RISK: basic concepts and objectives

RISK: basic concepts and objectives

Threats, knowing and identifying them

In today's world all business entities are encountered with challenges of various shapes, sizes and intensities Such challenges may impair the ability of the business entity either significantly or otherwise. These challenges could either be tangible or intangible in characteristic.

In the context of security, ***threat*** is such entity that has the ability to cause any harm to any or a specific **Information Asset**.

The *threat* arises out of any *threat source* or an **actor.** The actor has some agenda or intent to fulfill in disguise of the *threat*.

The *threat* to a specific Asset is said to be *focused* on that Asset. Also a threat gives rise to **risk**.

In summary:

- Threat is *able to cause some harm* to an Information Asset(s).
- Threat *Actor* is the entity or subject that drives the threat towards the Information Asset(s) with some selfish intention or mal-intention.
- Threat, only if *focused* on any Information Asset, will likely be effective against that prospective victim.
- Threats are source of *Risks*, as they may or may not occur and is able to impact the Asset mostly either negatively or at times positively.

Hence it is of utmost importance to identify the *threats* as soon as possible or at the source to devoid them of their potential impact causing ability.

RISK: basic concepts and objectives

Threats, knowing and identifying them

Identifying Threats

- Focused on assets
- Focused on attackers
- Focused on software
- STRIDE –
  - Spoofing,
  - tampering,
  - repudiation,
  - information disclosure,
  - denial of service,
  - elevation of privilege

Determining and Diagramming Potential Attacks

- Diagram the infrastructure
- Identify data flow
- Identify privilege boundaries
- Identify attacks for each diagrammed element

Preforming Reduction Analysis

- Trust boundaries
- Data flow paths
- Input points
- Privileged operations
- Details about security stance and approach

Prioritization and Response

- Probability × damage potential ranking
- Qualitative rating: High/medium/low
- DREAD –
  - Damage potential,
  - Reproducibility,
  - Exploitability,
  - Affected users,
  - Discoverability

RISK: basic concepts and objectives

Risks, what may go wrong

Enterprises today encounter not only threats but also are consistently under the apprehension that some threat actor may launched a focused attack on them that would result into a loss or an negative impact. This dread of some thing in the future may or may not go as per their plan, causing a loss is a risk to the organization.

In the context of security, an expected or unexpected event that may or may not occur that may cause either a negative or a positive impact, is a *risk* to any or a specific **Information Asset**. Risk has a chance factor that surprises many if not alert. Risk causes either a negative or a positive impact to any Asset. The negative impact events are risks. The positive outcome events are termed as opportunities. Risks are born of threats.

In summary:

- Risks are events in the future that caused by a/any threat
- Risks have uncertainty of occurrence – may or may not. It’s also called the probability or chance factor
- Risks have an impact or an effect on any Asset. That can be measured in terms of any commensurable unit
- Risks need to be managed – identified, measured, analysed, priorised and reduced before they can be further processed
- Risks need to be treated – from a choice of actions like, avoided, transfer, accept, reduced, such that the impact is minimised

RISK: basic concepts and objectives

Exploits, Vulnerabilities and Exposure

Today's organisation encounter roadblocks or obstacles of various forms from multiple directions. To stay safe in order to carry out business as usual they not only need to control the threats and minimize the risks but also deal with more aspects. They are faced with objects, common or exceptional, that can be used to cause harm to them. It is a fact that all organisation possesses some weakness of that can be used as a disadvantage point against them. All organisation take some countermeasure to protect it self from the perils of the threats and risks that haunt them. They are either not effective or not efficient in the protection effort.

In security context the objects of causing harm, the inherent weaknesses and the ineffective countermeasures are called, exploits, vulnerabilities and exposure. The definitions are as under.

Exploits – All objects or subjects that a threat actor may use to enhance the threat's effectiveness against a prospective victim.

Vulnerabilities – An inherent weakness or a default that an entity will likely possess. Those weaknesses will cause harm itself, if taken advantage of by a threat actor or a threat.

Exposure – The deficiencies in the existing or absence of any countermeasures that may be used by any perpetrator to attack.

