McKinsey & Company

NASCA

Building a risk management approach for state government

December 3, 2019

Speaker introductions

Allan McVey

Secretary of Administration
State of West Virginia

Allan was appointed Secretary of the West Virginia Department of Administration in January 2019. He previously served as the West Virginia Insurance Commissioner. Allan has worked as a licensed insurance agent; Medical Claims Examiner with the West Virginia Workers' Compensation Fund; underwriter with a large national insurance company; and led sales and management of the West Virginia operations for a large national insurance brokerage firm.

Dan Williams

McKinsey & Co, Partner
Washington, D.C.

Dan is a leader in McKinsey's Risk Practice, advising public sector and financial institutions seeking to improve risk management and ensure regulatory compliance. Deploying comprehensive compliance assessments and stress tests, he helps organizations pursue large-scale transformations that address regulatory mandates while creating value. Dan draws on previous experience as a national bank examiner with the Office of the Comptroller of the Currency at the U.S. Department of Treasury.

Jay Truesdale

McKinsey & Co, Associate Partner
Boston, Massachusetts

Jay is a leader in McKinsey's Public Sector and Risk practices and a member of the McKinsey Center for Government. He has served clients on five continents on strategy development and risk management, with a focus on building crisis preparedness and response capabilities as well as addressing geopolitical risk. He has a combined 20+ years of prior experience serving as a U.S. diplomat and Navy officer, and was a 2019 NASCA Research Partner.

Contents

McKinsey & Company and NASCA partnered to offer the 2nd Annual Business of Running State Government Operations survey and report

