# Information Security Risk Management (ISRM)

NAVEEN GUPTA (SR. CONSULTANT AND GOVERNANCE, INFORMATION SECURITY,27 YEARS EXP. GLOBAL MNC)

# Information security

Different people, different  ways to interpret

| | |
|---|---|
| Vendors: | Limited to their products |
| For Aware Leaders and professionals: | Essential and core requirement of their business |
| For some business leaders: | It is job of IT/ Security manager |
| For some users of technology: | It is disruption to their liberty |

# What compels us to adapt information security?

## Internet usage

User can reach anywhere in the world and so as the person with criminal mindset.

It has become world wide web for criminals to interact with reach other, share ideas and work on some common goals.

## Usage of cloud computing

Risks related to public network usage

At the end of the day, your data is handled by someone else

## Mobile Devices and embedded devices (IoT) usage

Small screen prone to more human errors and difficult to decide upon the security of app or website being used.

One never knows, if a spy is sitting besides you in the form of IoT device. Sometimes they may listen even when for your they are in switched off mode.

# What compels us to adapt information security?

Automation and usage of Artificial Intelligence (AI)

More machine dependence, more chances of error and surprises.

- Information Leakage

  AI learns from loads of data and sources and can be a medium of information from different sources which otherwise would be unknown.

- Introduction of new vulnerabilities

  Learning can happen from incorrect data, codes, models etc., which may result in outcomes with previously unknown vulnerabilities

- Incorrect decisions sometimes can be potentially dangerous to our systems or even humans

Increase of computer literacy and easy connectivity using BT, NFC, Wifi etc

It is a convenience which resulted in easy access and loss of information which otherwise was difficult.

# Information Security Risk Management (ISRM)

Why is it important?

In order to reduce the likelihood of risks that may jeopardize the confidentiality, integrity or the availability of information system/ asset, thus impacting the overall business objective.

To make a business case for getting the information security budget approved from CFO.

Impact of IS risk can have implications: Operational, Legal, Financial and Reputational.

Reality check:

This exercise mostly ends up in creating just a paper/ electronic record for compliance purposes

# Important aspects of ISRM strategy

Alignment to business objectives

Factor- in both insider and outsider threats

Accidental and deliberate threats

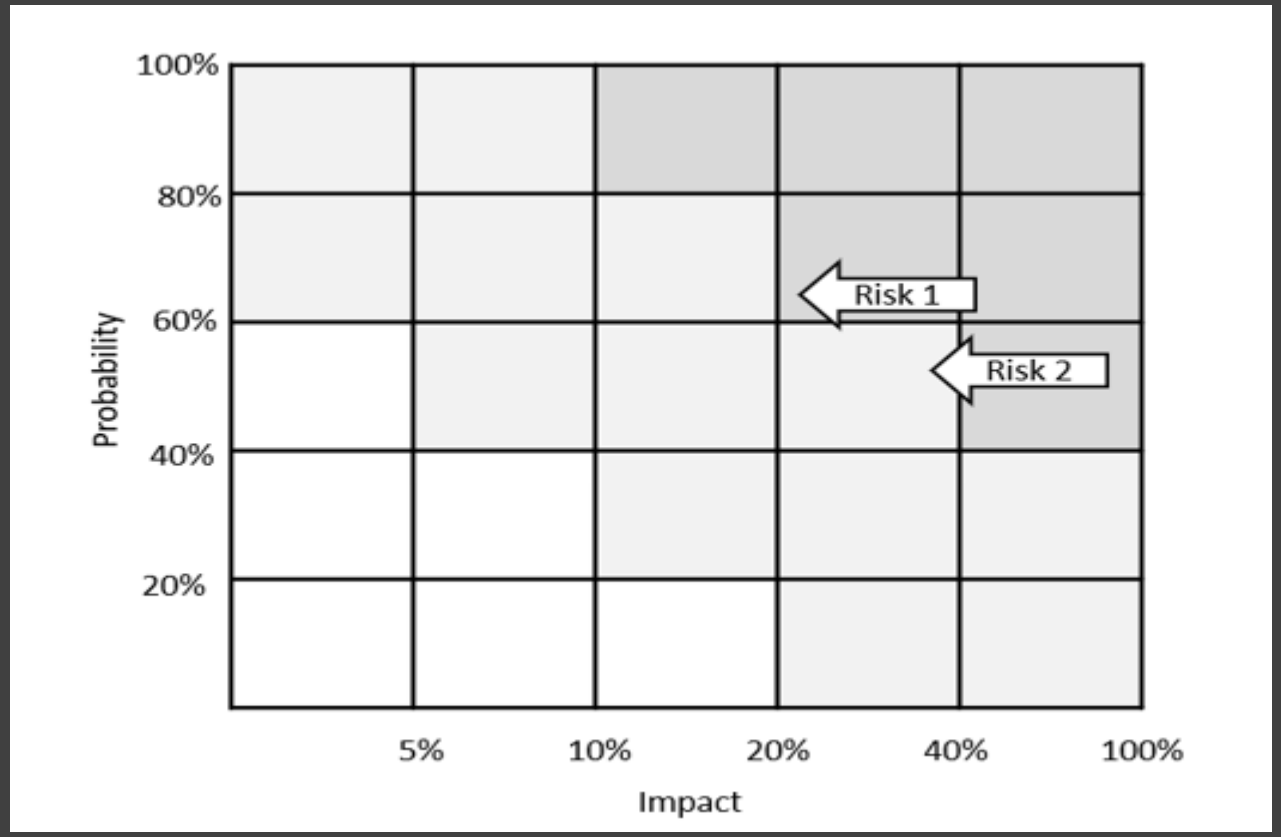
Human, technical, environmental and support system related threats

