A Comprehensive Approach to Building ERM

Rick Ouellette, BScDA, CPA, CGA, CISA, CISSP, CGEIT
Chief Risk Officer

Government of New Brunswick

An Approach

1. **Consider Perspectives**
2. **Research & Considerations**
3. **Scope**
4. **A Vision for ERM**
5. **Manage the Elements**

An Approach

1. Consider Perspectives

2. Research & Considerations

3. Scope

4. A Vision for ERM

5. Manage the Elements

Perspectives

Traditional RM Perspective

ERM Perspective

Investor Perspective (FCNB.ca)

Being informed is the best way to protect your money.
To be an informed investor you should:

Understand How the Investment Works:

Before buying, ask these important questions:

- How does the investment make money? Does it pay dividends or interest?
- What fees or commissions would I have to pay to buy, hold and sell the investment? What effect will these fees have on the overall value of your portfolio?
- What has to happen for the investment to increase or decrease in value?
- What risks are associated with this investment? How easy would it be to sell the investment if I needed my money right away? Are there any restrictions or penalties involved if I want to sell?
- Does the investment fit my goals and risk tolerance?

Understand What You're Investing In:

FINANCIAL AND CONSUMER SERVICES COMMISSION
regulation • education • protection

New Nouveau Brunswick

CEO / Shareholder Perspective (RBC)

KEY COMPANY METRICS	
Open	$101.25
Previous close	$100.82
High	$101.63
Low	$101.11
Bid / Ask	$101.34 / $101.35
YTD % change	+11.53%
Volume	671,529
Average volume (10-day)	1,772,662
Average volume (1-month)	2,242,101
Average volume (3-month)	2,166,037

52-week range	$81.82 to $101.63
Beta	0.96
Trailing P/E	13.84×
P/E 1 year forward	13.46×
Forward PEG	1.78×
Indicated annual dividend	$3.64
Dividend yield	3.59%
Trailing EPS	$7.32

Updated October 20 11:21 AM EDT. Delayed by at least 15 minutes.

Total Business Risk / ……
Cyber Risk /…..

Source: https://www.theglobeandmail.com/globe-investor/markets/stocks/news/?q=RY-T

New Nouveau Brunswick

Board-level Limited RM View

- Strategic Risks only
- Top 10

Board-level Broader ERM Perspective

20 Questions Directors Should Ask About Risk, 2003 – an extract:

1. How do we **integrate** risk management with the corporation's **strategic direction and plan**?
2. Are we taking the **right amount of risk**?

3. How do we ensure that risk management is an integral part of the planning and **day-to-day operations** of individual business units?
4. How is risk management **coordinated across** the organization?
5. How do we **take advantage of the organizational learning** that results from the risk management program and activities?

Source: Canadian Institute of Chartered Accountants publication 2003.

An Approach

1. Consider Perspectives

2. Research & Considerations

3. Scope

4. A Vision for ERM

5. Manage the Elements

One Size Does Not Fit All

"Risk management does not need to look the same for every organization and decision."

~Internal Auditor Magazine, October 2017, page 40.

Good ERM Resources

- **ISO 31000** is an internationally agreed standard for the implementation of risk management principles
- ***Leveraging COSO Across The Three Layers Of Defense*** published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in July 2015
- ***Managing Risk in Government: An Introduction to Enterprise Risk Management*** from the IBM Center for The Business of Government; authored by Dr. Karen Hardy; 2010 2nd Edition.
- **Organizational Risk and Opportunity Management**. Concepts and Processes for NASA's Consideration; NASA/SP-2014-615; November 2016.

Layered

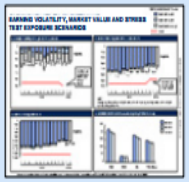
Exhibit 2

An integrated system of risk reports

CASE EXAMPLE

Reporting "cascade" includes:

1 Enterprise view of risk
- Enterprise risk heat map
- Top 10 risks
- Emerging risks
- Current market outlook
- Peer comparison



(10-20 pages providing an overview of enterprise-wide risk)

Board-level report

2 Risk and BU syntheses
- Synthesis page for each risk
- Synthesis page for each BU or function

(1 page per risk)
(10 – 15 pages overall)

3 Detailed risk sections
- Provides a chapter containing overall synthesis and detailed support pages for each risk
- Also includes reports on specific risks for each BU and function

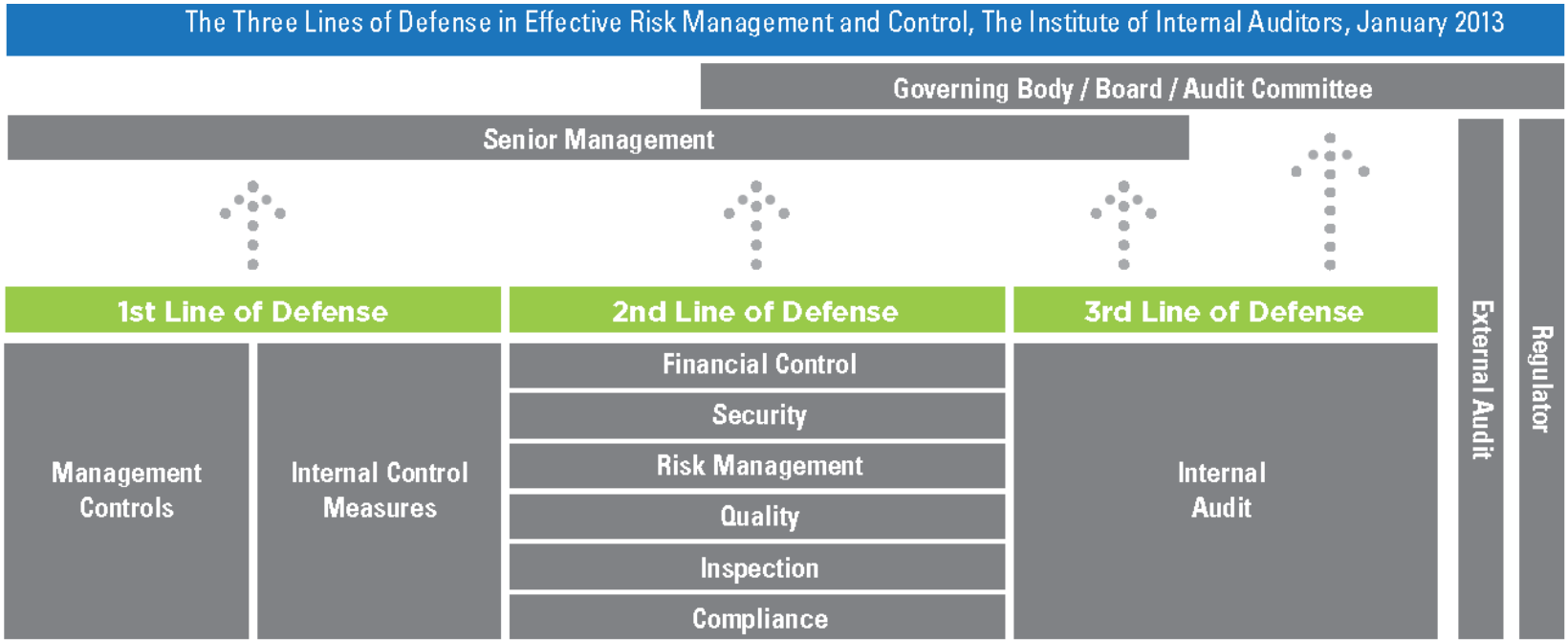
(15-20 pages per chapter)
(10 – 15 chapters)

