# Risk Management Methodology
# Basic IT Governance
# Phase I

**DRAFT VER 1.0**

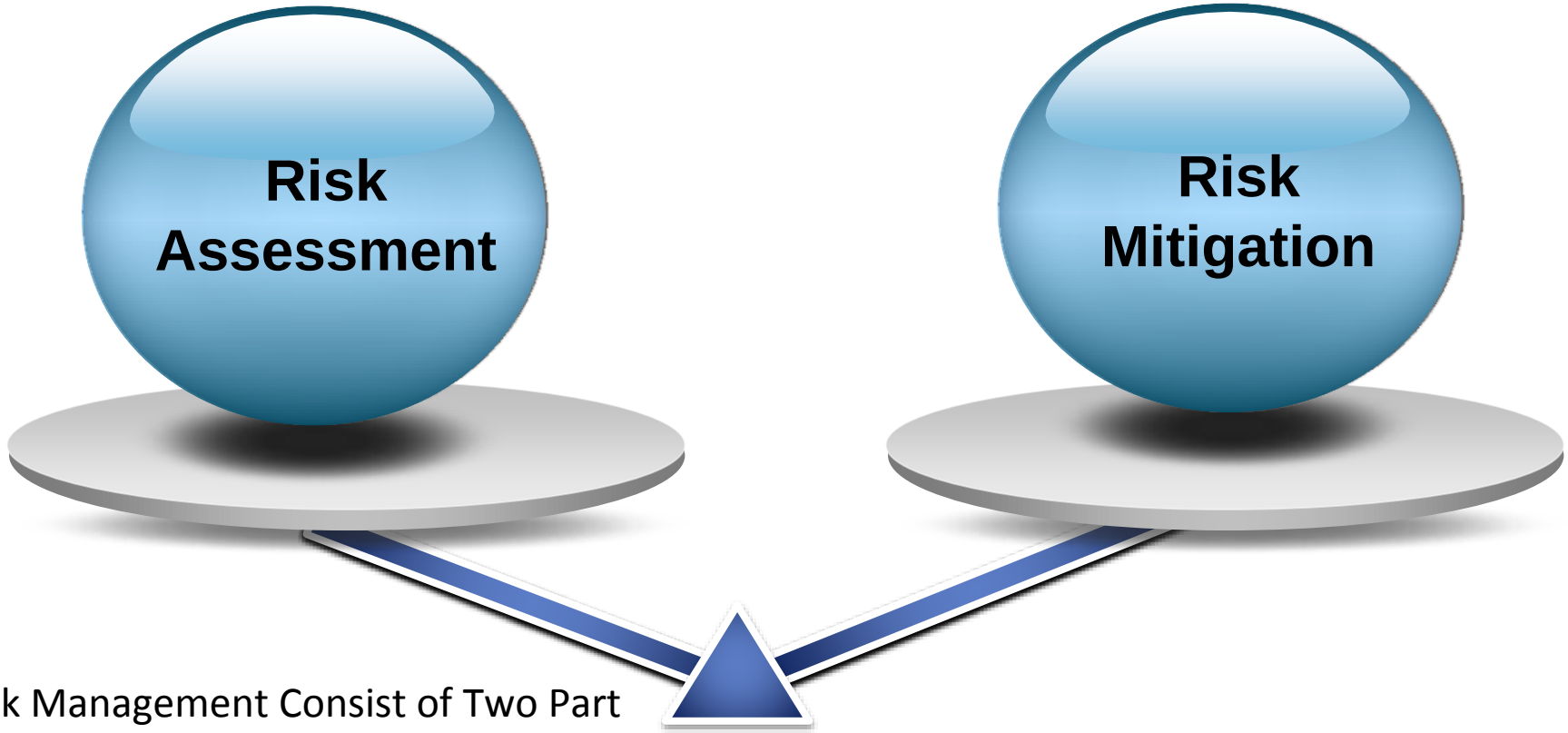
**Octobar 2015**

# Agenda

1. Risk Assessment Methodology

# I(TS)2 Risk Management based on

ISO/IEC 27001:2005 Standard and Guidelines for information security

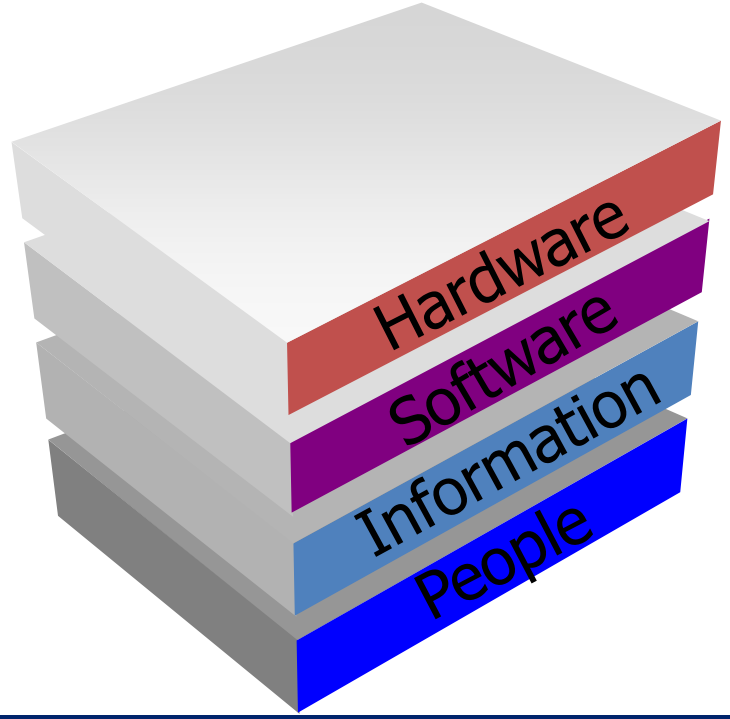



Risk Management Consist of Two Part


Monitor and Review
Monitor and Review
Monitor and Review
Establish Scope
ID Assets
Asset Valuation
ID T/V and Assessment
Calculate Risk
Threat Risk
Define Methodology

# Classification of Assets

Assets will be classified into four main categories




**ASSET**

| Category | Groups | Examples |
|---|---|---|
| **Hardware** | Computer Hardware | Servers, Desktops, Laptops, Storage<br>the end of that period. |
| | Computer Peripheral | Printers, Scanners, Shredders |
| | Electronic Device | Computer protection equipment (theft protection equipment etc. ) |
| | | Electric Device (Shredders, UPS, Power Stabilizer ) |
| | | Telecom Device (Phones, Faxes ,PDA's, Smart Phones |
| | Networking Devices | Routers, Hubs, Switches |
| **Software** | Commercialized Software | Core processing applications, Desktop and workstation office productivity software, Operating system, Network Devices OSI, Back office and environmental software (database engines, back-up and storage management software) |
| | Internally Developed Software | Financial Application, Personnel Application |
| **Information** | Physical Information Asset | Documents Hard Copies (Policies, Procedures), DVDs, CDs, Backup tape |
| | Electronic Information Asset | Documents Soft Copies (Policies, Procedures), Databases, Configuration files, Passwords file, Audit logs |
| **People** | Internal Resources | Security Admin, Network Admin, System Admin, Operator |
| | External Resources | Third Party, Vendors Engineers, Consultants. |

