Compliance Made Easy

A practical guide to modern governance, risk, compliance, and information security.

2026

this page is intentionally left blank

First Published in 2026

Disclaimer

This publication is provided for general information purposes only and does not constitute legal advice. While every effort has been made to ensure accuracy, laws, regulations and standards change over time, and their application depends on each organisation's specific circumstances. Compeas AB accepts no liability for actions taken or decisions made based on this publication. For advice on your organisation's specific situation, please consult qualified legal counsel.

Compliance made easy

A practical guide to modern governance, risk, compliance, and information security.

Foreword

Thank you for opening this book.

By taking the time to read it, you have already taken an important step towards strengthening your organisation's information security and achieving compliance with recognised security standards.

This book is intended to be used—not simply read. Please feel free to highlight passages, make notes in the margins, bookmark pages, and return to it whenever you need guidance. Our goal is to create a practical and accessible resource, rather than another book that gathers dust on a shelf.

Whether you are an experienced information security professional or just beginning your journey, this book is written for you. You may have been asked to lead your organisation's compliance efforts in response to new regulations such as NIS2. You may already be certified against ISO 27001, or perhaps you are starting with little or no formal security programme in place.

Wherever your organisation is today, we hope this book provides practical knowledge, clear guidance, and the confidence to build a stronger security and compliance programme. Combined with the Compeas platform, our aim is to simplify governance, risk, and compliance so that you can spend less time managing documentation and more time improving security.

Welcome to Compeas, we are delighted to be part of your journey.

Martin Karlsson
Founder & CEO, Compeas

Table of Contents

Contents

Executive Summary

Information security and compliance have become business-critical disciplines.

Organisations today face increasing regulatory requirements, growing customer expectations, rising cyber threats, and an expanding number of standards and frameworks. Requirements such as ISO 27001, GDPR, NIS2, and industry-specific regulations such as DORA continue to increase in both complexity and importance. At the same time, customers, partners, and regulators expect organisations to demonstrate effective governance, risk management, and security practices.

For many organisations, these demands have resulted in fragmented processes, manual administration, and growing complexity. Risk registers are maintained in spreadsheets, policies are stored in shared folders, evidence is collected manually, and compliance activities often occur only in preparation for audits or customer requests. Security and compliance efforts frequently become isolated projects rather than continuous business processes.

Compeas was founded on a simple belief: information security and compliance should be easy.

Our experience has shown that many organisations wish to improve their security posture, strengthen governance, and comply with recognised standards, but often lack the resources, expertise, or tools required to manage these activities efficiently. Existing approaches are frequently costly, consultant-driven, and difficult to maintain over time.

The purpose of Compeas is to make governance, risk management, compliance, and information security accessible, understandable, and practical for organisations of all sizes.

We believe that:

- Compliance should improve security
- Risk should drive priorities
- Controls should support multiple frameworks
- Documentation should remain manageable
- Security should be continuous rather than periodic
- Technology should simplify complexity

Compeas provides organisations with a structured platform for managing governance, risk, compliance, and information security activities. By bringing together risks, controls, policies, evidence, audits, and reporting within a single solution, organisations can reduce administrative burden, improve visibility, and establish sustainable compliance programmes.

Rather than treating compliance as an annual exercise, organisations can adopt a continuous approach to security and risk management. This enables better decision-making, stronger accountability, improved operational resilience, and increased confidence among customers, regulators, and stakeholders.

This book introduces the philosophy, methodology, and technology behind Compeas. It describes the challenges organisations face, the principles that guide our work, and the practical approaches that can help organisations strengthen their information security and compliance capabilities.

Our ambition is not simply to help organisations satisfy regulatory requirements. The ambition is to help organisations build trust. Because security and compliance should not be barriers to growth, they should be foundations for sustainable and responsible business.

Done right, information security becomes a business enabler — not a barrier.

The Current Security Landscape

Information security has evolved from a technical concern into a business-critical responsibility.

Organisations today operate in an increasingly interconnected environment where digital systems, cloud services, remote working, and third-party suppliers have become essential to daily operations. While these developments have created new opportunities, they have also introduced new risks, greater complexity, and higher expectations from customers, regulators, and business partners.

Security is no longer solely the responsibility of IT departments. It has become a matter of governance, risk management, operational resilience, and business continuity.

Artificial Intelligence is Creating New Challenges

Artificial Intelligence (AI) is transforming how organisations operate, from automating routine tasks to supporting decision-making, and has quickly become embedded in everyday business operations.

