COMPLIANCE AT THE SPEED OF RISK

Are you ready?

Raimund Laqua, PMP, P.Eng
ray.laqu@leancompliance.ca

LEAN COMPLIANCE CONSULTING, INC.
A few definitions we need to know

- **Compliance**: the outcome of meeting obligations with respect to quality, safety, environmental and regulatory objectives (ISO 19600)
- **Risk**: the effects of uncertainty on objectives (ISO 31000)
- **Speed**: the rate at which risk becomes a reality
PREFACE
Why are we talking about this?

PICTURES OF REALITY

STATEMENTS OF REALITY

- We are completely in compliance with all applicable laws, regulations, and statutes
- We are working to the highest standards
- We are following all the rules
- All our products function as designed
- We are doing nothing wrong

Not able to prevent risk from becoming a reality

COMPLIANCE AT THE SPEED OF RISK
PREFACE

All the rules were followed

PHOENIX PAY SYSTEM

WHAT HAPPENED

• In 2009 the Canadian government initiated the Phoenix project which rolled out in 2016.

• The original budget of $309m increased to $954m expected to rise to $2.3b by 2023 in unplanned costs.

• The Governor General Auditor in 2019 reported,

  “How could Phoenix have failed so thoroughly in a system that has a management accountability framework; risk management policies, program evaluations, internal audit groups, departmental audit committees; accounting officers; departmental plans; departmental performance reports; pay-per-performance compensation’; and audits by Office of the Auditor General?”

Not able to prevent risk from becoming a reality
In 2018 the first recorded fatality involving a self-driving vehicle occurred.

Uber reported that the vehicle performed as designed.

Uber argued that it did have safety policies, procedures, and engineering practices that, in aggregate, could be considered a safety plan.

Uber has since suspended use of autonomous vehicles.

Not able to prevent risk from becoming a reality.
In 2018 Cambridge Analytica harvested data of millions of Facebook profiles. Facebook claimed that users had given their consent to give away their information and that Facebook did nothing wrong. In response to the Cambridge Analytica scandal Facebook has promised to “do what it takes to protect our community” and has established “Social Science One” to prevent similar breaches in the future. Not able to prevent risk from becoming a reality.
PREFACE

Risk and compliance is falling behind

Not able to prevent risk from becoming a reality

COMPLIANCE AT THE SPEED OF RISK
How do we get ahead of all this?

Increase the number of:
- Training sessions
- Inspections
- Pre-audits
- Internal audits
- External audits

Assumptions:
- The problem is a lack of conformance to existing policies, standards, or regulations.
- Gaps will identify what to improve.
- We have the resources, capabilities, and time to make improvements before the next incident occurs.
How do we get ahead of all this?

Vision Zero

- Regulations and standards are changing from prescriptive and management-based to performance and outcome-based designs.
- Organizations will establish goals, objectives, and measures to make progress against these targets.
- Continuous improvement of capabilities is expected.

Assumptions:

- The problem is a lack of effectiveness.
- Prescriptive standards and regulations are not creating the intended outcomes.
- High consequence risk rarely occur due to a breakdown of a single activity but instead occur because of alignment of weaknesses across multiple activities.
- Cannot wait for audit findings to make improvements, companies need to be proactive.
The Big Idea

1. The risk and compliance landscape has changed.
   - It is no longer only about loss prevention and conforming to and verifying prescriptive specifications.
   - It is now focused on reducing risk, ensuring obligations and advancing compliance outcomes (e.g. vision zero).

2. Management approaches based on reactive processes (audit/fix cycle) are too slow and too late to keep up at the speed that risk becomes a reality.

3. A proactive approach is needed; one that is holistic, risk-based, and drives continuous improvement.
THE COMPLIANCE LANDSCAPE

Compliance is ineffective and costs are rising

Lack of effectiveness

- 70% of companies do not measure the effectiveness of their compliance programs
- Incomplete and invalid metrics
- Mistaking legal accountability for compliance effectiveness
- Self-reporting and self-selection bias
- Focusing on the elements and not the whole

The cost of compliance is too high and increasing

- Compliance alone is estimated to be between 8%-10% of a FTE (time and salary)
- Compliance can be 2 to 3 times that in highly-regulated, high-risk sectors (e.g., oil & gas, energy, etc.)
- Risk & compliance will be more

† Harvard Business Review (HBR)
How do you view compliance?

1. Necessary Good
   - Proactive: anticipate, plan, act to be more certain
   - Manage Risk: Goal is to meet obligations

2. Necessary Evil
   - Reactive: surprised, always behind, uncertain
   - Only concerned about non-conformance
   - Goal is to pass an audit

THE COMPLIANCE LANDSCAPE

Attitude towards compliance is mostly negative

COMPLIANCE AT THE SPEED OF RISK
Compliance focuses mostly on legal requirements.