The *exploits, vulnerabilities and exposures* enables a *threat agent* with a *threat vector,* of a particular *threat* or a *risk*, on a specific prospect or *victim* to launch a successful *attack*. This is then a *Cyber-attack* and an event of **Cybersecurity**.

RISK: basic concepts and objectives

The roles and responsibility and RACI matrix

Any Enterprise or an organisation or a Business entity that has an internal Information Technology Business Unit (IT BU) or an Information Systems (IS) Security Function, ensures that the BU or the function comprises of professionally and academically educated and competent people or employees to deliver the right value to the business functions or to the Senior Management (SM) or the 'top brass'.
In order to do so the IT BU must firstly, be aligned to the Business Objective (BO) and the Strategy of the Organisation as set by the SM. Then it prepare its own BO and Strategy such that the BU is able discharge the duties of Management and Governance of IS. Only then the IS BU will be able to deliver 'value' to the Business.
Key primary roles of IS Professionals may include as under, but not limited to:

Application / Business / Compliance / Crypto / Computer or Desktop Support / Data / Enterprise / Forensic investigation / Governance / Incident or Problem / Information Assurance / IS Security / Malware / Network / Process improvement or control / Personal Data / Quality or QA or QC / Risk / Regulatory / Systems / Senior / Technical – (Associate or Senior) Analyst , Architect, Administrator, Auditor, Consultant, Controller, Engineer, Manager, Operator, Officer, Responder, Writers or Chief Data Officer (CDO), Chief Information Officer (CIO), Chief Technology Officer (CTO), Chief Security Officer (CSO), Chief Information Security Officer (CISO), Associated Vice / Vice / Senior President or Director.

RISK: basic concepts and objectives

The roles and responsibility and RACI matrix

The IT BU to function or operate properly requires to assign clear and concise responsibilities to each of the roles. It assists in the proper track, measure, review & operate the daily operations or project works or Programme initiatives or Portfolio management and the governance tasks be done without any hitch or conflict or issue. An undisputed line of reporting and communication and collaboration are also achieved. The tools that assists here is called, RACI Matrix.
It is a tabular mapping of the roles against the specific tasks with each corresponding association attributes of **Responsibility** (one who does a job), **Accountability** (one who is *answerable* for a job), **Consulted** (an exchange of ideas or views between peers) and **Informed** (a one-way reporting, mostly to the top).

The Rules of the RACI Chart, for each task assignment, must have

1) Accountable: Maximum (at most) ONE role (can not be none)
2) Responsible: Minimum (at least) ONE role. (can be more)
3) Consulted: No limits apply. Its about peer-to-peer sharing
4) Informed: No limits apply. Its about bottom-up or top-down

Note: The first two rules are about count of head.
The last two are about communication direction.

Role Task	Role 1	Role 2	Role 3	Role 4
Task 1	R	A	C	I
Task 2	RA	R	C	--
Task 3	R	R	A	--
Task 4	R	A	I	R

RISK: basic concepts and objectives

The roles and responsibility and RACI matrix

Role Task	Role 1	Role 2	Role 3	Role 4
Task 1	R	A	C	I
Task 2	RA	R	C	--
Task 3	R	R	A	--
Task 4	R	A	I	R

Risk management

What are risks?

Any Enterprise or an organisation or a Business entity operating in any economic, geo-political technological and social environment has this fear of loss or incurring damage of income or reputation or both on any asset-physical or logical, from some unforeseen event or a known incident that may or may not happen in the future. Information Systems (IS) or IT records such loss or damage as Risk to Information Asset (IA), data or information and the containers in that the IAs exists when wither at the state of rest or in motion or when being processed. The IA can be either in physical or logical form.

In case of security, the only thing that changes is the context of the data or information. Here the IAs are only in digital form or state. So any data in hardcopy state are not included. All data or information residing in the Internet or Intranet or extranet domains, that is known as the Cyber World are in scope.

