



When Recognition Matters

A photograph of two men in business suits shaking hands. The man on the left is Black, wearing a blue suit and a red tie, and is smiling. The man on the right is white, wearing a grey suit, and is seen from the side. They are standing in front of a large glass window. The image is partially framed by a large red triangle on the right side.

WHITEPAPER





ISO 19600:2014

COMPLIANCE MANAGEMENT SYSTEMS
GUIDELINES

www.pecb.com



Principal Author

-  Eric LACHAPELLE, PECB
 -  Faton ALIU, PECB
 -  Enis EMINI, PECB
- 



CONTENT

- 4 Introduction
- 5 Culture – the major driver of a compliant organization
- 6 ISO 19600 – more than mere compliance to laws and regulations
- 7 The importance of leadership in ISO 19600
- 8 Risk-based approach in ISO 19600
- 9 ISO 19600 – a flexible guideline
- 11 The organization's compliance management system
- 13 The rewards of a compliance management system based on the ISO 19600

INTRODUCTION

In the English dictionary, compliance is briefly described as the act or process of being in conformity with applicable regulations, guidelines, and specifications. Many products, for instance, are developed in compliance with certain specifications set by some standards. This means, for example, that a certain bolt for fastening equipment has to be produced in compliance with a certain defined screw thread pattern. For organizations, compliance is the outcome of meeting their obligations set by government agencies or adhering to a set of guidelines or specifications established by standards or their own internal policies.

However, adhering to compliance-related requirements can be a challenge because of the many and diverse laws, rules, and standards that organizations face on a local, national, international, and industry-wide levels; and failure to comply with some of these matters can result in fiscal, legal, or even criminal penalties. On top of this, laws, regulations and standards continually evolve to fit the current social, political and economic landscape. Thus, compliance becomes a continuous process in an organization and not just a one-time project.

This is where the need for an international standard that would help organizations meet their compliance obligations becomes apparent; and this is the reasoning based on which the ISO 19600 was created. The ISO 19600 guides organizations in developing a compliance management system to identify new and existing rules, to identify and reduce the risk of breaching the existing rules, and to quickly, effectively, and efficiently correct any breaches that might occur. Furthermore, ISO 19600 helps organizations establish an effective, organization-wide compliance management system that enables organizations to demonstrate their commitment to compliance with relevant laws. Additionally the ISO 19600 helps organizations address legislative requirements, industry codes and organizational standards, as well as standards of good corporate governance, best practices, ethics, and community expectations; and offer the opportunity for the establishment of a successful and sustainable organization.



CULTURE

THE MAJOR DRIVER OF A COMPLIANT ORGANIZATION

A unique culture exists within every organization; and management gurus acknowledge that shaping an organization and its people to a wanted culture, plays a major role in how successfully an organization is going to operate in the future. But, what do we understand by the term *culture*? (Known also as “organizational culture”). Different scholars have varying opinions on how the organizational culture should be defined, but we can sum up the definition of culture as in the following:

“The set of values, norms and beliefs shared by the members of an organization that contribute to the unique social and psychological environment of that organization.”

The effect of culture, either positive or negative, can be observed in any company; two examples illustrate this point: a German engineering company and an American medical devices and pharmaceutical company. The German engineering company was plagued by a culture of widespread corruption-although not encouraged directly by the organization’s management- the employees firmly believed that bribery was not only acceptable, but it was encouraged amongst each other. Needless to say, pretty soon the company found itself in trouble with the law, paying hefty fines and dealing with a tarnished reputation. On the other hand, the American medical devices and pharmaceutical company, faced a crisis when somebody tampered with the packaging of one of their products, leading to a series of poison caused deaths. Because “customer-first” attribute was adamantly engraved within the organization’s culture, and regardless of the short-term profit losses, the organization’s management decided to recall the product from the shelves, and took actions to avoid such occurrences in the future. The organization’s actions are widely cited as an example of how a crisis should be managed and helped the organization not only maintain but also strengthen its positive reputation.

ISO 19600 emphasizes the importance of culture, especially the culture of integrity and compliance, and communicates this importance throughout the standard. In addition to giving us a definition of compliance culture, the standard also underlines that the development of a compliance culture requires such ingredients as active, visible, consistent, and sustained commitment of the organization’s governing body, top management and management towards a common standard of behavior that is required throughout every area of the organization.

Summarizing this, it can be concluded that a culture of integrity and compliance, not only is the foundation, but also an opportunity for a sustainable and successful organization and ISO 19600 can be the right tool on the organization’s hands in this journey.

