MARCH 29TH 2019

Fast, Cheap, and Under Control:
Strategies for Measuring and Reporting Compliance Program Performance in an Era of Stretched Resources and Low Attention Spans

---

Agenda

- Introductions & Learning Objectives (5 Minutes)
- Overview of Emera's Operations (2 Minutes)
- Measuring and Reporting Compliance Program Performance From A:
  - Strategic Perspective (15 Minutes)
  - Design Perspective (15 Minutes)
  - Implementation Perspective (5 Minutes)
  - Key Take Always & Lessons Learned (5 Minutes)
- Q&A

Introductions & Learning Objectives

Introductions:

- Tom Birmingham, VP, Corporate Compliance – Emera Inc.
- Adam Padgett, Manager, Corporate Compliance – Emera Inc.

Learning Objectives:

1. Share our recent experience around the development and implementation of a new way to measure and report compliance program performance
2. Improve your understanding of some potential ways to cost-effectively measure and report compliance program performance across a large, multi-jurisdictional company

3

Emera

Overview of Emera's Operations

Headquarters: Halifax, Nova Scotia - Canada
Revenue: 6.23 billion CAD (2017)
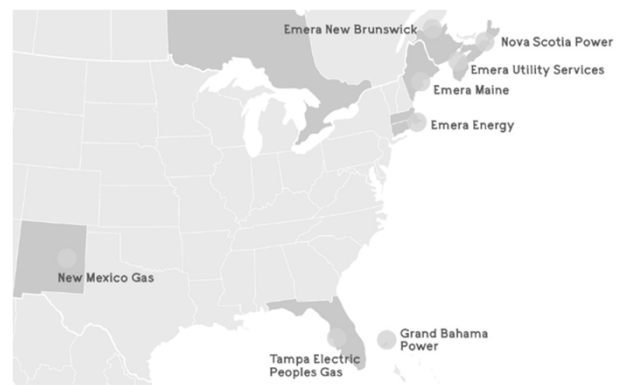Number of employees: 7,400 (2018)
Total assets: 28.8 billion CAD (2017)

Includes of the following major subsidiaries:

<u>Electric Utilities</u>
- Nova Scotia Power (500,000 customers)
- Tampa Electric (725,000 customers)
- Emera Maine (130,000 customers)
- Emera Caribbean (227,000 customers)

<u>Natural Gas Utilities</u>
- New Mexico Gas (513,000 customers)
- Peoples Gas (365,000 customers)

4

Emera

STRATEGY – Tom Birmingham (15 Minutes)

Our goal: Answer the following two questions:

1. Are we compliant?
2. How do we know?

Our objectives:

1. Develop and implement better tools and techniques to measure and report compliance program performance data within & across our affiliated companies
2. Spend less time capturing, formatting, and disseminating this data and more time analyzing it
3. Improve how we use this data to mitigate our compliance risks across our companies

5

Emera

Poll Question #1

- Pick the below activity that you are most interested in learning more about during today's presentation:
    - Developing ways to measure and report compliance program performance
    - Designing tools and techniques to capture compliance program performance data
    - Capturing, formatting and disseminating compliance program performance data
    - Analyzing and interpreting compliance program performance data
    - Improving how we use compliance program performance data to mitigate compliance

6

Emera

Scope, Metrics, Standards, Process & Tools

The steps we took:

1. Determined our **scope** – both in terms of (1) the most important compliance risks we are trying to mitigate, and (2) the perspective we should take (i.e., start at the program-level or "macro" perspective and eventually work toward the requirement/control-level or "micro" perspective)
   - See Slides 8 & 9

2. Established our **metrics** – the best way for us to demonstrate compliance (i.e., key performance indicators or KPIs)
   - See Slide 10

3. Defined our **standards** - what success looks like against these KPIs
   - See Slides 11 - 13

4. Established our **process & assessment tools** – how we capture, analyze and report on our KPIs given our current assessment tools
   - See Slide 14

Emera

Scope – Compliance Risk Areas

The following table provides a list of Emera's Corporate Compliance Risk Areas

1	Anti-Corruption & Government Relations
2	Ethics & Compliance Culture
3	Labor & Employment
4	Legal & Contract Management
5	Privacy & Data Protection
6	Public & Customer Interactions
7	Regulatory
8	Third-Party Management

Emera

Scope – KPIs

The following outlines the two different perspectives we considered when discussing which compliance metrics we wanted to start with first*

