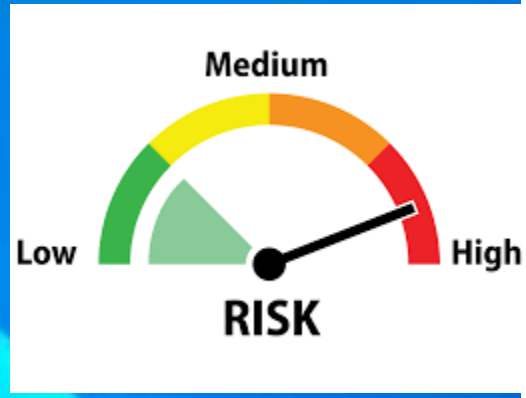
The Risk Management Best Practices

A practical approach



Day 2: Session 1

Mustapha B Mugisa, Mr. Strategy

Agenda

1) What is risk?
2) Why risk management
3) Risk management best practices
   a) Key roles of the Board and staff
   b) Risk appetite setting
   c) Risk reporting in practice

Test your knowledge…

Qn 1: Risk mitigation involves all but which ONE of the following:

A. Developing system standards (policies, procedures, responsibility standards)
B. Obtaining insurance against loss
C. Identification of project risks
D. Performing contingent planning
E. Developing planning alternatives

Test your knowledge…

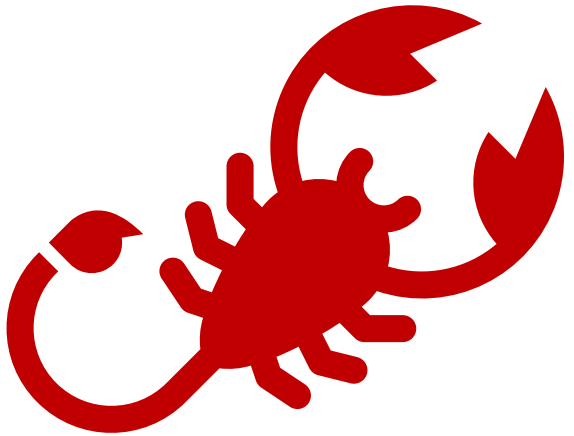
Qn 2: Answer True or False to each of the following statements and give a reason for your answer.

1. Something that could kill you must be very risky.
2. Risk combines the chance of something happening along with the amount of harm it can do.
3. A high-risk activity is quite likely to cause a lot of harm.
4. If something is very risky then it must also be very difficult to do.
5. Everyday things, like playing sport, or cooking are not risky at all.
6. Risk is only to do with industry and accidents at work.

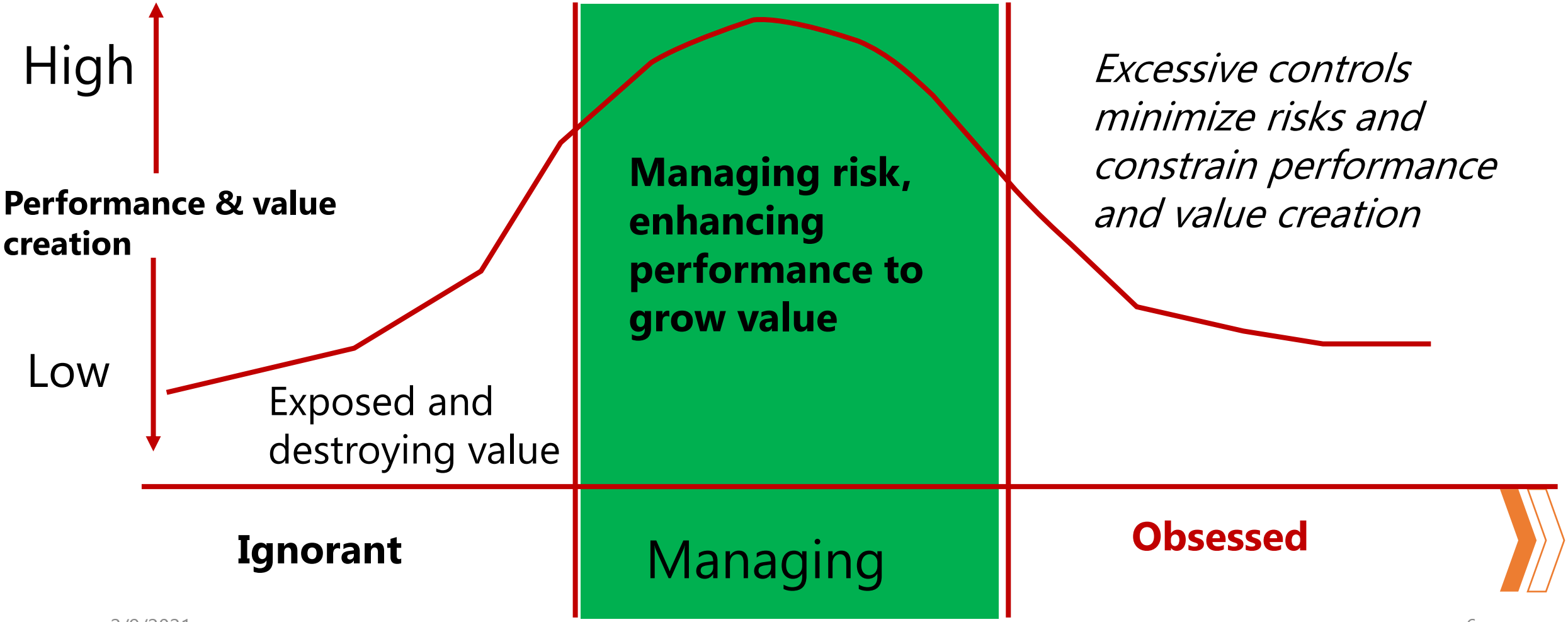
What is “Risk”?