Alongside these opportunities come challenges. Organisations must understand how AI systems are used, what data they process, and how they impact security, privacy, governance, and regulatory compliance. Rapid adoption also introduces risks such as unauthorised use of AI tools, inaccurate or misleading outputs, data leakage, and more sophisticated cyber threats.

For organisations operating in the EU, AI also raises issues around data sovereignty, regulatory compliance, and jurisdiction. Many AI services are developed and run outside the EU, so organisations must assess where data is processed, which legal frameworks apply, and whether sensitive information should be shared with external providers.

AI should never be the decision-maker, it should act as an assistant.

Rising Customer Expectations

Customers, partners, suppliers, and procurement teams increasingly expect organisations to demonstrate effective security practices.

Security questionnaires, supplier assessments, contractual requirements, and requests for evidence have become commonplace. Many organisations must demonstrate compliance with recognised standards before entering into new business relationships or participating in procurement processes. Trust has become a competitive advantage.

Organisations that can demonstrate strong governance, effective risk management, and robust security controls are often better positioned to win business and maintain customer confidence.

Growing Dependence on Third Parties

Modern organisations rely on a wide range of external suppliers, cloud providers, consultants, and technology partners.

While these relationships create value, they also introduce additional risk. Third-party incidents, supply chain vulnerabilities, and service disruptions can directly affect an organisation's operations, reputation, and regulatory obligations.

As a result, organisations increasingly need visibility not only into their own security posture but also into the risks associated with their suppliers and external partners.

The Challenge of Security Questionnaires

Many organisations spend considerable time responding to customer security questionnaires, due diligence requests, and audit enquiries.

Questions relating to policies, controls, risk management, incident handling, and regulatory compliance often require information from multiple systems and stakeholders.

Without a structured approach, these requests can become time-consuming, repetitive, and difficult to manage, placing significant demands on internal teams.

Audit Fatigue and Manual Processes

Despite increasing expectations, many organisations continue to manage security and compliance activities using spreadsheets, documents, shared folders, and email.

Evidence is collected manually. Policies become scattered across multiple locations. Risk registers quickly become outdated, and responsibilities are often unclear. As a result, audits become time-consuming projects rather than part of a continuous process.

These manual approaches reduce visibility, increase administrative effort, and make it more difficult to demonstrate compliance and maintain a strong security posture.

From Compliance to Continuous Improvement

Information security is no longer simply about passing audits or satisfying regulatory requirements.

Modern organisations increasingly recognise that effective governance, risk management, and compliance strengthen operational resilience, build customer trust, and support long-term business success.

Security is becoming a continuous process rather than a periodic exercise. Risk management is becoming part of everyday decision-making, and compliance is evolving from documentation to demonstrable action.

Organisations that embrace this shift are better equipped to manage uncertainty, respond to change, and build lasting trust with customers, regulators, and other stakeholders.

The challenge is no longer recognising that security matters—it is finding practical and sustainable ways to manage it.

The Regulatory Landscape

The European Union, together with its Member States, has introduced new cybersecurity strategies and adopted the Cyber Resilience Act and the NIS2 Directive to strengthen cyber resilience across the region. Everyone can agree that there is a lot happening within the regulatory landscape.

Increasing Regulatory Requirements

Across Europe and around the world, organisations face an increasing number of legal, regulatory, and contractual requirements relating to information security, privacy, and operational resilience.

Developments such as the NIS2 Directive reflect a broader shift towards stronger governance and greater accountability. Organisations are increasingly expected to demonstrate structured risk management, effective security controls, and ongoing compliance rather than relying on periodic compliance exercises.

A Shift Towards Accountability

Modern regulations place greater emphasis on accountability than ever before. Organisations are expected not only to implement appropriate security measures but also to demonstrate that risks are identified, responsibilities are clearly assigned, and security decisions are documented and regularly reviewed.

Information security is no longer solely an IT or product responsibility. Senior management and boards are increasingly expected to oversee security, allocate appropriate resources, and ensure that governance and risk management are embedded throughout the organisation.

One Organisation, Many Frameworks

Few organisations are required to comply with a single standard or regulation. Instead, they often need to satisfy multiple frameworks such as ISO 27001, GDPR, NIS2, DORA, and customer-specific security requirements at the same time.

Although these frameworks have different objectives, many of their requirements overlap. A risk assessment, access control policy, or incident response process may satisfy requirements across several standards simultaneously. Understanding these commonalities enables organisations to reduce duplication, simplify compliance activities, and maintain a more efficient governance, risk, and compliance programme.

