CCRO MEETING 1ST QUARTER, 2018

The Emera Compliance Risk Register, KRIs, and Related Audit Committee Reporting

Tom Birmingham – Emera Inc. VP, Compliance

Goals

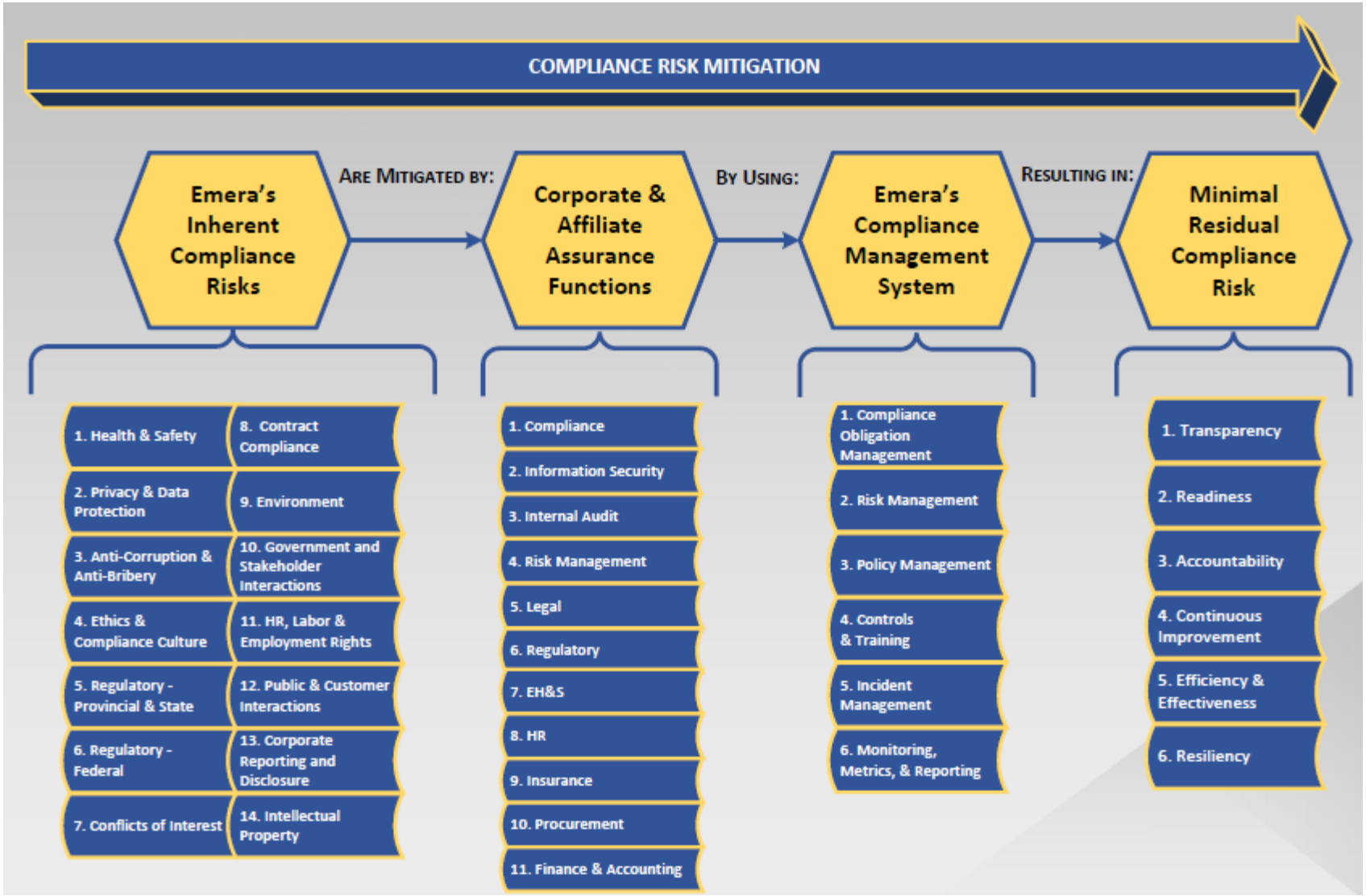
Discuss the following compliance risk management-related questions:

- What was the desired objective that caused Emera to develop a Compliance Risk Register?
- What does a "Compliance Risk Register" encompass at Emera? Who is involved?
- What does the Audit Committee expect from the Compliance Risk Report?