In ISO 31000:2018, risk is defined as:

The effect of *uncertainty* on your objectives.



The essence of risk management



Role of the Board in ERM...

01

Assess, approve and monitor enterprise risk management framework

Maturity model for risk management

Current assessment → Desired status

summit consulting

	Initial LEVEL 1	Developing LEVEL 2	Established LEVEL 3	Advanced LEVEL 4	Leading LEVEL 5
ERM Framework & Policy	- Fragmented/ limited ERM framework	- Framework developed but not approved by appropriate authority	**- ERM framework and risk appetite in place**	**- Escalation processes, ERM integrated in strategic planning - All operational entities - Risk scales for different levels**	- ERM framework reflects risk management practices and addressing all operational elements.
Governance and Org. Structure	**- Fragmented and informal structure - Accountability for ERM is informal**	**- Risk Governance structure (based on Three Lines of Defense) to oversee ERM**	- ERM governance structure in place - ERM Committee and entity to oversee is in place	- Fully integrated risk governance structure - Chief Risk Officer	- Structure applied across all operations - Accountability at each level & risk mgt is part of Agenda
Process and Integration	- Inconsistencies in methodology	**- Limited process to assess, monitor and report**	**- Systematic process for risk assessment, response, monitoring, escalation and reporting**	**- Links between internal controls & risks / control effectiveness & risk assessment - RBM and ERM fully aligned**	- Optimized with pre-defined indicators. Fully automated - Fully integrated risk & opportunity analysis
Systems and Tools	- Risks recorded in various documents	**- Manual risk assessment / response (spreadsheet)**	**- Consolidated risk register - ERM monitoring and reporting capabilities**	**- Dynamic risk dashboards - Financial risk modelling - Semi-automated operations**	- Advanced modelling, forecasting and scenario planning tools
Risk Capabilities	- Risk competencies perceived to have little value	**- Knowledge for certain managers - Indicators presented to senior mgmt. annually**	**- Recognized mgmt. competency - Accurate risk mgmt. information available**	**- Core competency for staff - Dynamic risk information reports across organization**	- Perfecting risk skills - Dynamic dashboards across organization
Risk Culture	- Limited commitment	**- Partial consideration of risk factors**	**- Clear expectations, info systematically collected - Risk mgmt. assessed in Staff Performance mgmt.**	**- Risk mgmt. integrated into strategic activities - Systematically collect and communicate information**	- Org.-wide awareness - Dynamic risk information - Learning from success and failures

Recommended actions

Current assessment → Desired status

Initial LEVEL 1	Developing LEVEL 2	Established LEVEL 3	Advanced LEVEL 4	Leading LEVEL 5

Role of the Board...

