Texas Education Agency

CYBERSECURITY TIPS AND TOOLS-
KEY ELEMENTS OF EFFECTIVE RISK MANAGEMENT

Frosty Walker

Chief Information Security Officer

Texas Education Agency

Frosty.Walker@tea.texas.gov

(512) 463-5095

Data Security Advisory Committee

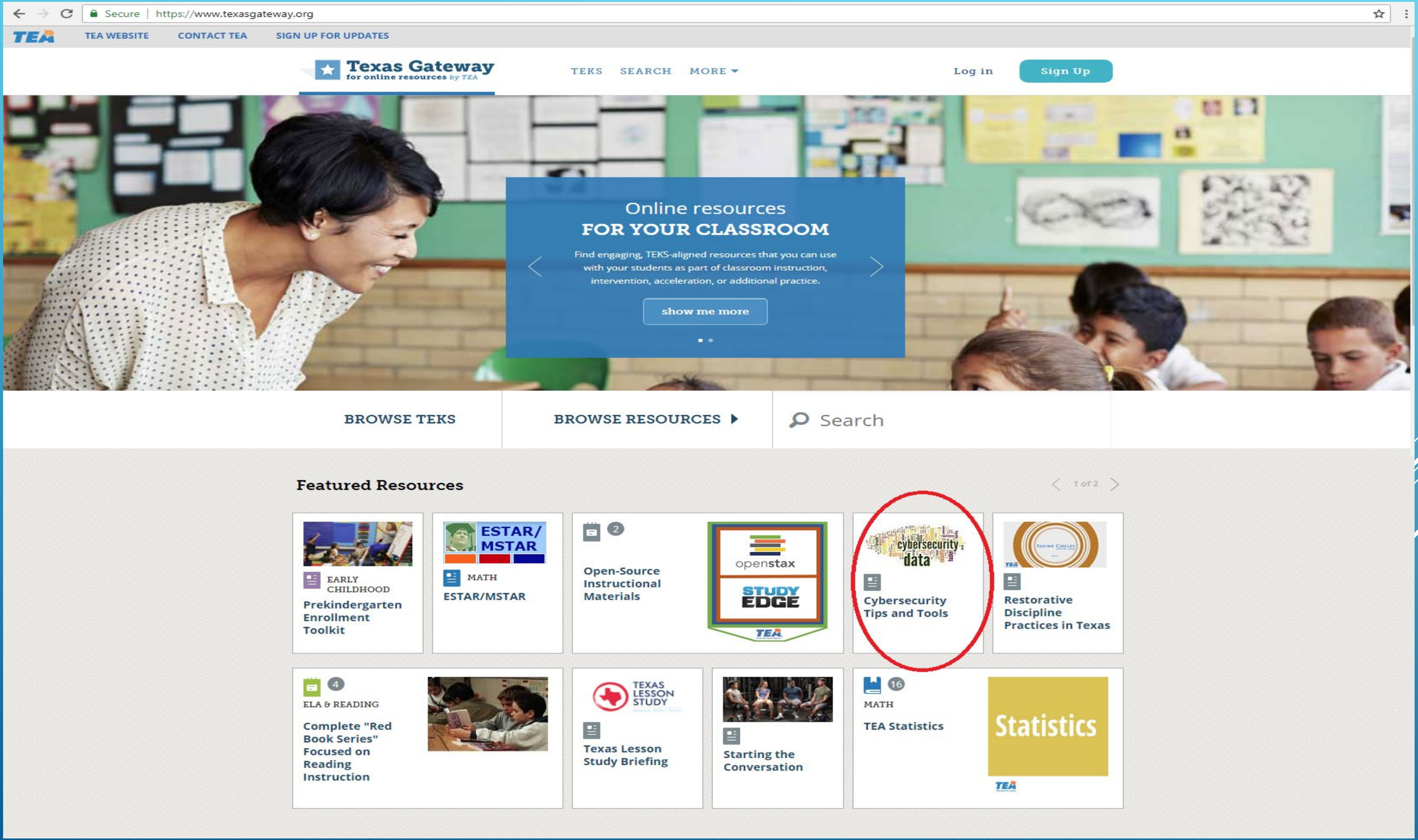
The Data Security Advisory Committee (DSAC) provides guidance to the Texas education communities, maximizing collaboration and communication regarding information security issues and resources which can be utilized within the educational communities served.

The DSAC is currently comprised of representatives from school districts, ESCs, TEA and the private sector.