Threats arising out of implementation of controls

Define your risk appetite

Define Risk Owners

# Prioritization and Mitigation of Risks

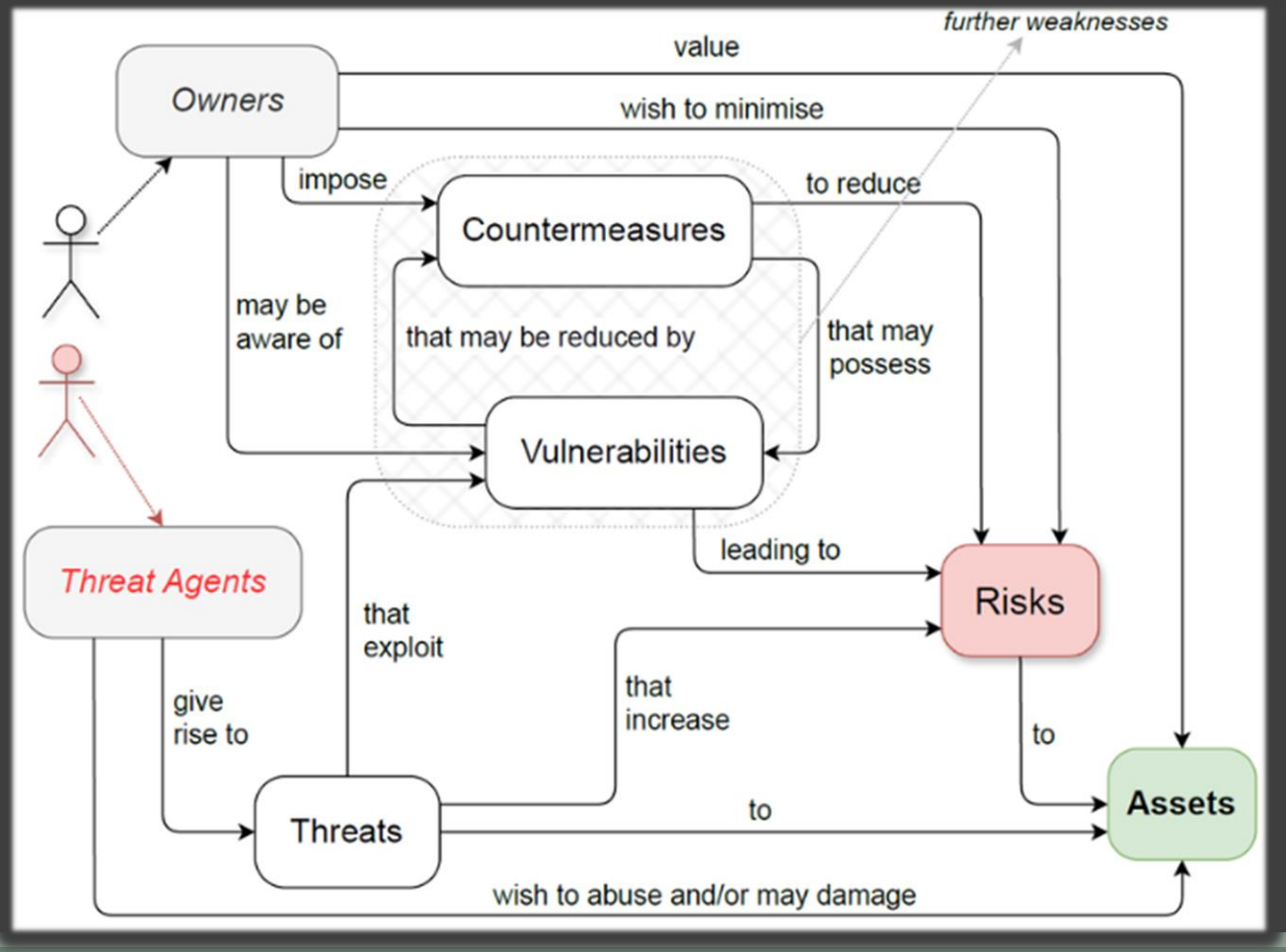



Picture Courtesy: Intaver .com

4 Ts in Risk Management

- Treat
- Tolerate
- Transfer
- Terminate

# Information security maze




Credits: Researchgate.net

# Expiration of IS Risks and outcome of ISRM

Do they really expire?

The answer is NO

Outcome: Set of security controls which may reduce them to the acceptable level

Keep them recorded in Risk Register

Re assess them at periodic interval in light of the environment applicable at time of assessment

Residual Risk
That remains after risk mitigation efforts are in place.
This may increase or decrease over a period of time.

Thus, ISRM is a continuous exercise during life cycle of an asset in an organization or a project.

# Choosing Risk Assessment (RA) Methodology (Objective or Subjective)

## Objective

- Attributes used are discrete. E.g. are Asset/ function type, its value, vulnerability, existing control threat, probability etc.
- Allows one to choose from a list of values for each attribute used in RA.
- Attributes which not straightforward e.g. motivation of threat actor, or surface area of attack etc. We can introduce objectivity by adding more sub- parameters to these attributes.
- E.g. ISO27005 methodology published by NIST

## Subjective

- E.g. Octave
- This helps in scrutinizing every single details about asset.
- Eg. What is asset, why it is used, for what it is used, criticality, its user, its location, its copies, who all access it, from where, its container and so on.
- This doesn't bank on keywords and use actual threat scenarios to assess risks.
- One ends up filling pages and RA for even a single asset.