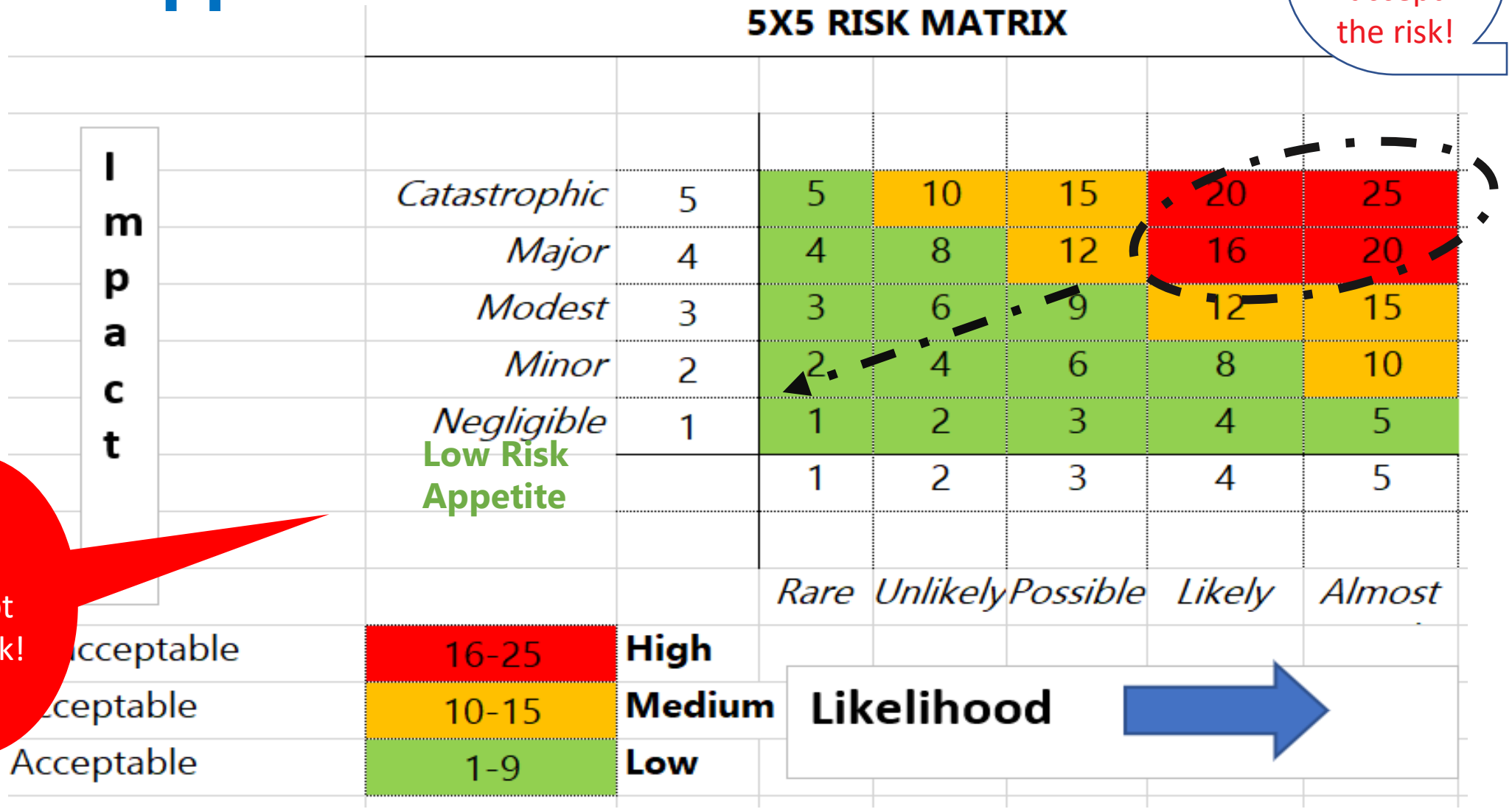
02

Set a risk appetite and provide oversight

Risk appetite articulation…

We cannot accept the risk!

High Risk Appetite



We accept the risk!

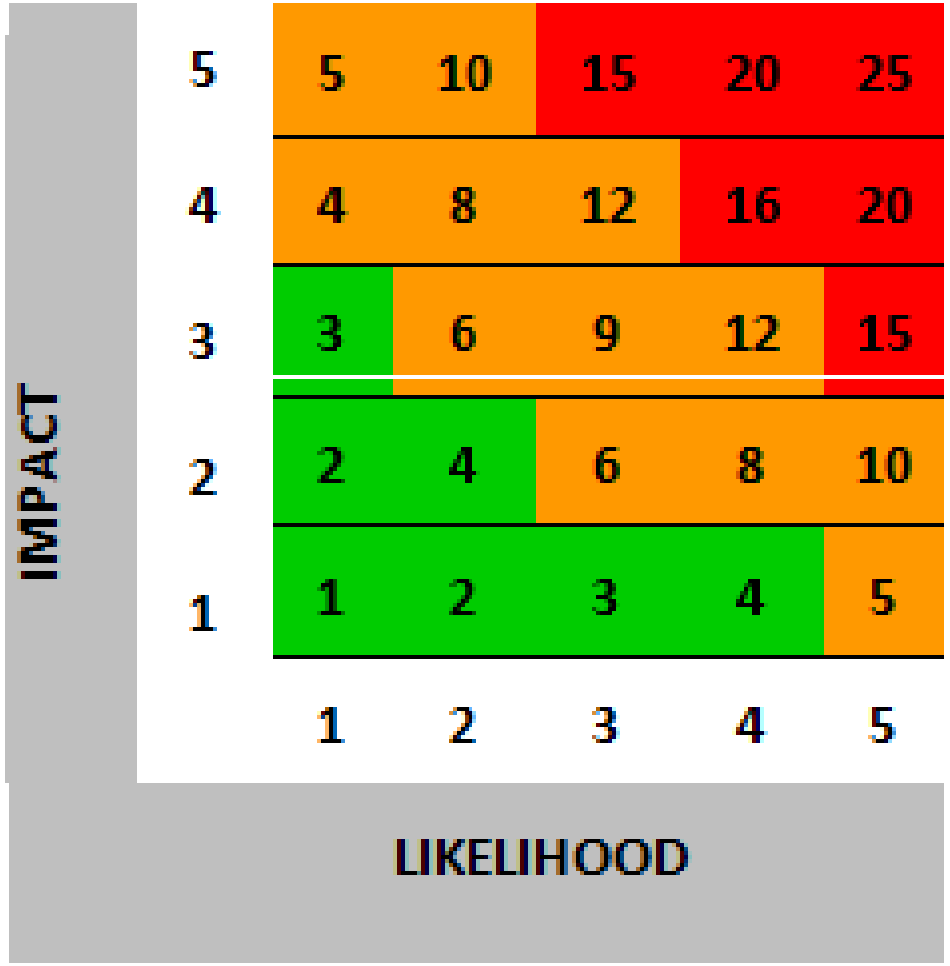
Threat event Likelihood (L)

