Nations Trust Bank

ISRM

Risk Assessment Report for 2022

Group Members

Weerasiri H.A.K.D.	**IT19154640**
Samaraweera S. A. R. P	**IT19177724**
Jayasuriya J.M.A.S.O	**IT19247564**
Kathriarachchi K A P A K P	**IT19990200**

1.0 Executive Summary

This report contains the risk assessment results of **Nation Trust Bank PLC**. Address No. 24, Gothami Road, Rajagiriya. The size is 20,000 square feet (about four times the area of a basketball court). Throughout this assignment, our focus is containing summarize evaluating the company's critical information assets, identify threats to those assets, calculate the effects, and determine mitigation actions.

This risk assessment tends to the three, key principal elements that dictate “information risk” which influence the confidentiality, integrity, and availability of the selected systems and data.

- An assessment of frequent and man-made threats,
- The presence and operational condition of reasonably expected cyber security controls,
- The general development of the IT security program spotlights the present capabilities of personnel, operations, and state-of-the-art technologies which are depended upon by the Nation Trust Bank PLC.

Key Issues and recommendations

The TechCert security audit discovered several critical vulnerabilities by concentrating on the company's classified information assets. These are the assets on which the organization relies to fulfill its objectives. Properties include hardware, software, people, and third-party suppliers. More information on the qualities may be found in Figure 2.0 The OCTAVE's primary concerns and recommendations are stated below.

Firewall Configuration and Client Database

The bank's analysts conduct detailed scans against the primary firewall at the company headquarters. Those assessments uncovered several weaknesses in the setup and security rules that were in existence. The bulk of the risks that the bank confronts may be reduced by changing existing rule sets and/or updating networking equipment.

The database, which contained all of the records and materials underlying the internal and internet banking procedures, was inspected for vulnerabilities. The revelation contains some extremely serious vulnerabilities that represent a significant risk of network compromise. Because the entire database network protection level falls short of the industry set standards by the PCI (Payment Card Industry) and DSS (Data Security Standards), those vulnerabilities must be addressed as soon as feasible. Among the significant results were weak authentications, DDOS assaults, and data leak-related vulnerabilities.

HR and Payroll Management System

When a DOS assault happens, it has an impact on the company's main objectives because this HRPMS is utilized for all of the workers' resource functions. Protocols can lessen the risk by deploying honeypot servers and updating software. When a DOS assault happens, it has an impact on the organization's key objectives because this HRPMS is utilized for all of the workers' resource functions. Protocols can lessen the risk by deploying honeypot servers and updating software.