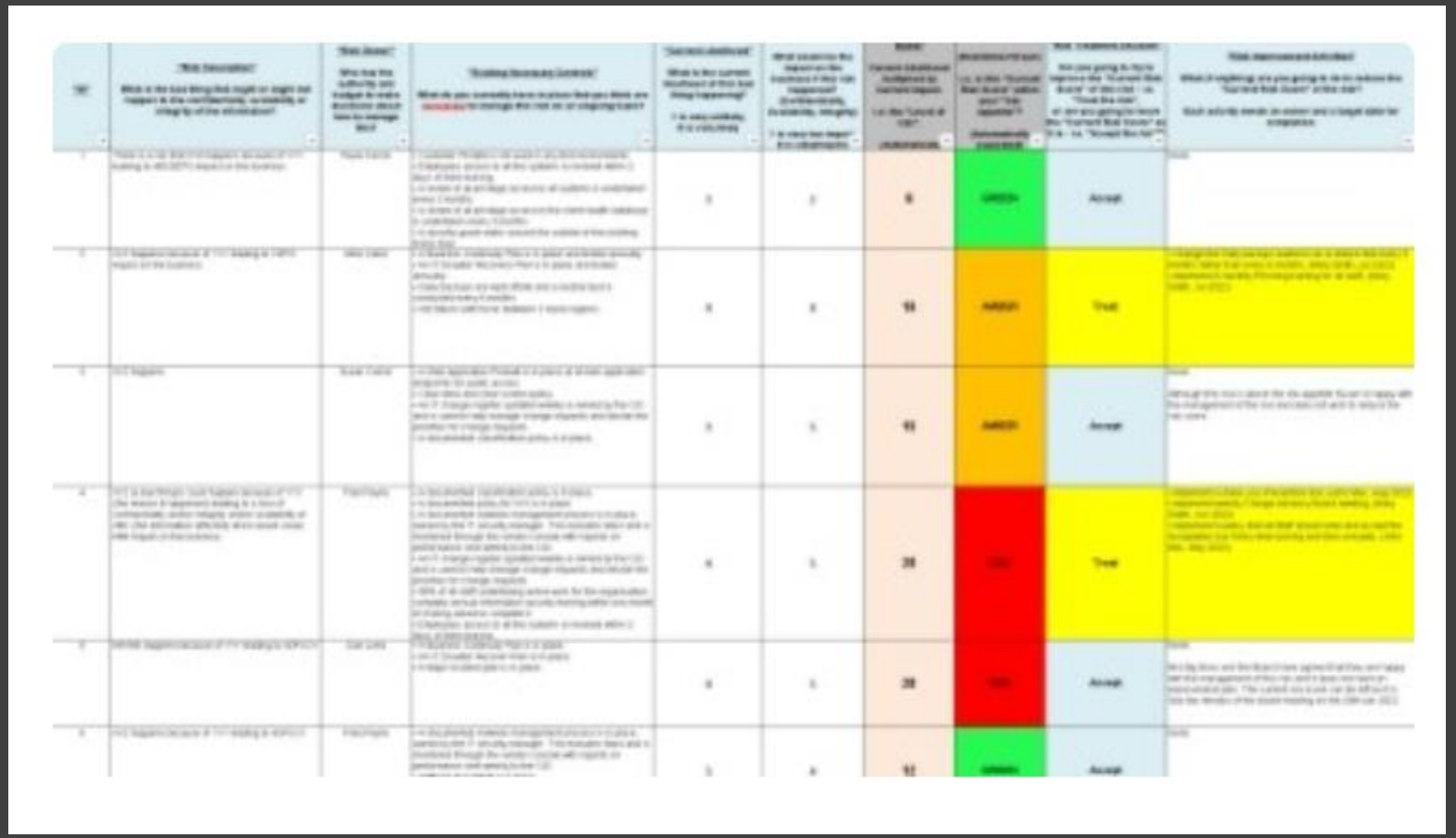
## Recommendation: A blend of both

# Thank you.

NAVEEN GUPTA (SR. CONSULTANT AND GOVERNANCE, INFORMATION SECURITY,27 YEARS EXP. GLOBAL MNC)

Naveen.gupta1977@yahoo.com

91- 9811811016



| Allegro - Worksheet 10 | | Information Asset Risk Worksheet | | | |
|---|---|---|---|---|---|
| Information Asset Risk | Information Asset | Configuration of the MDM system | | | |
| | Area of Concern | Proper access gives access to resource assets to inappropriate users | | | |
| | Threat | (1) Actor<br>*Who would exploit the area of concern or threat?* | Internal attacker | | |
| | | (2) Means<br>*How would the actor do it? What would they do?* | By using the administrator rights to give access to inappropriate user | | |
| | | (3) Motive<br>*What is the actor's reason for doing it?* | MDM configuration leakage | | |
| | | (4) Outcome<br>*What would be the resulting effect on the information asset?* | ✓ **Disclosure** ✓ **Destruction**<br>✓ **Modification** **Interruption** | | |
| | | (5) Security Requirements<br>*How would the information asset's security requirements be breached?* | Only the administrators of the MDM system can access and modify these data. | | |
| | | (6) Probability<br>*What is the likelihood that this threat scenario could occur?* | ✓ **High** | **Medium** | **Low** |
| | (7) Consequences<br>*What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* | | (8) Severity<br>*How severe are these consequences to the organization or asset owner by impact area?* | | |
| | | | **Impact Area** | **Value** | **Score** |
| | The user may steal the configuration of the MDM system | | Productivity | 3 | 6 |
| | Run a malicious code on the MDM servers | | Financial | 3 | 9 |
| | | | Productivity | 3 | 6 |
| | | | | **Relative Risk Score** | **21** |