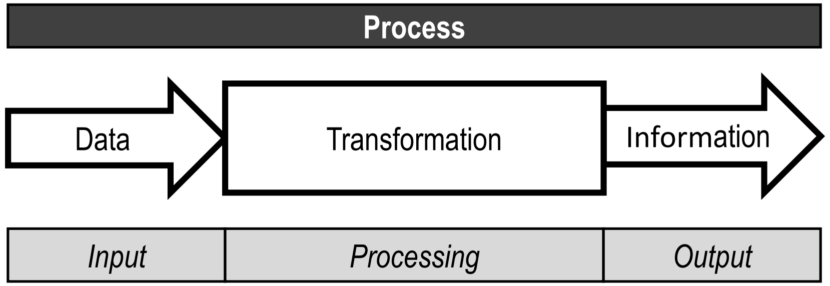
A **Risk** is any form of *risk* on any Asset (IA in digitized state) with an uncertainty of occurrence in future, arising of a threat with a focus on a target, executed by an agent, with the ability to cause negative impact, using any existing and fitting exploit aligned to the vulnerability and exposure of a prospective victim.

Risk management

The information assets at risk

Data = the facts and figures in their inherent raw and base state, that can be processed in various ways to arrive at decision points.

Information = the specific outputs produced from the transformation of data that was collected from a source.



Asset = Any item or an object of worth that may be tangible / physical or intangible / logical nature that a subject like an Organisation possesses or own by virtue of acquiring or building or inheritance at an instance or over time by itself or with the help of others or from other.

Physical asset = an asset that has attributes of physical or tangible nature. Can be seen, touched, experienced and possesses a specific monetary value.

Logical asset = an asset that has attributes of logical or intangible nature. Can not be seen, touched but can be experienced in an indirect means and possesses an specific value.

Risk management

The information assets at risk

Physical asset exists on their own as they are manifested by their physical attributes.

Logical asset in general are unable to exist just based on their intangible attributes. They need to reside in a **container** or a physical asset. Through this secondary asset the existence of the primary logical asset is realised.

All such **logical assets** that are generated from a gathering of raw data from any source and then transforming it to a meaningful and usable piece of assets that enables some one to arrive at a specific decision, that could add value.

In information systems context, we address such assets as information assets (IA). An organisation owns may such IA's along with many physical assets some of which are the container of IAs.

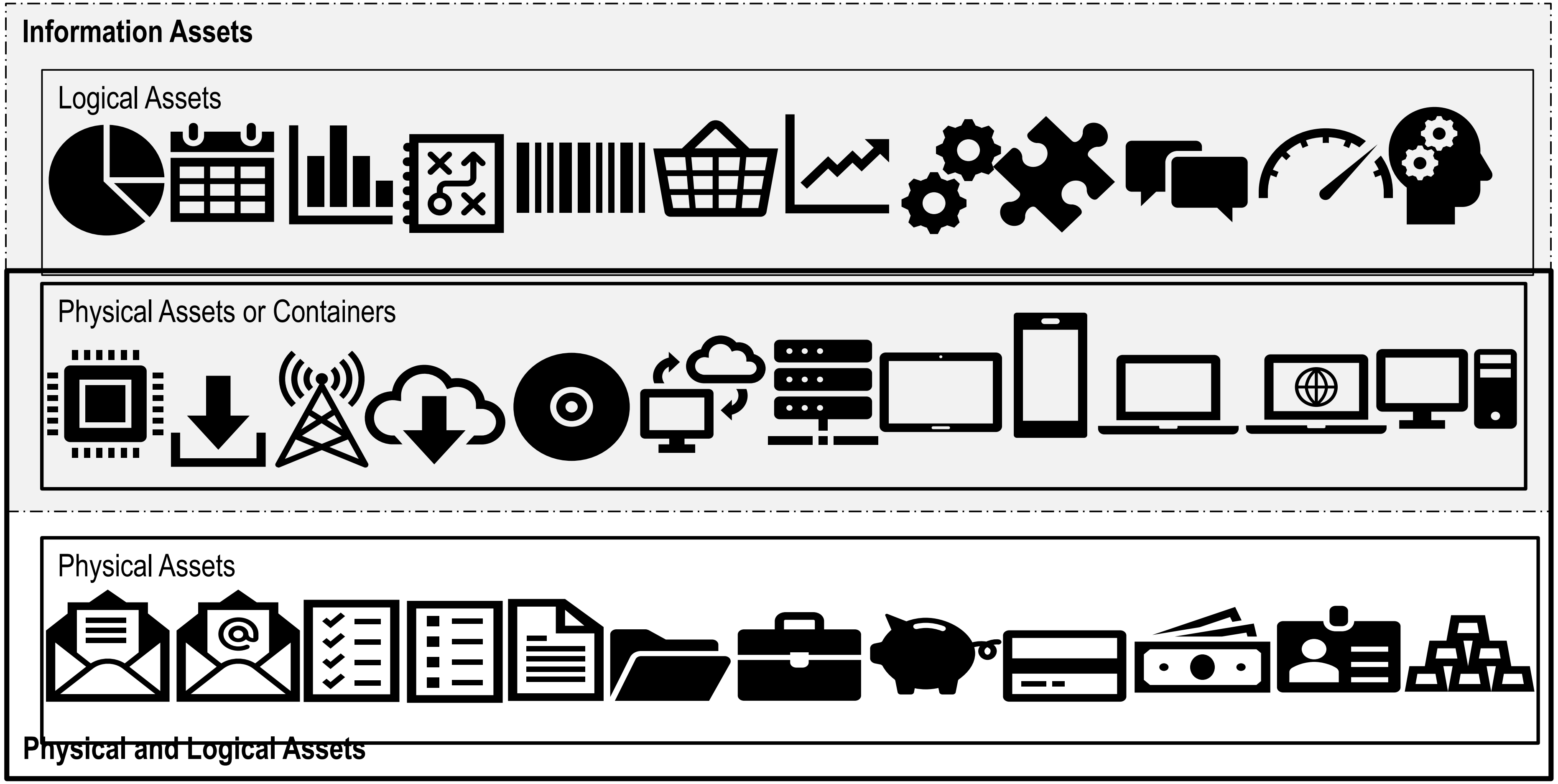
The ***Information Assets*** are impacted by the same threats and exposed to the same risks as any common asset.

