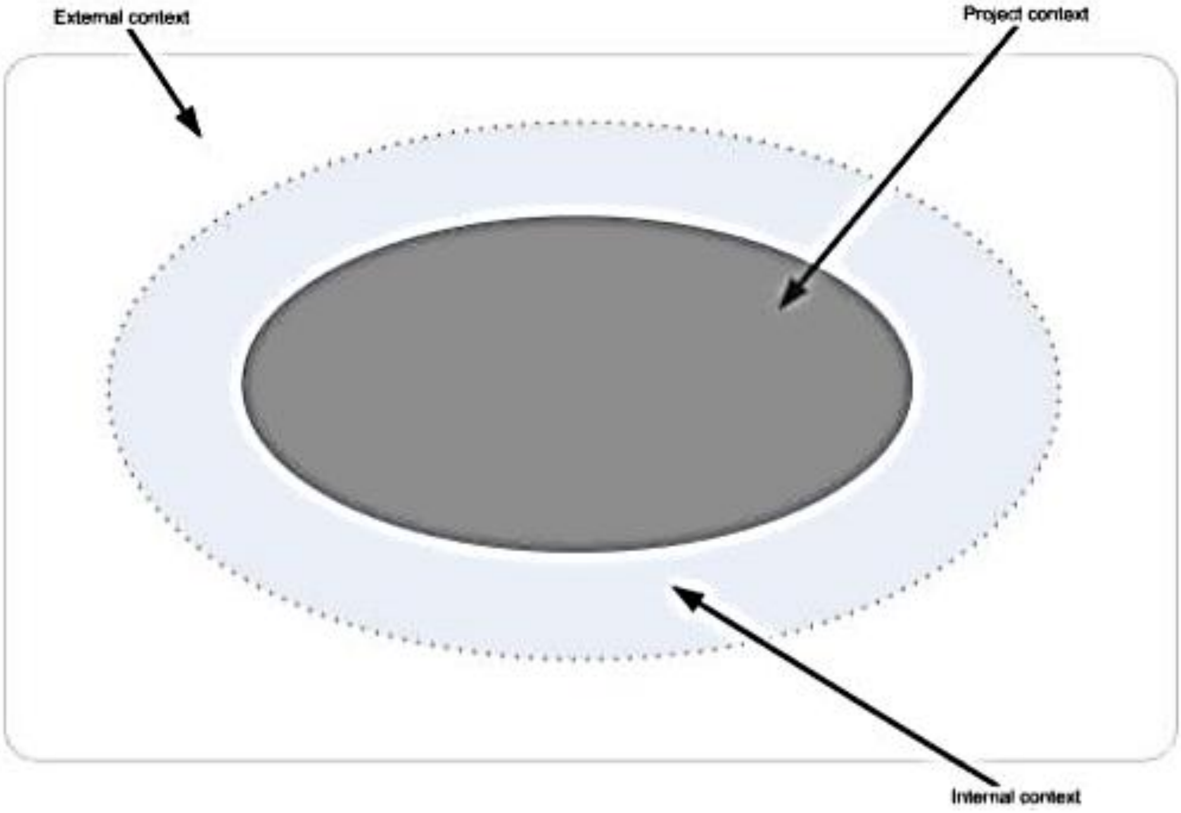


Figure 1 — Risk Assessment Perspectives

5.1 External Context

This is the external environment within which the organisation and CII operates. In accordance with US IEC/ISO 31010, the analysis of the external context shall encompass:

a) All applicable legislation such as the laws identified in DUS 2175: 2019 and their legal instruments;

b) Factors affecting the organisation's financial, economic and competitive environment, whether international, national, regional or local;

c) National standards such as DUS 2175:2019 and its supporting processes, for example, national security impact assessments and security clearance requirements;

d) Pertinent drivers and trends influencing the objectives of the organisation;

e) Good practice security standards and guidance; and

f) Perceptions and values of external stakeholders e.g. donors.

5.2 Internal Context

The internal context constitutes elements outside the project scope that have an impact on its accreditation. As a subset of the external context for example, the internal context shall reflect impact of DUS 2175:2019 requirements on corporate-level security. Projects shall capture the following information about the organisational environment in which the CII shall operate:

a) Governance, organisational structure, roles and accountabilities;

b) Policies, objectives, and the strategies that are in place to achieve them;

c) The capabilities, understood in terms of resources and knowledge e.g. capital, time, people, processes, systems and technologies;

d) Perceptions and values of internal stakeholders;

e) Information systems, information flows and decision-making processes i.e. both formal and informal;

f) Relationships with, and perceptions and values of, internal stakeholders;

g) Organisational culture;

h) Standards, guidelines and models adopted by the organisation; and

i) Form and extent of contractual relationships.

In addition, all parties shall adopt recognisable criteria for identifying, analysis and evaluating risks. As part of a broader risk management process, and in accordance with US IEC/ISO 31010, the risk criteria definition process shall capture:

a) How to measure the nature, types of (business) impacts of risk;

b) Approach for determining risk levels;

c) Criteria for determining when a risk needs treatment; and

d) Criteria for deciding when a risk is acceptable and/or tolerable.

Each organisation has a duty to decide its own acceptable and/or tolerable risk levels.

5.3 Project Context

Project risk assessments shall accommodate the requirements and/or constraints from external and internal context reviews. As outlined in DUS 2175:2019, risk management activities shall comply with the National Information Technology (IT) Project Management Methodology. In particular, the risk assessments shall occur at these stages:

5.3.1 Project Initiation and Planning

Parties shall assess the security risks of a CII project including national security implications during the initiation and planning phases of the project management methodology. Guided by information from the external and internal contexts, the project shall seek to identify the following details:

a) The laws and statutes applicable to the ICT project;

b) The business case/requirements and constraints for the ICT project;

c) Mandatory information, personnel and physical security requirements;

d) Interconnections, flows and relationships with other assets;

e) Relevant stakeholders;

f) Required skills; and

g) Relevant organisation risk policies and standards.

5.3.2 Project Risk Assessment Scope

This stage builds on the outputs of the security activities in the initiation and planning phase(s) to create a formal scope for the security assessment for the project. This activity shall involve detailed review of:

a) Business options and preferences;

b) Security information obtained in the initiation and planning phase(s);

c) The impact of security on the business requirements; and

d) Dependencies and applicable legislation.

5.3.3 Security Requirements Definition

Building on the previous two activities, this activity:

a) Reviews and revises list of security risks identified earlier;

b) Initiates work on the information risk management plan; and

c) Bolsters existing information on security requirements in preparation for the development of procurement documents such as Expression of Interest (EOI); Invitation to Tender (ITT); draft contract and Security Aspects Letter.

5.3.4 Review and Selection of Solutions

All parties shall carry out the following activities during this phase:

a) Use of defined security criteria to judge supplier responses to ITTs and EOIs;

b) Ensuring that supplier contracts contain clear security deliverables;

c) Validation of the existence of security deliverables in supply contracts; and

d) Revision and approval of the draft information risk management plan.

The following information is used as input for the risk assessment activity:

a) Organisational Risk Appetite that CII organisations shall use as the guide for all project-specific risk assessment activities.

b) Threat Sources & Actors as seen in clause 7

6 Assets View

6.1 Identifying and grouping Assets

Public and private sector organisations operating CII shall obtain sufficient details about the assets to facilitate the risk assessment exercise. The level of detail gathered depends on the requirements of the project. More information about the assets can be obtained during further iterations of the risk assessment exercises.