Source: McKinsey

Source: https://www.mckinsey.com/business-functions/risk/our-insights/a-board-perspective-on-enterprise-risk-management (2010)

The Three Lines of Defense

Layered and Integrated Risk Governance



Source: COSO-3 layers of defence_2015-3LOD.pdf

Interesting Impact Scale

Table 2: Risk Impact Scale

Impact Score	Short Description	Human Capital	Hazard/Safety/Legal Liability	Financial	Operational	Compliance	Strategic	Reputational
1	Minor	• Affects <5% of employees • No collective bargaining impacts • No impact on recruitment or retention	• Minor injury • Minor legal liability exposure • Minor, reparable environmental damage	• Annual loss of <$1 million in current fiscal year • 5-year cumulative liability/obligation <$10 million	• No disruption of critical operations and services • 1-2 day disruption of a department • Minor impact on efficiency, client/student programs and services, environmental sustainability, or infrastructure • No effect on leadership effectiveness	• Minor audit findings • Minor fines	Slows progress on one UVM strategic goal	• Limited negative publicity • No effect on UVM reputation/image
2	Moderate	• Affects 5-10% of employees • Collective bargaining required • <5% employee turnover	• Moderate injury • Self-insured workers' compensation injury/exposure possible • Moderate legal liability exposure • Moderate, reparable environmental damage	• Annual loss of $1>$5 million in current fiscal year • 5-year cumulative liability/obligation $10<50 million	• 3- to 5-day disruption of several departments or one critical service • Moderate impact on efficiency, client/student programs and services, environmental sustainability, or infrastructure • Moderate effect on leadership effectiveness	• Moderate audit findings • Moderate fines • Short-term agency scrutiny	Slows progress on more than one UVM strategic goal	• Local/regional negative publicity • Minor, short-term effect on UVM reputation/image
3	Substantial	• Affects 11-25% of employees • Collective bargaining required • 6-9% employee turnover	• Substantial injury • Self-insured workers' compensation injury/exposure possible • Substantial legal liability exposure • Substantial environmental damage requiring mitigation	• Annual loss of $5>$10 million in current fiscal year • 5-year cumulative liability/obligation $50<100 million	• 6- to 10-day disruption of a College, School, or Division or several critical services • Substantial impact on efficiency, client/student programs and services, environmental sustainability, or infrastructure • Substantial impact on leadership effectiveness	• Audit findings requiring programmatic changes • Moderate-term agency scrutiny • Enforcement action likely	Stops progress of one UVM strategic goal	• Local/regional negative publicity • Pressure for UVM to control the message • Moderate damage to UVM's reputation/image
4	Serious	• Affects 26-50% of employees • Collective bargaining required • 10-15% employee turnover	• Serious injury • Self-insured workers' compensation injury/exposure • Serious legal liability exposure • Environmental damage eligible for EPA National Priorities List	• Annual loss of $10>$25 million in current fiscal year • 5-year cumulative liability/obligation $100<150 million	• 10- to 14-day disruption of 2 or more Colleges, Schools, or Divisions or three or more critical services • Serious impact on efficiency, client/student programs and services, environmental sustainability, or infrastructure • Serious effect on leadership effectiveness	• Principal investigator debarred • Program funds rescinded • Long-term agency scrutiny • Enforcement action likely	Stops progress on more than one UVM strategic goal	• National negative publicity • Intense pressure for UVM to control the message • Significant damage to UVM's reputation/image
5	Severe	• Affects 51-75% of employees • Collective bargaining required • 16-24% employee turnover	• Severe injury or death • Self-insured workers' compensation injury/exposure • Severe legal liability exposure • Severe environmental damage eligible for EPA National Priorities List	• Annual loss of $25>$100 million in current fiscal year • 5-year cumulative liability/obligation $150<250 million	• 14-day to 3-month disruption of 2 or more Colleges, Schools, or Divisions or most critical services • Severe impact on efficiency, client/student programs and services, environmental sustainability, or infrastructure • Severe effect on leadership effectiveness	• Imposed settlement or corporate integrity agreement • Organizational criminal prosecution • Record financial judgment	Reverses progress on one or more UVM strategic goals	• National negative publicity • UVM cannot control the message • Severe, long-term damage to UVM's reputation/image
6	Business-Critical	• Affects >75% of employees • Collective bargaining required • >25% employee turnover	• Business-critical injury or death • Critical legal liability exposure • Major, irreparable environmental damage	• Annual loss of >$100 million in current fiscal year • 5-year cumulative liability/obligation >$250 million • Insolvency	• UVM shutdown >3 months • Insolvency • Leadership failure results in long-term damage to the institution	• Threatens viability of UVM or its research mission • Loss of all federal research or Title IV funds	University strategic plan failure	• Negative publicity could permanently impair UVM's image/reputation • Significant decrease in enrollment or research funding

