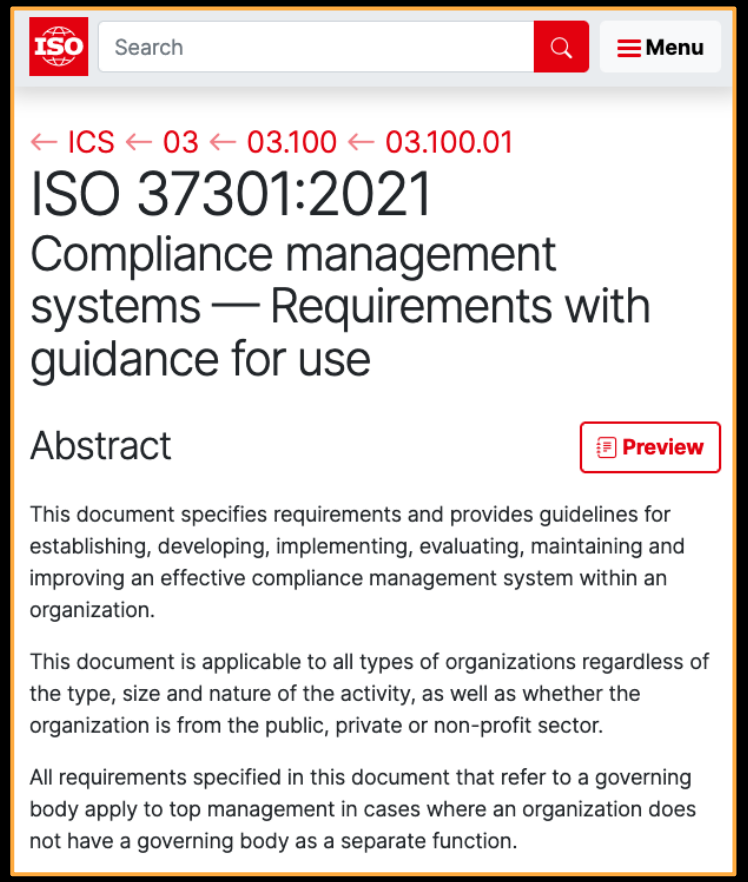
LEAN COMPLIANCE

ISO 37301:2021

Compliance Management Systems

Unlocking the Potential

Raimund Laqua, PMP, P.Eng.
Founder, Chief Compliance Engineer



Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

WEBINAR ETIQUETTE

Housekeeping rules



Video OFF



Mic OFF



Raise Hand



Type in Chat

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

OUR MISSION

Helping organizations always stay between the lines and ahead of risk



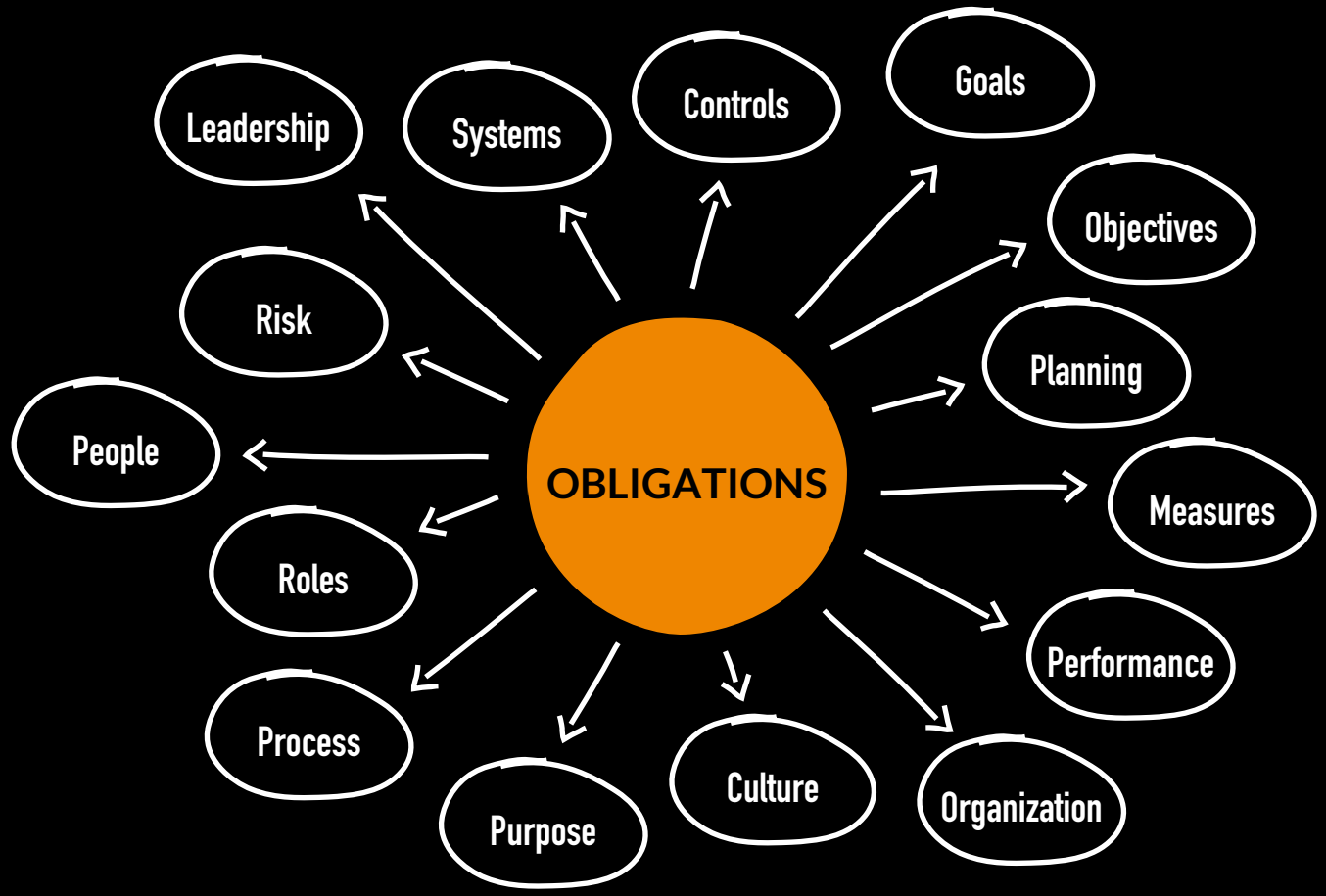
www.leancompliance.ca

- Mission success depends on compliance success.
- Taking ownership of all your obligations is necessary for compliance to be successful.
- Making and keeping promises is at the heart of compliance.
- Compliance is achieved by design not by hard work alone.
- Significantly better outcomes with greater certainty, lower risk, and less waste is achieved by taking a proactive and integrative approach to compliance.

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

THE BIG IDEA

For compliance to succeed you must manage your obligations, but more importantly you need to keep your promises





Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

OUTLINE

What we will cover today

1. Why Compliance Management?
2. What is ISO 37301?
3. What are the Benefits?
4. How does ISO 37301 Work?
5. How do you Implement ISO 37301?
6. Q & A

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

1. WHY COMPLIANCE MANAGEMENT?

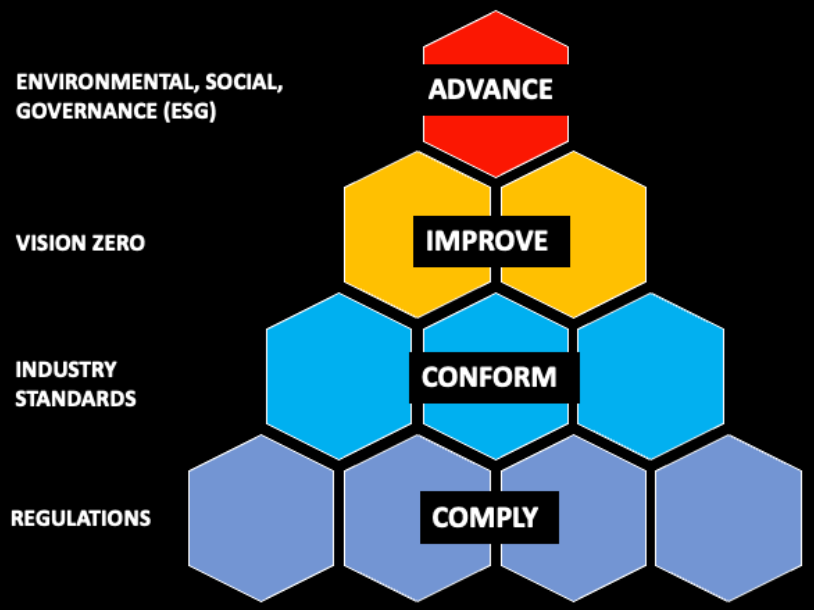
What has changed, what has not, and what needs to?