States of Data Any type of Data has 3 typical states of being or existence.

- □ **Data at Rest,** when data is stored in any conventional or unconventional media, temporarily or as archived.
- □ **Data in Motion**, when data is being transmitted between two points i.e., from a source and to a destination.
- □ **Data in Process**, when data is being processed or transformed in the Processer or CPU of any device.

Risk management

The information assets at risk



Risk management

How to minimize the risks

Risk is a common factor for all Enterprises, Organisations, Corporates and Businesses across all industry and sector for any size, capacity and maturity from any economy, nation, region or any commercial environment. A popular saying, “No Risk No Gain.” Risk may cause harm but not always.

We learnt that risk is the apprehension of something may cause harm in the future. Now if, the result is positive it is called not risk but opportunity. If risk is managed properly Businesses will be able to yield value. Otherwise, I may cease to exist.

The next consideration is to measure the value of risk. The two-prime component of risk are the chance factor or probability and the effect or the impact from the risk. The value of risk is a product of the probability and impact. While probability is always a number between 0 & 1, both inclusive, the impact is represented by an universally understood value, money or Dollar ($). In case of a loss -$ value or Risk and for a gain +$ value or Opportunity.

Risk = Probability x Impact or R = P x I.

Probability P can have a values range between 0 and 1. 1 for an assured event of happening, like it rains. 0 for an assured event of the complement of the first or not happening, like it does not rain. Any other value in between 1 & 0, like 0.5 indicates that there is a 50-50 chance of rain. The value of risk in this example are,

A. Opportunity situation: Here the impact is +$. Under this we can have two situations.
   a. For something that will surely happen in the future, P=1 and assume, I=$10. The Risk is - *R=P x I or 1 x $10 = $10*;
   b. For something that may or may not happen with equal chance in the future, P=0.5 and assume, I=$10. The Risk is *- R=P x I or 0.5 x $10 = $5;* and
   c. For something that will surely NOT happen in the future, P=0 and assume I=$10. The Risk is - R=P x I or 0 x $10 = $0; while
B. Risk situations: Here the impact is -$. Under this we can have two situations.
   a. For something that will surely happen in the future, P=1 and assume, I=$-10. The Risk is - *R=P x I or 1 x $10 = $-10;*
   b. For something that may or may not happen with equal chance in the future, P=0.5 and assume, I=$-10. The Risk is - *R=P x I or 0.5 x $-10 = $-5*; and
   c. For something that will surely NOT happen in the future, P=0 and assume I=$-10. *The Risk is - R=P x I or 0 x $-10 = $-0 .*

Risk management

How to minimize the risks

In this example,

1. A.a is a positive or an opportunity situation. The maximum value of opportunity.
2. B.a is a negative or a risk situation. The maximum value of risk.
3. A.b is a positive or an opportunity situation. The opportunity value is medium.
4. B.b is a negative or a risk situation. The minimum value of opportunity.
5. A.c is a positive or an opportunity situation. The risk value is medium.
6. B.c is a negative or a risk situation. The minimum value of risk.