Source: University of Vermont; Guide to Risk Assessment & Response; August 16, 2012; page 12

Effective Management is the Foundation

Plan

Organize

Direct

Control

Capabilities

Financial Management, Property Management, Portfolio Management, Change Management, Systems Management, Accounts Payable Management, Formal Management System, Enterprise Risk Management, ***…Enterprise Risk Management…..Cyber Risk Management***

Source: https://pixabay.com

Strive For Well-Managed

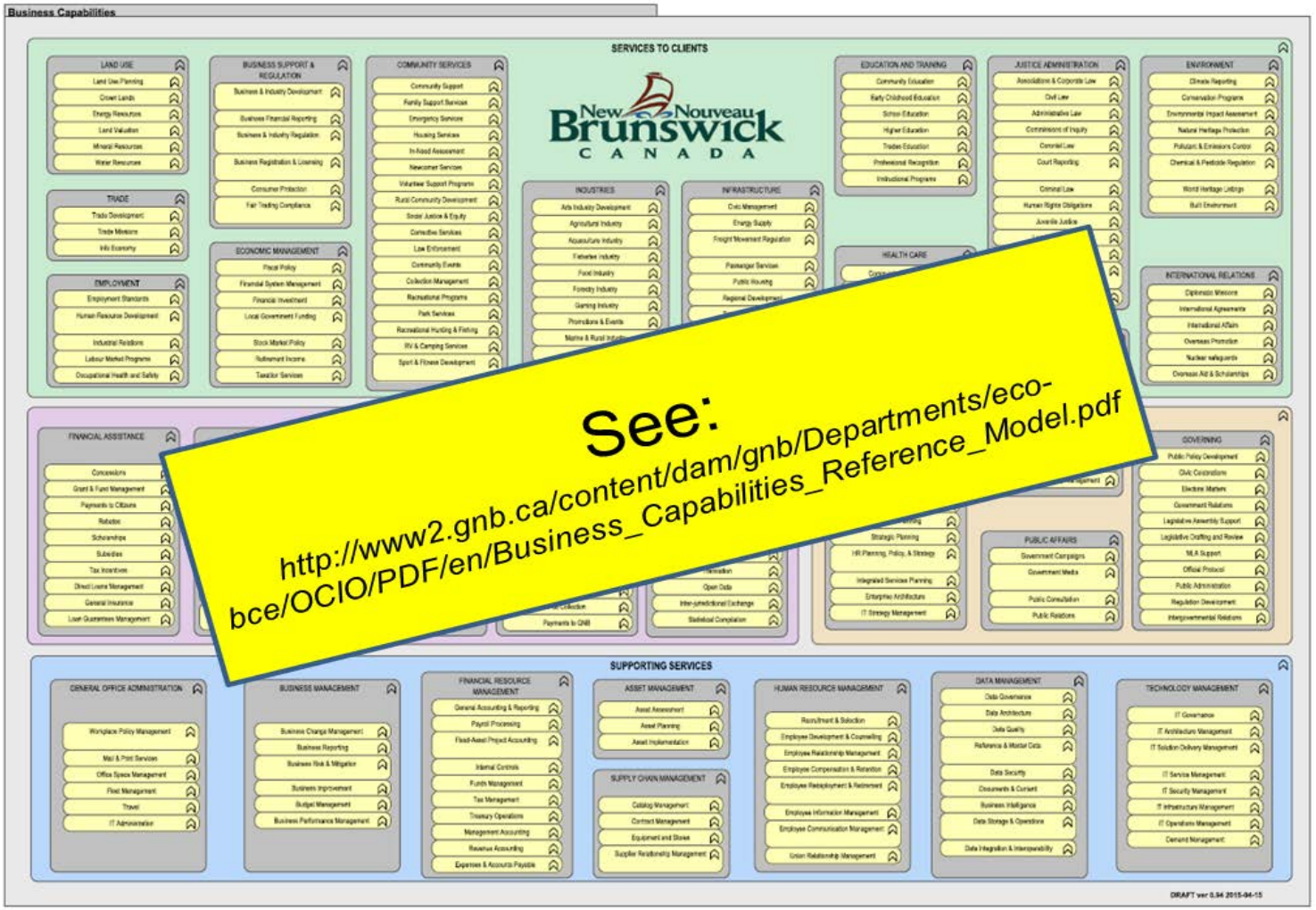
No magic wands required!

Source: https://pixabay.com

An Approach

1. Consider Perspectives
2. Research & Considerations
3. Scope
4. A Vision for ERM
5. Manage the Elements

Scope – Ideally Capabilities



See:
http://www2.gnb.ca/content/dam/gnb/Departments/eco-bce/OCIO/PDF/en/Business_Capabilities_Reference_Model.pdf

New Nouveau Brunswick

An Approach

1. Consider Perspectives
2. Research & Considerations
3. Scope
4. A Vision for ERM
5. Manage the Elements

Build The ERM Program Like Any Other Program

1. Strategy and Business Case
2. Required Policies & Directives
3. Awareness
4. Management System / Framework
5. Stabilize Team
6. Standardize Processes
7. Leverage Technology
8. Monitor Capability Maturity
9. Guides and User Manuals
10. Continuously Improve

ERM Build – Example Steps

Adopted from *Managing Risk in Government* [1]:

1. **Getting Started - examples**
   i. Complete ERM Build and Implementation Strategy
   ii. Develop a risk management framework (with lexicon)

