ISMS EXCERPTS – RISK MANAGEMENT PROCEDURE

aspire SYSTEMS

attention.
always.

RISK MANAGEMENT

RISK

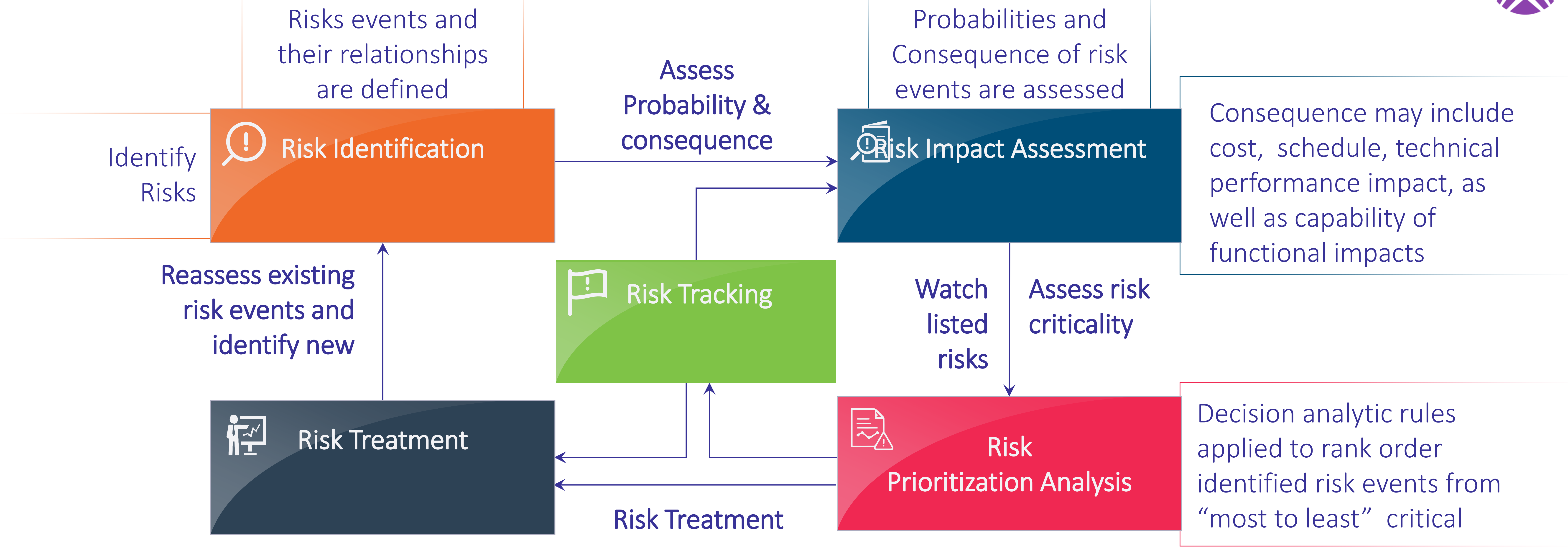
Risk is the possibility that a threat exploits a vulnerability in an information asset, leading to an adverse impact on the organization

- ✓ Threat: Something that might cause harm
- ✓ Vulnerability: A weakness that might be exploited
- ✓ Impact: Financial damage etc

Risk Management

- ✓ The process of understanding and responding to factors that may lead to a failure in the confidentiality, integrity or availability of an information or information system.

RISK MANAGEMENT @ ASPIRE



Risks events and their relationships are defined

Identify Risks

Risk Identification

Assess Probability & consequence

Probabilities and Consequence of risk events are assessed

Risk Impact Assessment

Consequence may include cost, schedule, technical performance impact, as well as capability of functional impacts

Reassess existing risk events and identify new

Risk Tracking

Watch listed risks

Assess risk criticality

Risk Treatment

Risk Prioritization Analysis

Decision analytic rules applied to rank order identified risk events from "most to least" critical

Risk Treatment

Risk events assessed as medium or high criticality might go in risk mitigation planning and implementation; low critical risks might be tracked/monitored on a watch list.

Tool Used :
PRISM – Risk Portal

THREAT & VULNERABILITY EXAMPLES

Threat	Vulnerability
Fire	Absence of Emergency Evacuation Plan
Earthquakes	No preparation against environmental Threats
Failure of a/c or water supply, telecom services, transport services	Absence of recording & monitoring of Temperature & RH in DC, Hub/UPS rooms
Breach of confidentiality, Theft of media or documents or information, Tampering with S/W and H/W	Weak controls on using IM systems
Equipment failure/malfunctioning	Inefficiency in operation and maintenance of supporting utilities
Unauthorized use/Misuse use of equipment's and facilities, Use of counterfeit or copied software, Illegal processing of data	Lack of adequate process for handling project movements
Error in use, Misuse of rights	Absence of regular review of User's access rights and privileges

RISK MANAGEMENT PROCEDURE

Risk Identification

- ✓ The needs and expectations of Interested Parties shall be identified. Issues in meeting these needs and expectation shall be identified as internal or external issues to Aspire by Business / Department Heads and QA Head / ISMS Officer.