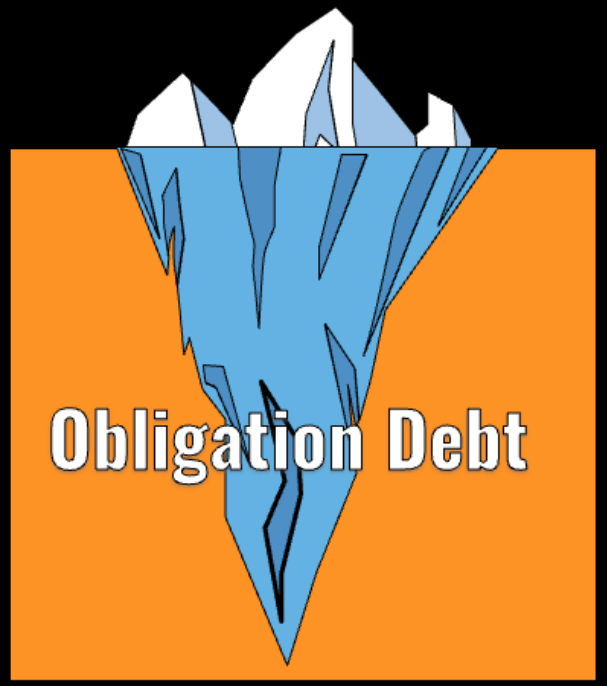
Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

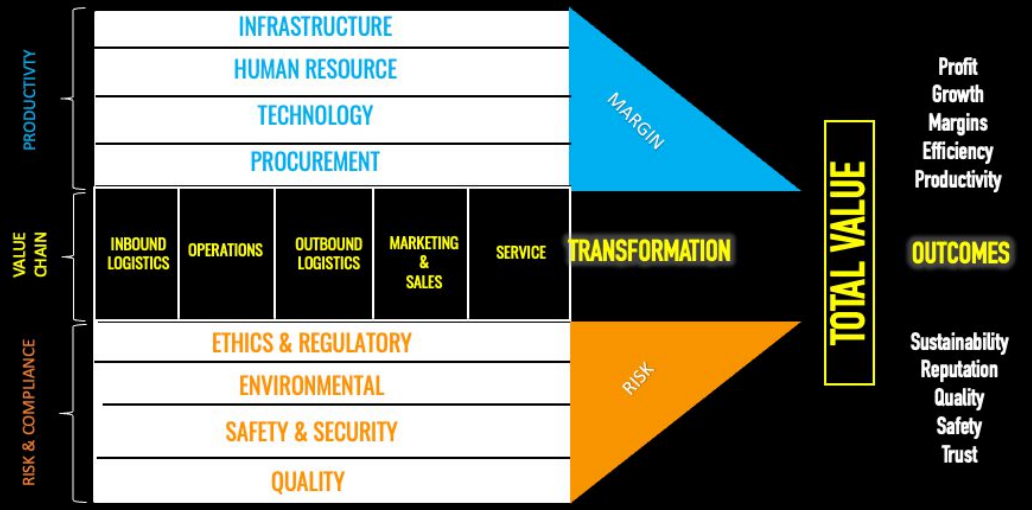
LEAN COMPLIANCE

WHY COMPLIANCE MANAGEMENT

What has changed?







1. OBLIGATIONS HAVE CHANGED

2. OBLIGATIONS HAVE INCREASED

3. OUTCOMES HAVE EXPANDED

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

WHY COMPLIANCE MANAGEMENT

What has not changed?







1. LESS THAN 30% MEASURE EFFECTIVENESS

2. MOST COMPLIANCE IS REACTIVE AND SILOED

3. MANY ARE CAUGHT IN A TRAP

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

WHY COMPLIANCE MANAGEMENT

What needs to change?



Compliance must be:

- **Operational** – able to deliver benefits.
- **Efficient** – able to achieve objectives with a minimum of waste.
- **Sustainable** - meeting the needs of the present without compromising the ability of future generations to meet their own needs.
- **Proactive** – stay ahead of risk.

This requires managed compliance not just compliance management.

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

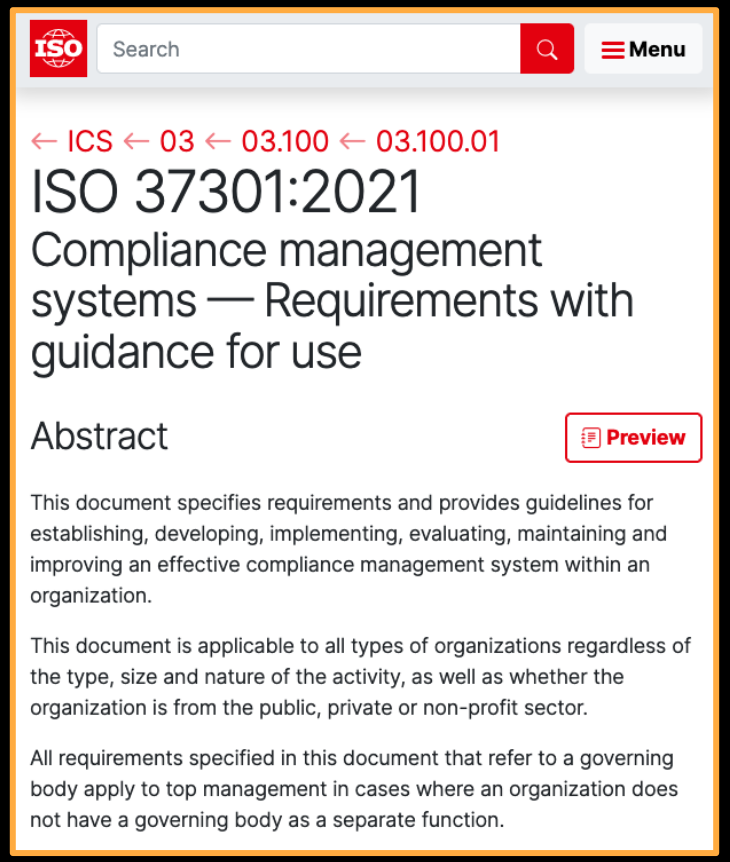
2. WHAT IS ISO 37301?

Overview

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

WHAT IS ISO 37301

Overview



- ISO 37301 replaces ISO 19600
- ISO 37301 is an international standard introduced in 2022 that provides guidance on establishing, implementing, maintaining, reviewing, and improving an effective compliance management system.
- This standard helps organizations ensure they comply with legal and ethical requirements, reduce the risk of non-compliance, and improve their overall performance.
- ISO 37301 provides a framework for organizations to integrate compliance into their business operations and to demonstrate their commitment to ethical behavior and social responsibility.

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

WHAT IS ISO 37301

Overview



ISO 37301 builds on and replaces ISO 19600 (guidelines) with important differences:

- ISO 37301 is now a Type A management standard that is certifiable compatible with other Type A Management System standards such as ISO 9001, 45001, 14001, etc.
- replaces **should** with **shall** statements (but not for everything)
- adds whistleblowing and expands culture and governance
- adds requirements for hiring or promoting staff to critical positions.
- adds assessment of staff in matters of regulatory compliance.
- provides description of what is considered a regulatory compliance culture.
- highlights the issues of independence, staffing and skills of Regulatory Compliance to operate without interventions and with appropriate staff.
- identifies Code of Ethics and Conduct as a key element in determining and controlling compliance.