The project team shall ensure that the activity only encompasses assets in the agreed scope of the risk assessment. The result would be a catalogue of Asset as seen in annex A with the fields indicated as a minimum

To catalogue assets, the project team shall:

a) Identify business/information assets, their locations, functions;

b) Obtain information exchange requirements of the information assets;

c) Identify other systems that support the information assets i.e. directly or indirectly.

Public and private sector organisations operating CII shall appoint heads of division, departments, or their equivalent as owners of named information assets. Information from the asset owner enables the determination of asset value.

The asset owner shall:

a) Identify the assets in accordance to Annex B of US ISO/IEC 27005:2018, which outlines the asset identification approach.

b) Know the information the assets under their responsibility hold;

c) Know who accesses the assets under their responsibility and why; and

d) Help identify risks to the assets under their responsibility.

After cataloguing all assets, Organisations shall group the identified assets into security domains.

Organisations shall record the reasons for allocating assets to security domains. Security domains aim to:

a) Standardise risk identification, analysis and evaluation activities;

b) Reduce the difficulty of conducting risk assessments across large, complex and interdependent system boundaries;

c) Reduce the effort of conducting risk assessments on individual assets;

d) Add context to risk assessment exercises by requiring analysts to consider cyber-attacks on other assets supporting the same function, or have similar characteristics and/or reside in the same operating environment;

e) Ensure end-to-end security for assets sharing common threat actors; and

f) Enable the consistent assessment of risks to assets with similar sensitivity.

Organisations shall use modelling techniques to represent security domains and their relationships. They can choose any technique as long as it presents the information in the format that makes it easy to explain, share and compare. Whatever modelling technique chosen, it shall be able to:

a) Identify the information assets requiring protection;

b) Identify actors and sources threatening to compromise the system's security;

c) Express the system's purpose and information exchange requirements;

d) Show direct or third parties and relationships with other systems; and

e) Show relationships within and between security domains.

The list below shows the security domains within which organisations usually group assets. CII teams usually create descriptions of each security domain in different environments such as production, pre-production and disaster recovery. The domains are:

a) Internet-facing systems including interfaces with external systems;

b) Core access zones organised on criteria such as classification levels;

c) Management networks;

d) Evidential components of CII with a need to safeguard the chain of evidence to maintain the legal weight and ensure admissibility of electronic records;

e) Internal support functions e.g. helpdesks, IT operations and test services;

f) Operational sites and facilities;

g) Data backup and restore services;

h) Third party and other externally managed infrastructure support functions;

i) Connections to the CII via (virtual) private connections e.g. remote access;

j) Connections to secure external networks for information exchange; and

k) Internet and public connected networks to commercial organisations.

6.2 Valuing Assets

Asset valuation follows the identification activity. This process is about assigning the asset a widely understood value to enable its secure handling across the organisation. Asset valuation focuses on the business impact of the breach of the asset's confidentiality, integrity and availability rather than its monetary value, a qualitative rather than a quantitative view of asset valuation.

6.2.1 Business Impact Tables

There are four tables to allow public and private sector organisations to assess the business impact level of a breach of confidentiality, integrity and availability. The tables are organised based on “protected computer” sectors in Section 20(2) of the Computer Misuse Act 2011. The tables shown in annex B. Business impact level scale from 0 (trivial) to 5 (catastrophic) is used to help compare business impacts across sectors.

6.2.2 Business Area Sub-Categories

The business impact tables contain sub-categories to help organisations choose the most relevant category for the asset or group of assets under consideration. Since more than one sub-category can apply, parties shall consider all the applicable categories to help identify the business impacts of security compromises on related business activities.

6.2.3 Classification and Business Impact Levels Relationship

For confidentially, business impact levels relate directly to classification levels as outlined in the table 1 below.

Table 1 — Relationship between Classification and Business Impact Levels

Classification Level	Impact Level	Business Impact
UNCLASSIFIED	0	Trivial
UNCLASSIFIED-PERSONAL	1	Low
OFFICIAL	2	High
SECRET	3	Extreme
TOP SECRET	4	Catastrophic

7 Analysing threats and Vulnerabilities

7.1 Identifying Threat Sources

After identifying and valuing assets, organisations shall identify and record threat sources. Threat sources often collaborate with threat actors who are the entities that execute attacks. The threat sources have attributes, which include capability, motivation, resources and consequences. Threat sources include, but are not limited to the following entities:

a) Insiders

b) Foreign Intelligence Services

c) Industrial Espionage

d) Extremist Organisations

e) Organised Criminal Syndicates

f) Hackers/Hacktivists

g) Investigative Journalists

Their description, capability and resources are highlighted in table C.1 in Annex C. The motivation and consequences of the threat sources have been detailed in annex C of US 27005:2018.

7.2 Calculating Threat Levels

Each organisation shall assess the threat levels. The assessment of threat levels shall summarise the following aspects about each threat source:

a) Capability; threat source's ability to exploit vulnerabilities to launch attacks against valuable information assets. Levels are on a scale of 1 to 5.

b) Motivation; measures the desire driving a threat source's interest in breaching security including monetary gain, ideology, coercion, disaffection and pursuit of notoriety. Motivation levels are on a scale of 1 to 5.

c) Clearance/Vetting Level;

d) Value for Information Security Property;

e) Threat Level; product of a threat source's capability and motivation.

The primary objective of the assessment is to identify the threat level because the level shows the most potent threat sources. The threat level points to ability and desire of a threat source to influence the actions of other entities i.e. threat actors. Threat levels are plotted ranging from TRIVIAL to CATASTROPHIC as illustrated in table C.2.1 in annex C.

7.2.1 Threat Source Values for C-I-A Elements

Threat sources may have different levels of interest and ability to inflict damage on the three security properties i.e. confidentiality, integrity and availability. Thus, it is useful to present capability and motivation values for the different properties because the overall threat level. The table C.2.2 illustrates how one could present foreign intelligence services example above:

7.2.2 Impact of Security Vetting on Threat Levels

DUS 2175: 2019 requires that organisations perform suitable Baseline Security and National Security Vetting checks to ensure that the character and personal circumstances of the individuals are such that they can be trusted with access to protected computers. The checks can help reduce threats level as follows in table C.2.3

7.2.3 Threat Source Assessment

Organisations shall use the example in C.3 as a starting point for threat source assessments. The example starts by identifying the threat sources and thereafter assessing their overall threat level as well as C-I-A specific levels. The example also considers the impact of security clearances on the overall threat level.

7.3 Identify Threat Actors

This clause focuses on an approach for identifying and determining threat actor capabilities. Threat sources and actors have an intricate relationship. The main difference lies in susceptibility to external influence factors such as coercion, blackmail and bribery. External influence is the factor that typically turns a threat source into an actor. Organisations shall consider the following threat Actor types:

a) Normal Users

b) Privileged Users

c) Partners

d) Suppliers

e) Consumers

f) Third Parties

g) Facilities

h) Physical Intruders

i) Intermediaries

j) Supply Chain Actors

k) Disasters

Organisations should note the following as they classify threat actors;

a) The capability, motivation with and without external influence is detailed in table C.4. It is evident that external influence like bribery and coercion increases the motivation of the normal users, privileged users, partners, Suppliers, Consumers, facilities, Supply Chain Actors and, Intermediaries

b) Holding a valid National Security Clearance such as SECRET could reduce the threat level of Privileged users. For partners with the highest capacity, a valid National Security clearance i.e. SECRET and TOP SECRET can help reduce the partner threat level too. Suppliers can obtain a Baseline clearance but may lack a valid national security clearance. Consumers have the same characteristics as normal users therefore, they are unlikely to have a clearance

c) Third Parties do not have a direct link to the CII but are susceptible to infiltration by other threat sources such as hackers/hacktivists. Naturally, they would not have a security clearance to reduce their threat level. Facilities team threat actor types are insiders because they have physical and often logical access to sensitive information assets. Having limited technical capacity and motivation to attack CII capabilities, Baseline Security checks could reduce their threat level to TRIVIAL. Parties that attempt to gain physical access to CII capabilities are highly capable and motivated. Unfortunately, burglars do not submit to security vetting.

d) For intermediaries, security vetting could reduce the threat level from HIGH to MODERATE. Threat actors within the supply or acquisition chain have similar attributes to suppliers. DUS 2175: 2019 identifies supply chain security as major area of focus for the public and private sector because operatives of foreign intelligence services increasingly target the supply chain. As such, the external influence is 4. Security measures such as national security assessment can reduce this group's threat level.

e) Natural disasters constitute threat actors because they cause interruptions and/or destruction to CII services. The capability estimate of 1 is purely academic. Natural disasters can destroy everything. Hence, organisations shall assume the worst. In accordance with DUS 2175: 2019, organisations shall have adequate business continuity and disaster recovery measures. Organisations, could for instance, mitigate natural disaster risks by transferring them e.g. through insurance.