- The "macro" or compliance program-level perspective
  - Measure changes in FERC, CFTC, NERC, cyber security, contract management compliance program risk & maturity scores over time
  - This approach generally relies on interviews, survey results, certifications and program-level documentation to establish compliance
  - Example 1 - Reduce the likelihood and impact of a given compliance risk from occurring
  - Example 2 - Increase the level of program maturity over time against an established standard(s)

- The "micro" or requirements / control-level perspective
  - Test the effectiveness of controls in preventing and/or detecting non-compliant behavior
  - This approach generally relies on direct measurement to establish compliance
  - Example 1 - The change in % / # of high risk controls (e.g., anti-market manipulation, trading, reliability, access, and/or credit controls) tested year-over-year (and results)
  - Example 2 – The # of compliance audits performed per year (and results)

* Consideration should also be given to whether we want to measure leading or lagging indicators (e.g., focus on metrics that can influence future change and/or metrics that record what has already happened.

9

Emera

KPIs – A Myriad of Options

The following table provides a sample of measurement categories, metrics & data sources to consider

Types	Measurement Categories	Metrics	Data Source
Macro	1. Program Governance	• % of Compliance Program Work Plan Activities Completed Per Plan	• Compliance Work Plan Activity Reports
	2. Requirements Management	• % of Regulatory Compliance Deadlines Met On Time	• Requirements Tracking Database
	3.a. Compliance Risk Management	• **Change in Inherent Compliance Risk Scores (Likelihood, Impact)**	• Annual Compliance Risk Assessment Reports
	3.b. Financial Risk Management	• # / Size of Non-Compliance Fines / Penalties / Disgorgement	• Non-Compliance Incident Case Management Reports
	3.c. Reputational Risk Management	• Changes in the # / Nature of News Articles	• Non-Compliance Incident Case Management Reports
	4. Policy Management	• # of New Policies Reviewed, Approved, and/or Implemented per Yr.	• Policy Management Tracking Reports
Micro	5. Controls Management	• The change in % / # of high risk controls (e.g., anti-market manipulation, trading, reliability, access, and/or credit controls) tested year-over-year (and results) • # of compliance audits performed per year (and results)	• Control Management Tracking Reports
Macro	6. Performance Management / Program Efficiency / Program Effectiveness	• **Change in Compliance Maturity Assessment Scores** • Employee Engagement Survey Results • % of Audit Recommendations Completed Per Plan • Reduced % of Time Employee Spends Performing Compliance Tasks Per Cycle	• Annual Compliance Maturity Assessment Reports • Employee Engagement Surveys • Action Item Tracking Reports • Time & Cost Studies
	7. Communications and Training	• % of Training / Communication Plan Completed • # / % of Certifications Completion	• Communications and Training Tracking Reports
	8. Ethics / Integrity	• # of Hotline Calls Received • % of Allegations Confirmed • # and/or Type of Disciplinary Actions Taken	• Hotline Database • Inquiry / Investigation Tracking System / Database • Same as Above

10

Emera

5

Standards: Macro-Perspective

The following provides an overview of how Emera measures compliance risk scores

IMPACT ASSESSMENT CRITERIA:

1. <u>FINANCIAL IMPACT</u>: Total financial impact based on a Materiality Threshold;

2. <u>OPERATIONAL IMPACT</u>: Level of operational impact absorbed under normal operating conditions;

3. <u>REPUTATIONAL IMPACT</u>: Level and duration an incident receives media attention;

4. <u>REGULATORY IMPACT</u>: Whether an incident meets a notice threshold and/or how likely is the incident to attract regulatory attention or action

Risk Rating Scale:	
Very Low	1
Low	2
Medium	3
High	4
Very High	5

11

Standards: Macro-Perspective, Cont'd.

The following provides an overview of how Emera measures compliance maturity scores

Compliance Management System (CMS) Standards

2.1 Requirements & Commitments Management	2.1. Utilize a systematic process to identify, assess, and manage applicable requirements & commitments (e.g., laws & regulations, standards, policies & procedures as well as permits, licenses, & contracts)
2.2 Risk Management	2.2. Utilize a systematic process to identify, assess, and prioritize how best to manage applicable compliance risks
2.3 Document Management	2.3. Utilize a systematic process to assess, author, publish, and/or manage the inventory of applicable governing documents (i.e., standards, policies, procedures, contracts, permits, and licenses)
2.4 Controls Management	2.4. Utilize a systematic process to develop, implement, test, certify, and refine applicable control environment
2.5 Incident Management	2.5. Utilize a systematic process to detect, notify, investigate, and manage applicable potential or actual incidents of non-compliance
2.6 Performance Management	2.6. Utilize a systematic process to monitor, measure and report on the performance of overall compliance programming
2.7 Training and Communications	2.7. Utilize a systematic process to develop, implement, and manage how employees learn to performed their responsibilities in a compliant manner.