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

WHAT IS ISO 37301

Where does it fit in with the other standards?

ISO 37301 is intended to work as a stand-alone system or in conjunction with others

ISO 37000	ISO 31000	ISO 37301	ISO 19011
Governance	Risk	Compliance	Audit

Topic Specific Standards

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

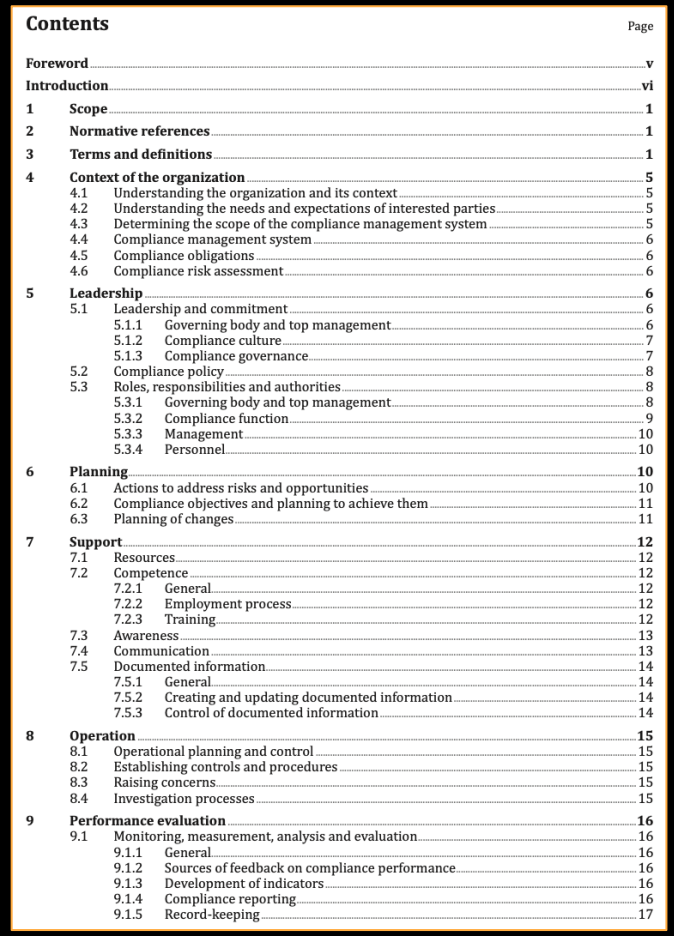
LEAN COMPLIANCE

WHAT IS ISO 37301

How is it the same as the other ISO standards?

ISO 37301:

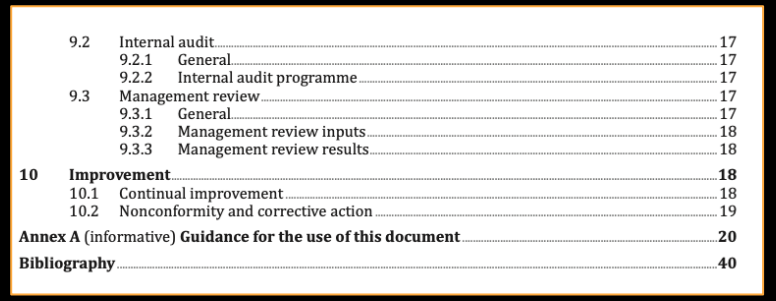
- follows Annex SL structure
- follows Type A MSS with respect to management system requirements.
- is harmonized with other standards
- is voluntary



Contents

Page

Foreword ... v
Introduction ... vi
1 Scope ... 1
2 Normative references ... 1
3 Terms and definitions ... 1
4 Context of the organization ... 5
4.1 Understanding the organization and its context ... 5
4.2 Understanding the needs and expectations of interested parties ... 5
4.3 Determining the scope of the compliance management system ... 5
4.4 Compliance management system ... 6
4.5 Compliance obligations ... 6
4.6 Compliance risk assessment ... 6
5 Leadership ... 6
5.1 Leadership and commitment ... 6
5.1.1 Governing body and top management ... 6
5.1.2 Compliance culture ... 7
5.1.3 Compliance governance ... 7
5.2 Compliance policy ... 8
5.3 Roles, responsibilities and authorities ... 8
5.3.1 Governing body and top management ... 8
5.3.2 Compliance function ... 9
5.3.3 Management ... 10
5.3.4 Personnel ... 10
6 Planning ... 10
6.1 Actions to address risks and opportunities ... 10
6.2 Compliance objectives and planning to achieve them ... 11
6.3 Planning of changes ... 11
7 Support ... 12
7.1 Resources ... 12
7.2 Competence ... 12
7.2.1 General ... 12
7.2.2 Employment process ... 12
7.2.3 Training ... 12
7.3 Awareness ... 13
7.4 Communication ... 13
7.5 Documented information ... 14
7.5.1 General ... 14
7.5.2 Creating and updating documented information ... 14
7.5.3 Control of documented information ... 14
8 Operation ... 15
8.1 Operational planning and control ... 15
8.2 Establishing controls and procedures ... 15
8.3 Raising concerns ... 15
8.4 Investigation processes ... 15
9 Performance evaluation ... 16
9.1 Monitoring, measurement, analysis and evaluation ... 16
9.1.1 General ... 16
9.1.2 Sources of feedback on compliance performance ... 16
9.1.3 Development of indicators ... 16
9.1.4 Compliance reporting ... 16
9.1.5 Record-keeping ... 17



9.2 Internal audit ... 17
9.2.1 General ... 17
9.2.2 Internal audit programme ... 17
9.3 Management review ... 17
9.3.1 General ... 17
9.3.2 Management review inputs ... 18
9.3.3 Management review results ... 18
10 Improvement ... 18
10.1 Continual improvement ... 18
10.2 Nonconformity and corrective action ... 19
Annex A (informative) Guidance for the use of this document ... 20
Bibliography ... 40

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

WHAT IS ISO 37301

How is it different from the other ISO standards?

Focus on Compliance

ISO 37301 is specifically designed to manage obligations

Risk Based Approach

ISO 37301 emphasizes a risk-based approach to compliance management

Integration with Other Standards

ISO 37301 is designed to be used with other management systems

Certifiable with Guidelines for Use

ISO 37301 is certifiable using accredited auditors.



Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

WHAT IS ISO 37301

Includes both requirements and recommendations

Requirements are found in the body of the standard

4.4 Compliance management system

The organization shall establish, implement, maintain and continually improve a compliance management system, including the processes needed and their interactions, in accordance with the requirements of this document.

The compliance management system shall reflect the organization's values, objectives, strategy and compliance risks, taking into account the context of the organization (see 4.1).

Recommendations are found in ANNEX A (Information)

A.4.4 Compliance management system

A compliance management system is a framework that integrates essential structures, policies, processes and procedures to achieve the desired compliance outcomes, and act to prevent, detect and respond to noncompliance.

Typically, a compliance management system framework is a structural matter: the necessary infrastructure on which to build this system. It then needs to be made operational through the implementation of policies, processes and procedures. Then it needs to be maintained and continually improved.

There are many elements to a compliance management system. Some elements of the management system will be designed to support desired behaviours, while others will be designed to prevent undesirable behaviours. Some elements are solely to monitor the compliance performance of the organization or provide alerts if noncompliance take place.

The compliance management system will recognize that mistakes do happen and will have processes to ensure there is appropriate reaction. An appropriate reaction will include remediation of processes, systems and impacted parties.

The compliance management system should be based on the principles of good governance, proportionality, integrity, transparency, accountability and sustainability.

The compliance management system should be available as documented information.

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

3. WHAT ARE THE BENEFITS?

Why you should be using this standard

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

WHAT ARE THE BENEFITS

You have these needs



ISO 37301 is applicable for organizations that:

- want to modernized their corporate compliance efforts with industry best practices.
- need a compliance management system for specific risk domains not currently covered by a standard.
- need to better address obligations contained within existing management systems.
- need an overarching assurance framework across existing compliance management systems (e.g., safety, security, environmental, EHS, ESG, etc.)