Here we observe that an unit-based measurable value of opportunity and risk are stated under options and sub options in A & B respectively. This is known as the quantitative valuation.

We also observe that an attribute-based non-measurable value of opportunity and risk are stated under options between 1 till 6. This is known as the qualitative valuation.

The assessing and listing the risks on the basis of a measurable values is called quantitative analysis and that of non-measurable values (High, Medium, Low, etc.) is called a quantitative analysis.

Risk management

How to minimize the risks

Before embarking into Risk Management let us watch how people deal with risk and how is it measured.

Case: One afternoon at work Mr Jit was fearing that if that day it rains at 5:30pm, when he would be returning home, then he will get wet and may fall sick. In such case next morning he will not be able to report to work but will have to visit the doctor and spend $25 on drugs to get well. What can Mr Jit now do to ensure that if it rains, he will still be able to stay fit the next morning?

Mr Jit has identified that if it rains in the evening and he gets wet as a result, he will fall sick. That will cost him $25.

Mr Jit does some quick calculations during the afternoon itself to prepare for the evening. He needs to ensure that he must do some thing to keep himself fit and not get drenched while returning home.

He will have to assess either the quantitative or qualitative values of the risk before listing them. He will also have to choose some options to reduce impact by applying some effective and appropriate countermeasure. This reduces the exposure and not the vulnerability. This is risk treatment.

Risk management

How to minimize the risks

Mr Jit now must plan some actions so that he is prepared to counter the rain and avoid getting wet or Risk Treatment. The options before Mr Jit are:

1. Not go home that evening to avoid getting wet from rain. **Risk Avoidance**. But he can not avoid all risk. To stay back at office (assuming it rains the whole night) he will have to order dinner to avoid staying hunger. He orders dinner from an online delivery service for $15.
2. To call a cab service to get a dry ride back home as a cost. **Risk Transfer**. The cab driver accepts the risk from Mr Jit by providing a service against a cost of $20.
3. He may choose to go home as usual, get wet, fall sick and visit a GP. **Risk Acceptance**. By doing so he accepts the full blow of the risk and has to incur $25.
4. He could also buy an umbrella and a rain coat/jacket that afternoon to prepare for returning home as dry as possible. He will then be able to stay fit and return to work the next day. The countermeasures, of an umbrella and a rain coat cost him $10.

Risk management

How to minimize the risks

Mr Jit would need to conduct a **Risk Mitigation or reduction** exercise. He is preparing to accept the risk after reducing it to an acceptable amount. This limit he must set in advance based on his ability to accept or **Risk Appetite** level or **Risk Acceptance Level.** Assuming that this limit is $12.

Mr Jit now lists the risks based on the quantitative and qualitative assessment, like as under,

1. Risk Acceptance cost = $25. This is > $12.
2. Risk Transfer cost = $20. This is > $12.
3. Risk Avoidance cost = $15. This is > $12.
4. Risk Mitigation cost = $10. This is < $12.

So, Mr. Jit will buy an umbrella and a rain coat as a countermeasure against the event it rains, to reduce the Risk value below the Risk Appetite level. This how Mr Jit managed his one-off risk.

Risk management

Managing the risks

Any Enterprise or an organisation or a Business entity operating in any economic, geo-political technological and social environment has this fear of loss or incurring damage of income or reputation or both on any asset- physical or logical, from some unforeseen event or a known incident that may or may not happen in the future.

Information Systems (IS) or IT records such loss or damage as Risk to Information Asset (IA), data or information and the containers in that the IAs exists when wither at the state of rest or in motion or when being processed. The IA can be either in physical or logical form.