Compliance Maturity Scale:	
Advanced/Strategic	3
Intermediate/Managed	2
Emerging/Reactive	1

12

Standards: Micro-Perspective

The following provides an overview of typical compliance requirement / control test activities one could measure

CONTROL TEST ACTIVITIES
1.1 Assess Effectiveness / Adequacy of Controls
1.1.1 Direct 3rd Party Assessment
1.1.2 Indirect Self Assessment / Attestation
1.2 Review Completeness, Accuracy and Current Validity of Documentation
1.2.1 Direct 3rd Party Assessment
1.2.2 Indirect Self Assessment / Attestation
1.3 Non-compliances Evaluated as Systemic vs. Isolated
1.3.1 Draft Findings
1.3.2 Review Findings
1.3.3 Authorize Findings
1.4 Exceptions / Corrective Actions
1.4.1 Exceptions / Corrective Actions Identified / Proposed
1.4.2 Exceptions / Corrective Actions Agreed To
1.4.3 Exceptions / Corrective Actions Taken
1.4.4 Exceptions / Corrective Actions Re-inspected, Retested and/or Re-evaluated

Emera

Annual Compliance Scorecard Planning Process

Macro Level

- **Purpose:** Identify & mitigate overall Management System-level risks though increased program maturity
- **Process:**

1. Program Scope & Risk Accountability	2. CMS Risk & Maturity Assessment	3. Likelihood and Impact Assessment	4. Residual Risk Results and Action Plan Development	5. Quarterly Scorecard Reporting
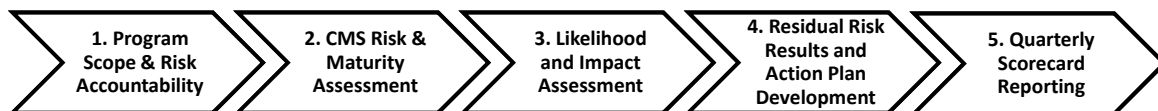
- **Technology:**
  - Current: Excel Template
  - Future: GRC Database
- **Outcome:** An action plan to increased program maturity of Management System Controls based on assessment results and Emera's Compliance Management System (CMS) Standards
- **Measurements:** Status of action plan will be reported quarterly on the Program Scorecard. The Program Scorecard will be collected as part of Emera's Quarterly Compliance Certification Process

Emera

Design – Risk & Maturity Assessment Overview

Annual Compliance Management System
Risk & Maturity Assessment
PRIVILEGED & CONFIDENTIAL

What is being measured?
- **Part A:** Compliance Program Scope
- **Part B:** Compliance Program Risk & Maturity
- **Part C:** Likelihood & Impact of Compliance Incident

How many assessments per company?
- **Eight** – One for each Compliance Risk Area

How much did the assessment cost?
- **Internal labor only:**
  - Development – 25-30 Hours
  - Assessment – 4-6 Hours per company (approx. 30-45 minutes per assessment)

What is the assessment criteria?
- **Objective Criteria:** Emera's CMS Standards
  - CMS Program Risk (Weighted Five Point Scale)
    - People (30%), Process (50%), Technology (20%)
  - CMS Program Maturity (Weighted Three Point Scale)
    - People (30%), Process (50%), Technology (20%)
  - CMS Program Residual Risk (Five Point Scale)
- **Subjective:**
  - Likelihood (Five Point Scale)
  - Impact (Five Point Scale)

What is the risk formula?
- **CMS:** CMS Risk – CMS Maturity = CMS Residual Risk
- **Total Risk:** Weighed Average of:
  - CMS Residual Risk (40%)
  - Likelihood (30%)
  - Impact (30%)

15

Design – Part A: Scope Detail

Does this risk area have a Formal Program?

Is the program documented?

Who is responsible for managing the program?

Is the program audited?