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

WHAT ARE THE BENEFITS

You want these benefits

INCREASED PROBABILITY OF MISSION SUCCESS

ISO outlines the following benefits for this standard:

- improving business opportunities and sustainability.
- protecting and enhancing an organization's reputation and credibility.
- considering expectations of interested parties.
- demonstrating an organization's commitment to managing its compliance risks effectively and efficiently.
- increasing the confidence of third parties in the organization's capacity to achieve sustained success.
- minimizing the risk of a contravention occurring with the attendant costs and reputational damage.

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

2. HOW DOES ISO 37301 WORK?

Concept of Operations

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

HOW DOES ISO 37301 WORK

Outcome Objectives



These are measures of effectiveness that need to be specified in units meaningful to the stakeholders.

- Integrity
- Culture
- Conformity
- Reputation
- Value
- Ethics

Capabilities for the CMS depend on the specific obligations associated with these outcomes.

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

HOW DOES ISO 37301 WORK

Essential Behaviors



These principles define essential behaviors for achieving compliance outcomes:

- Integrity
- Good Governance
- Proportionality
- Transparency
- Accountability
- Sustainability

These behaviors need to be present within the CMS and reinforced by the organizational culture.

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

HOW DOES ISO 37301 WORK

Essential Processes



The CMS implements essential processes to achieve compliance and risk objectives:

- **PLAN:** Commitment , Scope, Policy, Roles and responsibilities, Obligations and Risks
- **DO:** Support, Competence and awareness, Communication and training, Operations, Controls and procedures, Documentation
- **CHECK:** Internal audit, Management review, Monitoring and measurement, Raising concerns, Investigation process
- **ACT:** Managing non-compliance, Continual improvement

PDCA demonstrates how these processes interact with each other. However, they may not happen in sequence. For example, operating controls happen at the same time that conformance is verified.

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

HOW DOES ISO 37301 WORK

Context



These define internal and external environmental factors that need to be considered:

- Legal
- Social
- Cultural
- Digitalization
- Finance
- Structure
- Environment
- Interested parties

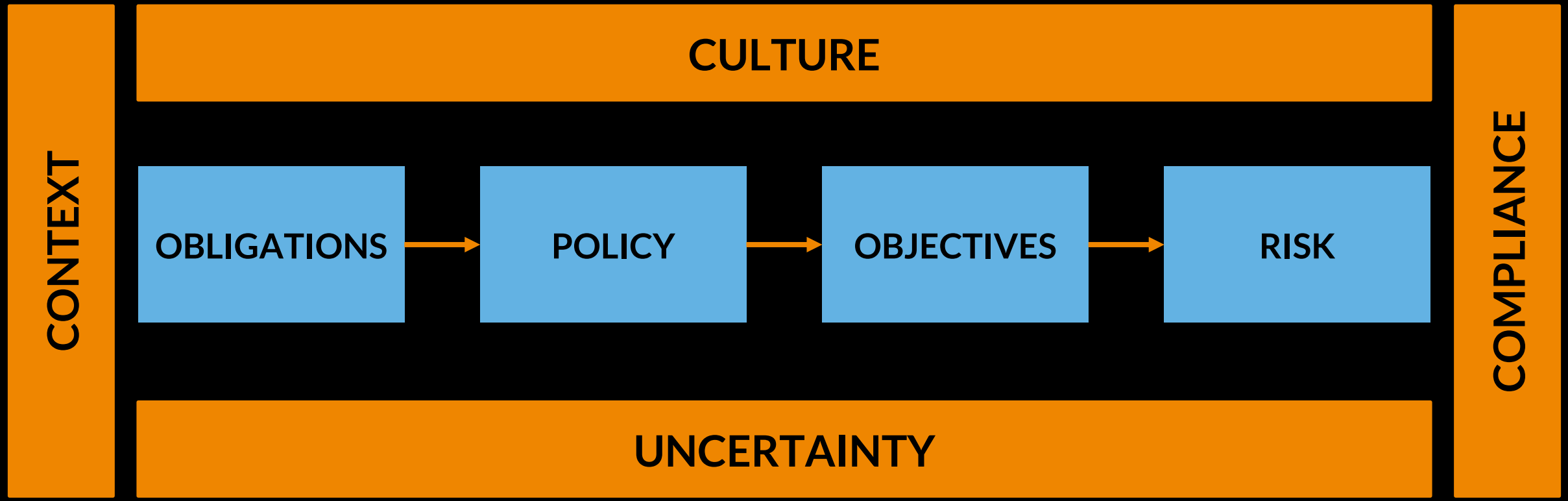
These factors are inputs into the planning process and define the climate the CMS operates within.

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

HOW DOES ISO 37301 WORK

Key concepts and how they are related



Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

HOW DOES ISO 37301 WORK

Key Definitions

ISO 37301 is a management system standard to achieve objectives resulting in compliance.

3.4
management system
set of interrelated or interacting elements of an *organization* (3.1) to establish *policies* (3.5) and *objectives* (3.6) as well as *processes* (3.8) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The management system elements include the organization's structure, roles and responsibilities, planning and operation.

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

HOW DOES ISO 37301 WORK

Key Definitions

Compliance is the outcome of an effective CMS

3.26
compliance
meeting all the *organization's* (3.1) *compliance obligations* (3.25)

3.13
effectiveness
extent to which planned activities are realized and planned results are achieved

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

HOW DOES ISO 37301 WORK

Key Definitions

Compliance involves establishing the behaviors that align with organizational policy

3.28
compliance culture
values, ethics, beliefs and *conduct* (3.29) that exist throughout an *organization* (3.1) and interact with the organization's structures and control systems to produce behavioural norms that are conducive to *compliance* (3.26)

3.5
policy
intentions and direction of an *organization* (3.1), as formally expressed by its *top management* (3.3)

Note 1 to entry: A policy can also be formally expressed by an organization's *governing body* (3.21).

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

HOW DOES ISO 37301 WORK

Key Definitions

3.25
compliance obligations
requirements (3.14) that an *organization* (3.1) mandatorily has to comply with as well as those that an organization voluntarily chooses to comply with

3.14
requirement
need or expectation that is stated, generally implied or obligatory

Note 1 to entry: "Generally implied" means that it is custom or common practice for the *organization* (3.1) and *interested parties* (3.2) that the need or expectation under consideration is implied.

Note 2 to entry: A specified requirement is one that is stated, e.g. in *documented information* (3.10).

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

HOW DOES ISO 37301 WORK

Key Definitions

3.6
objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as finance, health and safety, and environment). They can be, for example, organization-wide, or specific to a project, product, service or *process* (3.8)).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended result, a purpose, an operational criterion, as a *compliance* (3.26) objective, or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of compliance *management systems* (3.4), compliance objectives are set by the *organization* (3.1), consistent with the compliance *policy* (3.5), to achieve specific results.

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

HOW DOES ISO 37301 WORK

Key Definitions

3.7
risk
effect of uncertainty on *objectives* (3.6)

Note 1 to entry: An effect is a deviation from the expected – positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73) and "consequences" (as defined in ISO Guide 73), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73) of occurrence.