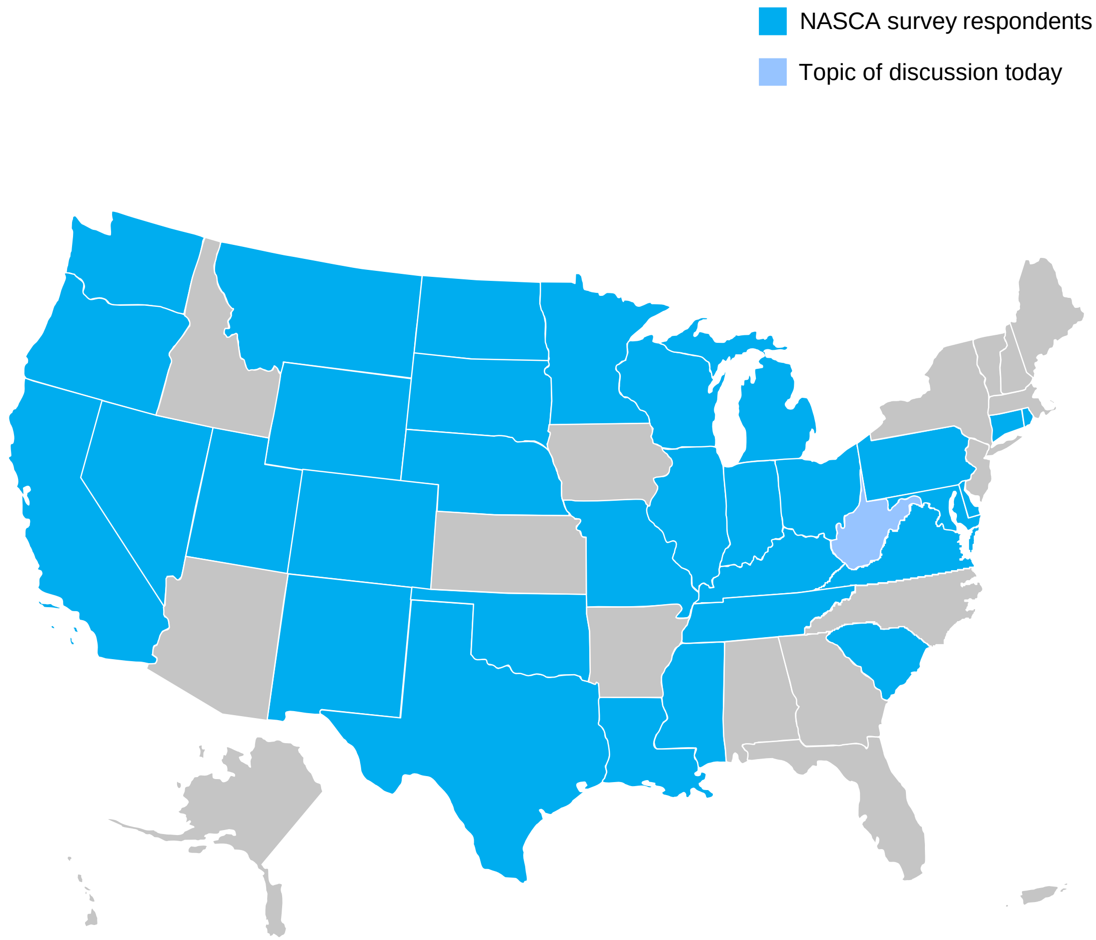
Purpose

- Provide government leaders with a robust set of data and insights to:
  - Compare each state's practices to peers
  - Inform forward-looking strategic decisions for state agencies

Methodology

- Survey NASCA member states to understand their priorities and best practices in selected topic areas
- Convene a working group of CAO members to provide analysis and insights
- Draw on McKinsey and NASCA knowledge and expertise to highlight best practices and action steps

33 states participated in the survey between May and July 2019



Survey Overview

Focus areas included three top priorities for CAOs:

- Digital Government
- Real Estate & Facilities Management
- **Risk Management**

There is a wide range of approaches to risk management, dependent on a state's governance structure and risk exposure

X % of states

4 most common *risk management* archetypes

Risk Owner

Centralized risk management authority

Regularly evaluate and update enterprise risk management strategy

Risk Responder

No central authority, each agency responsible for risk management

Risk evaluation by topic, no holistic review

Risk Collaborator

Centralized risk management authority

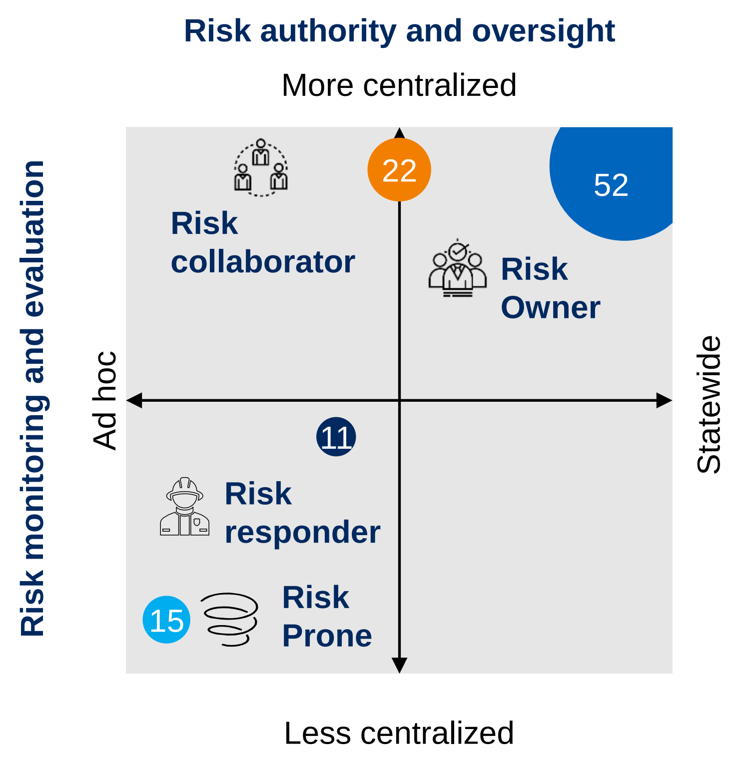
Risks evaluated at agency level, rather than across state