Texas Gateway

https://www.texasgateway.org/

Cybersecurity Tips and Tools



Secure | https://www.texasgateway.org

TEA | TEA WEBSITE | CONTACT TEA | SIGN UP FOR UPDATES

Texas Gateway
for online resources by TEA

TEKS | SEARCH | MORE ▾ | Log in | Sign Up

Online resources
FOR YOUR CLASSROOM

Find engaging, TEKS-aligned resources that you can use with your students as part of classroom instruction, intervention, acceleration, or additional practice.

show me more

BROWSE TEKS | BROWSE RESOURCES ▸ | Search

Featured Resources

1 of 2

EARLY CHILDHOOD
Prekindergarten Enrollment Toolkit

ESTAR/MSTAR
MATH
ESTAR/MSTAR

2
Open-Source Instructional Materials
openstax
STUDY EDGE
TEA

cybersecurity data
Cybersecurity Tips and Tools

Restorative Discipline Practices in Texas

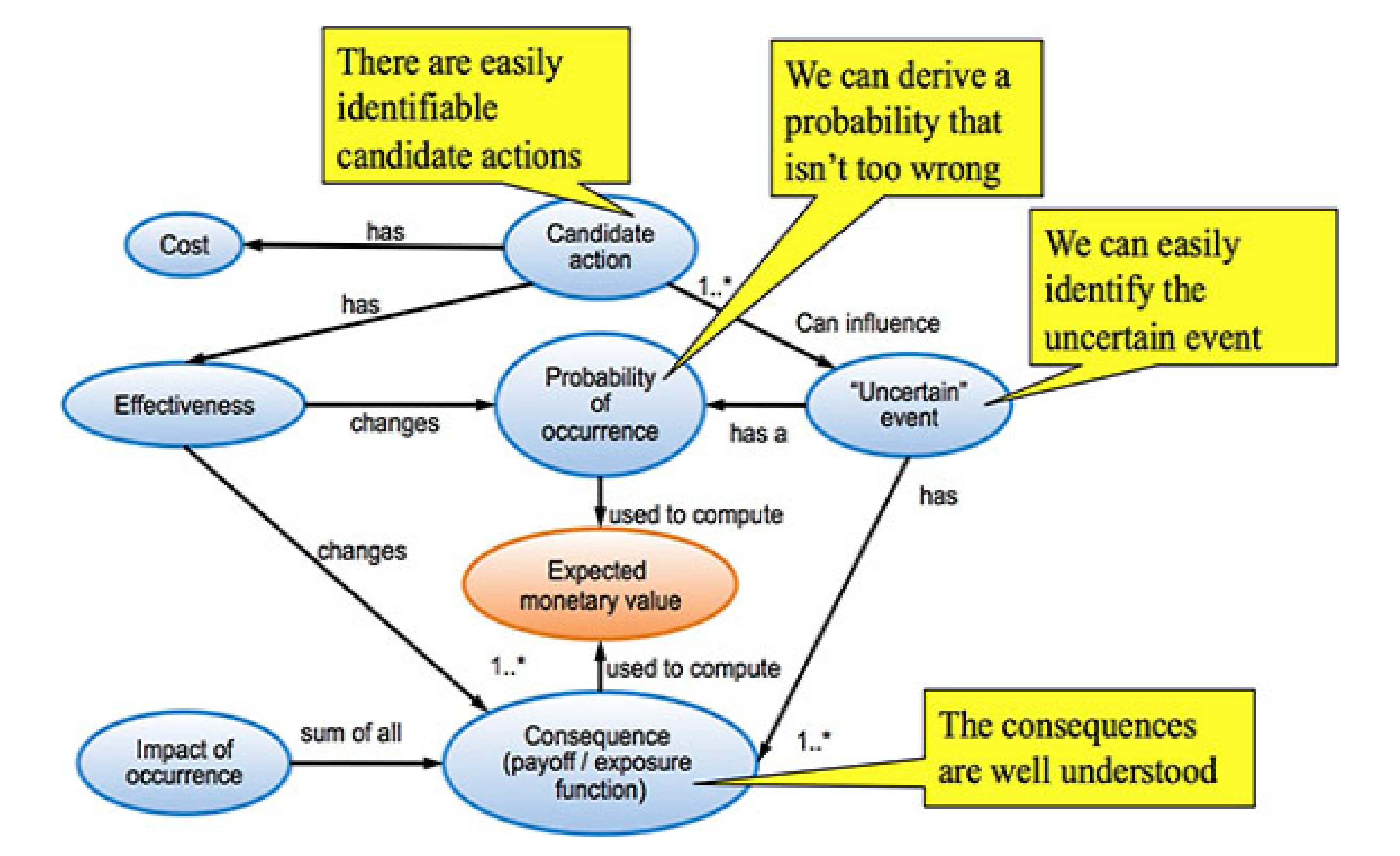
4
ELA & READING
Complete "Red Book Series" Focused on Reading Instruction