# Assets Valuation


**ASSET**

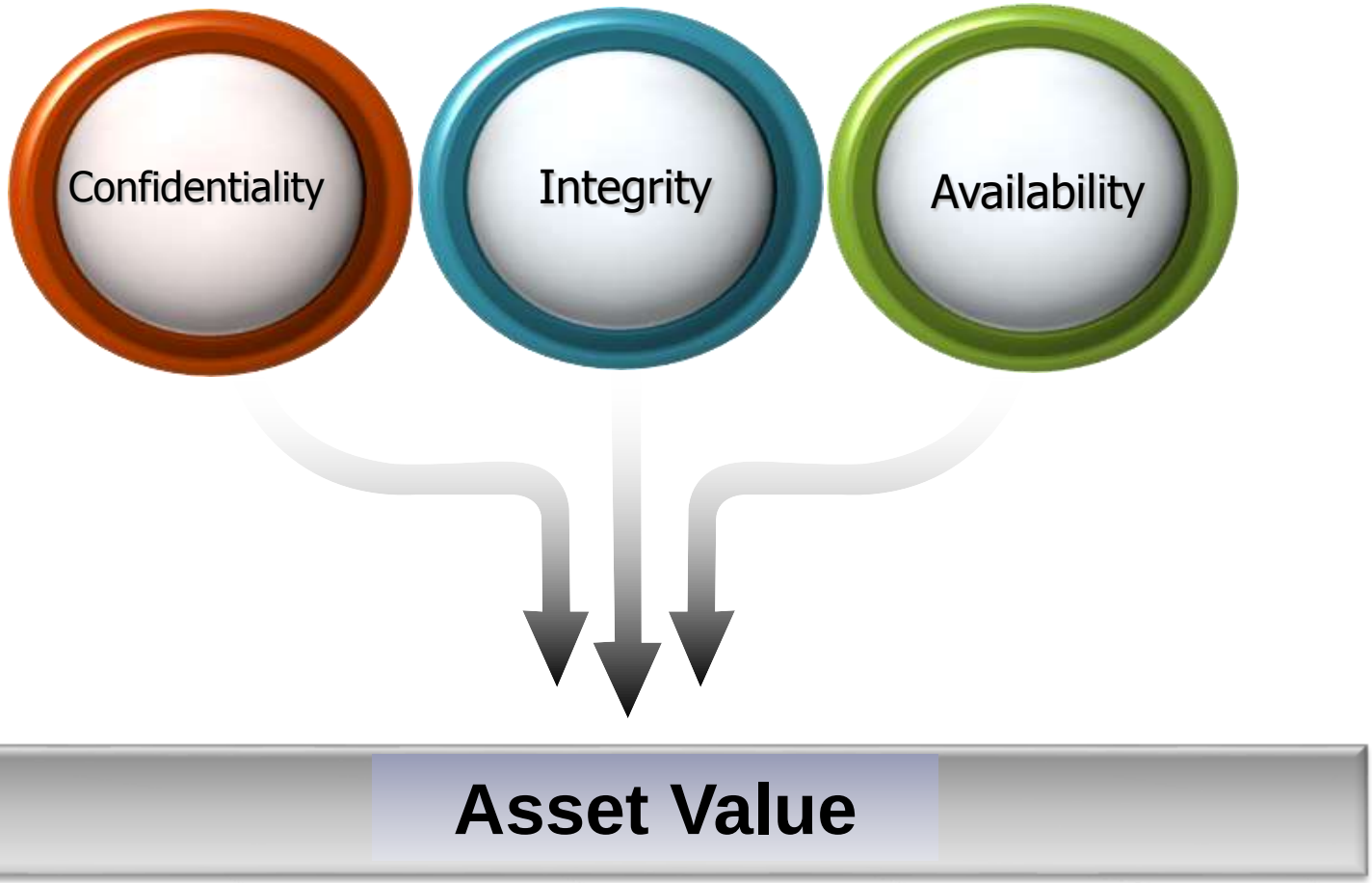
| Confidentiality Scales | | | |
|---|---|---|---|
| **Level** | **Value** | **Criteria** | **Description** |
| **Very High** | 5 | Strictly Confidential | Unauthorized, unanticipated, or unintentional disclosure of confidential information could result in **Extremely High, Serious, Immediate and/or Long** term loss of public confidence, embarrassment, financial or legal action against the organization. |
| **High** | 4 | Confidential | Unauthorized, unanticipated, or unintentional disclosure of confidential information could result in a **High, Serious, Immediate and/or Long** term loss of public confidence, embarrassment, financial or legal action against the organization. |
| **Medium** | 3 | Internal | Unauthorized, unanticipated, or unintentional disclosure of confidential information could result in **Serious, Gradual and/or Long** term loss of public confidence, embarrassment, financial or legal action against the organization. |
| **Low** | 2 | Private | Unauthorized, unanticipated, or unintentional disclosure of confidential information could result in **Serious, Gradual and/or Short** term embarrassment, financial or Non Major legal action against the organization. |
| **Very Low** | 1 | Public | Unauthorized, unanticipated, or unintentional disclosure of confidential information could result in **Non Serious, Gradual and/or Short** term embarrassment, financial or Non Major legal action against the organization. |