ISO 19600

MORE THAN MERE COMPLIANCE TO LAWS AND REGULATIONS

All organizations must endeavor to comply with statutory and regulatory requirements that are applicable to them. However, despite trying their best to meet these requirements, organizations may find themselves in trouble: their compliance costs can skyrocket whilst the effectiveness of their compliance management declines, exposing them to legal liability, loss of trust among its stakeholders and public scrutiny.

ISO 19600 can help organizations establish an effective and efficient organization-wide compliance management system. The standard helps the organization understand and adhere to the ever-increasing number of regulatory requirements while acknowledging the fundamental market drives. This alignment of strategic initiatives, objectives and compliance management system helps the organization unleash its full potential, establishing responsibility and accountability within the organization, increasing its effectiveness and reducing costs.

However, compliance management is more than just compliance to laws and regulations. Organizations are required to deal with varying requirements from a number of stakeholders (e.g. customers, community, etc.), industry codes, organizational standards and benchmarks voluntarily chosen by the organization, and last but not least, their own organizational policies and codes. In consequence, ethical codes of conduct are taken seriously as a sign of a healthy corporate governance and socially responsible organization. The standard acknowledges this fact and is written in such a way that helps the organization consider all of their compliance requirements, compliance commitments and compliance obligations in order to be successful in the long term.

“ISO 19600 can help organizations establish effective and efficient organization-wide compliance management system.”





THE IMPORTANCE OF LEADERSHIP IN ISO 19600

“For a compliance management system to be effective, the governing body and top management need to lead by example, by adhering to and actively supporting compliance and the compliance management system.”

An organization's approach to compliance is ideally shaped by its leadership applying core values and generally accepted corporate governance, ethical and community standards. Therefore the involvement of the top management in the organization's compliance management system is one of the critical factors to ensure effectiveness. Additionally, the top management's involvement provides the behavioral tone and sends a message of commitment and determination throughout the whole organization. Embedding compliance in the behavior of the people working for an organization depends above all on leadership at all levels and clear values of an organization, as well as an acknowledgement and implementation of measures to promote compliant behavior.

Being written in accordance with ISO's 'High level structure' means that particular emphasis is placed upon leadership in ISO 19600. Indeed, when one reads the standard, one sees that the organization's top management does

not simply have the responsibility of managing the compliance management system, and quite a bit of involvement and accountability is required from them. They are required to integrate the requirements of ISO 19600 into the organization's core processes, i.e. establish, develop, implement, evaluate, maintain and improve to ensure that the compliance management system achieves its intended outcomes. Furthermore, the organization's top management is responsible for clearly communicating the importance of the compliance through clear and convincing statements supported by actions.

Organizations are increasingly convinced that by applying binding values and appropriate compliance management, they can safeguard their integrity and avoid or minimize noncompliance with the law. Moreover, the organization's leadership and its commitment to lead by example are imperative for the creation of a successful compliance management system.

Risk-based approach in ISO 19600

A risk-based approach to compliance management is important; for it ensures that the system is in alignment with the organization's objectives and establishes the basis for the implementation of a compliance management system.

This means that the organization has to decide upon which requirements, needs, and expectations of its stakeholders are to be considered as obligations for the organization and that will be complied with.



The organization's needs **identify** compliance risks by relating its compliance obligations to its activities, products, services and relevant aspects of its operations in order to identify situations where noncompliance can occur. The organization should identify the causes for and consequences of noncompliance.

The organization should **analyze** compliance risks by considering causes and sources of noncompliance and the severity of their consequences, as well as the likelihood that noncompliance and associated consequences can occur. Consequences can include, for example, personal and environmental harm, economic loss, reputational harm and administrative liability.



Risk **evaluation** involves comparing the level of compliance risk found during the analysis process with the level of compliance risk the organization is able and willing to accept. Based on this comparison, priorities can be set as a basis for determining the need for implementing controls and the extent of these controls.

The risk-based approach to compliance management does not mean that the organization should accept the noncompliance for low compliance risk situations. Organizations establish a zero tolerance approach to compliance quite often, which makes sense in terms of introducing an appropriate mindset among the organization's personnel. Ignoring small wrongdoings may, in some cases, accidentally transmit an unintended message that compliance isn't really important. The reality is that some rules carry more significance than others, and resources always have limitations.

ISO 19600 – a flexible guideline

ISO 19600 does not specify requirements, but provides guidance on compliance management systems and recommended practices. This is as a result of having the majority of ISO members approve the project and agree that there are enough certifiable management system standards for specific disciplines which include compliance management as an important element.