TEXAS LESSON STUDY
Texas Lesson Study Briefing

Starting the Conversation

16
MATH
TEA Statistics
Statistics
TEA

When you start looking at Risk Models, it can be a little scary……

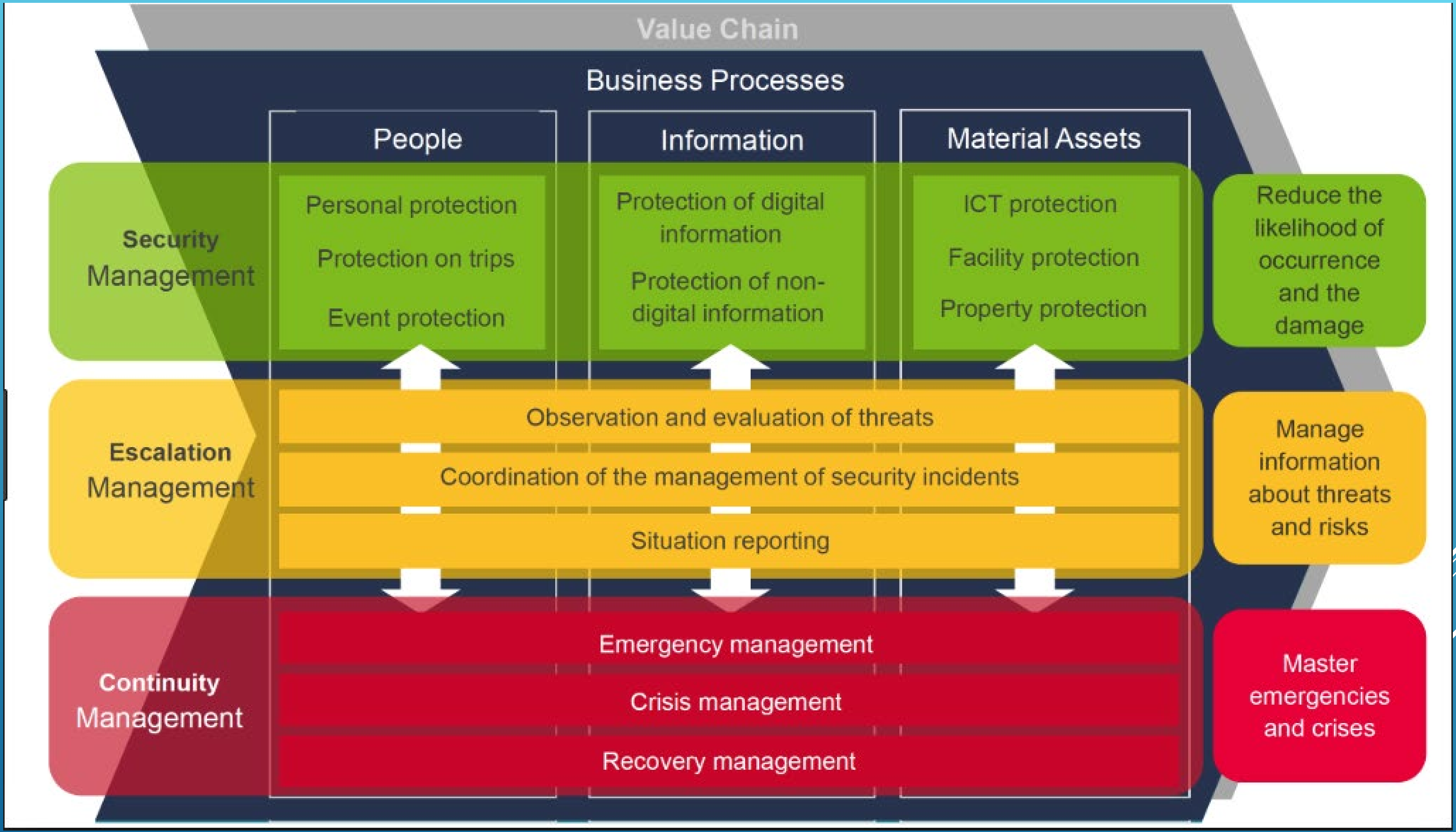


There are easily identifiable candidate actions

We can derive a probability that isn't too wrong

We can easily identify the uncertain event

The consequences are well understood



Value Chain

Business Processes

People

Information

Material Assets

Security Management

Personal protection

Protection on trips

Event protection

Protection of digital information

Protection of non-digital information

ICT protection

Facility protection

Property protection