The assessments shall identify the security domains that threat actor affect. The illustration in table C:4 uses the threat level with the external influence factor to show the worst-case scenario.

7.4 Attack Methods

Organisations increase the security of CII if they identify and defend against the accidental and deliberate methods a relevant threat actor may use to breach confidentiality, integrity and availability. Table C.5 shows how to present the attack methods against named threat actor types. The attack methods focus on information (C-I-A) and systems/infrastructure (configuration). The table C.5 uses the example of normal and privileged users. Organisations shall use the format to identify attack methods for actor types relevant to their project.

7.5 Identification of Vulnerabilities

After determining threat sources and actors, CII organisations shall identify vulnerabilities. In accordance with ISO/IEC 27001:2013, CII operators shall consider potential security vulnerabilities in the following areas:

a) Security governance, organisational structure, roles and accountabilities;

b) Processes and procedures;

c) Management routines;

d) Personnel;

e) Physical environment;

f) Information system configuration;

g) Hardware, software or communications equipment; and

h) Dependence on external parties i.e. supply chain risks.

The advice finds support in the ISO/IEC 27001:2013 observation that vulnerabilities without corresponding threats may not require action. Organisations shall record and monitor all vulnerabilities for potential changes. In accordance with ISO/IEC 27001:2013, the activity shall produce:

a) A list of vulnerabilities in relation to assets, threats and controls; and

b) A list of vulnerabilities that do not relate to any identified threat for review.

Annex D of US ISO/IEC 27005:2018 contains useful examples of vulnerabilities in various security areas and threats that might exploit these weaknesses. The list shall provide a starting point during threat and vulnerability assessments.

8 Impact and Risk View

8.1 Risk Levels

The level of risk describes the magnitude of risk as expressed in terms of the combination of impacts and their likelihood in accordance with ISO Guide 73:2009. The table D.1 shows that the Risk Level is a product of the comparison of the business impacts of risk realisation and the likelihood of occurrence. It shall be used by organisations to calculate Risk Level.

8.2 Risk Assessment Model

Organisations shall apply an in-depth risk assessment described above as the process that involves the identification and valuation of assets, the assessment of threats to those assets and assessment of vulnerabilities. The Figure 2 below summarises the risk assessment process.

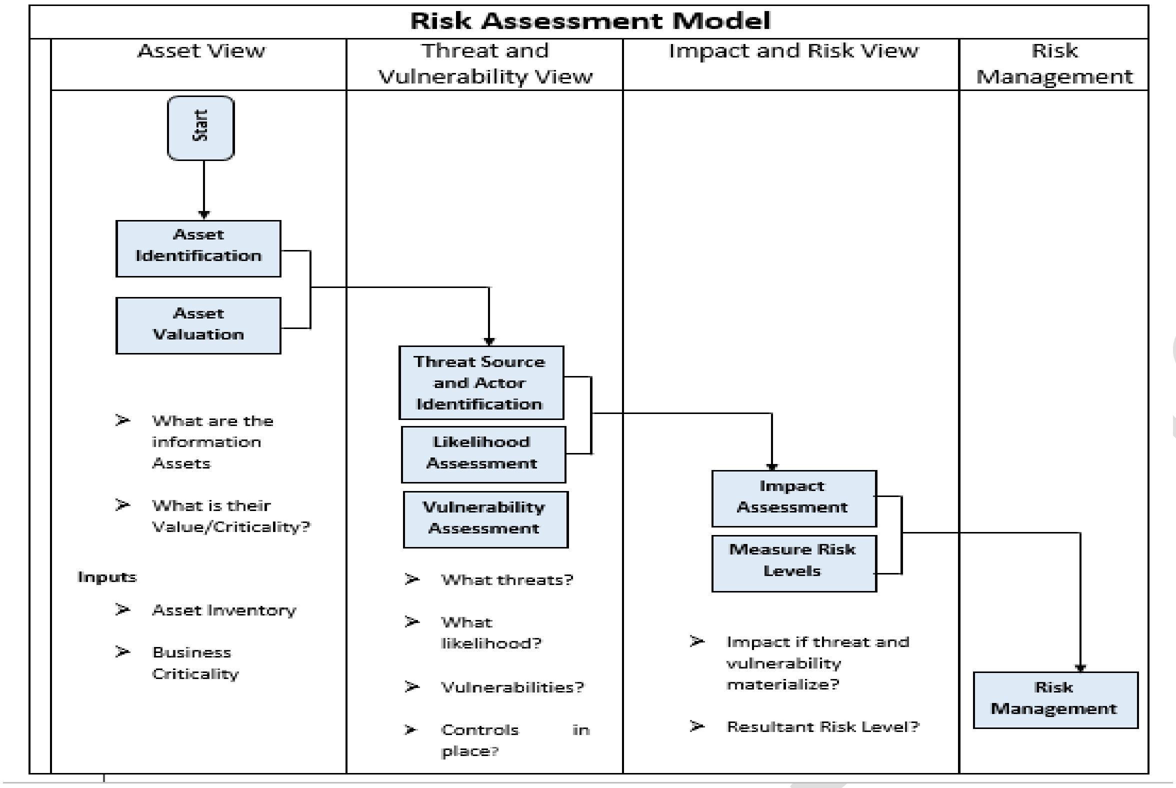


Figure 2 — Risk Assessment Model

8.3 Assessing Risks

After assets identification and valuation, threat and vulnerability identification, the next step identifies and assesses the risks that each threat actor type poses. Using two examples of the threat actor types for which attack methods are identified, tables D.2 and D.3 in annex D illustrate this.

8.4 Prioritised Risks

The purpose of this last step is to create an easy to understand list of all risks starting from the highest Risk Levels to the ones with lower Risk Levels. As a minimum requirement, the prioritised list of risks shall have the following fields:

a) Risk ID;

b) Security Domain;

c) Threat Actor Type;

d) Risk Description; and

e) Risk Level

Organisations may add as many fields as necessary for their business and security requirements.

The table below of prioritised risks from the two examples in annex D.2 (normal users) and D.3 (privileged users) is presented in table D.4.

8.5 Risk Assessment Reporting

Organisations shall create a summary to provide a quick view of the risks identified. The simple statement that shall appear as follows:

8.5.1 Executive Summary

The risk assessment identified [e.g. 200] risks each with unique ID including:

a) 10 Very-High Risks;

b) 50 High Risks;

c) 30 Medium-High Risks;

d) 60 Medium Risks;

e) 40 Low Risks;

f) 10 Very-Low Risks

8.5.2 Summary Description

Parties shall create a summary description of the risks by threat actor type. Below are examples on risks affecting supply chain and third parties.

