



GNB Treasury Board Enterprise Risk Management

- The likelihood of achieving desired business outcomes (GNB objectives) relies on managing the business-impacting negative effects of planned or unplanned unfortunate events (risks).
- Managing the business-impacting negative effects of planned or unplanned unfortunate events relies on risk management choices - accept, insure, defer, ignore, mitigate.
- On May 5th, 2016 GNB announced that Treasury Board will be establishing an Enterprise Risk Management (ERM) program.

- Establish an ERM Framework that:
 - Links to and supports the GNB Accountability Framework
 - Treasury Board monitors, evaluates, and directs; departments and agencies are responsible for their business risk
 - Driven by education, training, and awareness and enabled through standard processes and tools
 - Provides decision support to proposed senior-level Audit and / or Risk Committee
 - Contributes to the Balanced Scorecard
 - Aligns with the Internal Control—Integrated Framework of the Committee of Sponsoring Organizations of the Treadway Commission¹ (COSO)'s 3 Lines of Defense approach (see next slide)
 - Layered and Integrated

¹ – www.coso.org

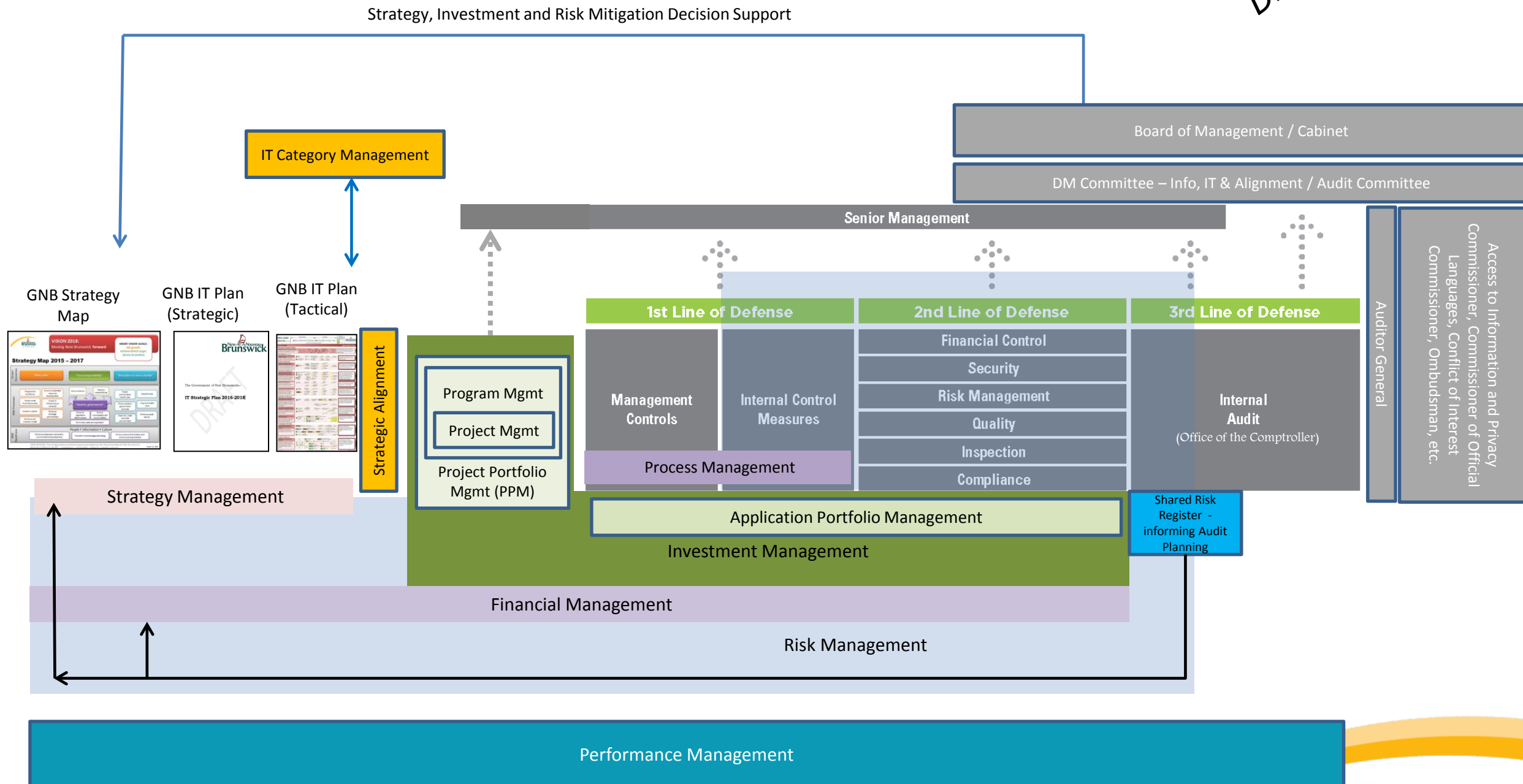
The Three Lines of Defense Layered and Integrated Governance