Risk Prone

No central risk management authority

No risk management strategy to be evaluated

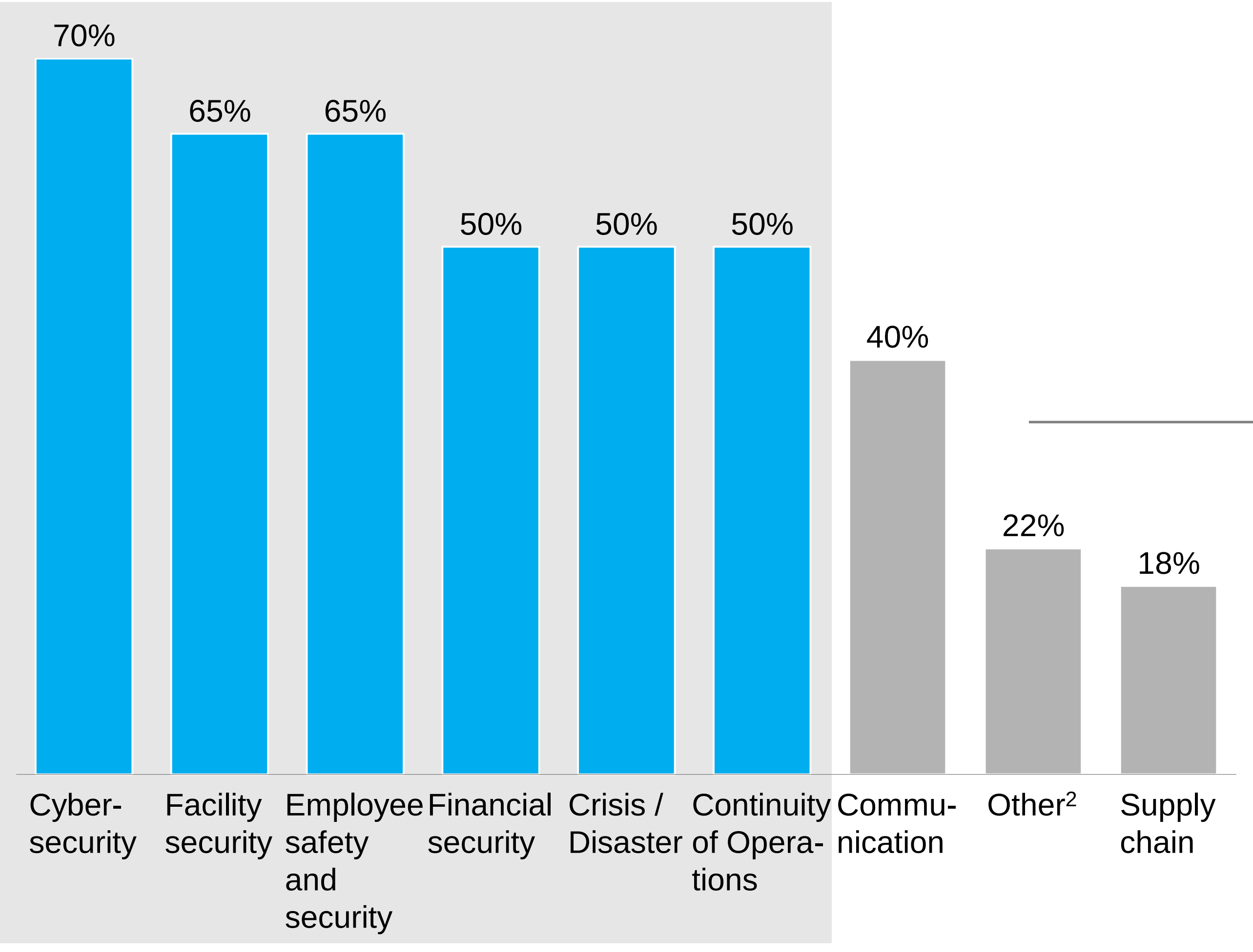
States should put in place a risk management strategy and ownership approach; "risk prone" states can begin by addressing overarching governance questions



CAOs are responsible for critical risk management topics, including cyber, facilities, employee safety and security, and crisis response

In majority of CAO portfolios

Percent of CAOs[1] responsible for risk management topic



Key observations:

- 1. Most states have not defined the **full taxonomy** of potential risks or prioritize those where the state has the **highest exposure and faces the greatest potential impact**
- 2. Many states have not designated an official responsible for overseeing risks; CAOs should consider **broadening risk management portfolios** or seeking the **appointment of a chief risk officer**
- 3. Where CAOs are not responsible for comprehensive risk oversight, they can do more to support fellow state leaders by **ensuring there is robust communication and coordination across agencies**

1. Count, n=27 2. Human resource and civil rights complaints, insurance contracts and claims, workers' compensation, etc.

Core take-aways on enterprise risk management for state leaders

- State should **strengthen enterprise risk management (ERM), rather than focus on "box checking" compliance or audit exercises**
- CAOs should find ways to **detect emerging risks and blind spots,** leveraging innovations in analytics before risks become full-blown crises
- **Addressing mindsets, behaviors, and other cultural factors is mission critical** for having robust risk management
- States can **strengthen muscle memory** to build situational awareness, anticipate the worst, and build capability for quick recovery
- No single state or city across the country has done risk management uniformly well – CAOs will need to **adopt best practices and lessons-learned from both public and private sectors**

Contents

West Virginia Code § 29-12-1 states in part:

"…good business and insurance practices and principles necessitate the centralization of responsibility for the purchase, control and supervision of insurance coverage on all state properties, activities and responsibilities and the cooperation and coordination of all state officials, departments and employees in the development and success of such centralized state insurance program."