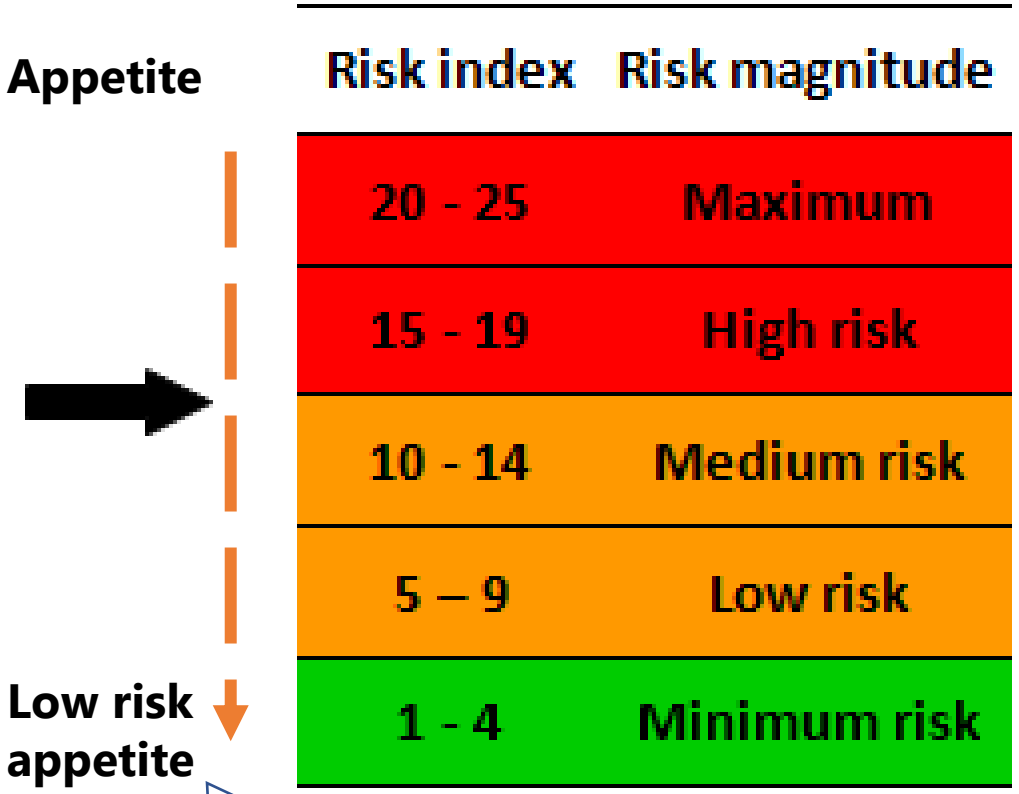
Rating	Score	Chances of an event occurring (Likelihood)
Almost Certain	5	a) > 75% chance of occurrence (e.g. Flooding in Kampala after heavy downpour). b) Very regular occurrence
Likely	4	a) >50%< 75% chance of occurrence b) Circumstances frequently encountered
Possible	3	a) >25% <50% chance of occurrence b) Likely to happen at some point in the next 2 years. c) Circumstances occasionally encountered.
Unlikely	2	a) > 5% < 25% chance of occurrence b) Only likely to happen once in 3 years. c) Circumstances rarely encountered.
Rare	1	a) Less than 5% chance of occurrence (e.g. a Tsunami will hit Kampala) b) Has never happened before

Threat event impact…

Rating	Definition	Monetary Impact (Ugx'm)	Consequence	Impact on your objectives	Reputation & image per event	Noncompliance
5	**Catastrophic**	> 50	Leads to termination of projects or withdrawal of financing and is fundamental to service delivery	Non achievement of objectives; performance failure	Maximum high headline exposure; Board Censure; loss of credibility	Serious wilful breach; criminal negligence or act; prosecution; Board censure.
4	**Major (Critical)**	> 10 < 50	Event which may have a prolonged negative impact and extensive consequences	Significant delays; performance significantly under target	Headline profile; repeated exposure; at fault or unresolved complexities; Board involvement; regulatory enquiry	Deliberate breach or gross negligence; formal investigation; disciplinary action; Board involvement
3	**Moderate**	> 5 < 10	Event which can be managed, but requires additional resources and management effort	Material delays, marginal under achievement of target performance	Repeated non headline exposure; slow resolution; Parliamentary enquiry/ briefing	Negligent breach; lack of good faith evident; performance review initiated
2	**Minor**	> 0.5 < 5	Event can be managed under normal operating conditions	Inconvenient delays	Non-headline exposure, clear fault settled quickly; negligible impact	Breach; objection/ complaint lodged; minor harm with investigation
1	**Negligible**	< 0.5	Consequences can easily be absorbed under normal operating conditions	Little impact	Non-headline exposure, not at fault, no impact	Innocent procedural breach; evidence of good faith; little impact

Risk = Impact x Likelihood





Risk appetite application…

Risk Category/ Universe	Your risk appetite articulation (statement) in the policies and procedures	Score /risk appetite	Color
"Strategic"	1. Zero tolerance for activities outside mandate & strategic objectives 2. Low appetite for reputational risk 3. Zero tolerance for disclosure of confidential information 4. Zero tolerance for poor funds accountability	0 -9 (Low)	
"Compliance"	1. You shall be 100% compliant with all applicable laws and regulations 2. Zero tolerance for budget deviations 3. Zero tolerance for health and safety violations	0 -9 (Low)	
"Financial"	1. Zero tolerance to fraud and or corruption practices 2. Zero tolerance for operational risk loss resulting from override of controls	0 -9 (Low)	
Etc…			