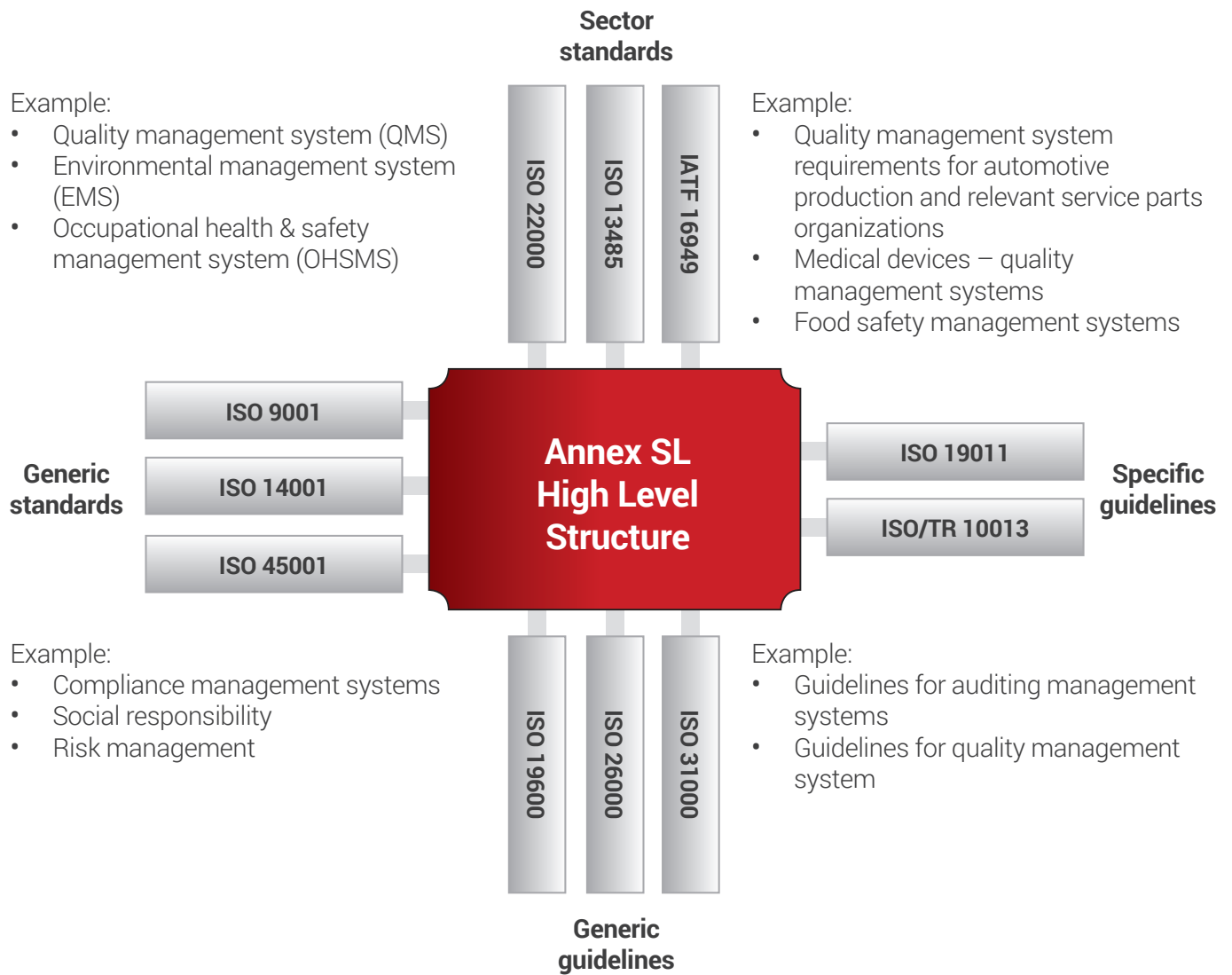


The origin of ISO 19600

In 2012, Australia proposed to start the development of an ISO standard for compliance programs based on the national Australian standard AS 8306, which existed since 1996, as a result of ever increasing compliance obligations. This proposal was accepted by the members of ISO and ISO/PC 271 “Compliance Programs” chaired by Martin Tolar, Managing Director of Australian Compliance Institute (now GRC Institute), was established to develop the standard.

As ISO 19600 is intended to assist organizations in improving and broadening their existing approach to compliance management it is helpful that it follows the ‘high-level structure’ for ISO management system standards. The standard can also be applied as a ‘plug-in’ to adapt the overall management system of an organization to systematically manage compliance matters.