West Virginia’s Board of Risk and Insurance Management (BRIM) provides centralized services for the state

Sixty years ago, the West Virginia Legislature recognized that centralized/shared services are best for certain specialized functions requiring specific knowledge and expertise.

It would be costly, inefficient, and not in the best interests of the state or its citizens for every agency to decide if it required insurance, types/coverages needed, appropriate contract terms, etc.

The focus of BRIM’s staff is to understand insurance markets, insurance products and services, and the most effective ways to minimize or transfer risk.

In the absence of BRIM's Centralized Services…

A "Patchwork" Approach to Insurance Products and Services

- Redundancy
- Inefficiency
- Higher cost
- Lack of predictability and budget stability
- Inability to effectively coordinate risk management "best practices"
- Legal uncertainty

BRIM is overseen by a Five Member Board

Board members must meet these qualifications

- Four members are appointed by the Governor and must be a West Virginia resident, and have experience in law, accounting, business, insurance, or actuarial science.
- The fifth member is the Vice Chancellor of Health Sciences of the WV Higher Education Policy Commission.
- The Insurance Commissioner serves without vote.

BRIM Staff

BRIM employs 26 people in the following areas

- Claims (7); Underwriting (5); Loss Control (5); Finance (4); Privacy Office (3); and Executive (2).
- Over half of BRIM staff have earned and maintain professional qualifications and appropriate certifications and licenses.
- BRIM employs a Chief Financial Officer and is independently audited annually.

BRIM's Insurance Program

BRIM Coverages

- Commercial General Liability
- Personal Injury Liability
- Professional Liability
- Stop Gap Liability
- Wrongful Act Liability
- Auto Liability (incl heavy equipment) and Physical Damage
- Cyber Liability
- BOE Excess Liability
- Aviation Coverage
- Statutory Bond
- Boiler & Machine Coverage
- First Party Property Coverage

BRIM's Insurance Program

- Some coverage is provided through "manuscript" policies, which are custom-designed by BRIM to best serve the state's needs.
- BRIM is often able to secure multiple-year pricing, saving money in the long run by controlling costs in markets experiencing cyclical fluctuation or responding to catastrophic weather events.
- Annual premium to fund each policy year is determined by independent actuaries.
- There is no unfunded liability in the program.

BRIM Insures State Agencies and “Senate Bill 3” Entities

- BRIM insures over 160 state agencies, boards, and commissions.
- BRIM insures over 950 entities in its Public Entities Insurance Program, commonly referred to as the “SB 3” program.

SB 3 Eligible Entities include

Political Subdivisions, Charitable Organizations, Public Service Organizations, and Emergency Medical Services Agencies

- Boards of Education
- County Commissions
- Cities and Towns
- Transit and Housing Authorities
- Volunteer Fire Departments
- For-Profit Ambulances
- Public Service Districts
- Solid Waste Authorities
- Not for Profit Health Clinics
- Public Defenders
- Other Not for Profit Entities

BRIM’s Underwriting Department

BRIM’s Underwriting Department works closely with independent actuaries to develop renewal premiums for our insured.

Premiums are allocated among BRIM insured after actuarial analysis of five-year claim loss data for each insured, exposure information provided by the insured, and consideration of administrative expenses.

Annual coverage renewal questionnaires

- Annually, our insured must update exposure information maintained by the Underwriting Department.
- Exposure information, used for renewal premium allocations and rating, includes:
  - General information, e.g. name, address, contacts
  - Vehicle exposures
  - Agency personnel, including officers and directors
  - Various liability exposures, e.g. fairs, carnivals, rodeos, patient encounters
  - Property structures and contents
  - Medical services by type of physician

Loss Control Department Mission

To provide BRIM's insured with tools to prevent or minimize claims through the following programs

- Loss Control Consultation Visits
- Property & Casualty Insurance Loss Prevention Inspections
- Boiler, Machinery & Air Conditioning Insurance and Inspection Services
- Standards of Participation Program
- Loss Control Education and Outreach Services

Loss Control Consultation Visits

- Areas of expertise include Fleet Management Programs, Employment Practices, Occupational Safety & Health Programs, Physical Hazard Inspection Programs, Boiler & Machinery Preventative Maintenance Programs, and Cyber Security/Privacy Issues.
- Outreach by BRIM's Loss Control Specialists establish effective two-way communication and positive business relationships.