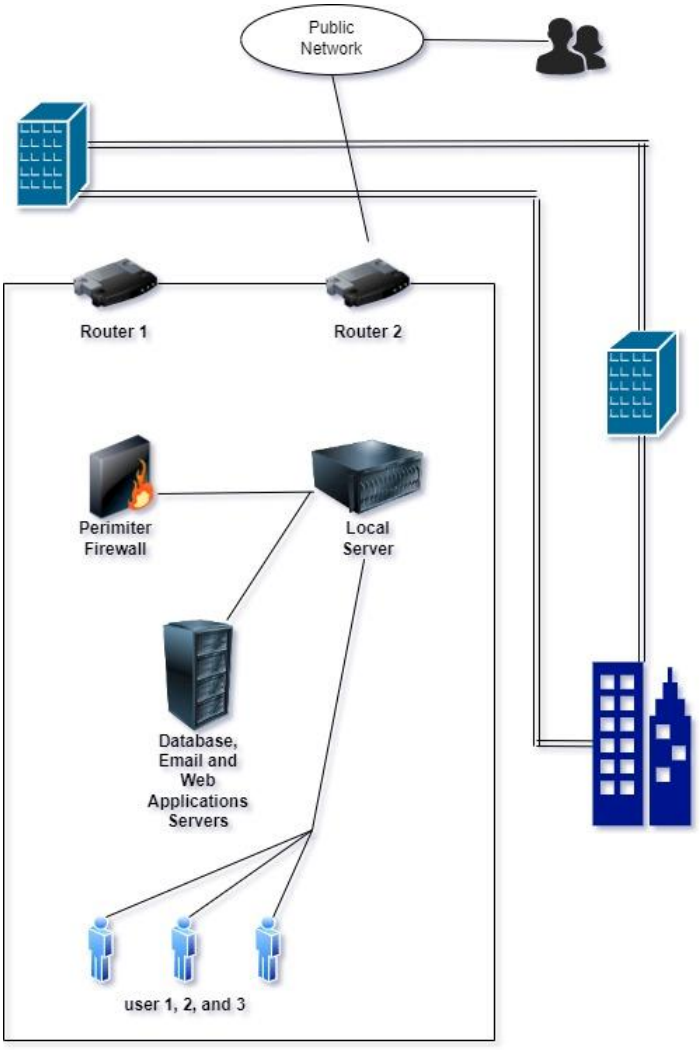
2.0 Technical Report

2.1 Risk evaluation framework and functions.

This Report is built on the Octave Allegro as a primary framework and a few distinct self-created operations for analyzing risk and effect. Finding the essential assertion and then using highest the methodology for implementing the sections to selected individuals with Developing the risk dimension standards that corporate objective is beneficial. The risk analysis for the finding is the qualitative risk analysis given in section 4.0.

2.2 Nations Trust Bank's Organizational Structure

The below figure picture illustrate how the Bank communicates and is interconnected with their others branches and clients. Most online services are connected to the organization's main office. The branches are then linked together utilizing Wide Area Networks. They have a central database storing all of the server's information in the main branch. A high executive official will oversee the auditions for each division. The headquarters constantly supervises the operations of its divisions.