8.5.2.1 Supply Chain Attacks

The acquisition of compromised hardware and software poses momentous risk to the confidentiality, availability and availability of [CII Project] infrastructure. The level of risk is significant across [CII Project Name] infrastructure giving rise to 5 Very High Risks, 15 High Risks and 3 Medium High Risks. The compromise of hardware and software assets during their acquisition poses a significant threat to [CII Project Name] given that it supports national security activities. [CII Project Name] team shall put in place a range of governance, information, personnel and physical security controls to mitigate the risk.

8.5.2.2 Attacks via Third Parties

External connections from the Internet that terminate in Zone X (Security Domain 1) pose a significant risk to the Confidentiality, Integrity and Availability of [CII Project] infrastructure. 3 Very High, 10 High and 3 Medium High Risks threaten the security of the infrastructure within Zone X and other Security Domains within the [CII Project]. [CII Project] shall harden Zone X to address this risk. Zone X requires strong technical controls to identify threats from the Internet. [CII Project] shall also adopt information and personnel security controls to bolster the technical measures such as the use of enforceable exchange agreements.

Annex A
(Normative)

Asset Catalogue Form

Public and private sector organisations that operate and/or own CII shall use the Asset Catalogue Form below to capture facts about information assets.

SD [Number]	[Name of Security domain e.g. backup environment]				
Asset Identifier	Description	Asset Owner	**Impact Levels**		
			C	**I**	**A**

Annex B
(Normative)

Business Impact Tables

B.1 Security, Defence and International Relations

Table B.1 provides organisations in the security, defence and diplomacy a consistent approach for assessing business impact of cyber-attacks that could disrupt and/or destroy military, intelligence and other related CII.

Table B.1 —Security, Defence and International Relations

Sub Category	**IL0**	**IL1**	**IL2**	**IL3**	**IL4**
Life and safety	A security compromise could cause an individual nuisance or anxiety	Disclosure of private information could threaten an individual's personal safety or liberty	A breach of security around certain official records could threaten the security or liberty of a group of people	A security compromise could then threaten life directly leading to limited loss of life	A compromise of security could cause widespread loss of life
Intelligence operations	None	A compromise of security could make it difficult to conduct low level intelligence operations	A compromise of security could hamper intelligence operations in support of public order and public safety	A compromise of security could hamper and damage capacity to conduct intelligence operations aimed to avert severe risks to national security	A compromise of security could hamper and damage capacity to conduct intelligence operations aimed to avert catastrophic risks to national security
Military operations	A security breach could have a minor impact on supply services	A security compromise could moderately reduce operational effectiveness or security of Ugandan and allied forces	A security compromise could significant damage to the operational effectiveness or security of Ugandan and allied forces	A security compromise could cause extreme damage to the operational effectiveness or security of a large group of Ugandan and allied forces in theatre	A security compromise could cause catastrophic damage to the operational effectiveness or security of an extremely large group of Ugandan and allied forces in theatre
International relations	None	A security compromise could cause low-level embarrassment in international relations	A security compromise could cause embarrassment in international relations e.g. leading formal protest or sanctions	A security compromise could cause extreme tension and serious damage to relations with friendly countries	A security compromise could cause a catastrophic damage to relations potentially provoking war and at best gravely damaging friendly relations
International trade negotiations	None	A security compromise could low-level damage to the prospects of a major Ugandan company	A security compromise could significantly damage to the prospects of a number of major Ugandan companies	A security compromise could cause extreme damage to Uganda's position in bilateral international negotiations	A security compromise could cause catastrophic damage to Uganda's position in major multi-lateral international negotiations

B.2 Law Enforcement, Public Safety and Public Order

The table B.2 below aims to provide parties involved in maintaining social order, protecting life and property of the citizens of Uganda a consistent approach for assessing the business impact of cyber attacks that can disrupt and/or destroy their CII.

Table B.2 —Law Enforcement, Public Safety and Public Order

Sub Category	IL0	IL1	IL2	IL3	IL4
Life and safety	A security compromise could cause an individual nuisance or anxiety	Disclosure of private information could threaten an individual's personal safety or liberty	A breach of security around certain official records could threaten the security or liberty of a group of people	A security compromise could then threaten life directly leading to limited loss of life	A compromise of security could cause widespread loss of life
Existence or identity of confidential source	A security compromise could lead to disclosure of existence of a confidential source beyond those with a Need-to-Know	A security compromise could lead to disclosure of identity of confidential source beyond those with a Need-to-Know	Disclosure of the identities of a small group of confidential sources identify could increase their vulnerability to attack	A security compromise significantly undermines the witness protection scheme leading to limited loss of life	A security compromise causes a catastrophic failure of the entire witness protection scheme nationwide leading directly to loss widespread loss of life
Police services	None	A security breach leads to minor disruption of police services for an individual	A security compromise leads to substantial disruption of police services to a small group of individuals	A security breach leads to an extremely serious disruption of police services to a large area threatening safety and/or leading to limited loss of life	A security breach leads to a catastrophic disruption of police services directly leading to widespread loss of life for example through riots
Health of citizens	A security compromise could a disruption of health services in one locality	A security compromise could cause a minor disruption of health services posing a risk to health e.g. spread of disease in a district	A security compromise could cause a major disruption of health services posing a risk to health e.g. spread of disease in several districts	A security compromise could cause an extremely severe disruption of health services posing a risk to health and limited loss of life across some regions of the country	A security compromise could cause a catastrophic failure of health services posing a risk to health and widespread loss of life across the entire country
Emergency services	Security compromise could disrupt emergency services in one locality	A security breach could cause a minor disruption of emergency services necessitating re planning at organisational and district levels	A security compromise could cause a major disruption of emergency services necessitating substantial changes in their organisation across several districts to meet service levels	A security compromise could cause an extremely severe disruption of emergency services necessitating drastic changes in their delivery mechanisms e.g. involvement of the Armed Forces to meet service requirements across several regions of the country	A security compromise could cause a catastrophic failure of emergency services posing a risk to the internal stability of the country and requiring assistance from neighbouring countries
Political stability	None	A security compromise could cause minor loss of confidence in Government	A security compromise could cause major loss of confidence in Government	A security compromise could cause could threaten directly Uganda's internal political stability	A security compromise could cause a catastrophic collapse of Uganda's internal political stability

Privacy of citizens	A security compromise could cause short-term agony to an individual e.g. disclosure of borrowing history	A security compromise could cause medium term agony to an individual or short term embarrassment to several citizens	A security compromise could cause major and sustained agony to a many citizens and extreme stress to an individual. For example, disclosure of a person's medical history	A security compromise could cause extreme agony to millions of citizens across the country e.g. disclosure of medical records in a national hospital and several regional hospitals	A security compromise could a catastrophic collapse of a national identity management system and disclosure of sensitive records for the majority of citizens

B.3 Public Services, Public Utilities and other Critical National Infrastructure

The table B.3 below provides a consistent approach for assessing the business impacts of cyber attacks on CII that support daily life, commerce and the activities of the public