| Integrity Scales | | | |
|---|---|---|---|
| **Level** | **Value** | **Criteria** | **Description** |
| **Very High** | 5 | Strictly Confidential | Unauthorized changes to the data or information system by either intentional or accidental acts will result in inaccuracy, fraud, or erroneous decisions. That will **lead to Extremely High, Serious, Immediate and/or Long** term loss of public confidence, embarrassment, financial or legal action against the organization. |
| **High** | 4 | Confidential | Unauthorized changes to the data or information system by either intentional or accidental acts will result in inaccuracy, fraud, or erroneous decisions. That will **leadt to High, Serious, Immediate and/or Long** term loss of public confidence, embarrassment, financial or legal action against the organization. |
| **Medium** | 3 | Internal | Unauthorized changes to the data or information system by either intentional or accidental acts will result in inaccuracy, fraud, or erroneous decisions. That will **lead to Serious, Gradual and/or Long** term loss of public confidence, embarrassment, financial or legal action against the organization. |
| **Low** | 2 | Private | Unauthorized changes to the data or information system by either intentional or accidental acts will result in inaccuracy, fraud, or erroneous decisions. That will **lead to Serious, Gradual and/or Short** term embarrassment, financial or Non Major legal action against the organization. |
| **Very Low** | 1 | Public | Unauthorized changes to the data or information system by either intentional or accidental acts will result in inaccuracy, fraud, or erroneous decisions. That will lead to **Non Serious, Gradual and/or Short** term embarrassment, financial or Non |

| Availability Scales | | |
|---|---|---|
| **Level** | **Value** | **Description** |
| **Very High** | 5 | Loss of data, system functionality and operational effectiveness for **Less than or Equal to 4 hours** will have an **Extremely High, Serious, Immediate and/or Long** term loss of public confidence, embarrassment, financial or legal action against the organization. |
| **High** | 4 | Loss of data, system functionality and operational effectiveness for **Less than or Equal to 10 hours** will have an **High, Serious, Immediate and/or Long** term loss of public confidence, embarrassment, financial or legal action against the organization. |
| **Medium** | 3 | Loss of data, system functionality and operational effectiveness for **Less than or Equal to 48 hours** will have a **Serious, Gradual and/or Long** term loss of public confidence, embarrassment, financial or legal action against the organization. |
| **Low** | 2 | Loss of data, system functionality and operational effectiveness for **Less than or Equal to 5 days** will have an **Serious, Gradual and/or Short** term embarrassment, financial or Non Major legal action against the organization. |
| **Very Low** | 1 | Loss of data, system functionality and operational effectiveness for **Less than or Equal to 7 days** will have an **Non Serious, Gradual and/or Short** term embarrassment, financial or Non Major legal action against the organization. |

| Level | Value | Description |
|---|---|---|
| Very High | 5 | The asset has extremely high financial or technical, or legal value and it's compromise will have very serious and/or long term negative reputation, financial, operational, marketing or legal consequences on the organization with an adverse effect on its critical business processes. |
| High | 4 | The asset has high financial or technical, or legal value and it's compromise will have serious and/or long term negative reputation, financial, operational, marketing or legal consequences on the organization with an adverse effect on its critical business processes. |
| Medium | 3 | The asset has moderate financial, technical, or legal value and its' compromise will have a noticeable negative reputation, financial, operational, marketing or legal consequence on the organization with a low effect on its critical business processes. |
| Low | 2 | The asset has low financial, technical, or legal value and its' compromise will not have a significant negative reputation, financial, operational, marketing or legal consequence on the organization. |
| Very Low | 1 | The asset has a very low financial, technical, or legal value and its' compromise will not have a any negative reputation, financial, operational, marketing or legal consequence on the organization. |

# Assets Valuation



Asset Valuation is based on qualitative approach and the value is described in terms of Very High, High, Medium, Low and Very low impacts.

| C | I | A | Asset Value | Level |
|---|---|---|---|---|
| 1 | 5 | 1 | 5 | Very High |
| 3 | 1 | 4 | 4 | High |
| 3 | 2 | 1 | 3 | Medium |
| 2 | 2 | 1 | 2 | Low |
| 1 | 1 | 1 | 1 | Very Low |