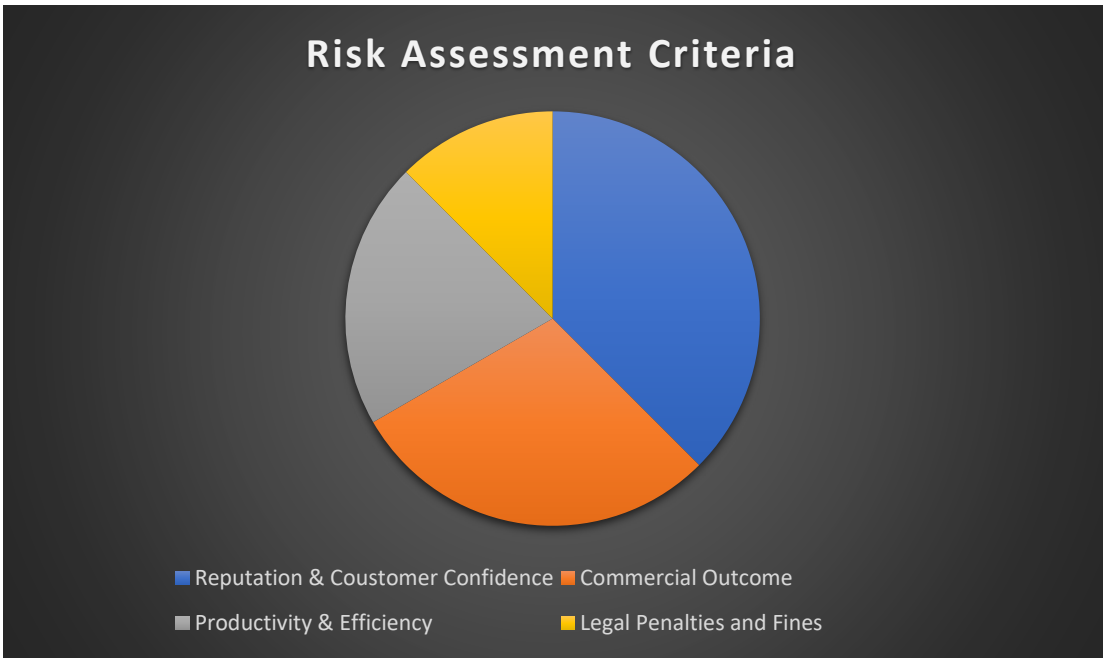


2.3 Members of Risk Management Evaluation

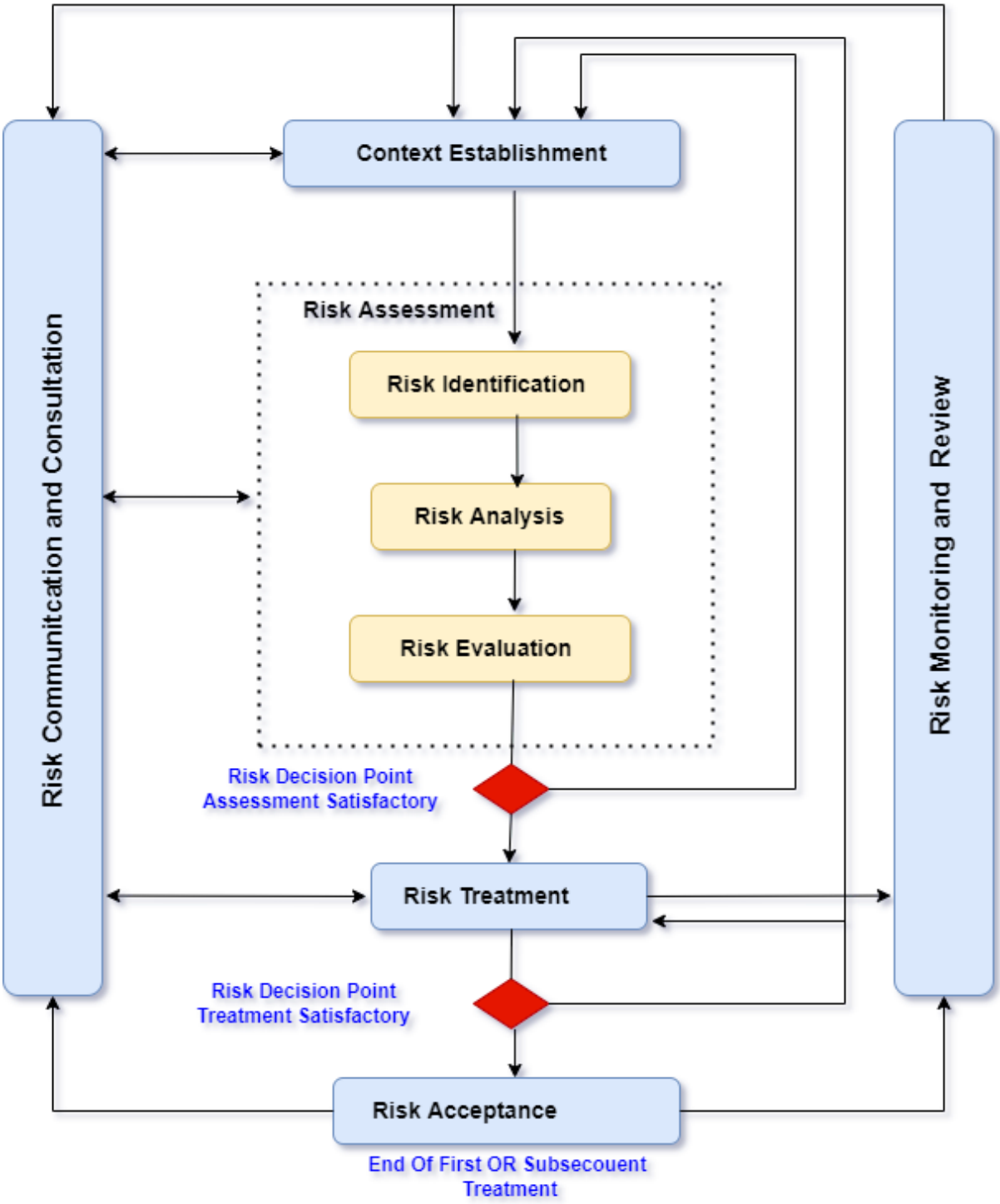
Role	Participant
CEO	**Mr. Prasanna Herath**
Network Manager	**Mr. Subash Gamage**
Financial Planning Team	**Mr. Dakshina Weerasiri, Mr. Kalana Wigesinghe, Mrs. Sayuri Onella**
Security Administrator	**Mr. Raneesha Chiran**
Chief Human Resources Officer	**Mr. Lahiru Prasanga**
System Owner	**Mr. Dayananda Pathirana**

2.4 Risk Assessment Criteria

Finding possible threats and each threat has vital properties. There it must prioritize based on the company's risk tolerance level, financial factors, and containment.