Risk appetite application…

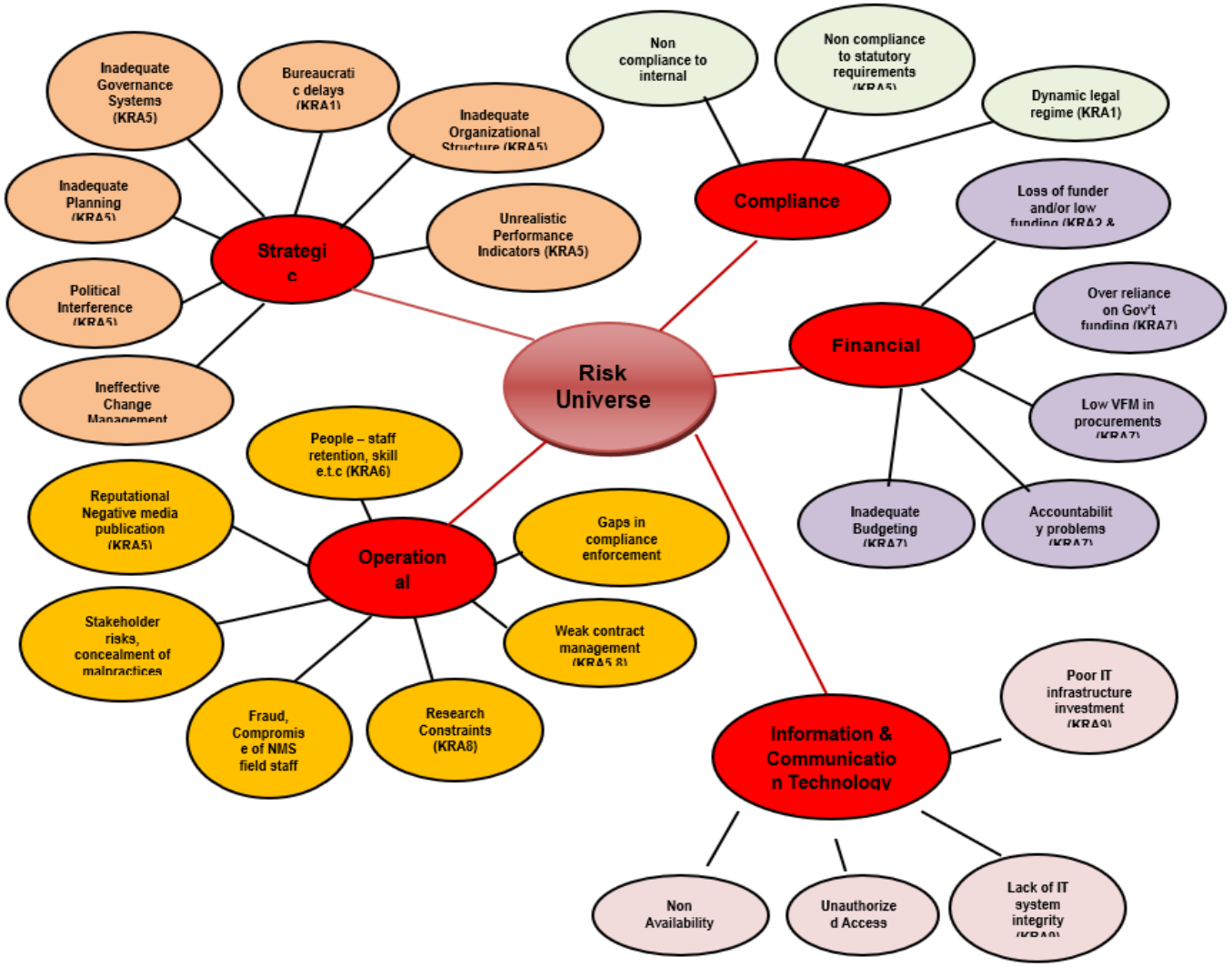
Risk Category/ Universe	Your risk appetite articulation (statement) in the policies and procedures	Score/ Risk appetite	Color
"Operational"	1. Average tolerance for slow turnaround time (TAT) for client enquiries – staff may fail to meet target only 3 times 2. We accept late coming on three occasions by any staff once a month, but no more	10-15 (Medium)	
"Cybersecurity"	1. Any staff can bring to work and use personal mobile devices like phone, laptop, etc 2. Use of personal emails for official business allowed 3. High tolerance for working from home, connecting to core IT systems without doing so through company owned VPN	16 – 25 (High)	
Etc…			