# Threats and Vulnerabilities Identification

Probability

Impact

Threat Level

Vulnerability Level

Zero Controls

ASSET

Vulnerability

| Threats Scales | | |
|---|---|---|
| **Level** | **Value** | **Description** |
| **Very High** | 5 | 1- Threats that affects Company's reputation (Industrial Espionage, Legal Violations, etc)<br>2- Very high likelihood of occurrence |
| **High** | 4 | 1- Deliberate Threats, Any occurrence that has premeditated intent, for example include a malcontent, employee shredding important documents etc. (Unauthorized Access, Social Engineering, etc)<br>2- High likelihood of occurrence |
| **Medium** | 3 | 1- Accidental Threats, Any occurrence that doesn't have premeditated intent, for examples an employee accidentally deleting an important file, failed backup etc. (User Operational Errors)<br>2- Natural Threats and Environmental Threats (Earthquake, lightening, High temperature, etc)<br>3- Medium likelihood of occurrence |
| **Low** | 2 | 1- Natural Threats and Environmental Threats (Earthquake, lightening, High temperature, etc)<br>2- Low likelihood of occurrence |
| **Very Low** | 1 | 1- Threat source is neither motivated nor capable<br>2- Very low likelihood of occurrence |

| Vulnerabilities Scales | | |
|---|---|---|
| **Level** | **Value** | **Description** |
| **Very High** | 5 | The vulnerability can be exploited by an unskilled attacker (e.g. script-kiddie), by using ready-made exploits. (For example: Lack of perimeter security control IDS, IPS, Firewall etc). |
| **High** | 4 | The vulnerability can be exploited by an advanced attacker via a sophisticated attack with custom-built tools/methods. Furthermore, the attacker must be considerably determined. (For example: Uncontrolled access to system utilities (Administrative privilege). |
| **Medium** | 3 | The vulnerability is considered to be exploitable by an advanced attacker, but only under certain conditions:<br>• Very determined attacker<br>• Substantial knowledge of the internal network (For example: Inadequate logical access controls) |
| **Low** | 2 | The vulnerability cannot be directly exploited, but there is a possibility to be exploited in the future (For example: Lack of physical controls.) |
| **Very Low** | 1 | The vulnerability is not considered exploitable at present.<br>(For example: Obsolete/age of the hardware) |

# Calculation of Risk

| Asset Value | Threat Value | Vulnerability |
|---|---|---|
| High | Medium | Low |
| 4 | 3 | 2 |

| MoR =Asset Value x Threat Value x Vulnerability Value |
|---|
| MoR= 4x 3x 2 = 24 |

Asset, Threat and Vulnerability Scale is set from

**1 to 5**

The Risk Level Scale will be from

**1 to 125**
*(5x5x5=125)*

| MOR Mapping to Risk Level | |
|---|---|
| **MoR** | **Risk Level** |
| 1 - 20 | Very Low |
| 21 - 32 | Low |
| 33 - 50 | Medium |
| 51 - 75 | High |
| 76 - 125 | Very High |