Table B.3— Public Utilities and other Critical National Infrastructure

Sub Category	IL0	IL1	IL2	IL3	IL4
Confidence in public services	A security compromise reducing in an individual's confidence in a public service e.g. crashing government website	A breach resulting in a minor reduction in confidence in a public service by several individuals and severe reduction in confidence by an individual e.g. cancelled hospital appointments	A security compromise resulting in a major reduction in confidence in the services a major government department e.g. hacking of a national identity database	A security compromise resulting in extreme loss of public trust in the services of several major government departments leading evident reduction in their use e.g. increased use of private clinics	A security compromise resulting in a catastrophic collapse in public trust in government services leading to loss of revenue with critical impact on service continuity
Communications infrastructure	A security breach causing the disruption telecoms for up to 6 hours	A security breach causing the disruption telecoms for up to 12 hours	A security compromise causing the loss of telecom services in a region for up to 24 hours	A security breach causing the loss of telecom services nationally for up to a week	A security breach causing the loss of telecom services nationally for up to more than 1 week
Power & energy	A security breach causing a local power failure for up to 6 hours	A security breach causing a power failure in a region for up to 12 hours	A security breach causing a power failure in a region for up to 24 hours	A security breach leading to the loss of power nationally for up to a week	A security breach leading to the loss of power nationally for more than 1 week
Water and sewerage	A security breach causing the breakdown of local water and sewerage services for less than 50 homes for more than a week	A security breach causing the breakdown of local water and sewerage services for less than 100 homes for up to 1 month	A security breach causing the breakdown of local water and sewerage services for more than 100 homes for up to 1 month	A security breach causing a severe breakdown of regional water and sewerage services for more than 100 homes for up to 3 months	A security breach causing a catastrophic breakdown of national water and sewerage services for more than 100 homes for more than 3 months
Transport	A security breach causing the disruption of vital local transport systems for up to 6 hours	A security breach causing the disruption of vital local transport systems for up to 12 hours	A security breach causing a major disruption of vital regional transport systems for up to 24 hours	A security breach causing extreme disruption to vital national transport systems for up to a week	A security breach causing catastrophic failure of vital national transport systems for over a month

Food supplies	A security breach causing the disruption of the distribution of food supplies at the local level for up to a month	A security breach causing the disruption of the distribution of food supplies at the regional level for up to a week	A security breach causing the disruption of the distribution of food supplies at the regional level for up to a month	A security breach causing the disruption of the distribution of food supplies at the national level for up to a month	A security breach causing the disruption of the distribution of food supplies at the national level for over a month

B.4 Banking, Financial Services and Public Finance

The table B.4 below provides a consistent approach for assessing the business impacts of cyber attacks on CII that support banking and financial activities of citizens, companies and the public.

Table B.4 — Banking, Financial Services and Public Finance

Sub Category	IL0	IL1	IL2	IL3	IL4
Public finances	A security breach causing the loss of public sector money up to UGX 1 million	A security breach causing the loss of public sector money several UGX millions	A security breach causing the loss of public sector money between UGX 10 million and UGX 50 million	A security breach causing the loss of public sector money between UGX 50 million and 1 billion	A security breach causing a catastrophic loss of public finances estimated at over UGX 1 billion
Trade and commerce	A security breach that undermines the financial viability of a number of small businesses in Uganda	A security breach that undermines the financial viability of a medium-sized Uganda-owned business organisations	A security breach that undermines the financial viability of major Uganda-owned business organisation	A security breach that causes extreme damage to trade and commerce in Uganda leading to perceptibly reduced economic growth	A security breach that causes catastrophic and long-term damage to Uganda’s global trade and commerce leading to drawn out recession and high hyperinflation
Banking and financial services	A security breach that causes minor financial loss to an individual	A security breach that causes significant financial loss to an individual causing real pressure on short-term finances and minor financial loss to a group of individuals	A security breach that causes a substantial loss of income for a large number of people causing real pressure on their short-term finances and bankrupting some of the affected individuals	A security breach that financially devastates a large group of individuals e.g. pensioners leading to extensive financial distress including personal bankruptcies and repossession of property such as homes	A security breach that catastrophic, widespread and causes long-term financial damage across the Ugandan economy bankrupting major corporations including banks and requiring GoU and international intervention

Annex C
(Informative)

Threat Sources, Threat Actors and Attack Methods

C.1 Threat Sources, their capability and resources

Table C.1 — Threat Sources, their capability and resources

Threat Sources	Capability	Resources
Insiders Individuals with legitimate access to protected systems are a problematic threat source. These users include disgruntled employees, suppliers, facilities teams and partners. Insiders have the following attributes	The capability of the insiders ranges from no skills at all to the highest degree of capability. Insiders with rudimentary technical capability include clerical staff. Facilities teams such as security guards, cleaners and maintenance teams may have varying degrees of technical capability. However, foreign intelligence services routinely "plant" extremely capable operatives into facilities teams. Thus, CII owners and operators shall exercise great care with this group. On the extreme, insiders such as system administrators have advanced technical skills that allow them to launch sophisticated and bespoke attacks.	Insiders have moderate resources to launch sophisticated attacks. Typical, insider attacks involve one person with occasional support from part-timers.
Foreign Intelligence Services Nations have always sought to protect their own interests by covertly obtaining information about plans and actions of hostile (and sometimes friendly) States, organisations and individuals since the beginning of time. ICTs have drawn the interest of foreign intelligence services as sources of intelligence. The spies also use ICTs to record, mark, retrieve, assess and adjust the gathered intelligence. Foreign intelligence services have the following attributes:	Foreign intelligence services have the most advanced technical skills. As such, spies are able to launch the most sophisticated attacks. Foreign intelligence services, especially those in developed countries, have skills to defeat the most advanced security technologies. Foreign intelligence services have some of the best brains in cryptography and cryptanalysis. Recent events have disclosed that intelligence services also seek to use financial and regulatory pressure to subvert the security of commercial encryption products.	Being government-financed, the resources of a foreign intelligence services usually match the wealth of the sponsoring nation. Some spies have unlimited resources with "black" budgets that enable them to run unlimited full-time attack teams of government employees, contractors and sometimes organised criminal groups. The resources enable the spies to devise sophisticated and/or bespoke attacks on particular systems. The budgets also enable the spies to purchase "zero-day" attacks from all sources including the criminal "underworld."
Industrial Espionage Industrial espionage attacks can involve large teams of highly trained individuals attempting to compromise a system either full-time or regularly. Perpetrators of industrial espionage can use tools such as Advanced Persistent Threats (APTs) to gain unfettered access to secrets and intellectual property. ICT suppliers can also act in concert with foreign spies in support of economic and political goals of their nations.	Same as above	Same as above

Organised criminal syndicates Organised criminal syndicates exploit the anonymity and global reach of the Internet to conduct attacks without ever having to be at the scene of the crime physically. Because of the global nature of their operations, criminals have the resources and capability to conduct sophisticated attacks. For example, the criminal gangs can use the Internet black market to purchase attack tools such as BotNets. Organised criminal syndicates have the following attributes:	The capabilities of organised criminal syndicates could range from moderate to substantial. Some groups with global reach can have the skills that match those of foreign intelligence services of medium-sized countries. As a result, criminal syndicates can have the capability to launch sophisticated and bespoke attacks. As noted earlier, organised crime syndicates can, and often, serve as threat actors for threat sources notably foreign intelligence services.	The resources of organised criminals range from moderate to substantial.
Hackers/Hacktivists DUS 2175: 2019 mandates that organisations to institute measures to detect and resist a compromise by hackers/hacktivists. This group has the following attributes:	Professional hackers are extremely knowledgeable. Individually, hackers are capable of launching both simple and sophisticated attacks. However, a hacker's capability increases exponentially when allied with a cause. Groups such as Anonymous, LulzSec, RedHack, LulzRaft and several others have unleashed stinging attacks against high profile corporate and government targets. This group has the following attributes:	Hackers/hacktivists have minimal to moderate resources. In many instances, hacktivists use opportunistic and unsophisticated tactics to exploit poor security such as lack of patching and weak password policies.
Extremist Organisations There are concerns that extremist groups such as terrorists are building capacity to use cyber-attacks against critical infrastructure such as power grids to cause violence against and terrorise civilians. This group has the following attributes:	The most potent extremist groups rely on government-finance. Therefore, the capabilities of such extremist groups match those of foreign intelligence services. In the spirit of assuming the worst, this Standard expects that extremist groups would have the capacity to launch the most sophisticated attacks.	If government-financed, extremist groups would have the resources similar to those of foreign intelligence service i.e. substantial.
Investigative Journalists Investigative journalists perform an important role in society by reporting on the activities of all branches of Government. However, all organisations shall have in place adequate measures to stop the unauthorised and/or untimely publication of sensitive information. This group has the following attributes:	Media organisations could be very capable. The media may use non-technical attacks such as social engineering, bribery and coercion of authorised users including disgruntled employees and contract staff. Investigative journalists may also work with political activists to attack CII to expose perceived weaknesses in Government operations.	Investigative journalists may have resources ranging from minimal to substantial. In some countries, investigative journalists have hired private investigators to hack the computers and telephones of Ministers and senior government officials.