Every IT submission must keep its own ISMS risk assessment conclusion, while risk items must be reported to the information security steering committee (IISSC) and the Board Integrated Risk Management Committee (BIRMC) via the head of information security and CTO.



2.2 Information Asset Identification and Valuation

The primary goal of risk identification is to identify risk sources, regions of influence, incidents and their consequences, and probable repercussions.

Risk identification will take place on a process-by-process basis, with information assets from the Bank Information Technology Division incorporated. As a result, the amount of process risk effect is determined by the value of its information assets.

The Information Technology Division may identify specific assets and categorize them into the asset groups shown in the table below.

The following are the information asset groups: (but not limited to). It is required to keep a record of the individual asset names under the appropriate asset grouping.

2.3 Critical Assets Identification

Critical Assert	Description	Security Requirements for Critical Asserts	Holder/Versions
Web Server	A web server is a computer that keeps bank websites on the Internet and serves web pages to customers as requested. A computer that hosts a website and a program that operates on such a machine. When a consumer wants information, the server is obligated to deliver it.	Least Privilege, SSL/TLS, Confidentiality, Integrity, Availability	1x DELL POWEREDGE R340 SERVER Apache Server
Database Of Client Records	It saves personal information about clients. That database contains very sensitive confidential data including mobile phone numbers, addresses, and client transactions that can be utilized for analysis and lifestyle characterization. Attackers can access or exploit these types of databases.	Confidentiality, Integrity, Availability	Zendesk online application
Perimeter Firewall	Which is a security program that protects the borderline between a bank's private network and public networks just like the internet, and that constant stream contains a wide range of confidential material information from and to clients, business contacts, and many others. This firewall also protects all communications (such as emails), conversations, accessing databases with remote control, cloud solutions, and internet banking.	Confidentiality, Integrity, Availability	Cisco Firepower 4112

HR and Payroll Management System	Payroll and HR Software services suggest a solution that streamlines and manages bank payroll operations and procedures, as well as any other Human Resources-related issues such as talent management and/or benefits. Employees will be able to engage in their tasks and perform their best, saving time and money by not having to worry about HR issues.	Non-Disclosure, Physical Office Security, Access Control and Encryption	FUJITSU Server PRIMERGY RX2520 M5
Card System	This is a centralized payment network that processes payments using credit and debit cards. Its principal function is to manage payment transactions such as processing and clearing. Transactions are processed following a set of protocols, regulations, and arrangements that allow cardholders to use their cards with third parties.	Confidentiality, Integrity, Availability	with the collaboration of third-party developers
Internal Hubs, Switches, and routers	Those routers connect internally and externally networks while also monitoring traffic. Hubs are useful for transferring data from one connection to all other connections in the bank.	Confidentiality, Integrity and Availability	Cisco 1000 and 900 Series Cisco NCS Series
Backup Power	Online mobile payment transfer has only raised the demand for more reliable backup power and 24/7 accessibility. With UPS to smooth over transitions to extended backup power throughout interruptions, and once the power failure happened, Backup powers will quickly startup.	Availability	APC Smart-UPS X 1500VA Rack/Tower LCD 120V

Internet Banking System	Internet Banking, often known as net banking or online banking, is an electronic payment system that allows Nations Trust Bank customers to conduct financial or non-financial transactions online over the internet. This service provides users with an internet portal to practically each bank function that was previously only available through a local branch, such as cash transfers, deposits, and electronic bill payments.	Confidentiality, Integrity, Availability	Top Model, the system used IBM Rational modeling products, Web Application – Java, Perl, PHP, Python Embedded with SQL Database Stored Procedures- C, Java, product-specific language