Source: 7 Tools of an Effective Board Member Book

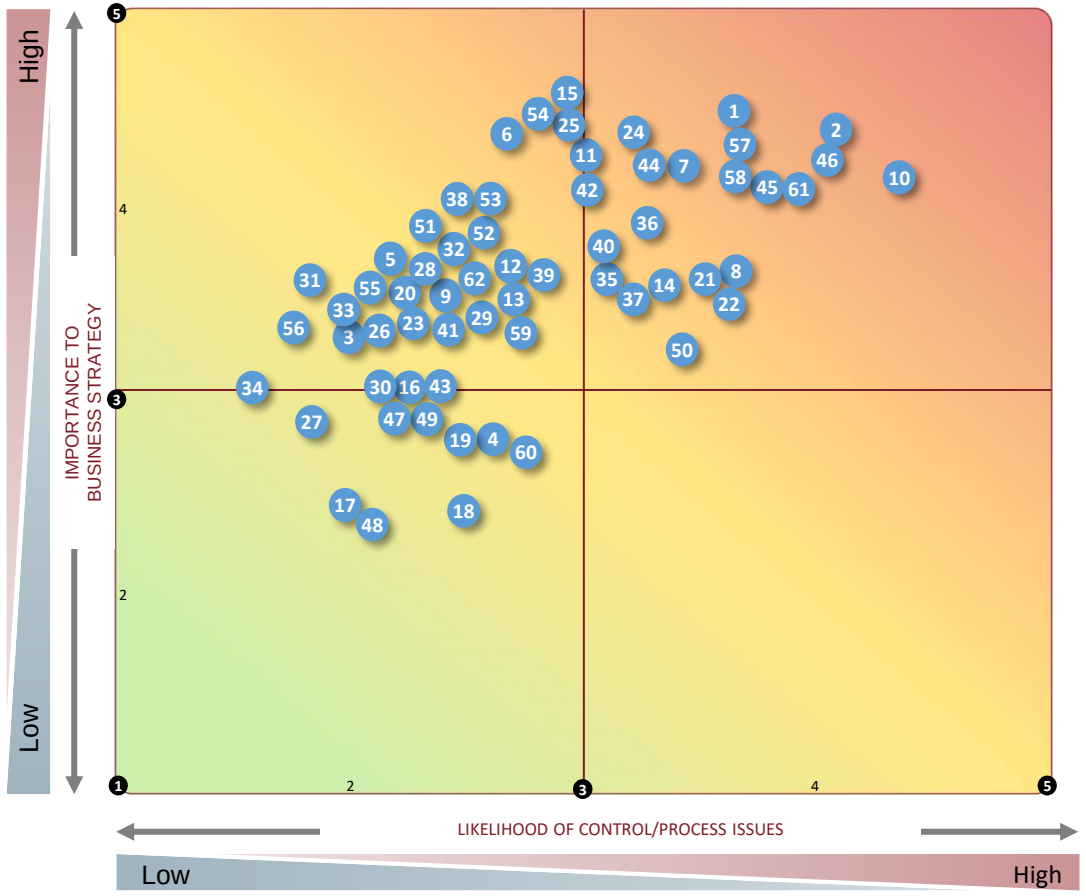
Risk reporting – contents

- Risk Assessment
- Risk Assessment Tools
- Risk Assessment Results
- Proposed Internal Audit Plan
- Proposed Internal Audit Project Map

1.1 The risk universe



1.2 The risk map…



Business Cycle/Process:

Power absorption
1. Failure to evacuate generation
2. Unstable regulatory regime
7. Wrong Customer Pricing
8. Order Entry/Billing
10. Software License Tracking
11. Fraudulent reporting by licensees
12. Information asymmetry

Revenues
13. Sales/Lead Generation
14. Pricing/Discounts
15 Credit Assessment/ Monitoring
4. Credit Memo Process
5. Customer Fulfillment
6. Customer Support
7. Licensee Support Pricing
8. Order Entry/Billing
9. Collections/Accounts Rec.
10. Software License Tracking
11. Revenue Recognition
12. Managing New Product Info.
14. Managing Product Lifecycle
15. Prof. Services Revenue

Expenditures
16. Purchasing
17. Accounts Payable
18. Fixed Assets
19. Capital/Operating Leases

Financial Reporting
24. Budgeting/Forecasting
25 Management Reporting
26 Tax Compliance
27. Access to Company Policies
28. Closing/Consolidation Process

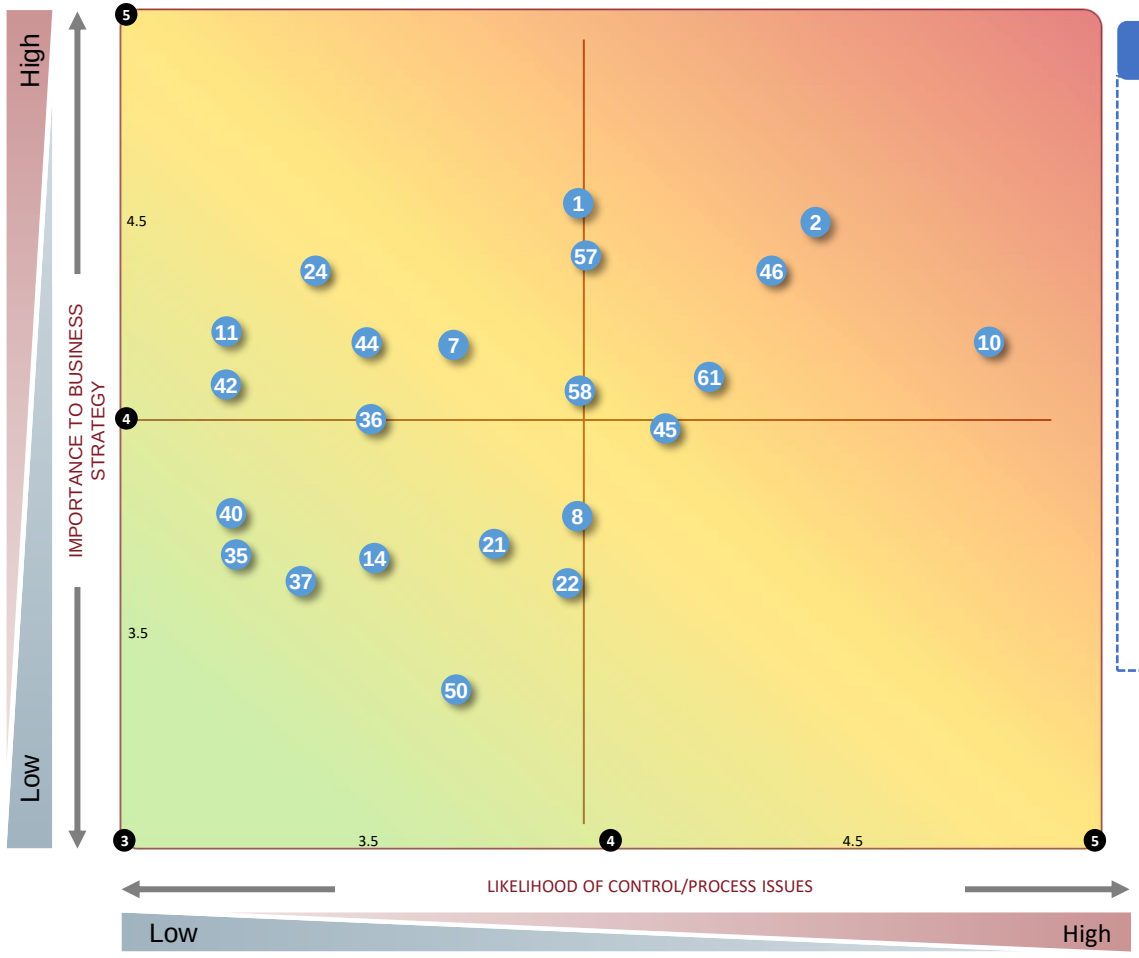
Payroll/Personnel
29. Recruitment
30. Performance Assessment
31. Training
32. Compensation/Benefits
33. Employee Satisfaction
34. Payroll Processing

Information Systems
35. Systems & Technology Planning.
36. Data Access/Security
37. Disaster Recovery Planning.
38. Source Code Security
39. Resource Prioritization
40. Key Business Applications
41. System Migration Mgmt.
42. Electronic Product Distribution

Operating Expenses
43. Travel & Entertainment
44. Commissions & Bonus Plans
45. Contract Negotiations/Mgmt.
46. Business Partner/ Royalties
47. Facilities Mgmt.
48. Materials Mgmt.
49. Overhead Cost Mgmt.