### OPERATIONS
- Quality
- Health & Safety
- Environmental

### REACTIVE APPROACH
- Checklists
- Inspections
- Audits
- Corrective Actions
- Inducements
- Training
- Culture

### ETHICS & COMPLIANCE
- Legal
- Regulatory
- Code of Conduct

Compliance at the Speed of Risk
THE COMPLIANCE LANDSCAPE

Compliance is fractionated

Regulatory Compliance → Process and Pipeline Safety → Occupational Health and Safety → Incident Investigations → CAR / CAPA → Quality (QA/QC)


Integrity → Damage Prevention → Responsible Care → Business Continuity → IT / Cyber Security → Document Keeping and Records Management

COMPLIANCE AT THE SPEED OF RISK
THE COMPLIANCE LANDSCAPE

Compliance effort is diluted across the organization

COMPLIANCE AT THE SPEED OF RISK

Compliance System

Organizational Structure

COMPLIANCE AT THE SPEED OF RISK
THE COMPLIANCE LANDSCAPE

Compliance is too reactive

Prescriptive-based Compliance

Standards Based
What should I do?

Audit Based
What must I do?

Continuous Improvement Based
How can I improve?

Outcome-based Compliance
Risk Based
How can I ensure objectives?

Reactive Thinking

Proactive Thinking

Findings / Lagging Actions
Ownership / Leading Actions
(Audit Centric)
(Obligation Centric)

COMPLIANCE AT THE SPEED OF RISK

Prescriptive-based

Compliance

Outcome-based

Compliance

Reactive Thinking

Proactive Thinking

Findings / Lagging Actions
Ownership / Leading Actions
(Audit Centric)
(Obligation Centric)

COMPLIANCE AT THE SPEED OF RISK
THE RISK LANDSCAPE

RISK

REGULATIONS

POLICY

PRACTICES

SECURITY

COMPLIANCE

RISK

computer
rules
control
AUDITORS

scope
external

report

process

PENETRATION

AUDIT

findings

governance

meeting

strategy

financial

backup

recovery

standards

LAWs

COMPLIANCE AT THE SPEED OF RISK
THE RISK LANDSCAPE

Risk management is changing

PREVENT LOSS

ENSURE OBJECTIVES

EARLY RISK MANAGEMENT

- Modern Risk Management
- Self Protection
- Insurance

1950

1960

TRADITIONAL RISK MANAGEMENT

- Increased focus on controls and compliance in the financial sector
- Tread–way commission on Fraudulent Financial Reporting (COSO)
- OSHA publishes 29 CFR 119 PSM – Hazardous chemicals

1970

1980

ENTERPRISE RISK MANAGEMENT

- Sarbanes–Oxley Act
- COSO publishes ERM Integrated framework
- ISO publishes 31000 risk management standard
- Risk becomes part of Project Management
- ISO publishes 9001:2015 ”risk-based thinking”
- ICH publishes Q9 Risk Management

1990

2000

CERTAINTY MANAGEMENT

- Uncertainty understood to be the root cause of risk
- Focus on outcomes, performance and continuous improvement
- Increasing understanding of complexity and emerging risk
- Increased focus on prediction, resilience (safe–to–fail)
- Risk management is seen as cross functional capability

2010

2015

COMPLIANCE AT THE SPEED OF RISK
THE RISK LANDSCAPE

Risk management maps are out-of-date

Value-at-Risk on Portfolio Loss Rate

- We need to solve for $VaR^p$ in
  $$\Phi\left(\frac{-\Phi^{-1}(VaR^p)}{\sqrt{p}}\right) = 1 - p$$

- which yields the following $VaR^p$ formula:
  $$VaR^p = \Phi^{-1}(1 - p) \times \Phi^{-1}(PD)$$
Everything happens in the presence of uncertainty

“effects of uncertainty on expected results”
ISO 9001

“effects of uncertainty on objectives”
ISO 31000

“an uncertain event or condition that, if it occurs, has a positive or negative effect on a project’s objectives.”
PMI PMBOK

THE RISK LANDSCAPE

COMPLIANCE AT THE SPEED OF RISK
Uncertainty is the root cause of risk.

**Aleatory**
- Natural variability
- Having to do with chance
- No ability to predict outcome

**Uncertainty**
- Distributions

**Epistemic**
- Lack of knowledge
- Probabilistic events and outcomes
- Having to do with knowledge
- Can predict outcome