The Acceptable Level of Risk will be

**All the Risks with Value below 32**

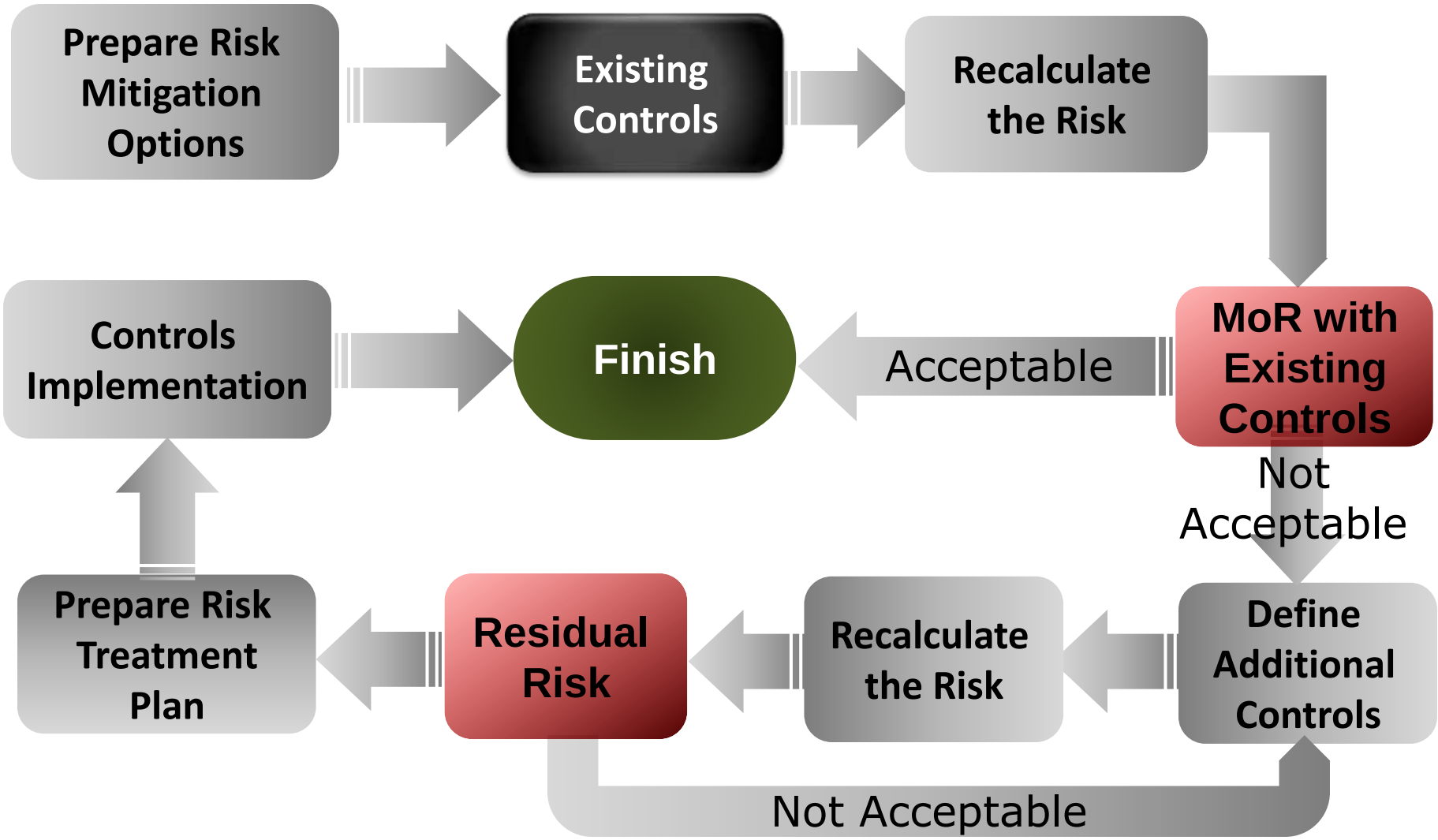
**All The Risks With The Risk Level of *Low and Very Low* will be Acceptable and The Risks With Values *Medium, High and Very High* Need to be Treated.**


Prepare Risk Mitigation Options
Existing Controls
Not Acceptable
Risk Level
Acceptable
Finish

Controls identified and selected in the risk mitigation options phase need to be:

- **Controls are Documented (Policies and Procedures)**
  - ✓ Policies and Procedures (Management Security Controls), are implemented to manage and reduce the risk of loss and to protect an organization's assets and mission.
  - ✓ Management controls focus on the requirement of information protection policy, , which are carried out through operational procedures to fulfill the organization's goals and missions.
- **Controls are Implemented**
  - ✓ Controls identified and selected in the risk mitigation options phase need to be implemented and evidences of the implementation must be available.
- **Implemented Controls are Effective**
  - ✓ Based on the assurance level the existing control or suggested control can provide to reduce or eliminate the vulnerability

*Note:* The effectiveness of the implemented controls will be based on Experience and/or Judgment and will be evaluated, checked and verified continually throughout ISMS Audits


Prepare Risk Mitigation Options
Existing Controls
Recalculate the Risk
MoR with Existing Controls
Acceptable
Finish
Controls Implementation
Not Acceptable
Define Additional Controls
Recalculate the Risk
Residual Risk
Prepare Risk Treatment Plan
Not Acceptable