C.2 Computing Threat Levels

Table C.2.1 — Threat Levels

		Capability Levels				
		1	**2**	**3**	**4**	**5**
Motivation Levels	0	Trivial	Trivial	Trivial	Trivial	Trivial
	1	Trivial	Trivial	Low	Low	Moderate
	2	Trivial	Trivial	Low	Moderate	High
	3	Trivial	Low	Moderate	High	Extreme
	4	Low	Low	Moderate	Extreme	Extreme
	5	Low	Moderate	High	Extreme	Catastrophic

Table C.2.2 — Different threat levels for C-I-A

Identifier	Threat Source	Property	Capability	Motivation
1	Foreign /intelligence Services	Confidentiality	5	3
		Integrity	5	3
		Availability	5	3

Table C.2.3 — Impact of Security Vetting on Threat Levels

		Threat Levels					
		Trivial	Low	Moderate	High	Extreme	Catastropic
Vetting Levels	None	Trivial	Low	Moderate	High	Extreme	Catastropic
	BASELINE	Trivial	Trivial	Low	Moderate	Extreme	Extreme
	SECRET	Trivial	Trivial	Trivial	Low	Moderate	Extreme
	TOP SECRET	Trivial	Trivial	Trivial	Trivial	Low	Moderate
	Grey-Trivial, Green-Low, Yellow-Moderate, Blue High, Red –Extreme, Pink-Catastrophic						

C.3 Example – Threat Source Assessment

The example starts by identifying the threat sources and thereafter assessing their overall threat level as well as C-I-A specific levels. The example also considers the impact of security clearances on the overall threat level.

C.3.1 Example – Threat Sources

Organisations shall describe the threat sources relevant to their CII project. The example below shall be of assistance:

C.3.1.1 Foreign Intelligence Services

This example assumes the following. Firstly, that foreign intelligence services, especially from developed countries, have first class capability and resources – technical, financial, influence and time – to launch sophisticated attacks. As noted above, this example estimates the capability of the spies at 5-5-5 for C-IA. The example assumes that foreign spies would have the capacity to attack a priority CII repeatedly using sophisticated techniques and be-spoke attacks including zero-day exploits. As mandated by DUS 2175: 2019, this example expects that foreign spies would attempt to infiltrate their operatives into the supply chain. Foreign intelligence services also employ non-technical attacks such as social engineering, bribery and coercion of employees, third party and contract staff. Regarding motivation, this example assumes it to be at 3-3-3 for C-I-A. As noted above, motivation is 3 because foreign spies do not target every system. However, where they do, the motivation estimate becomes 5 – the maximum.

C.3.1.2 Organised Crime Syndicates

This example assumes that organised crime groups are very capable and have the resources to carry out sophisticated attacks including be-spoke ones. Unlike spies who have unlimited resources, the capability of the criminal groups is at 4-4-4 for C-I-A. The criminal groups shall also seek to attack the system repeatedly if a successful attack supports their goals. The example assesses motivation at 4-4-4 for C-I-A. However, the motivation could increase or reduce. The groups would also launch non-technical attacks such as social engineering, bribery and coercion of employees, third party and contract staff.

C.3.1.3 Hackers/Hacktivists

This example regards hackers/hacktivists as a technically capable threat source because of their knowledge of IT. However, unlike foreign intelligence services, hackers/hacktivists rarely have the resources to launch sophisticated attacks on their own. However, this example recognises that hackers/hacktivists are more potent as threat actors for threat sources such as foreign intelligence agencies, organised crime syndicates and extremist organisations. Judged alone, this example estimates the capability of hackers/hacktivists at 4-4-5 for C-I-A. Availability is at 5 because Distributed Denial of Service (DDoS) attacks are one of the most common attack techniques of hackers notably hacktivists. Hackers also use the same non-technical skills as other threat sources notably social engineering. Hackers can have strong motivation to attack specific CII individually and as part of a group. Therefore, this example assesses motivate at 4-4-4 for C-I-A.

C.3.1.4 Extremist Organisations e.g. Terrorists

This example assumes that extremist organisations such as terrorists generally have adequate IT expertise to launch simple attacks. The groups may also lack the resources to conduct sophisticated attacks. Therefore, this example rates the capability of extremist organisations including terrorists as 2-2-4 for C-I-A. Yet, the low rating does not give organisations operating CII reason to ignore this threat source because extremist organisations exist to incite other parties, some of which might be competent, into serving as threat actors on their behalf. Given that extremist organisations gain notoriety through acts that cause fear, their interest in CII is low. Hence, this example rates motivation as 2-2-2 for C-I-A.

C.3.1.5 Investigative Journalists

This example regards investigative journalist as technically able. However, new organisations lack the resources required to mount sophisticated attacks. As such, this example assesses the capability of this threat source at 2-2-2 for C-I-A. On motivation, investigative journalists exist to gain access to confidential information. Hence, this example rates motivation at 3-3-3 for C-I-A. However, the motivation is not the maximum, because unlike sources such as organised criminal syndicates, journalists obey the law and do not usually do whatever it takes to access sensitive information. In common with other threat sources, investigative journalists use non-technical attacks such as social engineering, bribery and coercion of employees, third party and contract staff.

C.3.1.6 Industrial Espionage

Companies seek to gain commercial advantage by gaining unauthorised access to information about their rivals. This example regards companies conducting industrial espionage as technically able and adequately resourced to launch moderately sophisticated attacks. Therefore, their capability is at 3-3-3 for C-I-A. Financial gain usually motivates the entities that conduct industrial espionage. Thus, this example assesses the motivation of the entities at 3-3-3 for C-I-A. The motivation could be higher if the companies serve as threat actors in support of economic and political goals of threat sources such as their home countries, spy agencies, extremist organisations and even investigative journalists.

C.3.1.7 Insiders

C.3.1.7.1 Normal and Privileged Users

As a group, normal and privileged users are a serious threat source with considerable technical capability and resources to conduct attacks against because they already have access. As such, the capacity of this combined group is at 5-5-5 for C-I-A. About motivation, this example assumes that a disaffected employee would seek to attack a CII individually on a part-time basis. As such, the motivation is at 2-2-2 for C-I-A. As noted above, security vetting can help reduce the group’s threat level. The example, however, expects that the group is susceptible to pressure to serve as a threat actor for other threat sources such as foreign intelligence services, extremist organisations, organised criminal syndicates and journalists. Thus, risk assessment considers external influence.