**Risk**

**Irreducible Uncertainty**
- ALEATORY

**Reducible Uncertainty**
- EPISTEMIC

**Compliance at the Speed of Risk**

**Margins**

**Buy Down**
THE RISK LANDSCAPE

Uncertainty hides and needs to be discovered

BLIND SPOTS

BIASES

PRIORITY

MASLOW

PREDICTION

BLACK SWAN

CAUSE AND EFFECT

COMPLEXITIES

COMPLIANCE AT THE SPEED OF RISK
**THE RISK LANDSCAPE**

360° of protection is required

**EXTRINSIC**
- risks that are external to the organization.

**INTRINSIC**
- risks that are inherent within the organization.

**EMERGING**
- risks that arise because of changing conditions, behaviours, or capability

**COMPLIANCE AT THE SPEED OF RISK**
THE RISK LANDSCAPE

Risk management requires a different mindset

**Ostrich**
I don’t want to know

**Avoider**
I don’t want any risk

**Manager**
Let’s size the risk and decide

**Gambler**
Let’s play the odds

**Strategist**
Let’s reduce threats and exploit opportunities

**RISK TOLERANT**

**RISK INTOLERANT**

**RISK NEUTRAL**

**RISK SEEKING**

**RISK OPTIMIZER**

COMPLIANCE AT THE SPEED OF RISK
THE RISK LANDSCAPE

Risk management now has two objectives

Avoid Failure
• Protect (guard) against loss
• Minimize variation by preventing or recovery from threats
• Focus on efficiency (cost, schedule, technical performance)
• Pay attention to what might cause failure and what could go wrong

Pursue Success
• Ensure (make certain of) outcomes
• Maximize value by enabling and exploiting opportunities
• Focus on effectiveness (outcomes, value creation, benefits realization)
• Pay attention to what is critical to success and what needs to go right
HOW DO WE MEET OBLIGATIONS IN THE PRESENCE OF UNCERTAINTY?

RISK & COMPLIANCE
PROACTIVE RISK AND COMPLIANCE

Five Proactive Practices

1. MANAGE OBLIGATIONS
- Maintain registry of all mandatory and voluntary obligations requirements and specifications
- Model dependencies and relationships with outcomes, goals, objectives, capabilities, risks, and processes
- Estimate and evaluate uncertainties and risk
- Define measures of effectiveness, performance, and conformance

2. ENHANCE CAPABILITIES
- Free up resources to work on improvements
- Exploit existing technologies
- Develop proactive capabilities (goal setting, problem solving, learning, risk management, systems thinking, analytics, etc.)

3. EMBED RISK & COMPLIANCE
- Automate critical to compliance actions
- Incorporate evidentiary actions and documentation
- Incorporate Risk-based Thinking
- Utilize effective tools and practices to sustain and improve compliance
- Embed lessons learned, information and knowledge to guide decision making

4. UNLEASH PERFORMANCE
- Eliminate Non-Value-Added Activities
- Remove bottlenecks
- Eliminate work arounds
- Exploit constraints

5. IMPROVE CONTINUOUSLY
- Monitor measures of conformance, performance, and effectiveness
- Engage in continuous improvement between and across all levels of management
- Transition from reactive to proactive improvement cycles
- Learn from past experiences to improve future outcomes

† Based on ISO 19600, ISO 31000, CMMI, Theory of Constraints, Systems Thinking, Continuous Improvement, and Performance Management

COMPLIANCE AT THE SPEED OF RISK
1. Manage Obligations

- Maintain registry of all mandatory and voluntary obligations requirements and specifications
- Model dependencies and relationships with outcomes, goals, objectives, capabilities, risks, and processes
- Estimate and evaluate uncertainties and risk
- Define measures of effectiveness, performance, and conformance
2. Enhance Capabilities

- Free up resources to work on improvements
- Exploit existing technologies
- Develop proactive capabilities (goal setting, problem solving, learning, risk management, systems thinking, analytics, etc.)
**PROACTIVE RISK AND COMPLIANCE**

3. Embed Risk & Compliance and 4. Unleash Performance

**4. UNLEASH PERFORMANCE**
- Eliminate Non-Value-Added Activities
- Remove bottlenecks
- Eliminate work arounds
- Exploit constraints

**3. EMBED RISK AND COMPLIANCE**
- Automate critical to compliance actions
- Incorporate evidentiary actions and documentation
- Incorporate Risk-based Thinking
- Utilize effective tools and practices to sustain and improve compliance
- Embed lessons learned, information and knowledge to guide decision making

**COMPLIANCE AT THE SPEED OF RISK**
5. Improve Continuously

- Monitor measures of conformance, performance, and effectiveness
- Engage in continuous improvement between and across all levels of management
- Transition from reactive to proactive improvement cycles
- Learn from past experiences to improve future outcomes

- Vicious non-conformance cycle – the worst things get, and the faster things get worse.
- Virtuous conformance cycle – the better things get, and the faster things get better.
CONCLUSION

The Big Idea

1. The risk and compliance landscape has changed.
   • It is no longer only about loss prevention and conforming to and verifying prescriptive specifications.
   • It is now focused on reducing risk, ensuring obligations and advancing compliance outcomes (e.g. vision zero).

2. Management approaches based on reactive processes (audit/fix cycle) are too slow and too late to keep up at the speed that risk becomes a reality.

3. A proactive approach is needed; one that is holistic, risk-based, and drives continuous improvement.
CONCLUSION

Are you ready?

To prevent risk from becoming a reality

COMPLIANCE AT THE SPEED OF RISK
COMPLIANCE AT THE SPEED OF RISK

Are you ready?

Raimund Laqua, PMP, P.Eng
ray.laqua@leancompliance.ca

LEAN COMPLIANCE CONSULTING, INC.