2.4 Threat Profile

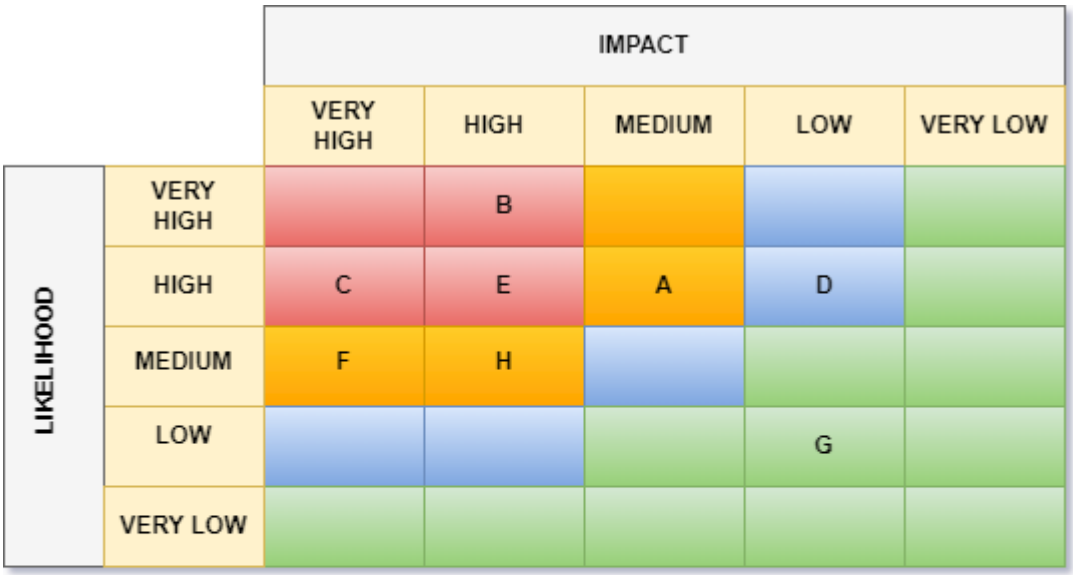
Critical Assert	Threat	Impact	Mitigation
Web Server	The Apache platform is the company's official web server platform. The development team delivered a beta version of their server vulnerability software as part of the security audit. It was effective in detecting a CVE-specified buffer overflow issue that had not been addressed. Following a review of the OCTAVE surveys, it was determined that one of the Apache fixes had been denied due to a hardware issue on the Apache server. This bug "allows remote attackers to cause a denial of service (heap) condition," execute arbitrary code, or even get confidential	There is no need for a Web server in today's world. Day-to-day operations and the organization's operations will continue for several days without the website. Even if the impact factor is set to "low," a susceptible server may open the door to more serious attack vectors.	The major strategy for mitigating vulnerability exploitation is to update the server with the most recent updates. The application of V-protection blocks can further safeguard web servers, and it may be able to apply with broad guidance to the server's whole hardware.

	credential information. And the final probability of an attack exploiting this vulnerability is rated "high."		
Database Of Client Records	Exploiting is conceivable when an intruder has command and control access from the server, however, this is commonly referred to as a "DOS" assault. It is difficult to spot these sorts of attacks without an Intrusion Prevention System.	This HRPMS is utilized by all human resource operations, and a DOS attack has an impact on the organization's (Bank) major goals, reputation, and even an employee's presence. The property will be irreversibly damaged as a result of this catastrophe.	Install the honeypot server to entice prospective intruders and divert their attention away from the production network. Restrict all incoming packets arriving from the service ports to prevent traffic from the reflection servers. Stop any operations that are not anymore in use or that are vulnerable. Check that the programs and protocols used are up to date, and thoroughly inspect the equipment for any unusual behavior.
Perimeter Firewall	An attacker will take advantage of this to obtain plain text SSL VPN credentials, which may subsequently be used to log into the SSL VPN. Credentials obtained from susceptible suppliers have been made available to the public. The list includes local users who were	If the vulnerable devices haven't been patched or have only recently been updated, the SSL VPN credentials might be obtained.	After the patch has been applied, change the passwords of any local SSL VPN users. If the VPN services are configured with multi-factor authentication, it can protect the use of compromised