Agenda

Topic	Time
Overview of Emera's Compliance Management System	5 Minutes
Purpose & Scope of Emera's Compliance Risk Register	5 Minutes
Emera's Corporate Compliance Risk Register	5 Minutes
Audit Committee Expectations	10 Minutes
Challenges	5 Minutes
Next Steps	5 Minutes
CCRO Discussion Questions	10 Minutes

Overview of Emera's Compliance Management System



Purpose & Scope of Emera's Compliance Risk Register

PURPOSE:

1. Create a standard taxonomy of compliance risk terms to be shared across the enterprise
2. Establish a common framework for monitoring and reporting compliance risk to our respective corporate and affiliate leadership, Emera Inc.'s Audit Committee, and our affiliate boards, and
3. Develop a key component of our overall governance, risk and compliance (GRC) software platform initiative

SCOPE:

- Includes 14 Risk Areas and 85 Risk Sub-Areas
- Based on the nature of an international, combined electric (vertically integrated) and natural gas T&D utility

Emera's Corporate Compliance Risk Register

EMERA INC.	
CORPORATE COMPLIANCE RISK AREAS	**DESCRIPTION**
Anti-Corruption / Anti-Bribery	Non-compliance with applicable anti-corruption and anti-bribery laws and policies, including improperly sharing agent fees, bid rigging, or giving / receiving kickbacks and bribes
Conflicts of Interest	Non-compliance with applicable conflicts of interest laws and policies, including inappropriately giving or receiving gifts, favors & entertainment, or participating in inappropriate outside activities, employment, & community involvement that interferes with Emera's best interests
Contract Compliance	Non-compliance with applicable Contractor & Vendor laws and policies, including incorrectly following Emera's vendor approval process and other vendor management obligations and procedures
Corporate Reporting and Disclosure	Non-compliance with applicable corporate reporting and disclosure laws and policies, including maintaining inaccurate books and records, not properly reporting to external stakeholders, not properly disclosing material information, improperly issuing securities, inappropriate legal entity management, and not correctly fulfilling Emera's tax obligations
Environment	Non-compliance with applicable environmental laws and policies, including violating air, water, land, solid waste, or hazardous waste obligations
Ethics & Compliance Culture	Non-compliance with Emera's ethics and compliance culture-related policies and standards, including not following our Code of Conduct and related compliance program standards, not following our integrity program standards, not appropriately documenting our compliance with applicable laws and policies
Government and Stakeholder Interactions	Non-compliance with applicable government and stakeholder interactions laws and policies, including not correctly contracting with the government, not cooperating with government investigations, or not following lobbying, political, or charitable contributions requirements
Health & Safety	Non-compliance with applicable health & safety laws and policies, including violating industry and Emera Company occupational health and safety program standards as well as our health and safety culture standards
HR, Labour & Employee Rights	Non-compliance with applicable HR, labor & employee laws and policies, including those related to outsourcing, disabilities, discrimination, drugs & alcohol use, benefits, discipline, pay & timekeeping, harassment, immigration, leave, retaliation, smoking & tobacco, and background checks
Intellectual Property	Non-compliance with applicable intellectual property laws and policies, including the inappropriate use of patented, trademarked, and/or licensed goods and services
Privacy & Data Protection	Non-compliance with applicable privacy and data protection laws and policies, including those related to credit card payments as well as the appropriate management, notification, choice & consent, collection, use, retention & disposal, access, disclosure, security, quality, monitoring & enforcement, data loss & breach response, and the export of data
Public & Customer Interactions	Non-compliance with applicable laws and policies governing Emera's interactions with the public and our customers, including inappropriate outreach and use of credit reports as well as unauthorized or inappropriate responses to media, public inquiries, and social media
Regulatory - Federal	Non-compliance with Emera's applicable federal regulations, including those governing our affiliate code & standards of conduct, electric & gas wholesale operations as well as the issuance of notifications & reports, and management of our records, wholesale rates, tariffs & market rules
Regulatory - Provincial & State	Non-compliance with Emera's applicable provincial and state regulations, including those governing our affiliate code & standards of conduct, electric & gas retail operations as well as the issuance of notifications & reports, and management of our records, retail rates, tariffs & market rules