Adopted and Adapted from The Institute Of Internal Auditors

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



Draft

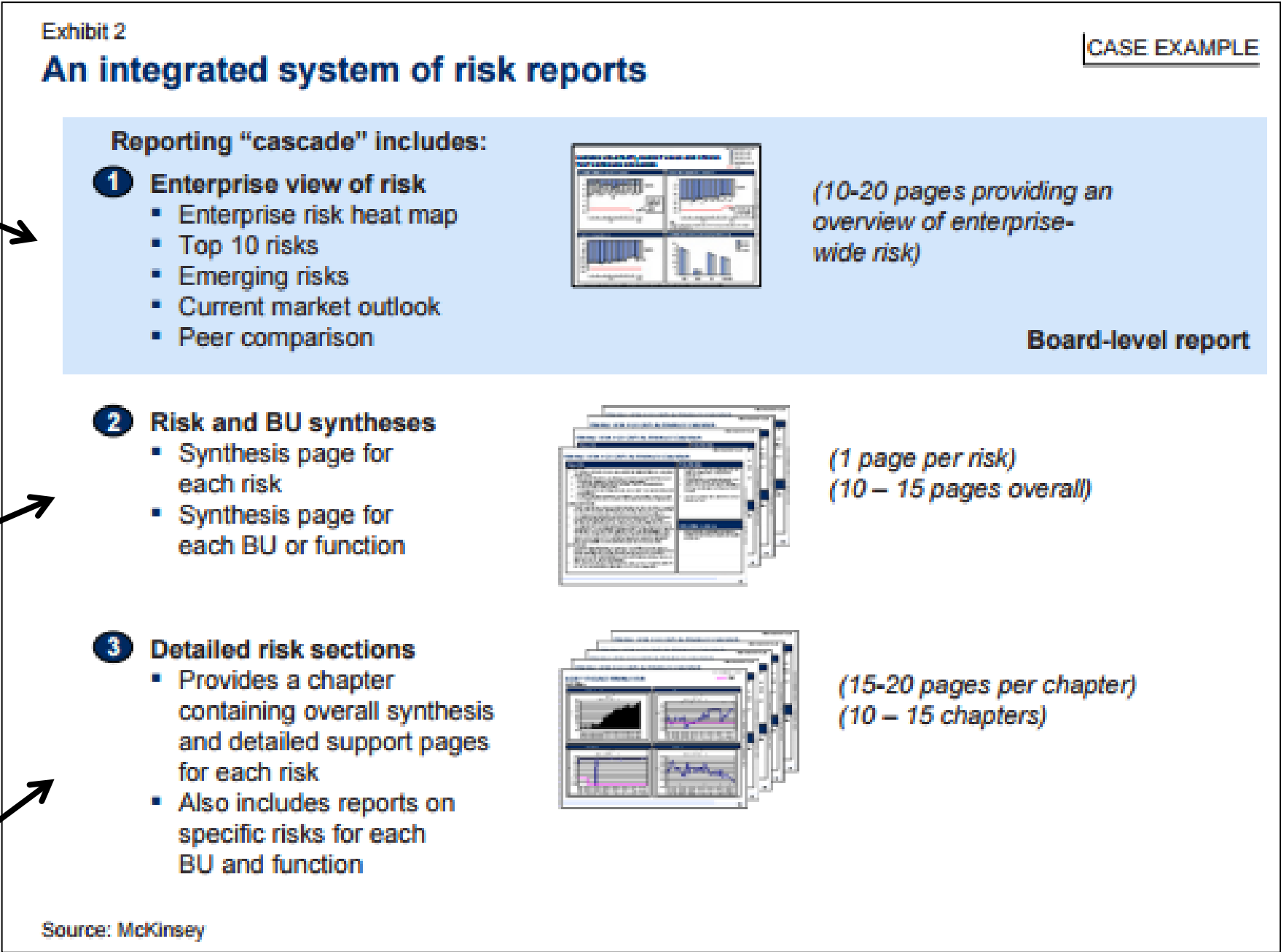


Layered and Integrated ERM Example (MED = Monitor, Evaluate, Direct)

Example: GNB-wide risk view for Board of Management via Treasury Board to consider decision support to MED GNB risk posture

Example: risk views for departments to MED risk posture,
OR
Risk views to MED for each function / capability such as IT Security, Business Continuity Planning, License and Permitting, Asset Management, Strategic Planning,

Example: views for detailed risk reports. MED specific risks such as flood risk, computer virus risks



Next Steps



Adopted from *Managing Risk in Government*¹:

1. Getting Started
 - i. Develop a risk management framework lexicon to ensure consistency of terminology across the organization
 - ii. Establish a communications plan and stick with it
 - iii. Support from senior leadership is critical to effectively identifying and addressing risks and opportunities
 - iv. Train your employees
2. Organizing for ERM
 - i. Establish a Risk Office or ERM organization
 - ii. Have a dedicated risk champion
 - iii. Head of the risk organization (risk champion) should be a member of executive management
 - iv. Establish and maintain executive-level support, ideally from the highest levels in the organization
3. Operating an ERM Program
 - 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
 - iii. Provide specific examples of risks tailored to the organization to help the learning process
 - iv. Reward risk identification, don't penalize it. *Note: this is the current approach with GNB IT Security.*
 - v. Engage those who manage risks, as well as areas with inherent risks, to develop analytical tools and recommendations
 - vi. Link risk training to business results where possible
 - vii. Seek diverse perspectives on issues, as they are critical to risk and opportunity management

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.



Appendix

Risk Management Framework and Process

Structural Framework

Process Overview