From Annual Compliance to Continuous Compliance

Traditionally, many organisations have approached compliance as a periodic activity driven by audits, certifications, or regulatory deadlines. Policies are reviewed shortly before an audit, evidence is gathered manually, and risk assessments are updated only when required.

Modern governance and information security require a different approach. Security risks evolve continuously, regulations change, and new threats emerge every day. As a result, compliance can no longer be treated as a once-a-year exercise.

Leading organisations are adopting continuous governance, risk, and compliance practices that embed security into everyday operations. By monitoring risks, maintaining documentation, and collecting evidence throughout the year, organisations are better prepared for audits, respond more effectively to change, and strengthen both their security posture and organisational resilience.

Demonstrating Trust Through Compliance

Information security has become an important factor in how organisations build trust with customers, partners, investors, and regulators. Increasingly, organisations are expected to demonstrate that appropriate governance, risk management, and security controls are in place before business relationships are established.

Security questionnaires, supplier assessments, certifications, and customer audits have become a standard part of doing business. Organisations that can quickly provide evidence of their security practices are often better positioned to win new business, respond to customer requirements, and strengthen long-term relationships.

Compliance should therefore not be viewed solely as a regulatory obligation, but as an opportunity to demonstrate professionalism, resilience, and a commitment to protecting information.

The Rise of Digital Resilience

As organisations become increasingly dependent on digital systems, maintaining resilience has become just as important as preventing security incidents. Cyberattacks, system failures, supply chain disruptions, and human error can all affect an organisation's ability to operate.

Modern security programmes therefore focus not only on protecting information but also on ensuring that critical services can continue during and after an incident. Effective governance, business continuity planning, incident response, and disaster recovery all play an essential role in building digital resilience.

Organisations that invest in resilience are better prepared to respond to disruption, recover more quickly, and maintain the trust of customers, partners, and regulators.

Governance Beyond IT

Information security and compliance are no longer the sole responsibility of IT departments. As organisations become more digital and interconnected, governance, risk management, and security responsibilities extend across the entire business.

Executive leadership is expected to set direction, allocate resources, and ensure that appropriate governance structures are in place. Legal, procurement, HR, operations, and finance all play an important role in managing risk and maintaining compliance.

Effective governance requires clear ownership of controls, well-defined responsibilities, and collaboration across departments. Security decisions are increasingly embedded into everyday business processes rather than handled as isolated technical activities.

Organisations that treat governance as a cross-functional discipline are better equipped to manage risk consistently, respond to regulatory expectations, and maintain strong security practices over time.

Preparing for the Future

The regulatory landscape will continue to evolve as technology advances, cyber threats become more sophisticated, and organisations become increasingly interconnected. New legislation, industry standards, and customer expectations will continue to shape how organisations manage information security and compliance.

Rather than treating each new requirement as a separate project, organisations should establish governance programmes that are adaptable, risk-based, and designed for continuous improvement. A strong governance, risk, and compliance framework enables organisations to respond more effectively to change while maintaining security, resilience, and trust.

Preparing for the future is not about predicting every new regulation, it is about building a foundation that allows organisations to adapt with confidence.

For a detailed overview of our approach to information security, data protection and regulatory compliance, see our Information Security White Paper, available at compeas.com. It explains the governance, technical controls and operational processes that underpin our platform and demonstrates how we support customers in meeting evolving regulatory requirements.

Why Traditional GRC Fails

For many organisations, governance, risk, and compliance have evolved gradually over many years. New regulations, customer requirements, and internal processes have often been addressed individually, resulting in a collection of disconnected documents, spreadsheets, and manual processes.

While these approaches may have been sufficient in the past, they become increasingly difficult to manage as organisations grow, regulations evolve, and security expectations continue to rise.

Modern governance requires more than documentation—it requires visibility, accountability, and continuous improvement.

In this chapter, we explore seven common reasons why traditional GRC approaches no longer meet the needs of modern organisations. Understanding these challenges provides the foundation for building a governance programme that is more efficient, resilient, and prepared for the future.

Reason 1

Information Becomes Fragmented

Policies, procedures, risk assessments, audit reports, and evidence are often stored across multiple systems, shared drives, and email conversations. As information becomes fragmented, it becomes increasingly difficult to maintain consistency, locate documentation, and demonstrate compliance.

Without a single source of truth, organisations spend valuable time searching for information instead of managing risk and improving security.

When information is fragmented, governance becomes reactive, collaboration becomes difficult, and demonstrating compliance requires unnecessary time and effort.