Audit Committee Expectations

Emera's Audit Committee expects the following four areas to be addressed in our Quarterly and Annual Chief Compliance Officer (CCO) Compliance Reports:

1. Maturity scores by compliance program
2. Status of compliance program activities
3. Material non-compliance incidents and corrective actions, and
4. Compliance risk ratings*

* We are proposing that our ethics & compliance risk ratings include:

1. Program Inherent Risk Score:
   - Operational Profile relative to *Emera's Compliance Risk Register*
   - Percentage of new or changing obligations
   - Significance/Impact of Organizational Change
   - Historical Program Performance
2. Program Residual Risk Score:
   - Instances of Confirmed Non-Compliance
   - Instances of repeat Confirmed Non-Compliance
   - Controls Environment Effectiveness (Evaluation & Monitoring Results)

**See also Slide 10 for a description of Emera's evolving Ethics and Compliance Risk Rating Method, and Slide 13 for sample Likelihood and Impact factors used to assess Emera's transmission pipeline safety risk.

Audit Committee Expectations, Cont'd.

Program Reporting Framework

PROGRAM MATURITY: Does the Company have a formal risk management program in place? If yes, how mature is it?

- A mature risk management program does the following over time:
  1. Keeps track of applicable legal, regulatory and contractual obligations;
  2. Identifies, assesses and mitigates financial, reputational, operational and compliance risks;
  3. Ensures its policies and procedures are fit for purpose;
  4. Periodically tests business activities to ensure compliance with controls;
  5. Identifies, escalates and mitigates non-compliance incidents and areas of concern; and
  6. Monitors, measures and reports on risks as well as program maturity, activities, incidents & corrective actions.
- SAMPLE BOARD REPORTS*: Risk Management Program Maturity Reports

PROGRAM ACTIVITIES: What is the Company's work plan to improve its risk management program? What is the status of this plan?

- Risk management program work plans should (1) focus on high-risk areas, (2) generally correlate the amount of effort to the level of risk, and (3) the status of these plans should be tracked and reported
- SAMPLE BOARD REPORTS*: Risk Management Activity Status Reports

INCIDENTS & CORRECTIVE ACTIONS: What is the Company doing to identify, assess and address non-compliance incidents, near misses and policy exceptions?

- Management should have a clear line of site to when non-compliance incidents occur (or areas of concern and policy exceptions are identified), and a means to ensure all incidents, areas of concern and policy exceptions are properly addressed
- SAMPLE BOARD REPORTS*: Incident Reports; Corrective Action Status Reports; Policy Exception Reports

RISK ASSESSMENT & PERFORMANCE: Does the Company have a means to assess risk (i.e., Key Risk Indicators or KRIs), and ensure its risk management activities are effectively mitigating the targeted risks (Key Performance Indicators or KPIs)?

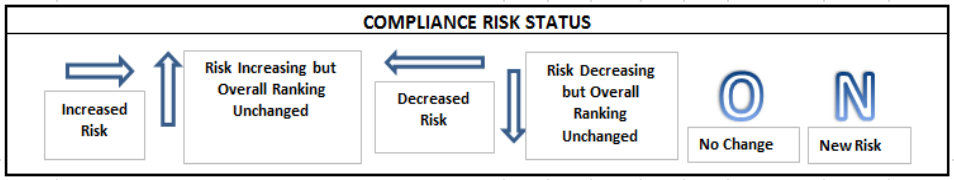
- Management should be able to measure changes in compliance risk over time
- SAMPLE BOARD REPORTS*: Compliance Risk Dashboards; Compliance Risk Reports; KRI & KPI Reports

Emera

ILLUSTRATION

Audit Committee Expectations, Cont'd.