	linked to the VPN at the recruitment stage.		credentials for the access to the VPN,
HR and Payroll Management System	DOS attacks are very common threats to HRPMS, which occurred due to not establishing the honeypot server.	Whenever a denial-of-service threat happens, it influences the company's main aims, credibility, as well as future of an employee.	Ensure the software and protocols utilized are up-to-date, and order to identify further requirements for the devices for any unusual behavior. Installing a honeypot server to impersonate a genuine server and attract hackers. Make sure to Disable any services that are no longer in use or are unsafe.
Card System	Outdated system software will force every time to vulnerability, which can C2C possibilities when sometimes critically level is more than high. The bulk of data breaches is caused by internal employee mistakes, which is an often-neglected truth.	While the card system interfaces with difficulties caused by vulnerabilities and human mistakes, it can directly infect customers' transactions, lowering the consumers' reputation with the bank.	Monitor and handle compromised accounts to guarantee the bank has one of the best levels of security. Although payment companies design, assess, and implement their PCI DSS compliance and reporting requirements, the PCI Security Standards Council offers a wide range of training, knowledge, and other tools.

Internal Hubs, Switches, and routers	After a connection has been established, an intruder can employ IP spoofing, sequence number prediction, alteration, or other ways to inject bogus IP packets.	Session hijacking, rerouting, and password guessing are all occurring. Unauthorized access is possible.	Update the patches to the software level and upgrade the devices when needed.
Backup Power	The most issue is the heating problem, and it could be able to reduce the power of consumption.	Once the devices are overheating, they also affect bank services to be unavailable at the time.	Use proper Air Condition System for that device. Service at least once a week.

Heat Map for Assessment



A - Web Server
B - Database of Client Record
C - Perimeter Firewall
D - HR and Payroll Management System
E - Card System
F - Internal Hubs, Switches, and routers
G - Backup Power
H - Internet Banking System

3.0 Summary and recommendation

The first step is to make sure that all of the patches listed in the table above are up to date. They should concentrate on the customer record database because it is the company's most valuable asset, and we discovered a few high-impact vulnerabilities such as DDOS attacks, weak authentications, and brute force attacks. As a result, it should be necessary to use mitigations techniques such as Application Delivery Controllers and install database updates from the vendor's website regularly. If they do not implement the above mitigations for the system security of their organization, the bank will face major challenges as a result of unauthorized parties gaining access to clients' credentials. Rather than that They can also change the configuration parameters for all databases.

The above-mentioned recommendations and mitigation solutions must be implemented quickly and effectively. The conversion of the remaining business hardware servers to the V-Block 100, is suggested. They have no data backup in this corporation because their business value will drop if there is a natural disaster in the main core. They can avoid this by maintaining a basic backup plant distance from the main core. As a result, if something goes wrong, employees return to work to maintain the network operational. They'll be able to outsource the maintenance of their backup plant to third-party providers.

We recommend completing a complete assessment of all monitoring system access policies in Nations trust and implementing new security policies to protect mission-critical live systems as the final step in the process. Regularly, these policies will be reviewed and changed.