In case of security, the only thing that changes is the context of the data or information. Here the IAs are only in digital form or state. So any data in hardcopy state are not included. All data or information residing in the Internet or Intranet or extranet domains, that is known as the Cyber World are in scope.

A **Risk** is any form of *risk* on any Asset (IA in digitized state) with an uncertainty of occurrence in future, arising of a threat with a focus on a target, executed by an agent, with the ability to cause negative impact, using any existing and fitting exploit aligned to the vulnerability and exposure of a prospective victim.

Risk management

Identifying, assess and mitigate

In the Corporate world Risk Mitigation is dome almost similarly. The steps of risk management are:

1. **Identify** the risks and threats from various sources. Industry best practices, Special research institutions, survey, interviews, Knowledge Bases, Lesson learned, regulations, compliance, etc. are some means to achieve the identification and relevance of risk events.
2. **Analyse** the risks in terms of **Qualitative and Qualitative** basis before listing or ordering them.
3. **Priorities** the risks on the basis on the analysis of the are the impact measures and the probability of occurrence. The higher the probability and impact more critical are such risks and their need of control by mitigation actions. The lesser are probability and impact less critical are such risks and their need of control by mitigation actions.
4. **Treatment,** here countermeasures or controls are applied to reduce the impact till the value of the risk is lesser than the Acceptable Level or Appetite.

Measuring risk for business accounting and asserting the value of the Controls that need to be implemented to achieve the desired objective of the control.

.