Emera Audit Committee Compliance Report – Privacy & Data Protection Risk



COMPLIANCE MATURITY SCALE	
1	Fragmented / As Needed
2	Foundational / Reactive
3	Evolving / Managed
4	Technology Enhanced
5	Scalable /Predictive / Strategic

COMPLIANCE INITIATIVE FOCUS	
L	Low: < 5% of Compliance Time
M	Med.: >5% - <15% of Compliance Time
H	High: >15% of Compliance Time

		RISK RATING				MATURITY	FOCUS	
RANK	COMPLIANCE RISK AREA	LOW		MED	HIGH	SCORE		COMMENTS
X	**Privacy & Data Protection** Non-compliance with applicable privacy and data protection laws and policies, including those related to credit card payments as well as the appropriate management, notification, choice & consent, collection, use, retention & disposal, access, disclosure, security, quality, monitoring & enforcement, data loss & breach response, and the export of data Emera Corp. Owner(s): CL&CO; CIO Affiliate Owner(s): Customer Care, HR, Compliance, Legal and/or IT Leads				N	3	H	• Risk "High" due to high likelihood (i.e., describe leading / lagging indicators), and high impact (i.e., describe material risks). • Maturity "Evolving/Managed" due to ... (describe current compliance programming activities against a maturity scale). • Focus "High" for ... (list impacted functions/departments) due to ... (describe reasons). **Corporate Compliance Initiatives** • PCI STANDARDS - Affiliate W: Completed Supplemental Gap Analysis Report, which confirmed remaining gaps to be completed at Customer Care Center as well as provided options, costs and benefits, and recommendations. Focus turning to remaining policy and procedural documentation gaps, broader training needs, and audit testing requirements; ON-GOING. • PCI STANDARDS - Affiliate X: Supplemental Gap Analysis underway with same outcomes planned as Affiliaite W's Report; Focus on Customer Care Center, local payment centers, and field collection agents; Focus remains on closing compliance gaps; ON-GOING. • DATA PRIVACY - Affiliaite Y: Completed Privacy Risk Assessment Report, which identified top 10 inherent and residual risks, including training, incident & breach response, and data inventory and transfer risks; Key activities for Q1 & Q2 2018 being developed in response to this Report; Implementation of other Work Plan items continues; ON-GOING. • DATA PRIVACY - Affiliaite Z: Initiation of Phase 2 of the Data Privacy Work Plan; PLANNED FOR 2018. • CYBERSECURITY INITIATIVES: Continued coordination among IT, cybersecurity, and privacy compliance initiatives; ON-GOING.

Audit Committee Expectations, Cont'd.

Ethics & Compliance Risk Rating Method

Impact

- The affect (financial, reputational, or other impact) on an Emera Company or Companies if the risk occurs
- May also consider:
  1. The ability of an Emera Company to manage the consequences of the risk, and
  2. The extent to which this event would disrupt normal operating activities
- Utilize E&Y's materiality thresholds to help determine the severity of the impact to a given Emera Company
  - i.e., (1) Insignificant, (2) Minor, (3) Moderate, (4) Major / Material, or (5) Catastrophic

Likelihood

- The probability that the risk will occur at an Emera Company
- Generally, the more frequently an event is anticipated to occur, the more urgent the attention is required to mitigate its occurrence
  - i.e., (1) Rare, (2) Unlikely, (3) Moderate, (4) Likely, (5) Almost Certain
- May also consider:
  1. The controls and mitigating activities in place
  2. The anticipated frequency of the event occurring
  3. The working environment
  4. History of previous events