C.3.1.7.2 Supplier Staff Insider Threat

This example also considers the threat of supplier, third party or contract staff performing highly privileged support functions. By the nature of this work, the staff have specialist technical capacity and resources to launch sophisticated attacks. As a result, their capability to attack the system is 4-4-4 for C-I-A. Like other privileged insiders, this example assumes that a disaffected supplier staff member would seek to attack a CII individually on a part-time basis. Therefore, this example considers their motivation to be 2-2-2 for C-I-A. However, privileged supplier employees are susceptible to external influence by other threat sources such as foreign intelligence services who increasingly plant operatives in IT companies. Therefore, security vetting can help reduce their threat level.

C.3.1.7.3 Partners

The third insider threat source deals with partners. These are public and private sector organisations with connections to CII. The partners are extremely capable and have the resources to carry out sophisticated attacks if they chose to. Thus, this example assesses the capability of partners to launch attacks as 5-5-5 for CI-A. Trusted public and private sector organisations have little motivation to attack a system they are benefitting from. If attacks occur, these are likely to be the work of a single actor working part-time. Hence, this example assesses the motivation for this group is 2-2-2 for C-I-A. However, connections from “trusted” partners are susceptible to infiltration by other threat sources such as foreign intelligence services. Partner employees are also susceptible to the same risks of bribery, coercion and blackmail as other threat sources. Thus, as mandated by DUS 2175: 2019, the staff shall meet security-vetting requirements.

C.3.2 Summary – Threat Source Identification

The table C.3 below summarises the activity involving the identification of threat sources. The table utilises the threat level calculation guidance in table C.2.1 and the values presented in the example outlined in C.3.1 above.

Table C.3 — Threat sources with threat levels

Identifier	Threat Source Name	Property	Capability	Motivation	Threat Level
1	Foreign Intelligence Services	Confidentiality	5	3	Extremet
		Integrity	5	3	Extreme
		Availability	5	3	Extreme
2	Organised Crime Groups	Confidentiality	4	4	Extremet
		Integrity	4	4	Extreme
		Availability	4	4	Extreme
3	Hackers/ Hacktivists	Confidentiality	4	4	Extremet
		Integrity	4	4	Extreme
		Availability	5	4	Extreme
4	Extremist Organisations	Confidentiality	2	2	Trivial
		Integrity	2	2	Trivial
		Availability	4	2	Moderate
5	Investigative Journalist	Confidentiality	3	3	Moderate
		Integrity	3	3	Moderate
		Availability	3	3	Moderate
6	Industrial Espionage	Confidentiality	3	3	Moderate
		Integrity	3	3	Moderate
		Availability	3	3	Moderate
7	Insider-Internal Normal & Privileged	Confidentiality	5	2	High
		Integrity	5	2	High

		Availability	5	2	High
8	Insider-Supplier Staff	Confidentiality	4	2	Moderate
		Integrity	4	2	Moderate
		Availability	4	2	Moderate
9	Insider-Partners	Confidentiality	5	2	High
		Integrity	5	2	High
		Availability	5	2	High

C.4 Summary – Threat Actor Identification

The table C.4 below summarises the activity involving the identification of threat actors. It utilises the guidance in table C.2.1 to calculate the threat level from the values presented in the example outlined in sub clause 7.3

Table C.4 — List of Threat Actors and External Influence

Threat Actor Type	**Threat Actors (Values in brackets refer to capability, Motivation)**	**capability**	**Motivation 1**	**Threat Level 1 no external Influence**	**Motivation 2**	**Threat Level 2 with external Influence**
Normal Users	Normal Users (2,2) Managers (3,2)	3	2	Low	4	Moderate
Privileged Users	System Administrator (5,2) Network Administrator (5,2) Firewall Administrator (5,2) Backup Personnel (5,2)	5	2	High	4	Extreme
Partners	MDAL staff (5,2)	5	2	High	4	Extreme
Suppliers	Supplier System Administrator (4,2) Supplier System Administrator (4,2) Supplier Network Administrator (4,2)	4	2	Moderate	4	Extreme
Consumers	MDAL staff (2,2)	2	2	Trivial	4	Low
Third Parties	Hackers/ Hacktivists (4, 4)	4	4	Extreme	4	Extreme
Facilities	Security Guards (1,1) Cleaners (1,1) Building Maintenance Personnel (1,1)	1	1	Trivial	4	Low
Physical Intruders	Burglars (1,1) Foreign Intelligence Services (5,4)	5	4	Extreme	4	Extreme

Intermediaries	Couriers (1,1) IT Maintenance Contractors (3,1)	3	1	Low	4	Moderate
Supply chain Actors	System Integrators (4,2)	4	2	Moderate	4	Extreme
Disasters	Force Majeure (1,0)	1	0	Trivial	0	Trivial

.

C.5 Attack Methods

Table C.5 — Threat Actors and Attack Methods

Threat Actor Type		**Attack Method**	
	Confidentiality	**Integrity**	**Availability**
Normal User	**Accidental Disclosure** User accidentally discloses to users without a valid Need To Know and / or security clearance	**Accidental Corruption** User accidentally reduces the accuracy and completeness of information	**Accidental Disclosure** User actions accidentally stop authorised entities from accessing and using information assets and systems upon demand
	Deliberate Disclosure User deliberately discloses to users without a valid Need-to-Know and / or security clearance	**Deliberate Corruption** User deliberately reduces the accuracy and completeness of information	**Deliberate Disclosure** User actions deliberately stop authorised entities from accessing and using information assets and systems upon demand
Privileged User	**Accidental Disclosure** User accidentally discloses to users without a valid Need To Know and / or security clearance	**Accidental Corruption** User accidentally reduces the accuracy and completeness of information	**Accidental Disclosure** User actions accidentally stop authorised entities from accessing and using information assets and systems upon demand
	Deliberate Disclosure User deliberately discloses to users without a valid Need-to-Know and / or security clearance	**Deliberate Corruption** User deliberately reduces the accuracy and completeness of information	**Deliberate Disclosure** User actions deliberately stop authorised entities from accessing and using information assets and systems upon demand
	Configuration Change User changes configuration leading to the disclosure of information to users without a valid Need-to-Know and / or security clearance	**Configuration Change** User changes configuration leading to the reduction of the accuracy and completeness of information	**Configuration Change** User changes configuration that stops authorised entities from accessing and using information assets and systems upon demand

Table C.6 — Threat Actors and affected Security Domains

Threat Actor Type	Threat Level with Influence	Threat Actors (Values in brackets refer to capability, Motivation)	Affected Security Domain (SD)		
			SD 1	SD2	SD (nth)
Normal Users	Low	Normal Users (2,2)	✓	✓	✓
		Managers (3,2)		✓	
Privileged Users	High	System Administrator (5,2)	✓	✓	✓
		Network Administrator (5,2)	✓	✓	✓
		Firewall Administrator (5,2)	✓	✓	
		Backup Personnel (5,2)		✓	
Partners	High	MDAL staff (5,2)		✓	
Suppliers	Moderate	Supplier System Administrator (4,2)			✓
		Supplier System Administrator (4,2)	✓		
		Supplier Network Administrator (4,2)	✓		
Consumers	Trivial	MDAL staff (2,2)		✓	
Third Parties	Extreme	Hackers/ Hacktivists (4, 4)	✓	✓	✓
Facilities	Trivial	Security Guards (1,1)	✓	✓	✓
		Cleaners (1,1)	✓	✓	
		Building Maintenance Personnel (1,1)		✓	✓
Physical Intruders	Extreme	Burglars (1,1)	✓	✓	✓
		Foreign Intelligence Services (5,4)	✓	✓	✓
Intermediaries	Low	Couriers (1,1)	✓	✓	✓
		IT Maintenance Contractors (3,1)	✓	✓	✓
Supply chain Actors	Moderate	System Integrators (4,2)		✓	
Disasters	Trivial	Force Majeure (1,0)	✓	✓	✓