Reduce the likelihood of occurrence and the damage

Escalation Management

Observation and evaluation of threats

Coordination of the management of security incidents

Situation reporting

Manage information about threats and risks

Continuity Management

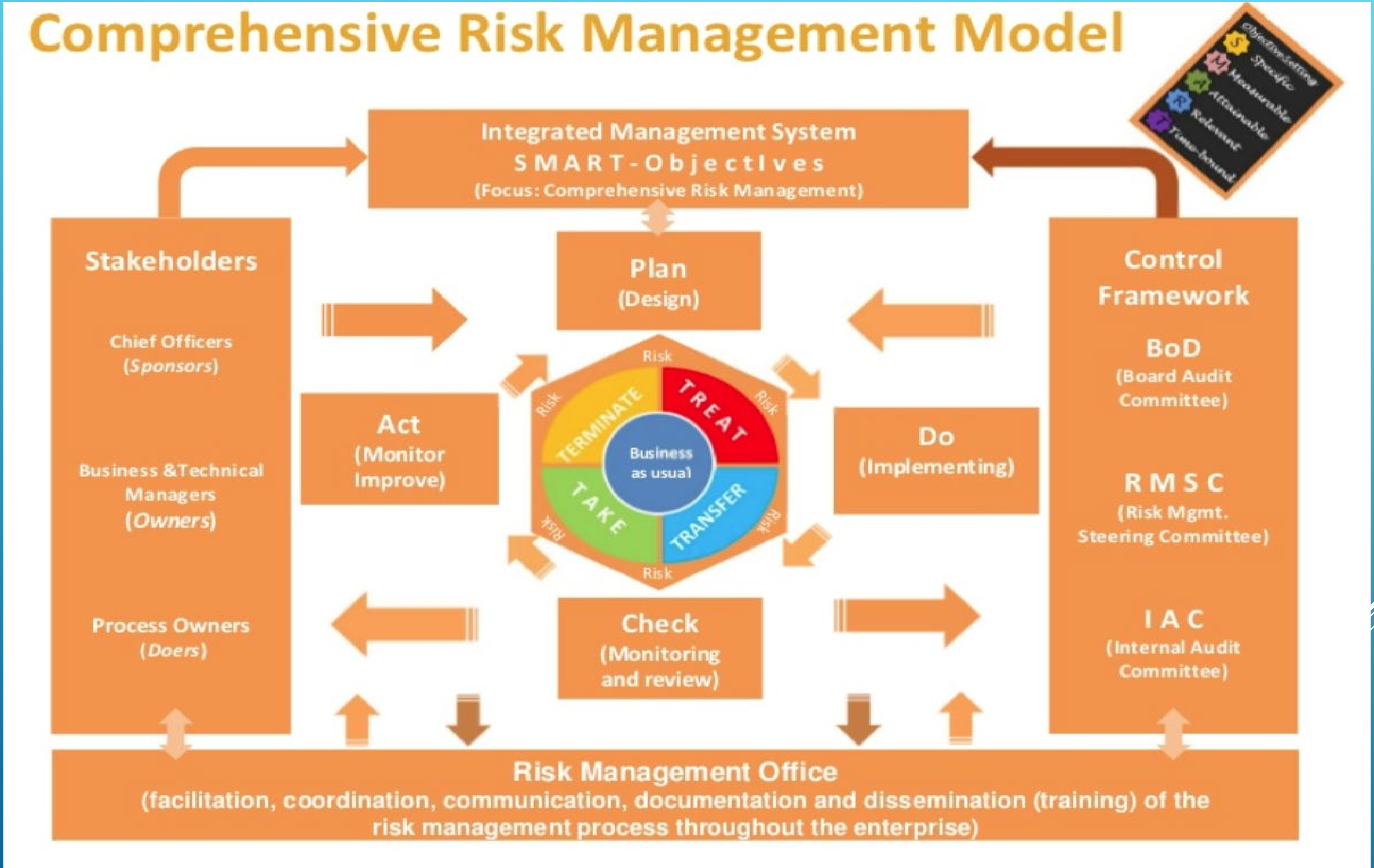
Emergency management

Crisis management

Recovery management

Master emergencies and crises

Comprehensive Risk Management Model



Integrated Management System

SMART-ObjectIves

(Focus: Comprehensive Risk Management)

Stakeholders

Chief Officers (*Sponsors*)

Business &Technical Managers (*Owners*)

Process Owners (*Doers*)

Plan (Design)

Do (Implementing)

Check (Monitoring and review)

Act (Monitor Improve)