Another reason why it has been important to create a guideline instead of a certifiable management system is the fact that small and medium size companies should be able to evaluate and implement solutions appropriate to them, rather than be burdened to create a management system that would position these companies in a considerable disadvantage. These businesses should embrace compliance and set up such a management system that fits the needs and possibilities of the enterprise as such, and assist it in achieving their compliance goals.



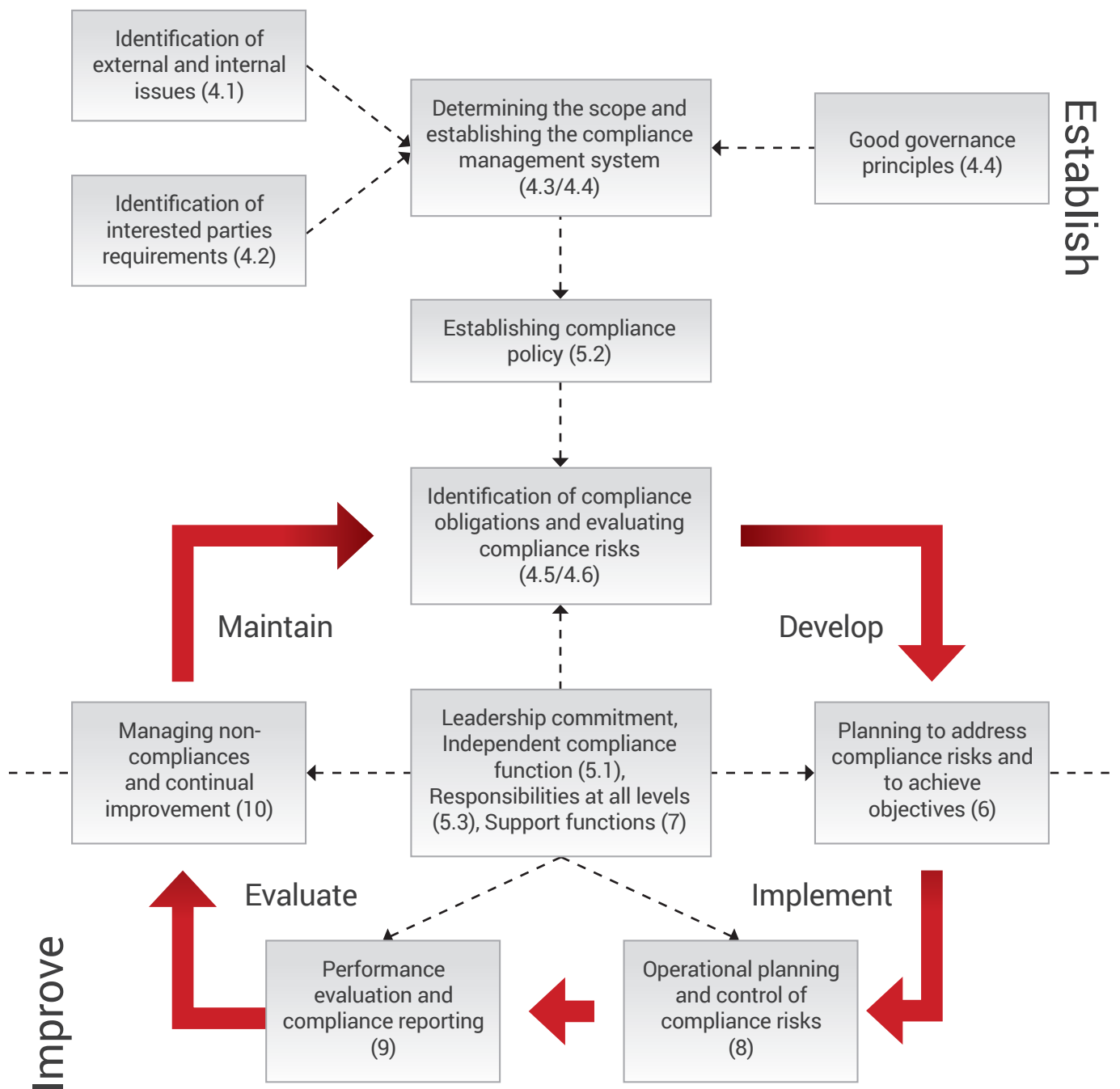
The organization's compliance management system

As stated above, ISO 19600 follows the 'High level structure' (HLS) for ISO management system standards. All the standard elements of a management system are adapted and supplemented for the subject of compliance. On top of devoting quite a bit of attention to the roles and responsibilities of the governing body, top management, and employees of an organization, the standard also underlines the importance for the independence of the compliance officer (or more general: the compliance function).