Loss Control Education and Outreach Services

- Each year, BRIM partners with Liberty Mutual Insurance to provide two regional seminars to our insured on safety, operation and maintenance of boiler and air conditioning systems.
- BRIM's Loss Control Manager presents at meetings and seminars on topics related to safety and risk management, when requested.
- BRIM's Loss Control Specialists are certified OSHA General Industry Trainers.
- The Loss Control Department periodically sends notification to all insured on topics as needed, e.g. severe weather mitigation strategy, etc.

BRIM’s Standards of Participation Program

- BRIM manages a pro-active loss control “Standards of Participation” program applicable to all insured.
- The Standards are minimum risk management requirements intended to form a comprehensive approach to preventing losses and mitigating insurable loss and insurance costs.
- Every year BRIM audits 1,133 safety and loss control programs of our insured.
- Compliance with the Standards generates a credit (savings) on premium and non-compliance results in a surcharge (increase) to premiums.
- Credits and surcharges are applied to all lines of coverages.

Claim department staff

BRIM employs 5 licensed insurance adjusters

- One Claim Manager (32 years experience in private sector and government)
- One Asst. Claim Manager (40 years experience in private sector and government)
- Two claim specialists (combined 35 years experience in private sector and government)
- Total combined experience of Claim Staff in private sector insurance: 60 years
- Total combined experience of Claim Staff in government insurance: 52 years

What types of claims are handled by BRIM claim staff?

- Civil Rights Claims (e.g. employment, ADA, sex/gender discrimination, age, free speech, wrongful incarceration, etc.)
- Law Enforcement Claims (e.g. excessive force, wrongful arrest, etc.)
- Medical Malpractice Claims
- Motor Vehicle Claims
- Premises Liability Claims
- Sexual Assault/Abuse Claims

BRIM's financial plan

BRIM's financial plan has six primary objectives

- Fully fund all liabilities for its insurance programs.
- Ensure adequate working capital to minimize premium rate fluctuations from year to year for agencies' budget predictability.
- Maintain sufficient funds to fully support normal program operations.
- Maximize the overall return on investments within a conservative comprehensive investment policy.
- Maintain sufficient short-term liquidity to provide for unexpected or extraordinary cash flow needs.
- Meet or exceed key financial ratios.

All BRIM liabilities are fully funded

- Effective July 1, 2005, BRIM established an annual pre-funded trust program that covers liability claims for each policy year.
- Comprehensive rating model helps to insure recovery of program costs.
- Investment returns are anticipated to recover the cost of pre-funding the discounted liability claims within the trust and to help fund the cost of all claims paid outside the trust (i.e. property, cyber and mine subsidence).
- Annual pre-funding of the trust, a comprehensive rating model and investment returns work in concert to help maintain a positive net position within each program.

BRIM's Net Asset Reserve Policy

Why is the NAR important?

- An adequate level of net asset reserves provides funds to offset operating deficits resulting from unexpected events, economic uncertainties, and lean funding periods.
- It is critical for predictability of premiums and avoidance of large premium fluctuations from year to year.
  - **Budget predictability**

Contents

Risk identification and management: To develop a comprehensive risk strategy, it is important to consider risk elements across the organization

- **Potential to inadequately define organizational mission and scope** to meet the needs of constituents and legislative mandates

- **Potential for breakdown of critical physical or technological infrastructure**
- **Potential for process failure** that impacts organizational ability to deliver relevant services to constituents

- **Potential limitations to access, quality, and/or availability of data** necessary to execute organizational mission

- **Potential for extensive harm to human health and safety** for constituents, employees, or third parties

- **Potential susceptibility to internal and external cybersecurity threats**
- **Potential misuse of data**, including violations of data privacy for constituents, employees, or third parties

- **Potential for inappropriate behaviour** among employees or third parties
- **Potential inability to attract and retain talent** required for effective execution of organizational mission

- **Potential for inadequate financial management and planning for external economic factors** to impact organizational solvency, crisis preparedness, and payroll management

Risk identification and management: A tailored risk taxonomy helps classify known risks; it also provide structures for discussions of emerging risks