Control Framework

BoD (Board Audit Committee)

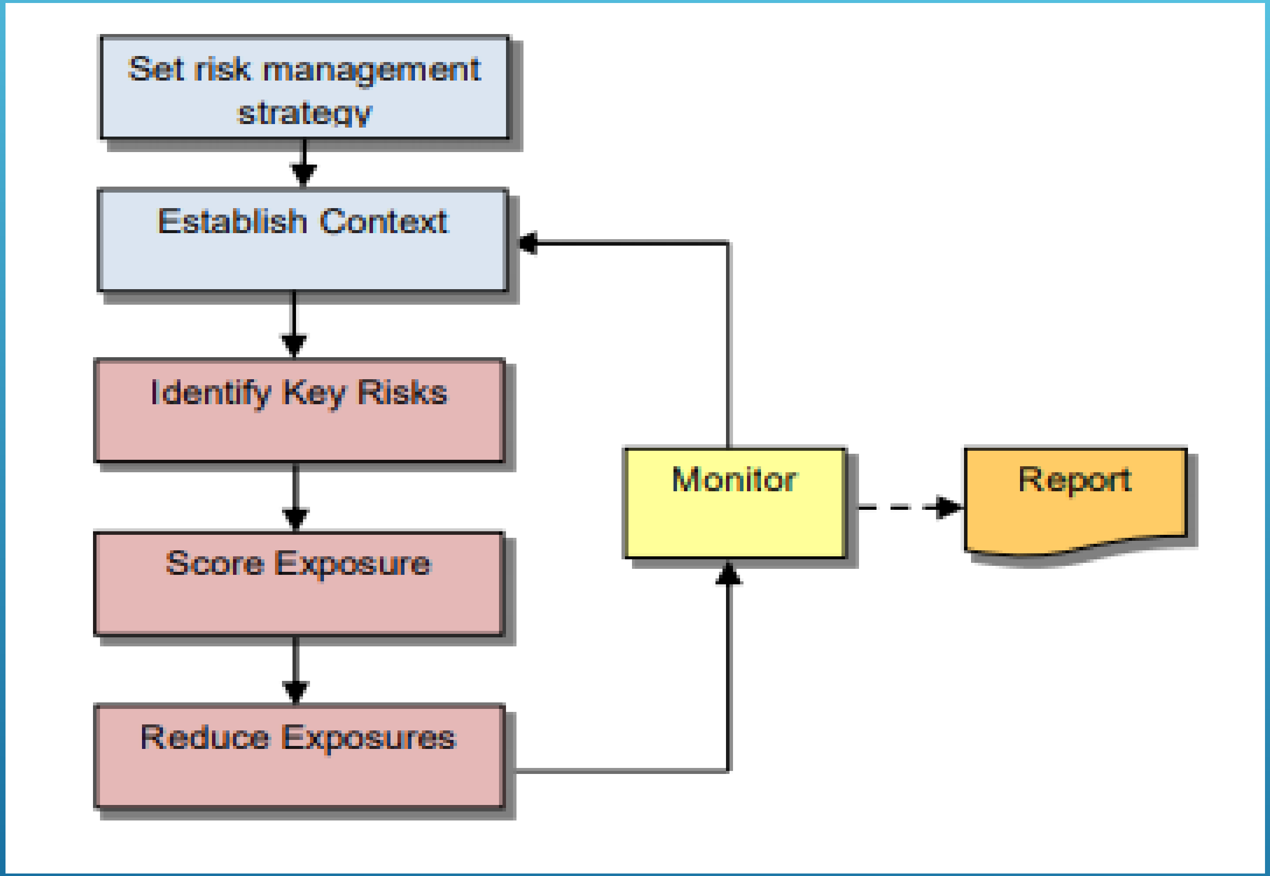
R M S C (Risk Mgmt. Steering Committee)

I A C (Internal Audit Committee)

Risk Management Office

(facilitation, coordination, communication, documentation and dissemination (training) of the risk management process throughout the enterprise)

Analytical Risk Model



Step 1: Set Risk Management Strategy

- **Risk management strategy setting is an imperative task to guide the response to uncertainties (both risks and opportunities) and requires a clear understanding of the strategy and the risks in executing that strategy.**
- **The risk management strategy identifies how risks are going to be identified and managed, including the roles of the different actors.**

Set Risk Management Strategy

Roles:

- Who is responsible for maintaining the records of risks and managing escalation?

- Whose agreement is required for a risk to be finalized?

- To whom are risks escalated and what is their responsibility for helping the management of risk?

Set Risk Management Strategy

Process and standards:

- What standards, procedures and other structures will govern risk management in the strategy?