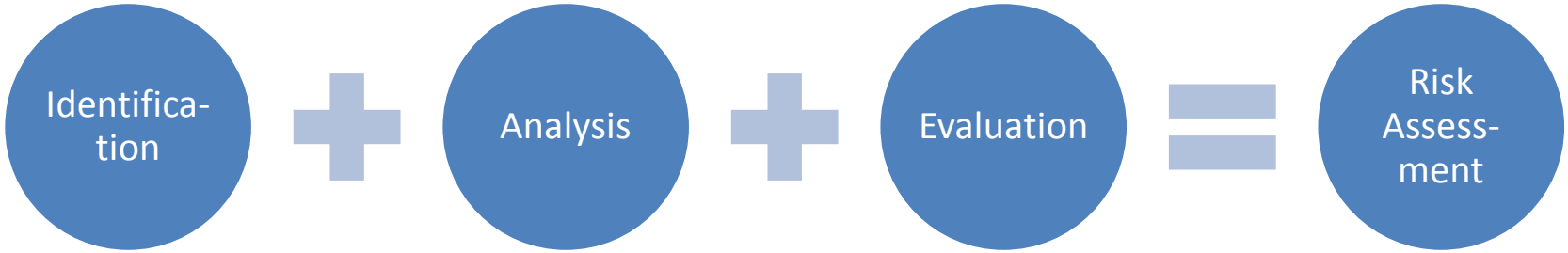
2. **Organizing for ERM - examples**
   i. Establish a Risk Office or ERM organization

3. **Operating an ERM Program - examples**
   i. Develop a policy that outlines the organization's expectations regarding the management of risks
   ii. Document the process and analysis so that it can be replicated

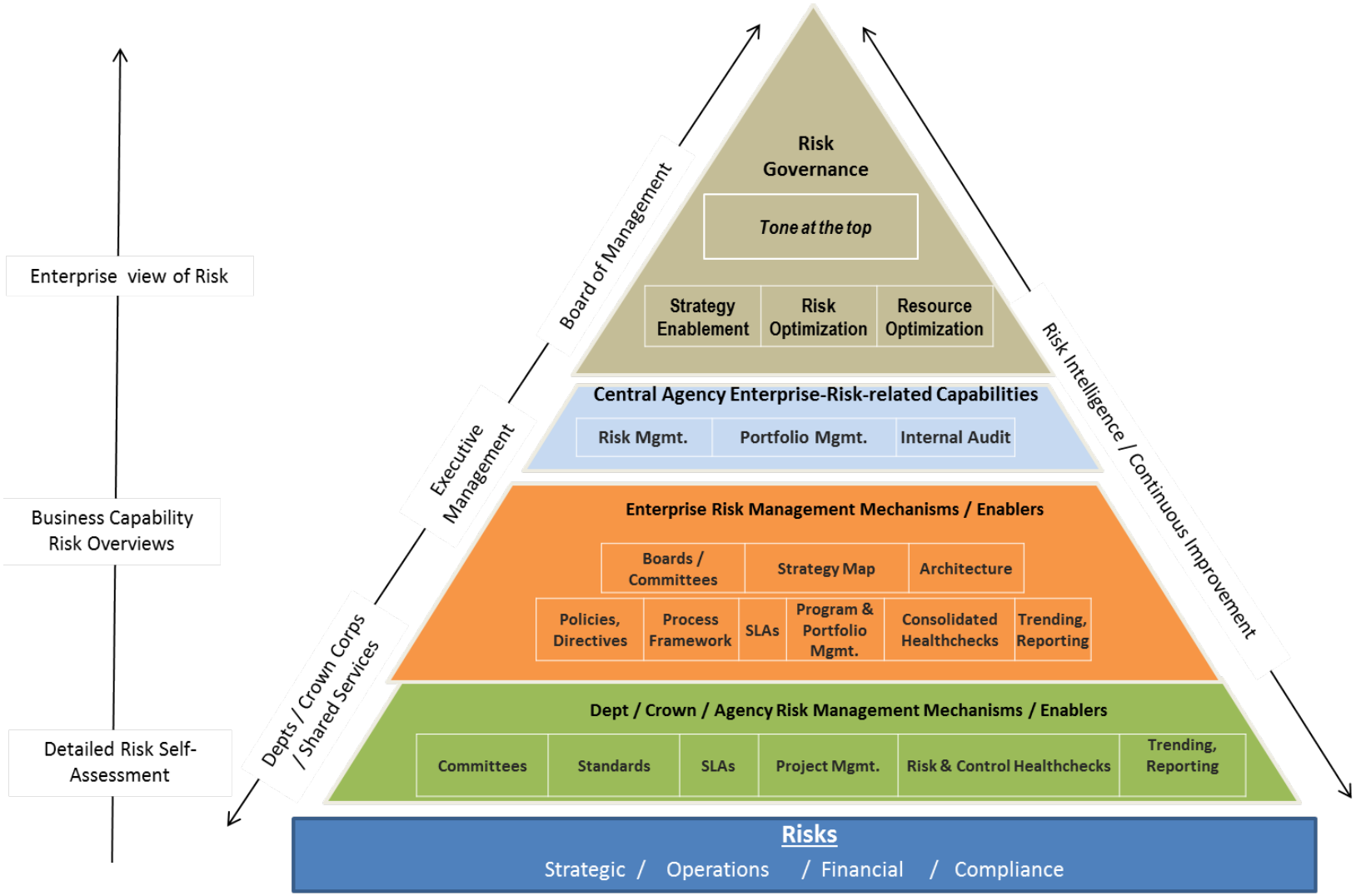
[1] *Dr, Karen Hardy, IBM Center for The Business of Government, Managing Risk in Government: An Introduction to Enterprise Risk Management, Financial Management Series, 2010, Second Edition.*

Risk Assessments → Decision Support

- Start with a question! What could go wrong (operations)?