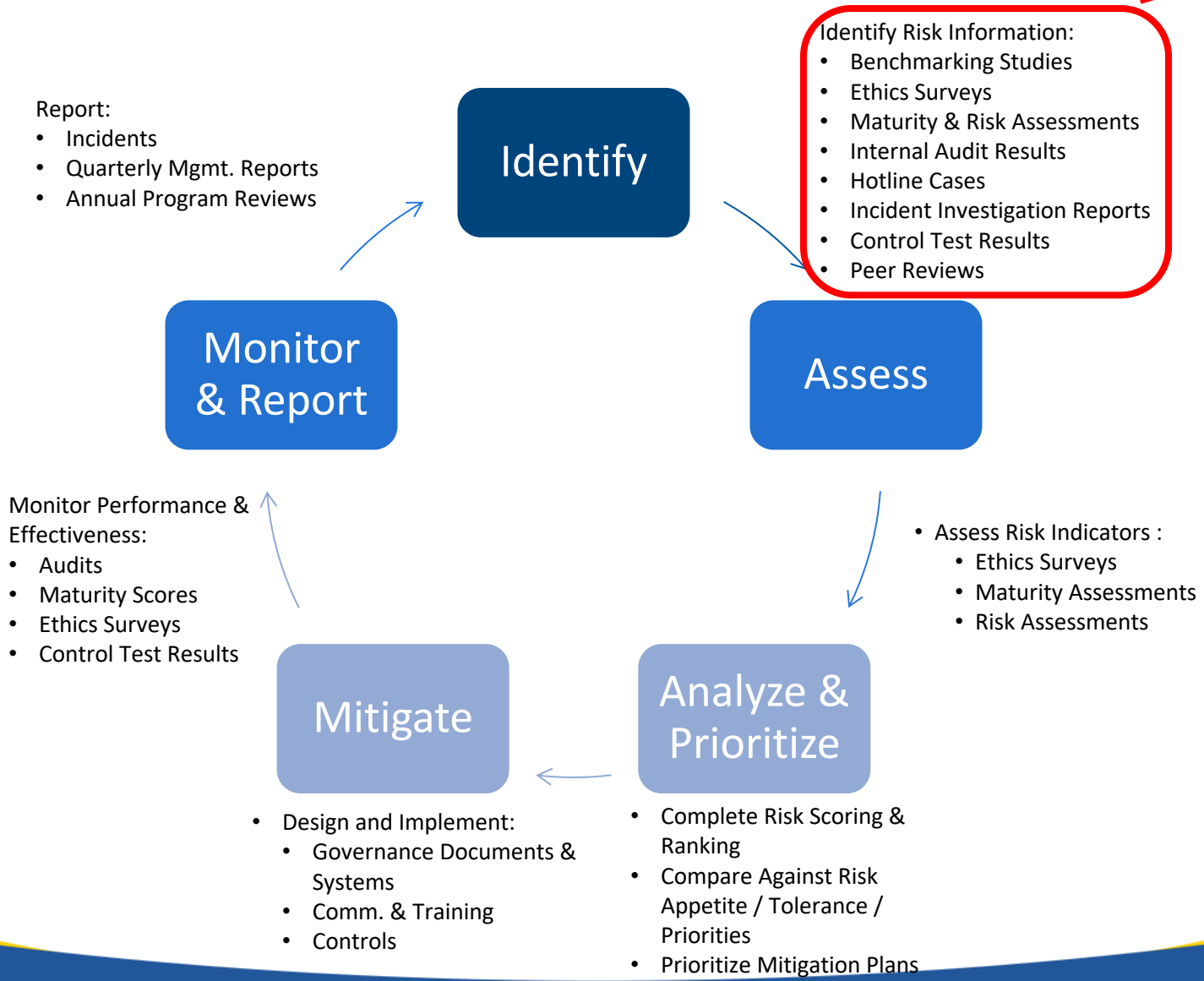
Control Effectiveness

- Controls include people, processes and technology put in place to help reduce the likelihood of a risk occurring

E&C Risk Management Life-Cycle

Other Risk Data We're Considering

Our approach to managing ethics and compliance risks:

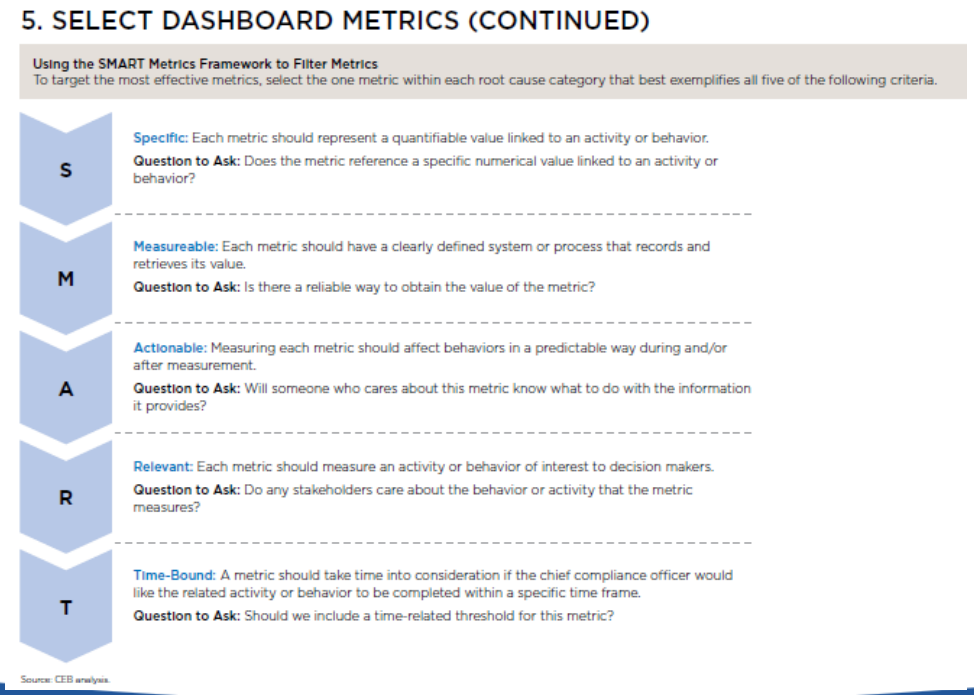


Emera

Building KRIs and KPIs

Selection Criteria

- Focus on the most important risks (according to the risk assessment)
- Give special consideration to those risks that can change quickly
- Pick KRIs & KPIs that do not require a significant resource investment to monitor
- Attach a threshold to each metric that triggers corrective action when breached
- Make sure the metric is easily understandable
- Determine if there is available benchmark data for comparative purposes
- Be able to link metrics to your critical risk areas on your heat map
- Keep it S.M.A.R.T.



Emera

Natural Gas Transmission Integrity Management Program (TIMP)

Risk of Failure = Likelihood of Failure * Consequence of Failure

Consequence of Failure is a function of :

- Pipeline pressure
- Impact on the business (i.e., loss of a single pipeline feed)
- Impact on the environment (i.e., sensitive environmental area, major waterway, minor waterway, wetlands)
- Impact on Population (i.e., Proximity to population centers, road crossings)

Likelihood of Failure is a function of:

- 3rd Party Damage
- External Corrosion
- Weather & Outside Forces
- Equipment
- Construction
- Incorrect Operations
- Internal Corrosion
- Manufacturing
- Pipe Type, Coating Type, Age & Leak Rates