Set Risk Management Strategy

Frequency:

- How often will the record of risks be refreshed (i.e. a simple update with new information)?

- How often will a full risk assessment be undertaken?

Set Risk Management Strategy

Cooperation:

- What are the expectations of the risk assessment regarding required and optional risk information?
- In particular, how should preparation for risk assessment exercises be done?
- How should reporting on implementing mitigations and significant risk events be reported?

Set Risk Management Strategy

Reporting:

- How frequently will risks be reported and to whom?
- Keeping all parties informed of key risks is necessary for good governance and essential for transparency.

Set Risk Management Strategy

Information Management:

- How frequently will risks be reported and to whom?
- Collection and use of information needs to be described and a division of labor established.
- How will the confidentiality of information that is collected be maintained?
- Who will the collected information be shared with?

Step 2: Establish Context

Establishing the context (both internal and external) is focused on:

- Gaining an understanding of the topic and its associated risks in preparation for an assessment.

- Establishing the scope of the risk assessment being undertaken, and for developing a structure for the risk assessment.

Establish Context

The context of the risk assessment may include:

- Confirming the purpose and objectives of the risk assessment
- Setting scope and boundaries
- Identifying possible critical linkages between the risks in scope and other activities
- Defining and limiting the preliminary research and analysis to be done
- Setting the methodology for the risk assessment
- Confirming the management arrangements (i.e. assigning resources and setting a timetable).

Step 3: Identify Key Risks

To identify key risks, gather information on historical incidents and emerging issues pertaining to the subject of the risk assessment. This could include specific information as well as general information relevant to the subject under assessment. Gathering this information may be obtained from various sources such as internal incident data, results from audits, staff interviews or group discussions, questionnaires and open source data.

Identify Key Risks

Risk source:

- Describes the nature of the risk which has the inherent potential to harm or facilitate harm.

Risk outcome:

- What could happen if the risk materializes: Events or incidents that could occur whereby the source of risk or threat has an impact on the achievement of objectives.

Identify Key Risks

Where it could happen:

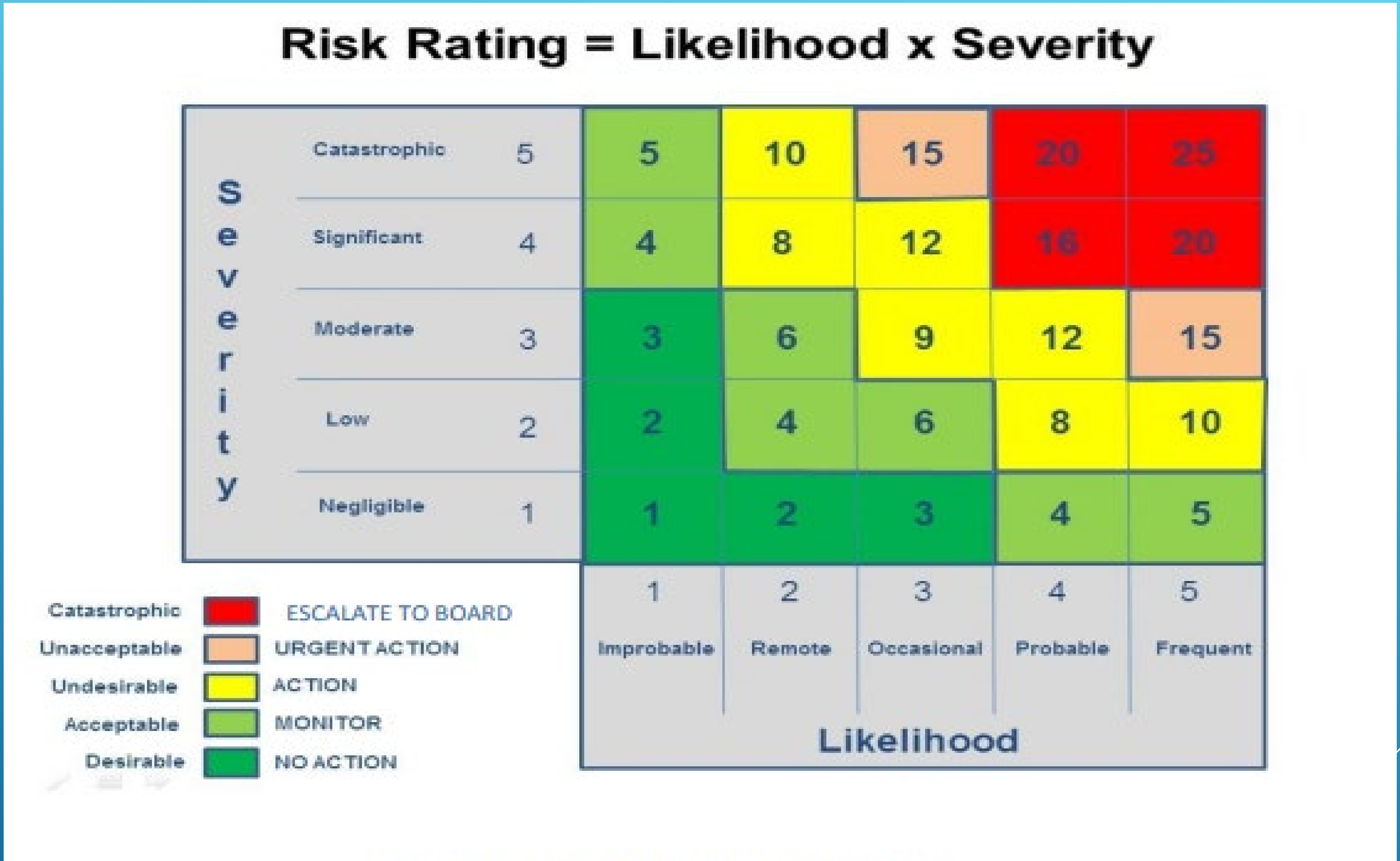
- These are the physical locations/assets where the event could occur or where the direct or indirect consequences may be experienced.