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

HOW DOES ISO 37301 WORK

Section 4. Context of the organization



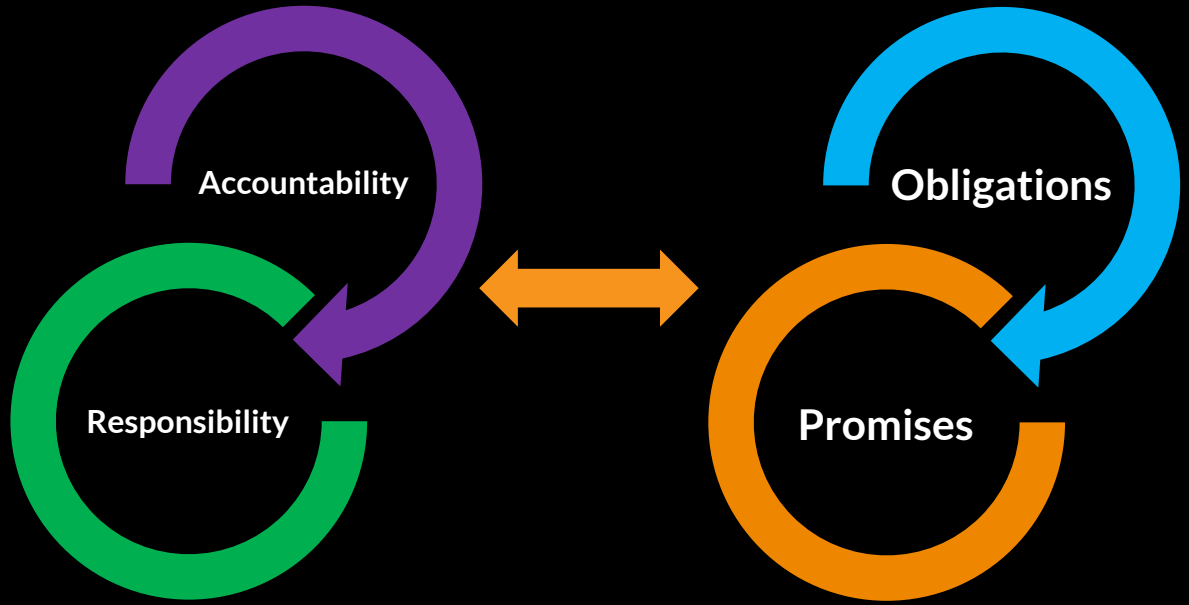
- 4.1 Understanding the organization and its context
- 4.2 Understanding the needs and expectations of interested parties
- 4.3 Determining the scope of compliance management system
- 4.4 Compliance management system
- 4.5 Compliance obligations
- 4.6 Compliance risk assessment

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

HOW DOES ISO 37301 WORK

Section 5. Leadership



5.1 Leadership and Commitment

- 5.1.1 Governing body and top management
- 5.1.2 Compliance culture
- 5.1.3 Compliance governance

5.2 Compliance Policy

5.3 Roles, responsibilities and authorities

- 5.3.1 Governing body and top management
- 5.3.2 Compliance function
- 5.3.3 Management
- 5.3.4 Personnel

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

HOW DOES ISO 37301 WORK

Section 6. Planning

FACTOR	ASSESSMENT	ANALYSIS	ELEMENTS
Capability	Do we have the needed abilities to advance compliance outcomes and meet all our obligations?	What strategies are needed to improve capabilities?	• People • Process • Technology
Capacity	Do we have enough time, money, knowledge, people, and specific capacities to meet our obligations?	What strategies are needed to unleash capacity?	• People • Process • Technology
Performance	Are we performing at the level we need to keep our promises?	What strategies are needed to achieve and sustain required performance?	• People • Process • Technology