Reason 2

Manual Processes Do Not Scale

Many governance activities still rely on spreadsheets, documents, and manual reminders. As the number of controls, assets, suppliers, and regulatory requirements increases, these processes become difficult to maintain and increasingly prone to human error.

What begins as a manageable process can quickly become an administrative burden that consumes valuable time and resources.

Reason 3

Compliance Becomes Reactive

In many organisations, governance activities intensify only when an audit, certification, or customer assessment approaches. Documentation is updated, evidence is gathered, and risks are reviewed shortly before deadlines.

This reactive approach places unnecessary pressure on teams and limits the organisation's ability to identify and address risks proactively.

Reason 4

Responsibilities Become Unclear

Effective governance depends on clear ownership. Every policy, control, risk, asset, and compliance activity should have an identified owner who is responsible for maintaining it and ensuring it remains effective.

In traditional GRC programmes, responsibilities are often spread across departments without clearly defined accountability. As organisations grow, tasks may be overlooked, duplicated, or delayed simply because it is unclear who is responsible.

Clearly assigning ownership enables organisations to strengthen accountability, improve collaboration, and ensure that governance and compliance activities become part of everyday business operations rather than isolated initiatives.

Reason 5

Controls Become Duplicated

Many organisations manage each regulation, standard, or customer requirement as a separate compliance initiative. As a result, similar controls, policies, and procedures are often created multiple times, despite addressing the same underlying security objective.

For example, access management, incident response, supplier management, and information security policies are common requirements across frameworks such as ISO 27001, GDPR, NIS2, and DORA. Managing these controls separately increases administrative effort, creates inconsistencies, and makes ongoing maintenance more difficult.

A mature governance programme recognises these commonalities. By implementing controls once and mapping them to multiple frameworks, organisations can reduce duplication, improve consistency, and maintain compliance more efficiently.

Reason 6

Limited Visibility

Effective governance depends on accurate and timely information. Decision-makers need clear visibility into risks, controls, compliance activities, and the overall security posture of the organisation in order to make informed decisions.

Traditional GRC approaches often rely on spreadsheets, documents, and manual reporting, making it difficult to obtain an up-to-date view of compliance. Information quickly becomes outdated, progress is difficult to track, and identifying gaps or emerging risks requires significant manual effort.

Without meaningful visibility, organisations are forced to make decisions based on incomplete or outdated information. A centralised and continuously maintained governance programme enables better oversight, supports informed decision-making, and helps organisations respond more effectively to changing risks and regulatory requirements.