ERM Provides Decision Support



Source: Rick Ouellette

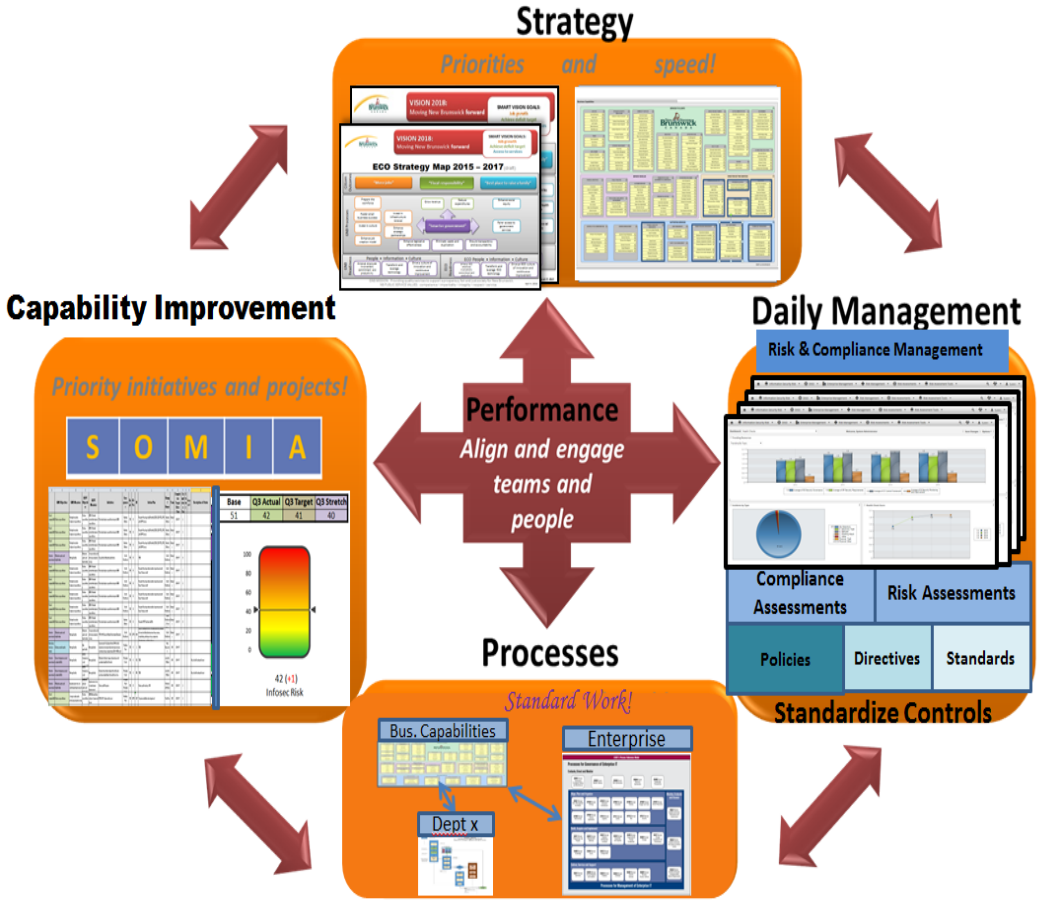
New Nouveau Brunswick

Management System

ISO/IEC 31000 – Risk Management

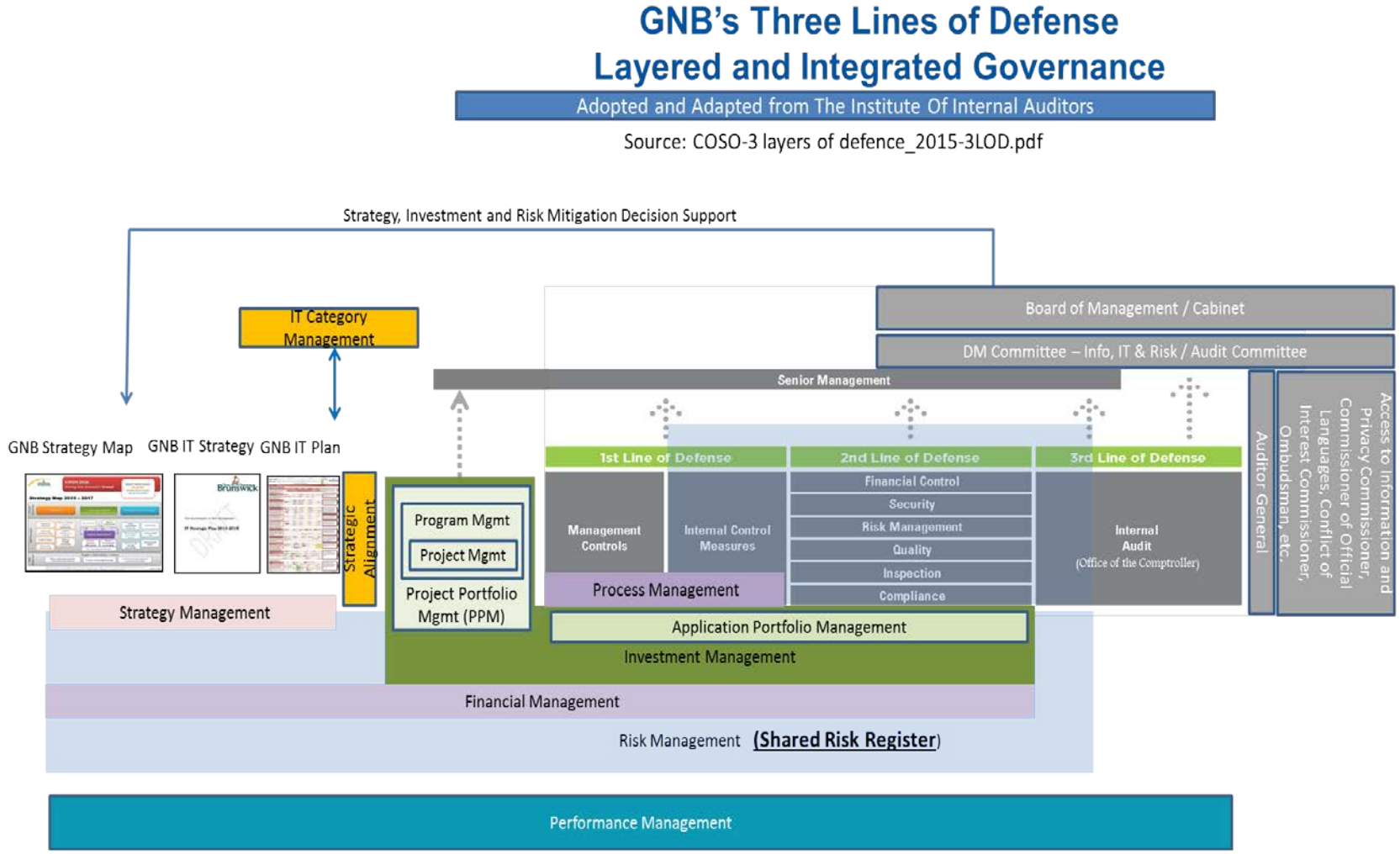
ISO/IEC 27001 - Information security management