6.1 Actions to address risks and opportunities

6.2 Compliance objectives and planning to achieve them

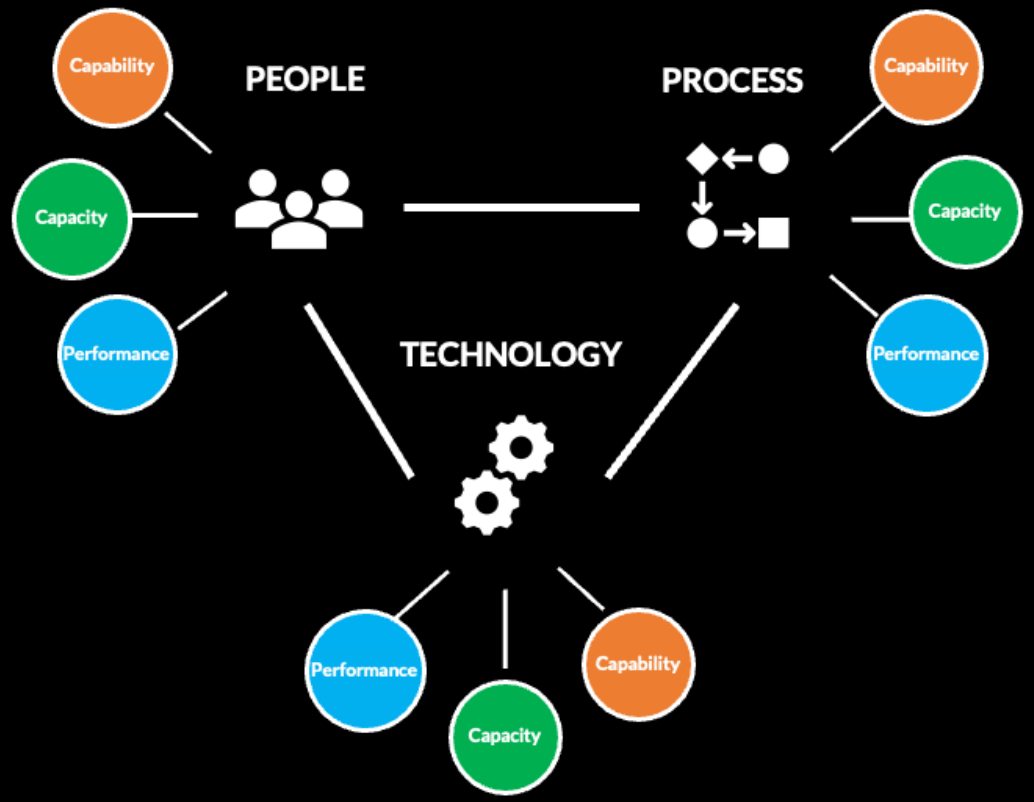
6.3 Planning of changes

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

HOW DOES ISO 37301 WORK

Section 7. Support



7.1 Resources

7.2 Competence

7.2.1 General	7.2.2 Employment process	7.2.3 Training

7.3 Awareness

7.4 Communication

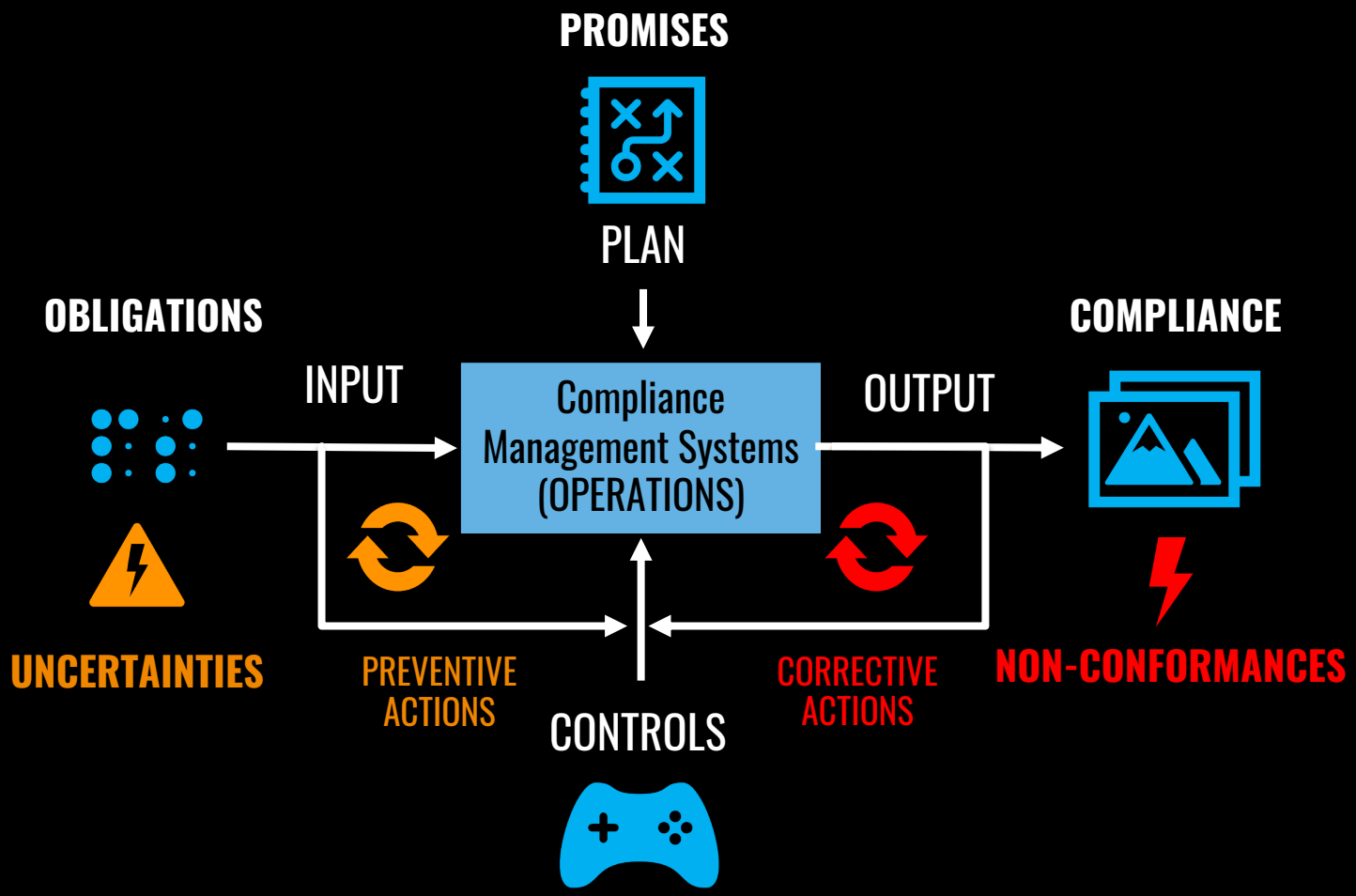
7.5 Documented information

7.5.1 General	7.5.2 Creating and updating documented information	7.5.3 Control of documented information

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

HOW DOES ISO 37301 WORK

Section 8. Operation



- 8.1 Operational planning and control
- 8.2 Establishing controls and procedures
- 8.3 Raising concerns
- 8.4 Investigation processes

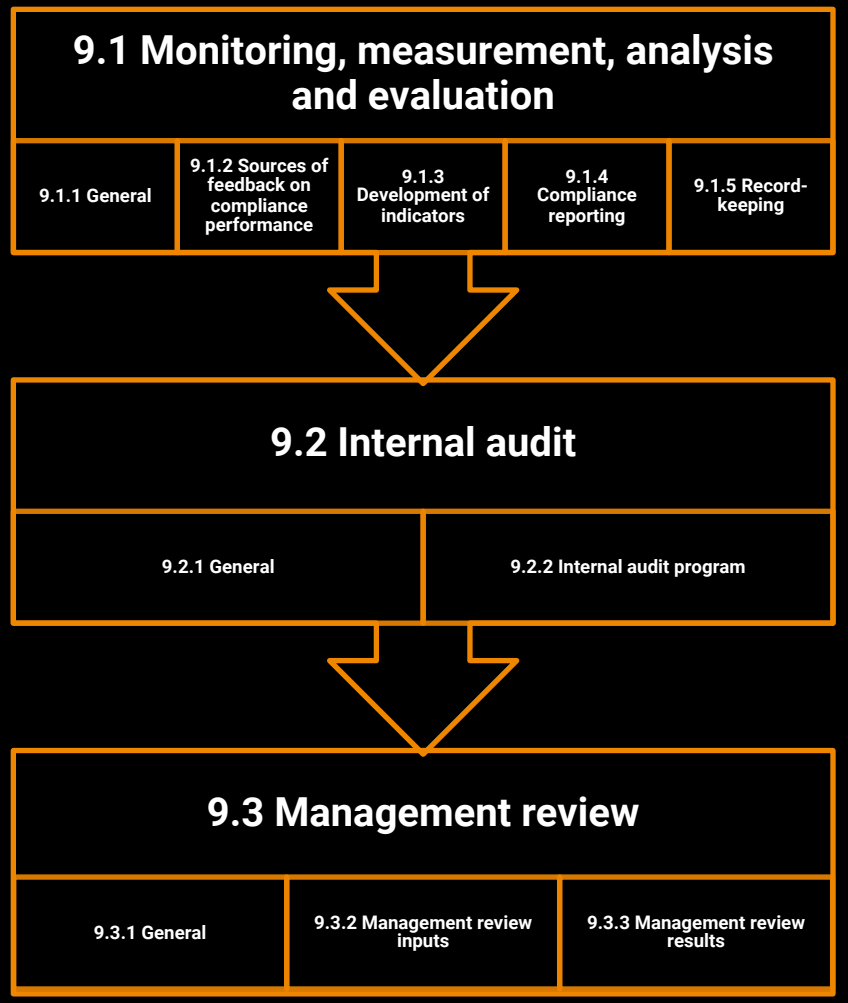
Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

HOW DOES ISO 37301 WORK

9. Performance Evaluation

MEASURES OF SUCCESS	EVALUATION	MEASURE
Measure of Conformance (MoC)	Are we staying between the lines?	count of evidence of compliance
Measure of Performance (MoP)	Are we keeping our promises and contending with uncertainty? Are we making a quantitative difference in compliance?	rate we are buying down compliance risk, and capacity to keep our promises
Measure of Effectiveness (MoE)	To what extent are we meeting all our obligations? Are we making a qualitative difference in outcomes?	progress (advancement) towards compliance outcomes
Measure of Assurance (MoA)	How certain are we of meeting all our obligations today, tomorrow, and every day we choose to operate?	confidence in our ability to always stay between the lines and ahead of risk

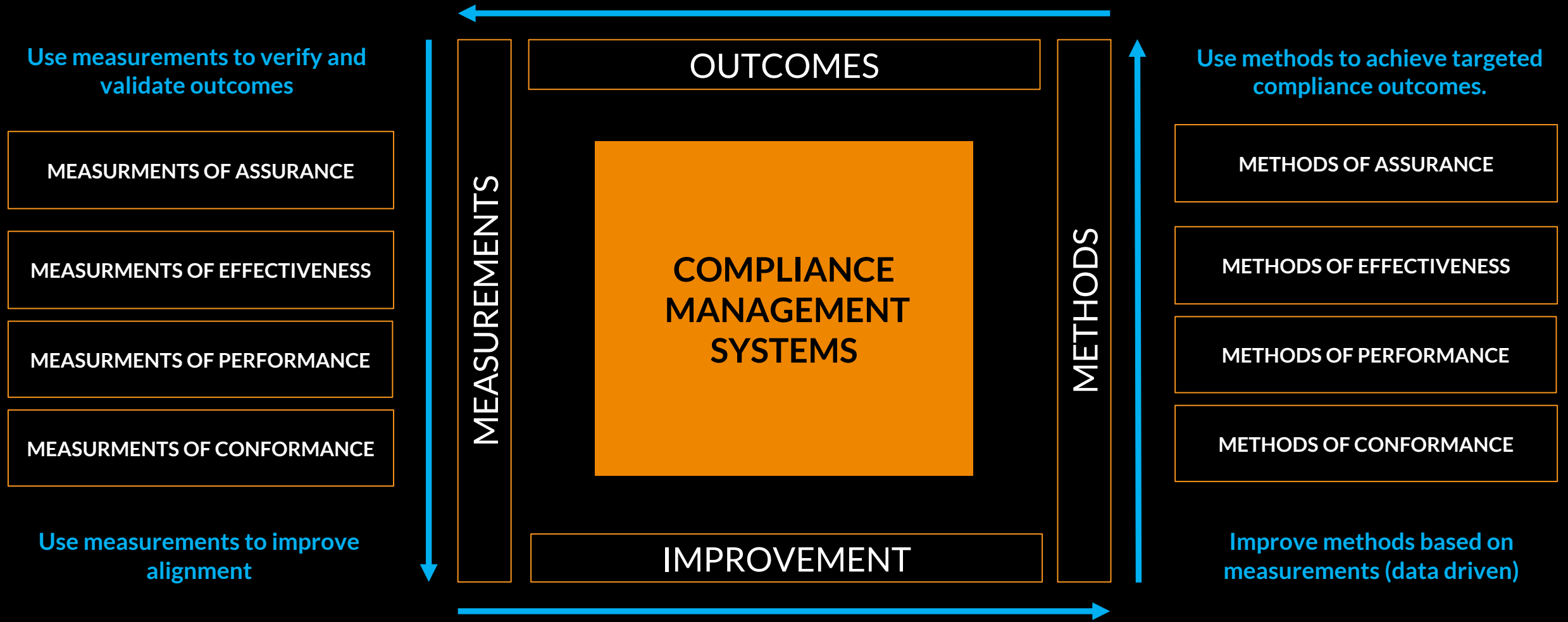


Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

HOW DOES ISO 37301 WORK

Section 10. Improvement



Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

5. HOW DO YOU IMPLEMENT ISO 37301?

Depends on what you want to achieve

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

HOW DO YOU IMPLEMENT ISO 37301

Which path should you take?