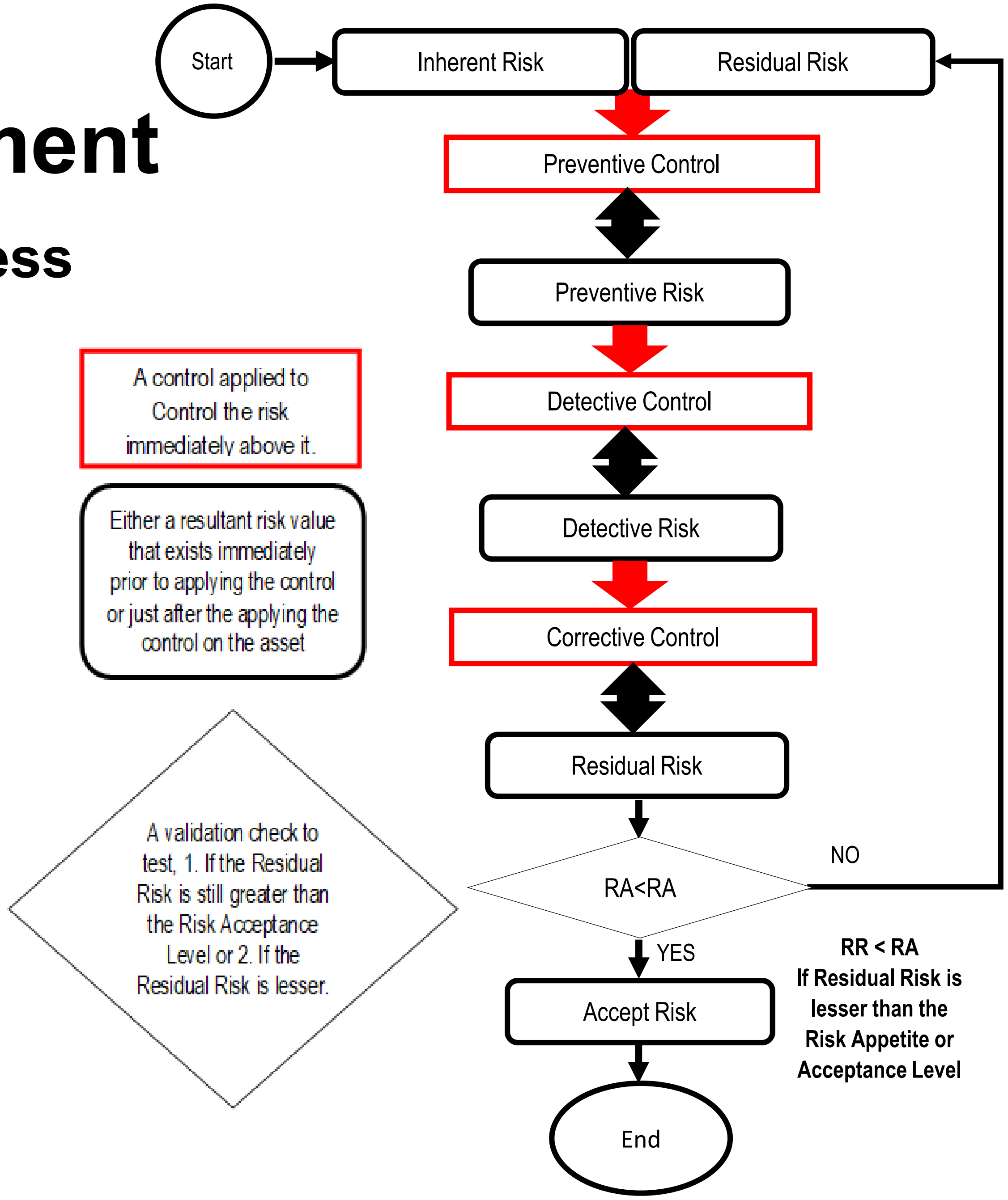
Risk management

Risk Treatment Process

The risk treatment process flow.

An identified risk with an about certain probability and the highest impact needs to be reduced below the acceptance level by applying the relevant and enough control measures.

At the beginning there is an **Inherent Risk** associated with any Asset. It is the default risk associated with the asset. At this point in time no Control measure is deployed on the Asset. This type of risk is also at a raw state.



Start

Inherent Risk

Residual Risk

Preventive Control

Preventive Risk

Detective Control

Detective Risk

Corrective Control

Residual Risk

RA<RA

NO

YES

Accept Risk

End

A control applied to Control the risk immediately above it.

Either a resultant risk value that exists immediately prior to applying the control or just after the applying the control on the asset

A validation check to test, 1. If the Residual Risk is still greater than the Risk Acceptance Level or 2. If the Residual Risk is lesser.

RR < RA
If Residual Risk is lesser than the Risk Appetite or Acceptance Level

Risk management

Risk measurement:

Companies do not do accounting of any event one time as they exists for a short duration by they operate for years. So they apportion their risk values over time. They are also required to do yearly record and review their financial performance.

Hence they need to do evaluation of the risks on a yearly basis. There is the need of annualization the expected loss amount.

Annualised Loss Expectancy (ALE) = **Single Loss Expectancy** (SLE) X **Annualised Rate of Occurrence**, some threat that happens once in so many years, (ARO)

ALE = SLE X ARO, where SLE = *Single Loss Expectancy* value. It is derived as - **Asset value**, the cost to buy the asset from the market on that day. (AV) X **Exposure Factor**, the percentage of the concerned asset that is exposed to the threat or risk. (EF).

Then **ALE = AV X EF X ARO**, assume, *AV* = *$100,000.00, EF* = *25% and ARO* = a threat occurring in once in 25 years, or *1/25.* ALE = $100,000.00 X 25/100 X 1/25 = <u>*$1000.00*</u>.

Next, assume that some Controls are applied on the Asset so *the EF = 10%.* The reduced value due to the application of the Controls. The new ALE = *$100,000.00 X 10/100 X 1/25 =* <u>*$400.00*</u>*.*

So, we can assert that benefit gained by applying control is the different between pre-control risk value or ALE = $1000.00, the post-control risk value is *$400.00, ($1000.00-$400.00) =* <u>*$600.00.*</u>

Risk management

Risk measurement:

How much control is enough control?

What could be the investment on implementing a control or countermeasure can be best evaluated by a cost benefit analysis.

In the above example, the benefit gained by implementing a control is $600.00. The Maximum spent on the control should not exceed the benefit gained or the value of $600.00. In fact, the cost of control should be at least possible then $600.00

Risk management

Risk measurement:

How much control is enough control?

What could be the investment on implementing a control or countermeasure can be best evaluated by a cost benefit analysis.

In the above example, the benefit gained by implementing a control is $600.00. The Maximum spent on the control should not exceed the benefit gained or the value of $600.00. In fact, the cost of control should be at least possible then $600.00