- ✓ At the time of project initiation, when the planning is done, Project Managers complete the project risk assessment sheet and identify risks in achieving the planned objectives of the project.

- ✓ All Information Assets are identified and recorded in every department. Any event that can impact the confidentiality, integrity and availability of these information assets is identified as a risk.

- ✓ An access risk assessment should be done to identify risks related to any physical and logical access required to be provided to third parties including service providers and customers.

- ✓ When a decision regarding any process relating to quality management or information assets is to be taken by the organization, a risk based approach will be adopted. The Process Risk Assessment Form must be filled, detailing the current scenario, the risks and the recommendations.

RISK ANALYSIS

Risk owners along with the relevant department head analyse the risk and provide the probability and impact rating for each identified risk.

Rating	Probability criteria	Impact Criteria
5	Almost certain to happen several times in a year	Significant disruptions to organization strategy/human life/business operations with customer/regulatory/reputation impact
4	May occur under certain circumstances in a year, but not frequently	Significant disruptions to business operations but no customer/regulatory impact
3	Chances of occurrence in a year are not common, but does occur very rarely	No customer/regulatory impact but requires extensive effort to manage
2	Could occur a couple of times over a 3-5 year period	No customer/regulator impact and can be contained easily
1	Rarely occurs, maybe once in 5 years	No customer/regulatory impact and can be tolerated.

RISK ANALYSIS

Data Protection Impact Assessment (DPIA)

Aspire has defined the DPIA processes relating to processing of personal information, which

- ✓ Establishes and maintain privacy risk criteria.
- ✓ Ensures that repeated privacy risk assessment processes are consistent, valid and comparable.
- ✓ Identifies the data protection risk associated with privacy risk assessment process.
- ✓ Identify the high personal information and related process that are high risk.

When the risk type for a risk is “Privacy” and the sub-type is “Processing”, risk analysis takes the form of DPIA.

The DPIA is conducted to analyse the type of personal data processing involved based on the following criteria:

i. Evaluation of scoring including profiling and predicting

ii. Automated decision making with legal or similar significant effect

iii. Systematic monitoring

iv. Sensitive data

v. Large-scale data processing

vi. Data concerning vulnerable data subjects (Example: Child, mentally affected person)

vii. Innovative use of applying new technologies

RISK RATING

The risk rating for risks can be one of the following:

- ✓ High
- ✓ Medium
- ✓ Low

This rating is calculated as a factor of the probability and impact rating of a given risk with the exception for a risk for which DPIA is conducted.

When DPIA is conducted for a risk, the risk rating is obtained based on the number of criteria of personal data processing is involved as following:

- ✓ High – When any three of the processing criteria are involved (There is a higher probability of occurrence of the risk when such processing criteria are associated)
- ✓ Medium – When one or two of the processing criteria is involved
- ✓ Low – When none of the processing criteria is involved

RISK TREATMENT

Risks that are rated as “High” and “Medium” must be treated mandatorily. Risk treatment options shall include the following:

- ✓ Accept
- ✓ Mitigate
- ✓ Avoid

Mitigating Risk

- ✓ Reducing the likelihood an adverse event will occur
- ✓ Reducing impact of adverse event
- ✓ Risk Treatment Plan has to be created for risk mitigation

Avoiding Risk

- ✓ Changing the project plan to eliminate the risk or condition

Accept Risk

- ✓ Making a conscious decision to accept the risk
- ✓ Risk Assessment has to be created for Risk Acceptance

RISK STATUS

- ✓ When a risk is newly created, it will be in the “Open” status.
- ✓ When the mitigation plans and new controls are approved and are getting implemented, the status is updated to “WIP”.
- ✓ When a risk occurs, the risk status is updated to “Occurred” and the counter “Risk Occurrence Count” will be incremented and an associated issue will be created and tracked to closure.
- ✓ When the occurred risk is addressed and the corresponding issue status is marked as “Closed”, the risk status is again updated to “WIP”.
- ✓ When the risk scenario is completely not present, the risk can be closed by updating the risk status to “Closed”.

RESIDUAL RISK

- ✓ Risks left over after implementing safeguards is known as Residual risk.
- ✓ This project or organization is exposed such residual risks even after the treatment. Hence it is required to monitor and treat them periodically

THANK YOU :)