Annex D
(Normative)

Risk View

D.1 Computing Risk Levels

Table D.1 — Risk Levels

			Likelihood					
			Very Low	**Low**	**Medium**	**Medium-High**	**High**	**Very High**
Impact of Risk Realisation	UNCLASSIFIED	IL0	Very Low	Very Low	Low	Low	Low	Low
	UNCLASSIFIED-PERSONAL	IL1	Very Low	Low	Low	Medium	Medium	Medium
	OFFICIAL	IL2	Low	Low	Medium	Medium	Medium-High	Medium-High
	SECRET	IL3	Low	Medium	Medium	Medium-High	High	High
	TOP SECRET	IL4	Medium	Medium	Medium-High	High	Very-High	Very-High

D.2 Example 1 – Normal Users

The risk assessment table below uses information from table C.2.1, C.3 and C.4

Table D.2 — Normal User Risk Assessment

Threat Actor Type	**Normal User**		**Affected Security Domain**		**SD1**			
Property	**Attack Method**	**Capability**	**Motivation(Influence)**	**Threat Level (Capability + Motivation)**	**Impact Level of Risk Realisation**	**Likelihood**	**Risk Level (Impact + Likelihood)**	**Risk ID**
Confidentiality	Accidental Disclosure	2	4	Low	4	Low	Medium	1
	Deliberate Disclosure	2	4	Low	4	Very Low	Medium	2
Integrity	Accidental Corruption	2	4	Low	4	Medium	Medium-High	3
	Deliberate Corruption	2	4	Low	4	Low	Medium	4
Availability	Accidental Disruption	2	4	Low	3	Medium	Medium	5
	Deliberate Disruption	2	4	Low	3	Very Low	Low	6

D.3 Example 2 – Privileged Users

The risk assessment table below uses information from table C.2.1, C.3 and C.4. The risk assessment chooses different likelihoods to those of normal users.

Table D.3 — Privileged User Risk Assessment

Threat Actor Type	**Privileged User**		**Affected Security Domain**		**SD1**			
Property	**Attack Method**	**Capability**	**Motivation(Influence)**	**Threat Level (Capability + Motivation)**	**Impact Level of Risk Realisation**	**Likelihood**	**Risk Level (Impact + Likelihood)**	**Risk ID**
Confidentiality	Accidental Disclosure	5	4	Extreme	4	Medium	Medium - High	7
	Deliberate Disclosure	5	4	Extreme	4	Medium	Medium - High	8
	Configuration Change	5	4	Extreme	4	Medium - High	High	9
Integrity	Accidental Corruption	5	4	Extreme	4	High	Very -High	10
	Deliberate Corruption	5	4	Extreme	4	Medium	Medium-High	11
	Configuration Change	5	4	Extreme	3	High	High	12
Availability	Accidental Disruption	5	4	Extreme	3	High	High	13
	Deliberate Disruption	5	4	Extreme	3	Medium	Medium	14
	Configuration Change	5	4	Extreme	3	Very -High	High	15

Table D.4 — Prioritised List of Risks

Risk ID	Security Domain (Number)	Threat Actor	Risk Description (Format5)	Risk Level
10	SD[N]	Privileged User	Given that privileged users have powerful privileges [identify the privileges] and that [e.g. it is difficult to monitor their access] there is a risk that their accidental actions [specify actions and/or system] would significantly reduce the accuracy and completeness of information [specify system] leading to [e.g. serious damage the [organisation's] finances and reputation etc]	Very High
9	SD[N]	Privileged User	Confidentiality – Configuration change [use format in Risk ID 10 above to describe risk]	High
12	SD[N]	Privileged User	Integrity - Configuration Change	High
13	SD[N]	Privileged User	Availability – Accidental disruption	High
15	SD[N]	Privileged User	Availability – Configuration Change	High
7	SD[N]	Privileged User	Confidentiality – Accidental Disclosure	Medium High
8	SD[N]	Privileged User	Confidentiality – Deliberate Disclosure	Medium High
11	SD[N]	Privileged User	Integrity – Deliberate Corruption	Medium High
3	SD[N]	Normal User	Integrity – Accidental Corruption	Medium High
14	SD[N]	Privileged User	Availability – Deliberate Disruption	Medium
1	SD[N	Normal User	Confidentiality – Accidental Disclosure	Medium
2	SD[N	Normal User	Confidentiality – Deliberate Disclosure	Medium
4	SD[N	Normal User	Integrity – Deliberate Corruption	Medium
5	SD[N	Normal User	Availability – Accidental Disruption	Medium
6	SD[N	Normal User	Availability – Deliberate Disruption	Low

Bibliography

[1] Uganda (1964), *The Official Secrets Act, The Government of Uganda, Entebbe, Uganda*.

[2] Uganda (1987), *The Security Organisations Act, 2005, The Government of Uganda, Entebbe, Uganda*.

[3] Uganda (2005a), *"The Access to Information Act, 2005", in The Uganda Gazette, The Government of Uganda, Entebbe, Uganda*.

[4] Uganda (2005b), *The Uganda People's Defence Forces Act, 2005, The Government of Uganda, Entebbe, Uganda.*

[5] Uganda (2006), *The Police (Amendment) Act, 2006, The Government of Uganda, Entebbe, Uganda.*

[6] Uganda (2009a), *"The National Information Technology Authority, Uganda Act, 2009", in The Uganda Gazette, The Government of Uganda, Entebbe, Uganda.*

[7] Uganda (2009b), *The National Security Council Act, The Government of Uganda, Entebbe, Uganda.*

[8] Uganda (2010), *"The Regulation of Interception of Communications Act, 2010", in The Uganda Gazette, The Government of Uganda, Entebbe, Uganda.*

[9] Uganda (2011a), *"The Computer Misuse Act, 2011", in The Uganda Gazette, The Government of Uganda, Entebbe, Uganda*.

[10] Uganda (2011b), "*The Electronic Signatures Act, 2011", in The Uganda Gazette, The Government of Uganda, Entebbe, Ugand*a

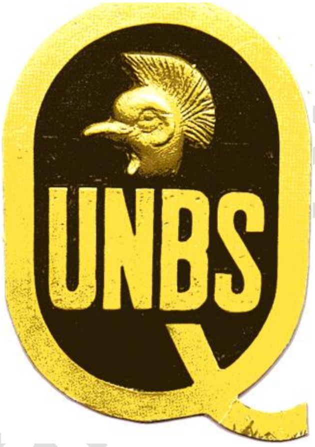
[11] Uganda (2011c), *"The Electronic Transactions Act, 2011", in The Uganda Gazette, The Government of Uganda, Entebbe, Uganda*

Certification marking

Products that conform to Uganda standards may be marked with Uganda National Bureau of Standards (UNBS) Certification Mark shown in the figure below.

The use of the UNBS Certification Mark is governed by the Standards Act, and the Regulations made thereunder. This mark can be used only by those licensed under the certification mark scheme operated by the Uganda National Bureau of Standards and in conjunction with the relevant Uganda Standard. The presence of this mark on a product or in relation to a product is an assurance that the goods comply with the requirements of that standard under a system of supervision, control and testing in accordance with the certification mark scheme of the Uganda National Bureau of Standards. UNBS marked products are continually checked by UNBS for conformity to that standard.

Further particulars of the terms and conditions of licensing may be obtained from the Director, Uganda National Bureau of Standards.



US 2209: 2019

ICS 35.030

Price based on nn pages