Other
50. Remote Location Controls
51. External Customer Satisfaction
52. Customer Complaint Tracking/Resolution
53. Intellectual Property Protection
54. Technological Developments/ R&D
55. Litigation Management
56. Regulatory Compliance
57. Business Partner Relationship Mgmt.
58. Channels Distribution Mgmt.
59. Software Piracy
60. International Development Issues
61. Partner/Royalty Controls
62. Shareholder Relations

1.3 The risk map after controls



Business Cycle/Process:

Power absorption
1. Failure to evacuate generation
2. Unstable regulatory regime
7. Wrong Customer Pricing
8. Order Entry/Billing
10. Software License Tracking
11. Fraudulent reporting by licensees
14. Information asymmetry

Treasury
21. Transfer Pricing
22. Acquisitions/Alliances

Financial Reporting
24. Budgeting/Forecasting

Information Systems
35. Systems & Technology Planning.
36. Data Access/Security
37. Disaster Recovery Planning.
40. Key Business Applications
42. Electronic Product Dist.

Operating Expenses
44. Commissions & Bonus Plans
45. Contract Negotiations/Mgmt.
46. Business Partner/VAR/ OEM Royalties

Other
50. Remote Location Controls
57. Business Partner Relationship Mgmt.
58. Channels Distribution Mgmt.
61. Partner/Royalty Controls

1.4 Top 10 risks register

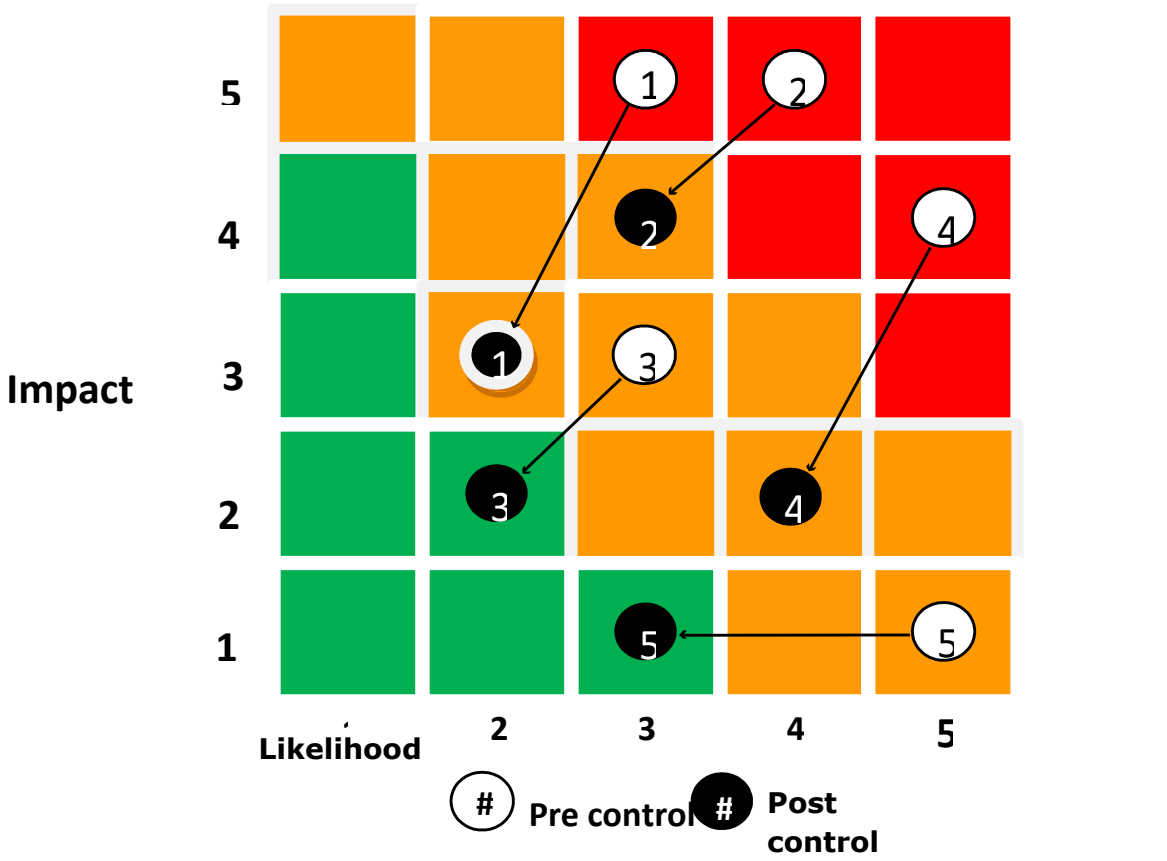
Risk id	Risk Description	Risk Impact	Risk Likelihood	Risk Score	Risk Rank
		(1- 5)	(1-5)	(RIxRL)	
R1	Funding or financing risk – no assured funding sources for going concern	4	5	20	1
R2	Regulatory risks. Set aside funds to absorb risks	4	5	20	1
R3	Low economic performance affecting loan repayments. Need to review and restructure all loans.	4	4	16	2
R4	Cybersecurity risks	4	4	16	2
	Etc…				

