Qualitative Risk Assessment Template

All information in this template are **incomplete examples** only! You will need to add additional information (including but not limited to roles, information asset valuation, information asset prioritisation, descriptions of vulnerabilities and threats) to achieve the highest grade.

## Classification definitions

Subheading

|  |  |
| --- | --- |
| CIA Triad | Requirements |
| Confidentiality | Ensure that assets are viewed only by authorised parties. |
| Integrity |  |
| Availability |  |

|  |  |
| --- | --- |
| Value | Description |
| Confidential | Used for the most sensitive corporate information that must be tightly controlled, even within the organisation. This information must be securely stored and accessed only by authorised personnel.  Highly sensitive data intended for specific use or group of individuals with a legitimate need-to-know. |
| Private/Internal |  |
|  |  |

**Likelihood**

|  |  |
| --- | --- |
| Likelihood | Description |
| Certain |  |
| Highly probable | It is feasible for a threat to exploit the vulnerability. |
| Possible |  |
| Possible but unlikely |  |
| Almost never |  |

**Impact**

|  |  |
| --- | --- |
| Impact | Description |
| Severe | There is economic loss.  There is loss of life.  Legal liabilities and/or breach of SLAs.  There is loss of corporate or public image.  Communications and recovery must be shared with customers. |
| Significant |  |
| Moderate |  |
| Minor |  |
| Minimal |  |

Valuation Criteria

|  |  |
| --- | --- |
| Impact | Description |
| High | It will result in a loss of concern between TrueServer and its customers or result in a large legal action or cause TrueServer significant revenue or earnings. |
| Medium |  |
| Low |  |

# Information assets and classifications



## People Assets

|  |  |  |  |
| --- | --- | --- | --- |
| **Item ID** | **Asset Category** | **Asset Name** | **Asset Description/Attribute** |
| 001 | Employees | CEO | Role: CEO |
|  |  |  |  |

## Hardware Assets

|  |  |  |  |
| --- | --- | --- | --- |
| **Item ID** | **Asset Category** | **Asset Name** | **Asset Description/Attribute** |
| 031 | Network components | Server | Description: High density heat and dedicated servers.  Quantity: X  Category: Systems and peripherals  Location: ….. |
|  |  |  |  |
|  |  |  |  |

## 

# Risk Assessment

The analysis of the system’s vulnerabilities, the threats associated with them, and the probable impact of that vulnerability exploitation results in a risk rating for each missing or partially implemented control. The risk level is determined on the following two factors:

1. Likelihood of Occurrence

It is the probability that a specific vulnerability within TrueServer will occur.

1. Impact

It is the consequence of an event, if it occurs.

The risk rating is the point where the likelihood and impact ratings intersect.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Impact | Severe | 15 | 19 | 22 | 24 | 25 | |
| Significant | 10 | 14 | 18 | 21 | 23 | |
| Moderate | 6 | 9 | 13 | 17 | 20 | |
| Minor | 3 | 5 | 8 | 12 | 16 | |
| Minimal | 1 | 2 | 4 | 7 | 11 | |
|  | | Almost never | Possible but unlikely | Possible | Highly probable | Certain | |
| Likelihood | | | | |



## Security Risks

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk ID** | **Asset ID** | **Threat** | **Vulnerability** | **Risk Description** | **Consequence** | **Gross Risk** | | |
| **Impact** | **Likelihood** | **Risk Rating** |
| R01 | 031 | Theft | * There is no screening, monitoring or logging process for employees entering the company premise. | * This allows a disgruntled employee to steal the asset. | Economic loss  Disruption of business operations  … | Severe | Highly Probable | 24 |
| * This allows an outsider to enter the premise and steal the asset. | Economic loss  Loss of confidentiality  Disruption of business operations  … | Severe | Possible but unlikely | 19 |
| R03 |  | Fire | * Lack of adequate fire detection and suppression system | * A fire could potentially start and reach all sections of the building | Loss of life  Legal liabilities as a result of loss of life  … |  |  |  |

# Risk Controls

Brief description of the control



## Recommended Controls

|  |  |  |
| --- | --- | --- |
| **Risk ID** | **Existing safeguards** | **Recommended Controls** |
|
|  |  |  |
| R03 | * smoke detectors and extinguishers currently installed. * Back-up available. | Business Continuity Plan including a cold site  Additional standard-compliant smoke detectors must be installed  Back up of essential company data must be kept off premise (e.g. on the cloud) |
|  |  |  |

# Reference List

Whitman, M.E., Mattord, H.J. (2014). *Principles of Information Security* (5th ed.). United States of America: Cengage Learning