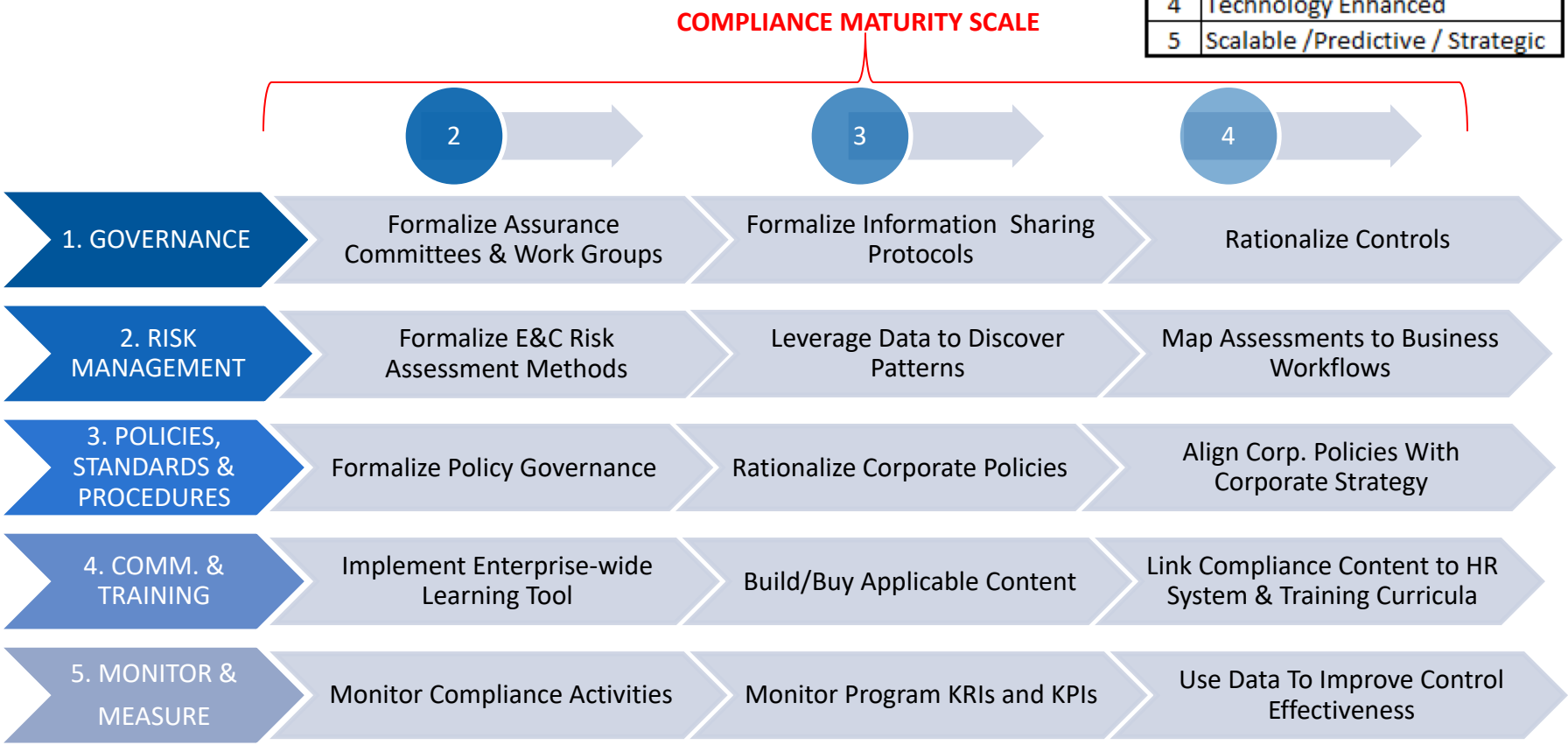
Challenges

- What have been the primary challenges to developing Emera's Compliance Risk Register?
  - Determining which categories to pick and why, and
  - How to organize and define all of the sub-areas in a way that made sense
- What have been the primary challenges presenting the CCO Reports to the Audit Committee?
  - Striking a balance between too much and too little detail, and
  - Addressing affiliate-level information
- Does all management support this process as valuable? Any resistance?
  - There was some confusion about the difference between strategic risks captured as part of our ERM process and compliance risks
  - Still need to roll this reporting structure out to Emera's affiliates
  - Requires certain data to be captured and reported that has not previously been done

Next Steps

Move our current maturity scores from 2s to 3s to 4s in the following five areas over the next 3-5 years:

COMPLIANCE MATURITY SCALE	
1	Fragmented / As Needed
2	Foundational / Reactive
3	Evolving / Managed
4	Technology Enhanced
5	Scalable /Predictive / Strategic



Emera

CCRO Discussion Questions

1. What are appropriate / manageable Key Performance Indicators (KPIs) we should use to reasonably inform our affiliate leaders as well as affiliate and corporate boards on the status of our compliance risk?
2. How have you been able to demonstrate the value of your ERM monitoring and reporting process?
3. How can we transfer that success to compliance risk monitoring and reporting?
4. What techniques have members used to consolidate ERM risk scores across multiple business functions and/or affiliates?
5. What ERM monitoring and reporting lessons have members learned that may be transferable to compliance risk monitoring and reporting?