Source – www.iso.org



New Nouveau Brunswick

GNB Conceptual Framework



1

Source: Rick Ouellette

An Approach

1. Consider Perspectives

2. Research & Considerations

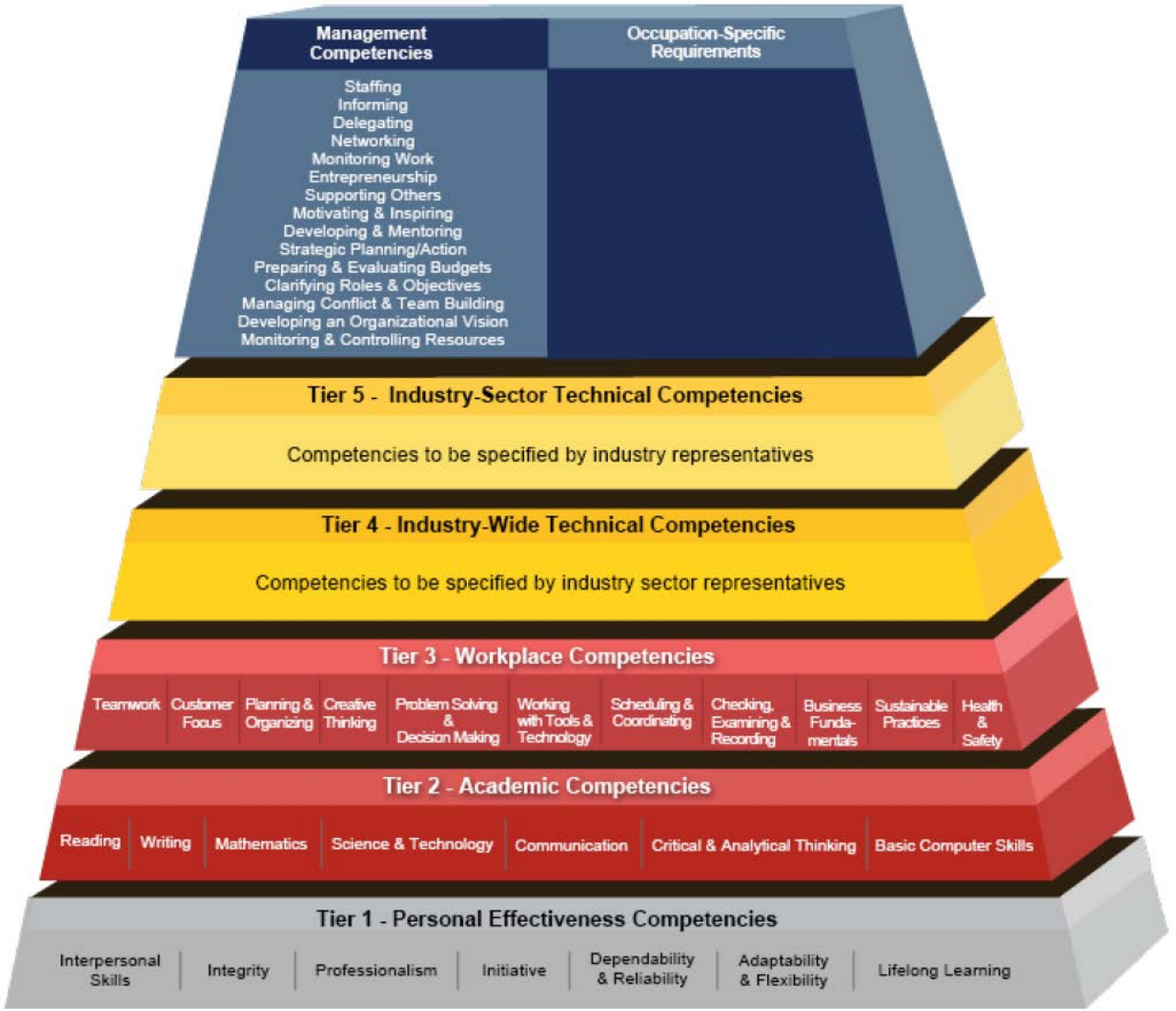
3. Scope

4. A Vision for ERM

5. Manage the Elements

ERM is a Business Capability

People



Source: https://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx

New Nouveau Brunswick

Process

Level 5
Well-Managed
(Optimizing)

Processes are performance managed towards continuous improvement.

Level 4
Managed

All in-scope processes standardized, documented, measured and controlled.

Level 3
Documented

Proactive approach; more processes standardized with enterprise approach.

Level 2
Repeatable

Processes reactively established with some measures; not disciplined.