When it could happen:

- These are the specific times or periods when the event is likely to occur and or the consequences realized.

Step 4: Assess Risk and Score exposures

Risk is assessed as part of the due diligence process taking into account the risks and commensurate due diligence measures. Risk is analyzed in the context of the impact on the achievement of objectives and the results of the risk assessment forms the basis to manage the risk. For risk management to be effective, results based management and roles, responsibilities and delegations to project manager(s) need to be formalized.



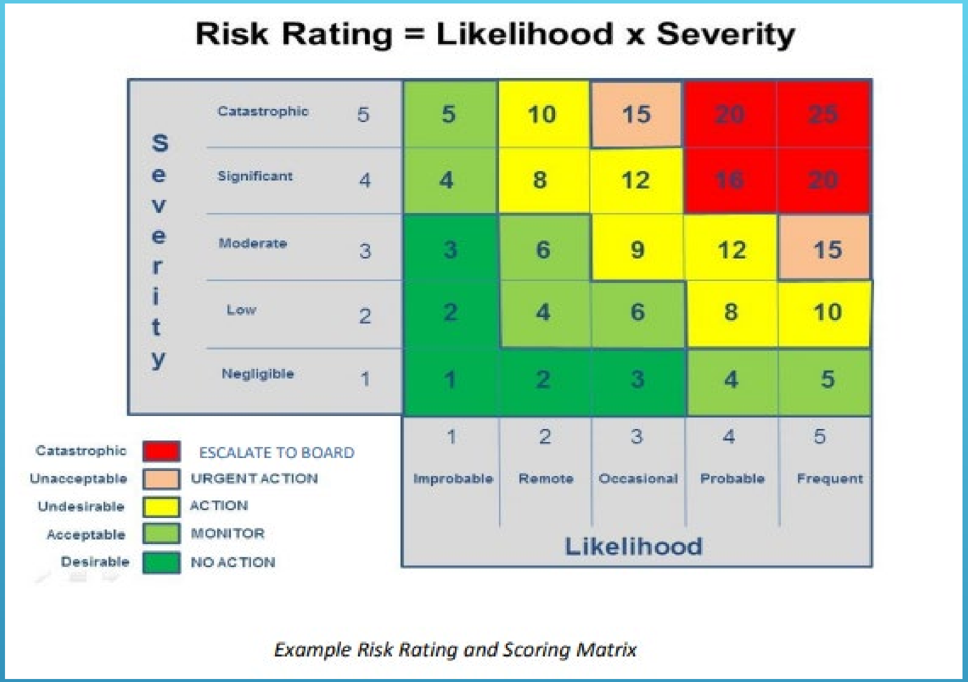
Risk Rating = Likelihood x Severity

Severity		1 Improbable	2 Remote	3 Occasional	4 Probable	5 Frequent
Catastrophic	5	5	10	15	20	25
Significant	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Low	2	2	4	6	8	10
Negligible	1	1	2	3	4	5

Likelihood

Catastrophic	🟥	ESCALATE TO BOARD
Unacceptable	🟧	URGENT ACTION
Undesirable	🟨	ACTION
Acceptable	🟩	MONITOR
Desirable	🟩	NO ACTION