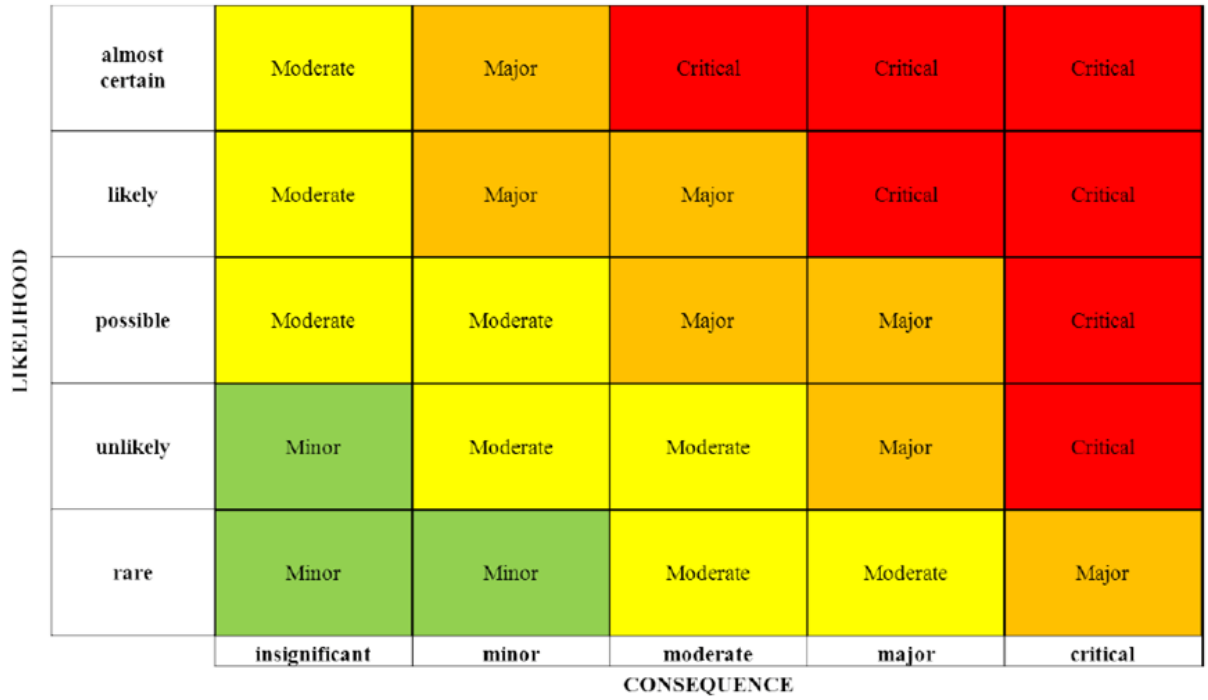
4.0 Qualitative Analysis Parameters

We apply the model presented below to assess the risks associated with the Nations Trust Bank (NTB) system.

Risk = Consequences x Likelihood

Risk = Threat Probability x Impact

4.1 Heat Map



4.2 Threat Probability Scale

- **90% - HIGH :**
  - The threat source has a high risk of defeating the system, and the present defenses are ineffective. Effective countermeasures must be introduced right away.
- **50% - MEDIUM :**
  - The threat source poses a modest threat to the system, and existing safeguards include specific defenses that might greatly reduce the threat.
- **20% - LOW :**
  - There is extremely little chance that the threat source will be able to disable the device, and existing defenses give a reasonable level of security.

4.3.0 The magnitude of Impact (Consequences)

- 1 – LOW :
  - It has only a minimal effect. This will cause minor financial and wealth losses. It may be required, or it may not be necessary, to try to reduce management effort.
- 5 – MEDIUM :
  - It makes a substantial difference. As a result, recoverable assets will be destroyed, as well as financial losses. It's tolerable under normal circumstances.
- 10 – HIGH :
  - It has a massive impact. There will be an irrevocable asset and financial damage as a result of this. Either careful management or modification will be required, or it will be impossible to manage.

4.3.1 Quantitative Risk Analysis Variables

- **Annualized Rate of Occurrences (ARO)**

  The probability of a threat occurring during the year.

- **Single Loss Expectancy (SLE)**

  SLE = Asset Value x EF (Exposure Factor)

- **Annualized Loss Expectancy (ALE)**

  ALE = SLE x ARO

- **Safeguard Cost/Benefit**

  Safeguard cost/benefit =

  ALE before safeguard – ALE after safeguard – Annual cost for safeguard

- **Exposure Factor (EF)**

1. **Are there any, backups, redundancies, or duplicates of the system under attack?**
   Yes – subtract 25%

2. **Is the attacked system protected by a firewall?**
   Yes – subtract 10%

3. Is the attack from outside?
   Yes – subtract 20%

4. **What is the rate of damage caused by the attack?**
   Subtract 8% if rate 25% damage/hour
   Subtract 20% if rate 5% damage/hour

5. **What are the chances that the attack will go unnoticed long enough for a full recovery?**
   Subtract 10% if undetected for less than 20% of recovery time
   Subtract 20% if undetected for less than 10% of recovery time

6. **How long will it take to put countermeasures in place?**
   Subtract 25% implement countermeasures less than ½ hour
   Subtract 20% implement countermeasures less than 1 hour
   Subtract 15% implement countermeasures less than 2 hour

7. **Is the system being attacked vulnerable to SQL injection?**
   No – Subtract 15%

8. **Is the system under assault vulnerable to cross-site scripting (XSS)?**
   No – Subtract 12%