Alice's Dilemma

"Would you tell me, please, which way I ought to go from here?"

"That depends a good deal on where you want to get to," said the Cat.

"I don't much care where," said Alice.

"Then it doesn't matter which way you go," said the Cat.

"so long as I get SOMEWHERE," Alice added as an explanation.

"Oh, you're sure to do that," said the Cat,

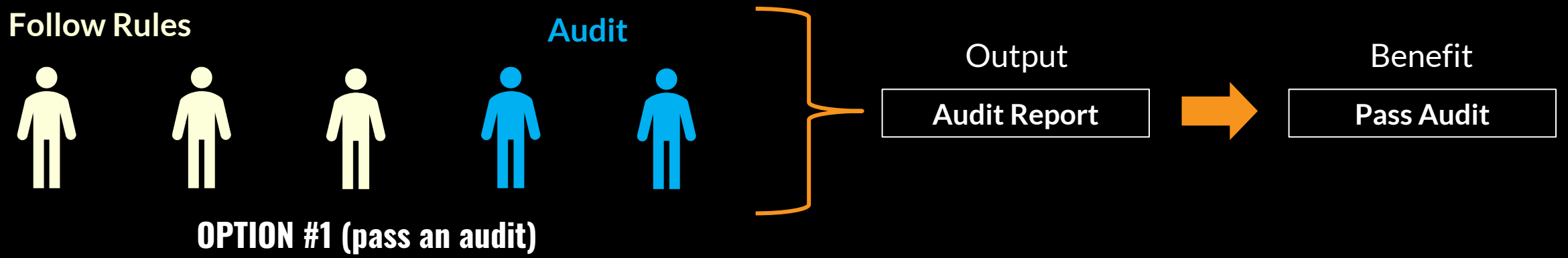
"if you only walk long enough."

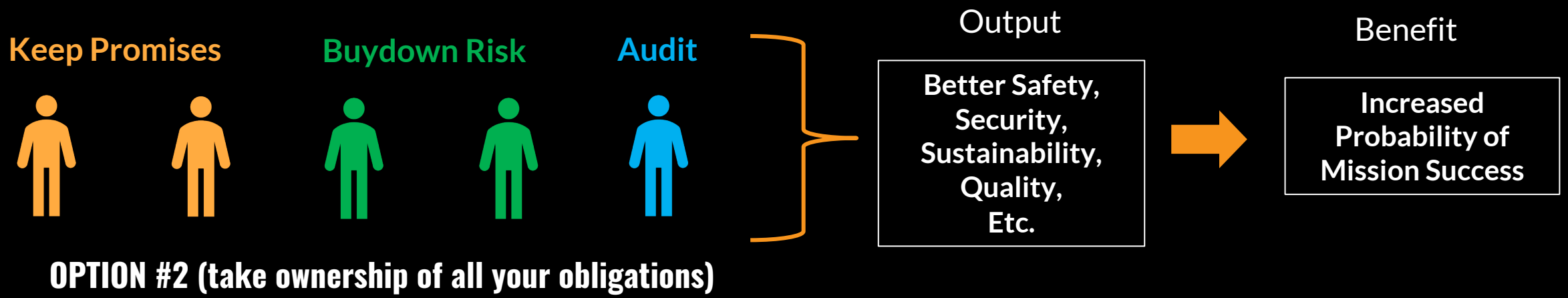
Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

HOW DO YOU IMPLEMENT ISO 37301

The benefits you receive depend on your intentions





Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

HOW DO YOU IMPLEMENT ISO 37301

Where do you want to go?

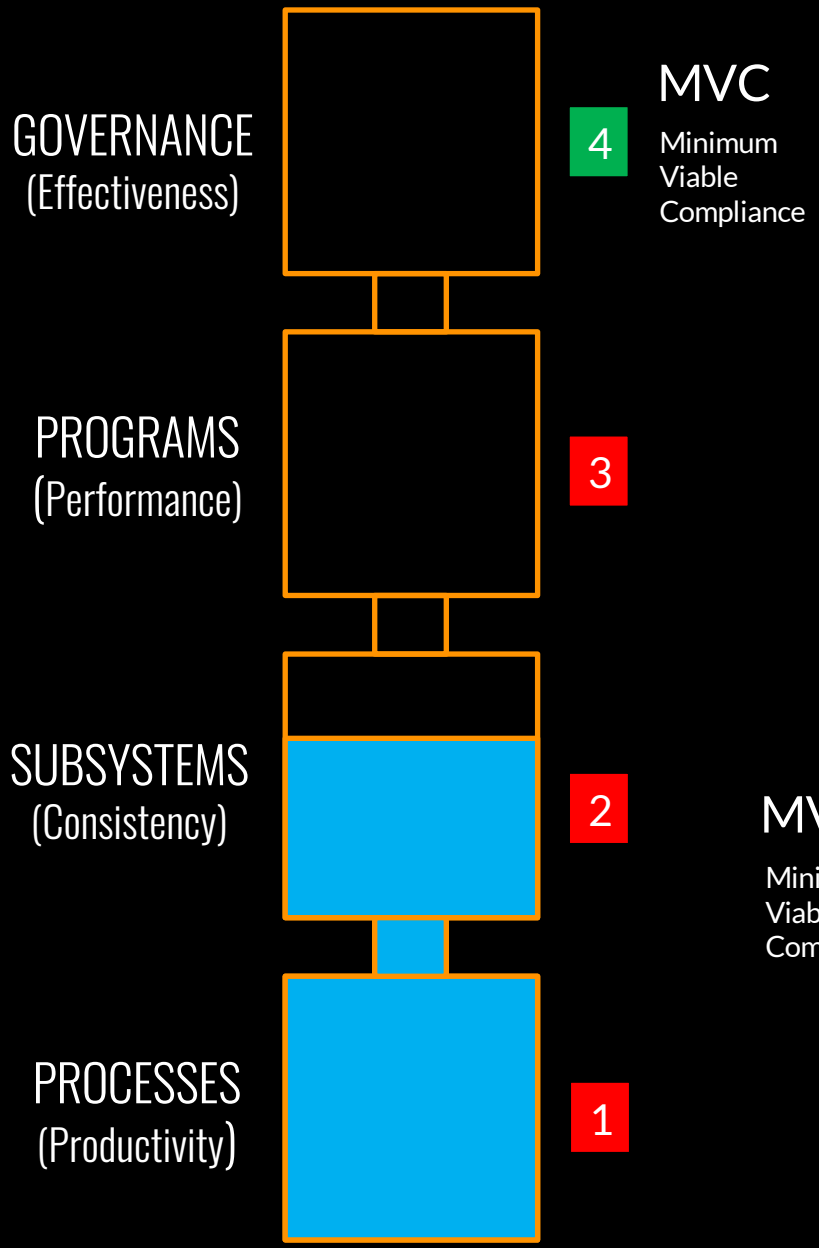
TAKE OWNERSHIP OF ALL YOUR OBLIGATIONS

1. Operationalize existing risk & compliance program	Realize Benefits
2. Establish overarching program for all obligations	Consolidate Governance
3. Establish program for obligations not covered by a program or standard	Handle New Obligations
4. Establish compliance program for corporate compliance	Increase Trust
5. Integrate multiple management systems under one roof	Exploit Common Capabilities
6. Implement LEAN governance, risk, and compliance (GRC)	Lean GRC



Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE



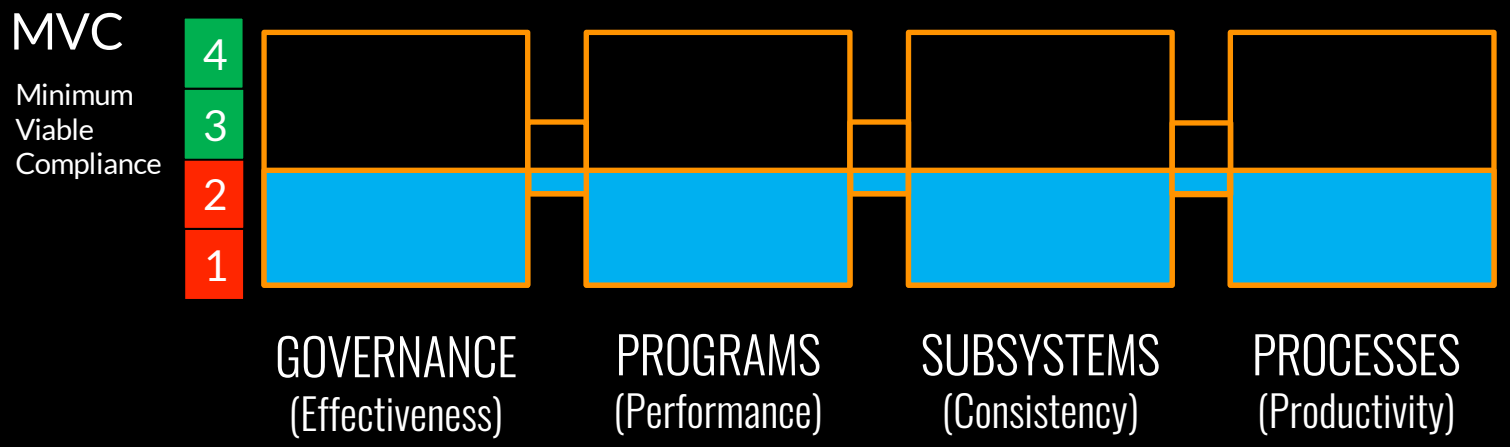
Traditional Approach

Compliance is the outcome of meeting obligations.

This requires compliance to be operational.

Compliance operability is achieved when essential functions, behaviors, and interactions exist at levels sufficient to produce a measure of effectiveness – this defines Minimum Viable Compliance (MVC).

Traditional approaches never reach MVC until the very end which is too slow and often too late to protect value creation and stay ahead of risk.



Whole System Approach

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

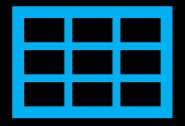
HOW DO YOU IMPLEMENT ISO 37301

Lean Compliance Play Book

1. 
   Identify and define mandatory and voluntary: prescriptive, performance, and outcome-based obligations.

2. 
   Identify and define measures of conformance, performance, effectiveness, and assurance.

3. 
   Identify and define essential capabilities, capacity, and performance to meet and sustain obligations.

4. 
   Map obligations to existing governance, programs, systems, and processes.

5. 
   Identify and evaluate uncertainties and risks to meeting targeted goals and objectives.

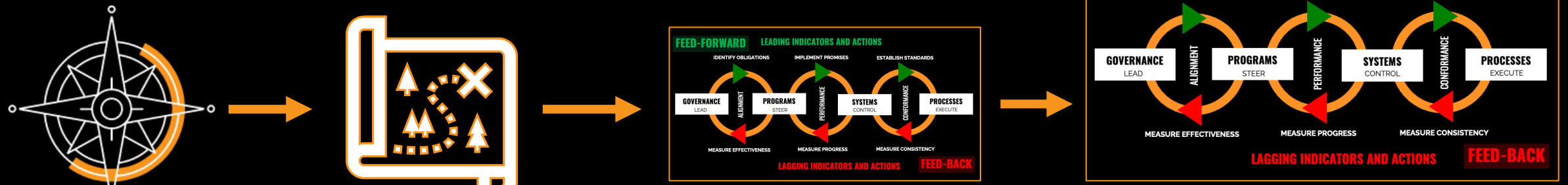
6. 
   Develop and implement improvement roadmap to achieve operability (MVC)

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

HOW DO YOU IMPLEMENT ISO 37301

The Proactive Certainty Program™



1. ORIENT

Assess your compliance situation and identify areas of risk and improvement.

2. MAP

Learn as you chart your roadmap towards operational and effective compliance.

3. OPERATIONALIZE

Implement essential capabilities to reach operational readiness.

4. ELEVATE

Continuously improve your compliance effectiveness over time.

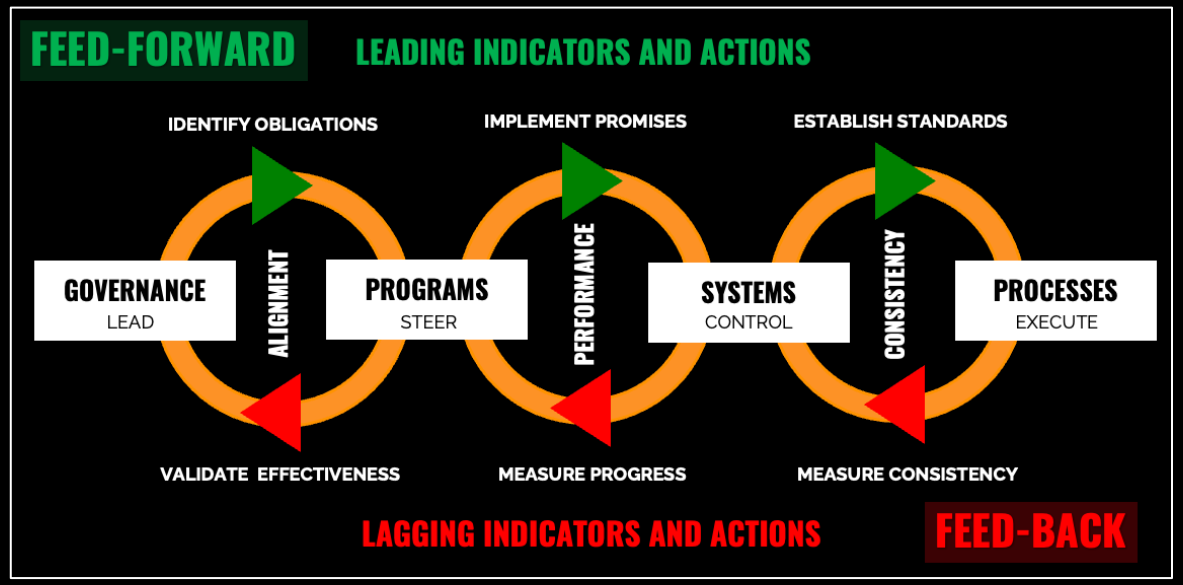
https://www.leancompliance.ca/the-proactive-certainty-program

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

HOW DO YOU IMPLEMENT ISO 37301

Compliance Operability Foundations Course - September



- **Four 2-Hour live Zoom sessions**
- **Coach led instruction**
- **Weekly assignments**
- **Certificate upon completion**

- **Who should attend?** all who want to transform compliance.

Operational Compliance is a state of operability when all essential compliance functions, behaviours, and interactions exist and perform at levels necessary to realize compliance outcomes

https://www.leancompliance.ca/lean-compliance-academy

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

SUMMARY

What did we cover

1. Why Compliance Management?
2. What is ISO 37301?
3. What are the Benefits?
4. How does ISO 37301 Work?
5. How do you Implement ISO 37301?
6. Q & A

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

6. QUESTIONS & ANSWERS

You made it this far, you most likely have some questions, comments, and feedback

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved

LEAN COMPLIANCE

Thank You!

Copyright, © 2023 Lean Compliance Consulting, Inc.—All rights reserved