	High Level Structure for ISO management system standards	ISO 19600
Clause 4	Context of the organization	<ul style="list-style-type: none"> Understanding the organization and its context Understanding the needs and expectations of interested parties Principles of good governance Compliance obligations Assessment of compliance risks
Clause 5	Leadership	<ul style="list-style-type: none"> Leadership and commitment Establishing the organization's compliance policy Defining the organizational roles, responsibilities and authorities (including the governing body, top management, employees and compliance officer)
Clause 6	Planning	<ul style="list-style-type: none"> Planning of actions to address risks related to compliance Establishing the compliance objectives
Clause 7	Support	<ul style="list-style-type: none"> Determining and providing the necessary resources for the operation of a compliance management system Competence & training Awareness (behavior of top management & compliance culture) Communication (both internal and external) & documentation
Clause 8	Operation	<ul style="list-style-type: none"> Operational planning and control Establishing controls and procedures
Clause 9	Performance evaluation	<ul style="list-style-type: none"> Monitoring of compliance Analysis of information and reporting of results Internal Audit and Management Review
Clause 10	Improvement	<ul style="list-style-type: none"> Actions on non-compliances and nonconformities (including escalation) Corrective actions Continual improvement

ISO 19600 is written in such a form that the guidance provided there is intended to be adaptable, and the use of this guidance can differ depending on the size and level of maturity of an organization's compliance management system and on the context, nature and complexity of the organization's activities, including its compliance policy and objectives.

Determination of the compliance obligations and implementation of measures to ensure compliance with these obligations is a step-wise process. It starts with gaining insights in important external and internal circumstances, conditions and factors: the context in which the organization operates and its stakeholders. Followed by the identification of compliance obligations that the organization has and determining the compliance risk, i.e. probability and consequences of non-compliances with the identified requirements. Finally, the organization should plan, implement and monitor measures to control the compliance risks.



If an organization does not have an established management system standard or a compliance management framework, ISO 19600 can be easily adopted as a stand-alone guidance within the organization.

ISO 19600 can be combined with existing management system standards that the organization may have already implemented, such as ISO 9001, ISO 14001, and other generic guidelines.

Main terms & definitions in ISO 19600

Compliance – meeting all the organization's compliance obligations

NOTE: Compliance is made sustained by embedding it in the culture of an organization and in the behavior and attitude of people working for it.

Compliance obligation – compliance requirement or compliance commitment

Compliance requirement – requirement that an organization **has** to comply with

Compliance commitment – requirement that an organization **chooses** to comply with

Compliance culture – values, ethics, and beliefs that exist throughout an organization and interact with the organization's structures and control systems to produce behavioral norms that are conducive to compliance outcomes

Noncompliance – non-fulfilment of a compliance obligation

NOTE: Noncompliance can be a single or a multiple event and may or may not be the result of a nonconformity.

Compliance risk – effect of uncertainty on compliance objectives

NOTE: Compliance risk can be characterized by the likelihood of occurrence and the consequences of noncompliance with the organization's compliance obligations.

THE REWARDS OF A COMPLIANCE MANAGEMENT SYSTEM BASED ON THE ISO 19600

*“Let the great world spin for ever down the ringing grooves of change.”
- Alfred, Lord Tennyson*

Change is never easy, and organizations, either as a result of their own doing or simply as a result of the change in times, have no other choice but to go through this difficult path. Whether as a result of increased costs, or increasing cases of nonconformities from not meeting compliance obligations, or a bit of both, organizations face breakdowns, therefore establishing a truly effective and efficient compliance management system can be imperative.

Some organizations are already there: quickly understanding the tremendous benefits associated with being compliant. Other organizations have yet to undertake

this journey. When one considers the costs and lack of effectiveness, together with the tremendous potential, a decision to get this right becomes apparent. Those organizations that do get it right, position themselves to harvest the fruits of their success.

This is where **ISO 19600** fits into this puzzle: a compliance management system based on ISO 19600 sets up all of the prerequisites necessary to help the organization meet its obligations, both regulatory and to other stakeholders, through maintaining a culture of integrity and compliance, and through a set of best practices proven to be successful.

PECB



+1-844-426-7322



customer@pecb.com



[Help Center](#)

www.pecb.com