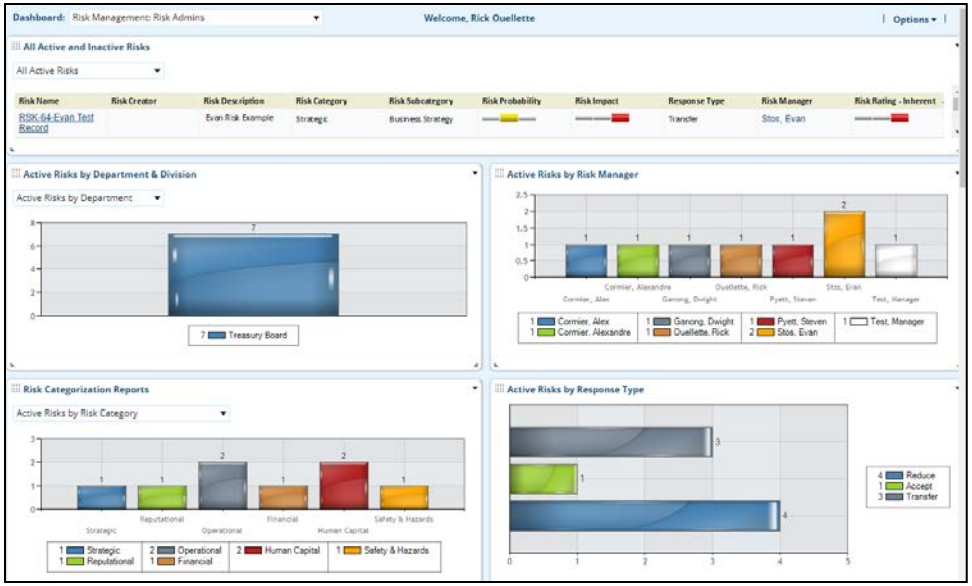
Level 1
Adhoc / Initial

Non-standardized unpredictable processes; success depends on heroes.

Resources: COBIT, ISO 27002

New Nouveau Brunswick

Technology



Risk Name	Risk Creator	Risk Description	Risk Category	Risk Subcategory	Risk Probability	Risk Impact	Response Type	Risk Manager	Risk Rating - Inherent
RSK-64-Evan Test Record	Tom	Evan Risk Example	Strategic	Business Strategy	Medium	High	Transfer	Larry	High
RSK-118-Failure of mission critical past warranty servers	Dick	A large portion of the infrastructure on which corporate solutions are housed are old and past warranty and could	Operational	IT Infrastructure	Medium	High	Reduce	Curly	High
RSK-119-Hazardous materials	Harry	Asbestos findings in some locations	Safety & Hazards	Enviornmental	High	High	Transfer	Mo	High
RSK-62-Evan Test Risk	Tom	This is an example risk.	Operational	IT systems and solutions	Medium	Medium	Reduce	Larry	Low
RSK-117-Enterprise Risk business disrpution	Dick	Lack of capability and capacity, including role redundancy, there is a risk that TB will not be able to provide	Human Capital	Resource capacity	High	Low	Reduce	Curly	Low
RSK-120-TEST Entry 192	Harry	This is a test entry	Financial	Capital managment	Medium	Low	Reduce	Mo	Low
RSK-121-TEST Risk Entry 085	Tom	This is a test entry	Human Capital	Employee skills and capability	Low	High	Accept	Larry	Low
RSK-122-TEST Risk Entry 457	Dick	This is a test entry	Reputational	External communications	Medium	Medium	Transfer	Curly	Low