16

Design – Part B: Risk and Maturity Assessment

Maturity Question

CMS Standard

Risk Questions

Part B: Compliance Program Management System Risk & Maturity Assessment	
PART N INSTRUCTIONS: Part B is broken into the following three Sections: (1) People, (2) Process, and (3) Technology. Complete the following Steps for each Section Step 1. Review the respective Compliance Program Standard. Step 2. Review the Compliance Program Maturity-related questions (MQs), click on the drop-down menu, and select the response that best describes how closely your compliance program meets the respective Standard; Step 3. Review the Risk Assessment-related questions (RQs), click on the drop-down menu, and select the response that best describes the current state of your overall compliance program.	
1. People	
STANDARD DESCRIPTION:	To ensure our resiliency and achieve our business objectives in a principled manner, compliance-related roles and responsibilities should be clearly identified and documented consistent with the "three lines of defense" model.*
MQ 1	Does your compliance program identify and document its roles and responsibilities consistent with the "three lines of defense" model?
MA 1	
RQ 1	Changes in personnel may lead to higher incidents of non-compliance. Over the past 3 years, how would you describe the amount of turnover in key personnel that contribute to your compliance program?
RA 1	
RQ 2	An understanding of, and appreciation for, the importance of a strong compliance culture may vary among personnel. How well do you think those employees involved with your compliance program generally embrace a "culture of compliance?"
RA 2	
RQ 3	Managing an effective compliance program requires knowledgeable personnel who understand the business, laws and regulations, risks, policies and procedures, controls, etc. How would you describe the overall level of knowledge that the current personnel have who contribute to your compliance program?
RA 3	
RQ 4	Managing an effective compliance program also requires a significant level of cooperation and support from different business areas. How would you describe the overall level of support your compliance program receives from the business areas that support your program?
RA 4	

Emera

Design – Filling out the Assessment

1. People	
STANDARD DESCRIPTION:	To ensure our resiliency and achieve our business objectives in a principled manner, compliance-related roles and responsibilities should be clearly identified and documented consistent with the "three lines of defense" model.*
MQ 1	Does your compliance program identify and document its roles and responsibilities consistent with the "three lines of defense" model?
MA 1	
RQ 1	Changes in personnel may lead to higher incidents of non-compliance. Over the past 3 years, how would you describe the amount of turnover in key personnel that contribute to your compliance program?
RA 1	
RQ 2	An understanding of, and appreciation for, the importance of a strong compliance culture may vary among personnel. How well do you think those employees involved with your compliance program generally embrace a "culture of compliance?"
RA 2	
RQ 3	Managing an effective compliance program requires knowledgeable personnel who understand the business, laws and regulations, risks, policies and procedures, controls, etc. How would you describe the overall level of knowledge that the current personnel have who contribute to your compliance program?
RA 3	
RQ 4	Managing an effective compliance program also requires a significant level of cooperation and support from different business areas. How would you describe the overall level of support your compliance program receives from the business areas that support your program?
RA 4	
2. Process	
	To foster best practices and continuous improvement, the following seven core compliance processes should systematically* be developed and implemented as part of each Emera Company's compliance programming consistent with their respective operations, risk appetite, policies &

Emera

Design – Part C: Likelihood & Impact of Non-Compliance

Risk Areas   Likelihood & Impact Rankings   Ranking Scales

Emera Corporate Ethics & Compliance

Part C: Likelihood & Impact of Compliance Incident

Risk Ranking:	Compliance Risk Area:	Likelihood	Impact
	Affiliate Overall	#DIV/0!	#DIV/0!
1	Privacy & Data Protection		
2	Third-Party Management		
3	Legal & Contract Management		
4	Ethics & Compliance Culture		
5	Regulatory		
6	Labour & Employment		
7	Anti-Corruption & Government Relations		
8	Public & Custom Interactions		

Likelihood of Non-Compliance Scale

Description: Consider the most likely potential, unmitigated conditions that could trigger the occurrence of the sub-risk in question. The more these conditions exist, the higher the likelihood that the Sub-Risk may be triggered. These triggering conditions often include, but are not limited to: (1) pressure to "make the numbers"; (2) the complexity of the operations; (3) the level of change / lack of stability within the business; and/or (4) the level of morale and/or turnover of the people involved with the given process(es).

1) Rare / Very Low	2) Unlikely / Low	3) Moderate	4) Likely / High	5) Almost Certain / Very High

Impact of Non-Compliance Scale

Description: Consider the highest potential, unmitigated impact that could result to your company if the Sub-Risk in question were triggered. The more impact that could occur, the higher the score. These impacts may include, but are not limited to: (1) financial impact; (2) operational impact; (3) reputational impact; and/or (4) regulatory impact.