Example Risk Rating and Scoring Matrix



Risk Rating = Likelihood x Severity

Severity	Catastrophic	5	5	10	15	20	25
	Significant	4	4	8	12	16	20
	Moderate	3	3	6	9	12	15
	Low	2	2	4	6	8	10
	Negligible	1	1	2	3	4	5
			1	2	3	4	5
			Improbable	Remote	Occasional	Probable	Frequent
			Likelihood				

Catastrophic	🟥	ESCALATE TO BOARD
Unacceptable	🟧	URGENT ACTION
Undesirable	🟨	ACTION
Acceptable	🟩	MONITOR
Desirable	🟩	NO ACTION

Example Risk Rating and Scoring Matrix

- **Risk Rating 1,2,3: No action required**
- **Risk Rating 4,5,6: Monitor risk**
- **Risk rating 8,9,10, 12: Treatment action required**
- **Risk rating 15: Urgent treatment action required**
- **Risk rating 16 and up: Escalate to Board**

Step 5: Reduce Risk Exposure- Treatment Actions

Decide how to address each risk. There are four risk treatment options. The four parts of risk treatment options outline how identified risks can be responded to. The choice can be made to take no action beyond what is already being implemented, and adding no additional control mechanisms other than those already in place, if it is perceived that the risk is acceptable (**Accept/Retain**). The risk can be controlled, by engaging in mitigation actions to reduce the seriousness of risk to an acceptable level (**Control/Reduce/Limit**). If there is no reasonable way to reduce the risk to an acceptable level, the risk can be avoided altogether (**Avoid**). Or the risk can be transferred to other parties that have a stronger capacity or authority to deal with the risk (**Transfer/Share**).

Reduce Risk Exposure- Treatment Actions

Accept/Retain:

Risk is accepted without the need for any further mitigating measures. A decision is made to tolerate the risk as further measures would not be cost effective. Risk retention can also be seen as accepting the loss as well as the benefit of the opportunity in taking the action. All risks that are not avoided or transferred are retained by default.

Reduce Risk Exposure- Treatment Actions

Control/Reduce/Limit:

Implement additional mitigation measures to reduce the risk to an acceptable measure. This includes prescribing a specific action to be taken (preventative, corrective, directive, detective etc.) Reducing the risk involves a reduction in the likelihood of the risk from occurring as well as a reduction in the severity of the impact should the risk materialize.

Reduce Risk Exposure- Treatment Actions

Avoid:

Exit or terminate the activity to avoid any exposure to the risk. Use of this risk modality also implies avoiding the activity linked to the risk. In this way, avoiding the risk also leads to avoiding the potential gain that can be achieved from the activity and not being able to achieve the objective.

Reduce Risk Exposure- Treatment Actions

Transfer/Share(outsource or insure):

Typically a financing solution paid to a third party to handle the risk. The decision is made to sub-contract implementation to other parties who (based on a structured risk assessment) are able to operate with lower risk. It is important to note that we don't just transfer a risk and forget about it. It is important to note that this response does not imply transferring the risk itself, but the response for that risk. If a risk has been identified, there is still the possibility of an event that could affect the achievement of stated objectives. Transferring emphasizes the need for monitoring and tracking in order to have a full overview of the risk seriousness.

Step 6: Monitoring and Report Risks

One important component of monitoring is ensuring that threats are adequately constrained and opportunities are appropriately taken as a way of reducing uncertainty. Monitoring of treatment actions should be a planned part of the risk management process and involve regular review, where results are recorded and reported internally and externally. It benefits an Agency’s risk management framework as a valuable input to continuous improvement of the system.

Step 6: Monitoring and Report Risks

The monitoring of treatment actions should include consideration of the following:

- Effectiveness and efficiency of controls
- Attain information from various sources to mature and improve risk assessment
- Benefit from lessons learned from risk events, including near-misses, changes, trends, successes and failures
- Changes in the external and internal environment, to risks and risk criteria and to the risks, may need periodic updating or revision
- Identification of emerging risks and risk trends.

Step 7: Due Diligence Within the Context of Enterprise Risk Management

- The overall framework in managing risks and identifying due diligence mechanisms need to take into account what areas have clear areas of thresholds (finance, procurement, delegations of authority, etc.) and the areas where quantifiable thresholds are not possible.
- Due Diligence is a component of a comprehensive Enterprise Risk Management framework, which encompasses policy, procedures, guidance, tools, techniques, etc., in the areas of operations.
- Due Diligence measures refer to common measures that can be applied at the strategy. These are complementary to the already existing measures that are adhered to by the organization.

Questions?