Spreadsheet

ERM Solution

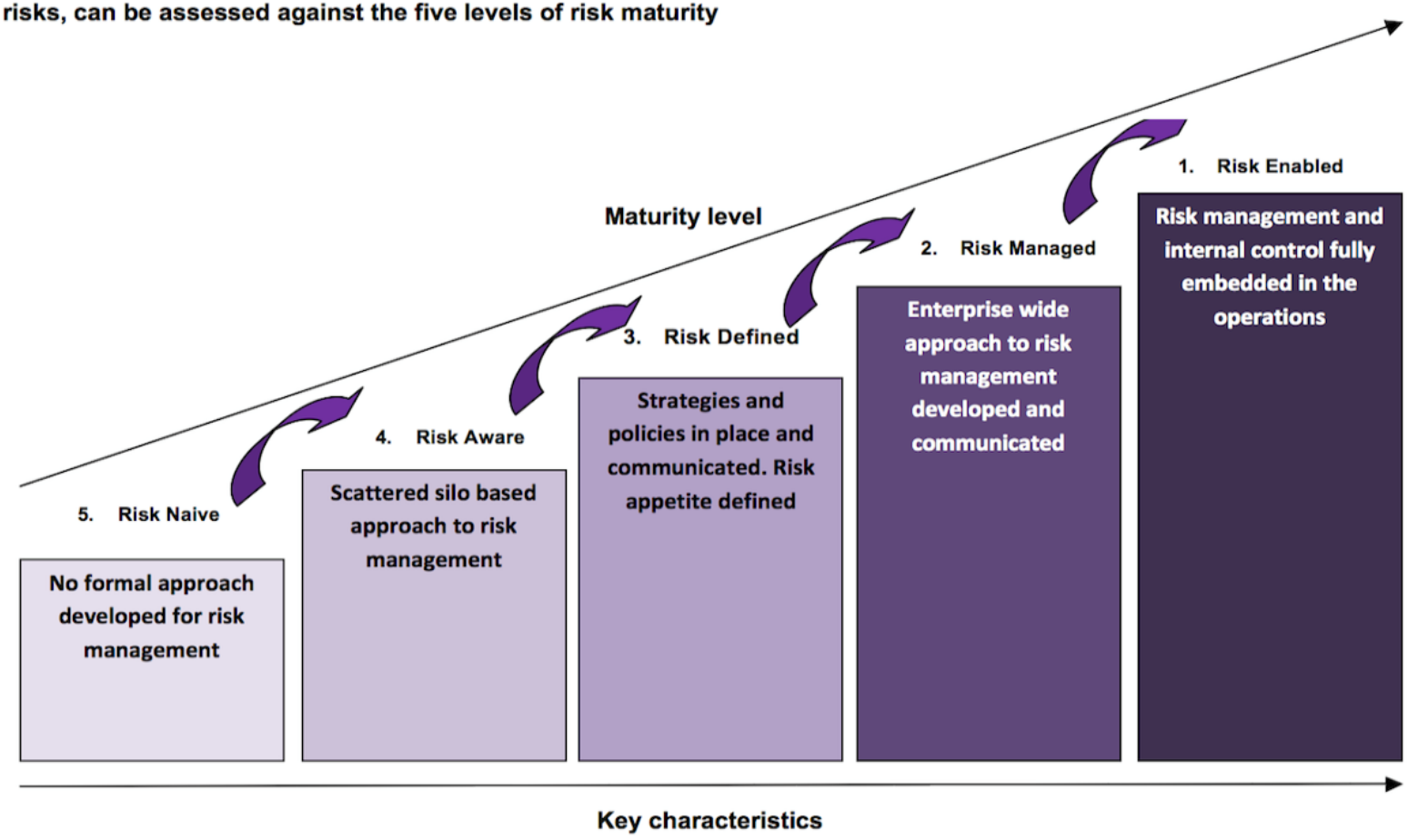
New Nouveau Brunswick

Information

Information ⇨ Intelligence ⇨ Decision Support

Risk Management Maturity Model

The effectiveness of a company's risk management system, in identifying and managing their principle business risks, can be assessed against the five levels of risk maturity



Source: http://www.grantthornton.lu/online/www/navMain/Advisory_Services/522/527/567/contentContainer/2262/710/ENG/RiskLevelsBig.png

New Nouveau Brunswick

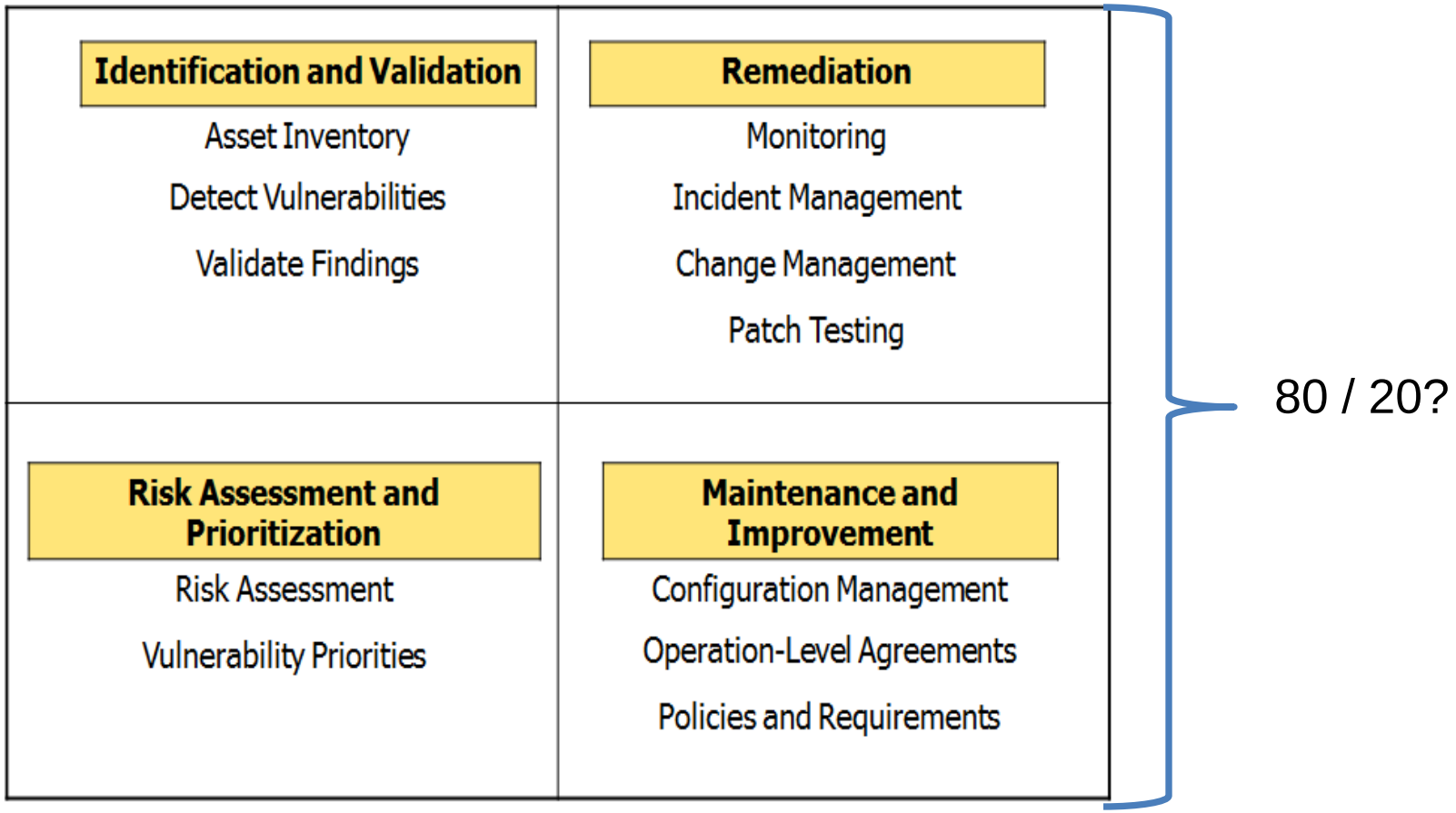
An Approach

Bonus Material ☺

6. Cyber Security Risk Management

Simple Math

Vulnerability Management Highlights



Source: IIA's Global Technology Audit Guide – Managing and Auditing IT, 2006

Vulnerability Management Performance

Identification and Validation

Low Performer

- Small % of IT assets are scanned and managed – or cannot measure what is being managed.
- Incomplete or limited network architecture diagrams.
- Inability to validate scanning results.
- Limited remediation or no remediation.
- No asset management system.
- High level of configuration variance.

High Performer

- Effective asset management.
- Know % of critical assets scanned and managed.
- Scans are validated and false positives are identified.

Source: IIA's Global Technology Audit Guide – Managing and Auditing IT, 2006

Citizen / Customer Perspective

Business-as-usual.

OpportunitiesNB
Built for Business

New Nouveau Brunswick

Thank you!