Level one (L1) risks	Associated level two (L2) risks	Examples of relevant level two risks
1 Strategic	1.1 Mission	Inadequate breadth of services provided to constituents
	1.2 Strategic planning	Lack of long-term innovation strategy
	1.3 Governance	Limited organizational structure, managerial alignment, policy setting/oversight
	1.4 Stewardship	Inappropriate management of public assets; lack of stakeholder accountability
2 Infrastructure and service delivery	2.1 Physical infrastructure	Failure of physical infrastructure and/or assets (e.g., highway or bridge breakdown)
	2.2 Technology infrastructure	Failure of technology systems and/or assets (e.g., cloud system breakdown)
	2.3 Process failure	Failure of processes critical to service delivery (e.g., transaction processing failure)
3 Health and safety	3.1 Human safety	Occurrences of violence, suicide, sexual assault among constituents, employees and/or third parties
	3.2 Health	Potential for epidemics / pandemics and/or mental health issues
	3.3 Emergency response	Inadequate response to natural disasters, severe weather events, terrorist attacks
4 Talent management	4.1 Conduct	Inappropriate or unethical behavior among employees and/or third parties
	4.2 Human capital	Lack of human capital/skills necessary for execution of organizational mission
	4.3 Diversity and inclusion	Inadequate diversity among staff and/or third parties (e.g., gender, race, age)
5 Financial management	5.1 Financial management	Inadequate cash management, audit, or accounting practices
	5.2 Fraud	Losses due to internal or external fraud, embezzlement, theft, conflicts of interest
	5.3 Funding	Exposure to tax volatility and source concentration
	5.4 Investment risk	Potential for asset misallocation and exposure to market risk
	5.5 Liquidity management	Unrestricted unreserved fund balance and/or inadequate contingency funds
	5.6 Debt, access to credit	Inadequate credit availability or employee liability management (e.g., pensions)
6 Information security risk	6.1 Cybersecurity	Violations of data security from internal and external threats
	6.2 Data misuse and privacy	Lack of appropriate data privacy policies and enforcement
7 Data risk	7.1 Data access	Lack of controls around access critical data (e.g., unauthorized access)
	7.2 Data quality	Inadequate data quality for execution needs (e.g., errors in data sources)
	7.3 Data availability	Limited availability of critical data (e.g., lack of visibility into underlying analyses)

Public sector organizations can leverage ERM building blocks to improve risk outcomes

		Description
Strategy and framework	**1 Vision and mission**	Mission and vision integrated with the company's overall strategy and business objectives, and provides the purpose of managing and overseeing operational risk
	2 Risk appetite	Cascading risk appetite framework across risk types, with defined escalation processes and breach protocols, qualitative and quantitative statements, metrics and thresholds
	3 Policies and procedures	Frameworks and policies to guide risk management and help create a common language about risk, e.g., risk lexicon and risk taxonomy
Processes	**4 Risk identification**	Processes for identifying risks; e.g., through use of RCSA, output from root cause analysis, review of external events, ongoing input from the front-line
	5 Measurement	Measurement of risk is completed with sufficient tools, subject to periodic review and validation (where appropriate)
	6 Monitoring and testing	Monitoring in place to ensure review of risk positions and exceptions; testing has specific objectives and requirements, and executed using a risk-based approach
	7 Remediation and continuous improvement	Processes for remediating gaps or for enhancing process and controls with approaches embedded in the first line for continuous improvement
Organization and governance	**8 Organization design and structure**	Organization design and structure consistent with the lines of defense, with consideration of stature of 1BLODs and SLODs units and leadership
	9 Roles and responsibilities across lines of defense	Detailed roles and responsibilities across the line of defense that supports risk ownership by the first line and effective risk oversight by the second line
	10 Committee structures and representation	Committee structures cover relevant risks across the organization, with business and risk representation to support decision making and ensure appropriate oversight
Capabilities	**11 Skills**	Required skills derived from a target operating model, team members assessed against target skills profiles for their positions, and portfolio of interventions available
	12 Capacity	Target capacity derived through the articulation of expected activities in the target operating model, capacity reviewed and challenged on a periodic basis
	13 Cultural mindsets and behaviors	Cultural mindsets and behaviors enable risk ownership, responsiveness, co-operation and challenge
	14 Process improvement	Program to catalogue, trace, dissect and diagnose core processes effectively, enable process improvement, and identify potential break points
	15 Technology, data and analytics	Technology infrastructure, data, analytics supporting each element of the framework
Operational risk outcomes		Reduction in risk exposure as observed through fewer operational risk incidents, lower dollar losses, lower severity scenario assessment results; enhanced business value through observable operating environment improvements (e.g., reduced rework, faster cycle times, better customer experience)

Contents