1) Insignificant / Very Low	2) Minor / Low	3) Moderate	4) Major / High	5) Catastrophic / Very High

19

Design – Company Compliance Scorecard

Example Company Scorecard with Assessment Results:

Risk Ranking:	Compliance Risk Area:	CMS Maturity				Risk Level				Risk Tolerance & Targets	
		People	Process	Technology	Overall	Likelihood	Impact	Controls	Overall	Target	Risk Tolerance & Target Rationale:
	Affiliate Overall	2.3	2.0	1.6	2.0	1.8	3.4	2	2.5		
1	Privacy & Data Protection	3.0	1.9	1.9	2.2	3	4	2	2.9	2	Overall residual risk level rejected. Maturity will increase with completion of goals 1-8 generally and goal 4 specifically.
2	Third-Party Management	2.0	1.7	1.1	1.7	2	3	3	2.7	2	Overall residual risk level rejected. Maturity will increase with completion of goals 1-8 generally and goal 5 specifically.
3	Legal & Contract Management	2.0	1.9	1.4	1.8	2	3	3	2.7	2	Overall residual risk level rejected. Maturity will increase with completion of goals 1-8 generally and goal 6 specifically.
4	Ethics & Compliance Culture	1.0	1.1	1.1	1.1	1	3	3	2.4	N/A	Overall residual risk level accepted. Maturity will increase with completion of goals 1-8 generally and goal 7 specifically.
5	Regulatory	2.0	2.1	1.8	2.0	1	4	2	2.3	N/A	Overall residual risk level accepted. Maturity will increase with completion of goals 1-8 generally and goal 8 specifically.
6	Labour & Employment	3.0	1.9	1.9	2.2	2	3	2	2.3	N/A	Overall residual risk level accepted. Maturity will increase with completion of goals 1-8.
7	Anti-Corruption & Government Relations	2.3	2.3	1.5	2.1	1	4	2	2.3	N/A	
8	Public & Customer Interactions	3.0	2.9	1.7	2.7	2	3	2	2.3	N/A	

Compliance Maturity Scale:

Advanced/Strategic	3
Intermediate/Managed	2
Emerging/Reactive	1

Risk Rating Scale:

Very Low	1
Low	2
Medium	3
High	4
Very High	5

- Is senior management OK with the level of Residual Risk (Risk Appetite)?
- If yes, maintain current control environment
- If no, determine what improvements would give you the biggest benefit (i.e., mitigate the highest risks relative to your resource capabilities)
- Design, implement, and report on the status & impact of continuous improvement activities

20

Design - Survey Questions

Question: How does your Organization develop compliance risk and/or maturity assessments?

    A. Use a third-party consultant (CEB, EY, Deloitte, etc.)

    B. Use internal resources

    C. Use a survey service (Survey Monkey, Qualtrics, Survey Gizmo, etc.)

    D. N/A – We do not conduct assessments

Question: Do you verify compliance status using objective or subjective tools and techniques?

    A. Subjective – Using employee surveys, questionnaires, certifications and/or acknowledgements

    B. Objective – Using evidence including documentation, control test results, and/or audit results

    C. A mix of both

    D. N/A – We do not verify compliance status

Emera

Implementation - Overview

How was the assessment exercise introduced?
- **Through Emera's CMS Governance Structure**
  - Presented to the enterprise compliance committee
  - Committee Members are affiliate compliance leaders

How were the participants identified?
- **Affiliate compliance leaders identified risk area owners**

How were the assessments conducted?
- **One of three approaches**
  - Self-Guided
  - Guided by Compliance Leader
  - Guided by Corporate Compliance

How long did participants have to complete?
- **Approx. 30 calendar days**

How were the assessments managed?
- **SharePoint environment**
  - Restricted access on an affiliate basis
    - Maintain confidentiality
    - Comply with affiliate rules for information sharing
  - One source of truth

What was challenging for participates?
- **Being assessed against a set of new standards (CMS)**
  - Understanding CMS
  - Understanding Applicability
    - Non-traditional risk areas especially

Emera

Key Takeaways

1. **Great Awareness Builder**
   - This process exposed our compliance network to the meaning and purpose of our new CMS Standards

2. **Provided a Roadmap To Action**
   - Measuring relative risk showed us what we should focus on in the future
   - It did not try to quantify the precise level of risk associated with a given activity
   - Resulted in a strong commitment to undertake specific compliance activities in 2019

3. **Balances Time, Cost and Precision**
   - Important to know how much evidence you need to verify compliance
     - i.e., Do you need independent, data driven results (i.e., third party control test results) or will employee surveys, certifications or acknowledgements be sufficient?
   - Also important to know if your focus is broad (i.e., on a large, diverse organization) or narrow (i.e., on a specific set of requirements)
   - Emera's approach provides reasonable assurance that the likelihood of a material non-compliance event is low if seeing relatively low residual risk scores and relatively high program maturity scores
   - Compliance with specific requirements needs to me determined using more direct, evidence-based testing

23

Emera

Q&A

Questions?

24

Emera