1.5 Internal Audit projects to assure risk mgt

Project Description	Estimated Hours*	Estimated Costs
Audit Committee Reporting and Follow Up on Prior Findings/Action Plans (# Quarters @ # Hours per Quarter)	# Hours	xx
Development Services Agreement/Operating Agreement Contract Compliance • Accuracy/use of performance evaluation metrics defined in/required; Compliance with ERA act/ Operating Agreement terms and conditions	# - # Hours	xx
Investment Policies and Practices • Authorization for transactions/policies and procedures • Investment valuation; Investment allocation and performance monitoring	# - # Hours	xx
Information Security and Privacy • IT system security and protection of data from persons external to company; Data encryption; • Privacy policy/practices for sharing customer information with affiliates	# - # Hours	xx
General Controls Review • System access controls/roles and responsibilities (segregation of duties); Input/data integrity controls; • Data backup and recovery • Support management	# - # Hours	xx

1.6 Risk control strategy…

Figure 3: Risk Impact/Likelihood control



The risk management strategy aims to move risks from the **red** category to the **green** one, on an on-going basis…

Risk management strategies… (4 Ts)

Terminate

Treat

Tolerate

Transfer

Role of the Board…

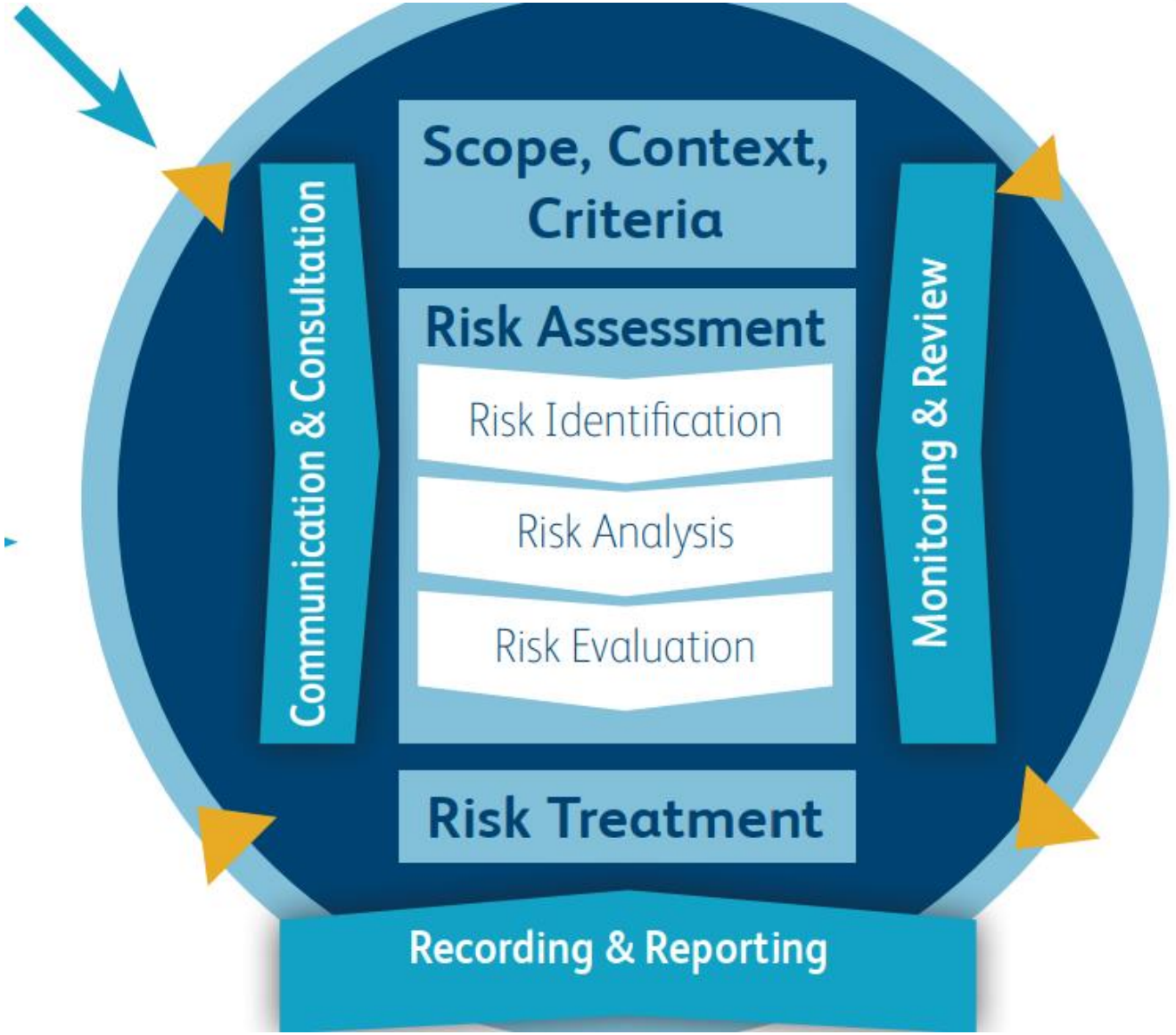
03

Must understand and approve the entity's risk management process…

The ISO 31000:2018 Risk Management Process

Involves:

- Understand context
- Risk assessment
- Risk treatment
- Monitoring, communication
- Recording and reporting



Thank You

summitFORENSICS

Know the Truth. Transform.