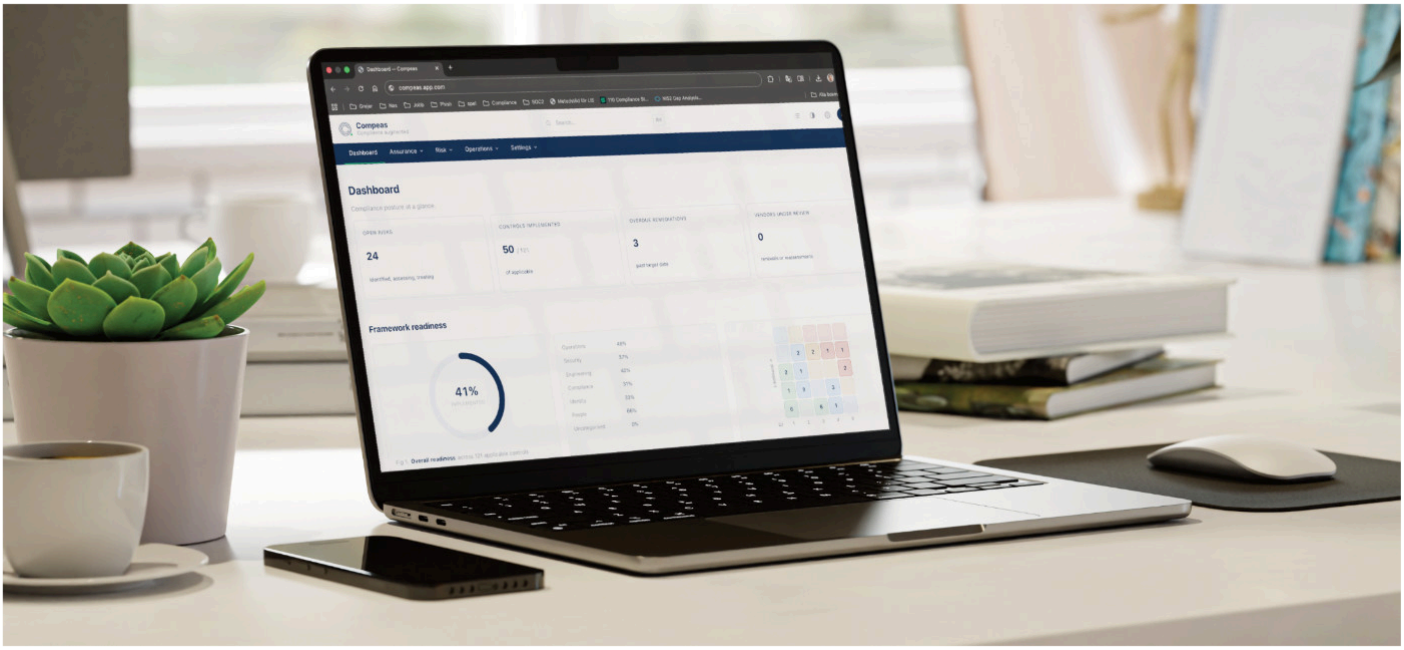
Reason 7

Continuous Improvement Becomes Difficult

Effective governance is not a one-time project but an ongoing process of evaluating risks, reviewing controls, and adapting to changing business and regulatory requirements. As organisations grow and technologies evolve, governance programmes must evolve with them.

Traditional GRC approaches often make continuous improvement difficult. Manual processes, fragmented information, and unclear ownership limit an organisation's ability to monitor progress, identify opportunities for improvement, and respond proactively to change.

Organisations that embrace continuous improvement are better equipped to strengthen their security posture, maintain compliance, and build long-term resilience. Governance should not be viewed as a destination, but as a continuous journey towards greater maturity, accountability, and trust.



Traditional governance approaches were developed for a different era. Today's organisations require governance programmes that are collaborative, continuously maintained, and capable of adapting to changing risks, technologies, and regulations. Effective governance is no longer about managing documents—it is about enabling better decisions, reducing risk, and building organisational resilience.

The Compeas Philosophy

Compliance Made Easy is more than a motto, it reflects our belief that governance, risk, and compliance should be accessible, practical, and integrated into everyday business operations.

Technology alone does not create better governance, stronger security, or improved compliance. Successful organisations combine people, processes, and technology to establish governance programmes that are sustainable, effective, and aligned with their business objectives.

At Compeas, we believe governance, risk, and compliance should empower organisations rather than create unnecessary administrative burden. Security should be embedded into everyday operations, compliance should support better decision-making, and governance should enable continuous improvement rather than periodic audits.

The principles in this chapter reflect the philosophy on which Compeas was built. They are not simply product features, but guiding principles that we believe help organisations build stronger security, reduce complexity, and create lasting organisational resilience. After all, making compliance easier should never mean compromising on security, it should mean making good governance achievable for every organisation.

Principle 1

Compliance Should Improve Security

Compliance should never become an objective in itself. While regulations, standards, and certifications provide valuable guidance, their true purpose is to help organisations establish stronger governance, reduce risk, and improve information security.

An effective compliance programme should therefore lead to measurable improvements in security rather than simply producing documentation for audits. Policies should be implemented because they support good governance, controls should reduce real organisational risks, and evidence should demonstrate that security practices are operating effectively in everyday business.

When compliance is treated as a tool for strengthening security rather than satisfying auditors, organisations create lasting value that extends far beyond meeting regulatory requirements.

Principle 2

Controls Should Support Multiple Frameworks

Modern organisations are rarely required to comply with a single standard or regulation. Instead, they must satisfy multiple frameworks, contractual obligations, and customer requirements, many of which address the same underlying security objectives.

Rather than managing each framework independently, organisations should implement security controls that can be mapped to multiple frameworks.

A well-designed access control process, supplier risk management procedure, or incident response plan can often satisfy requirements across ISO 27001, GDPR, NIS2, DORA, and other recognised frameworks.

By reducing duplication and maintaining a single set of well-managed controls, organisations can simplify compliance, improve consistency, and spend more time strengthening their overall security posture.

Principle 3

Simplicity Creates Adoption

Governance, risk, and compliance should be accessible to everyone within an organisation, not just information security specialists. Processes that are overly complex, difficult to understand, or time-consuming to maintain often discourage participation and reduce the effectiveness of a governance programme.

When policies are easy to understand, responsibilities are clearly defined, and governance activities fit naturally into everyday business operations, employees are more likely to engage with them and contribute to a stronger security culture.

Simplicity is not about lowering standards or reducing quality. It is about removing unnecessary complexity so organisations can focus on managing risk, improving security, and achieving compliance with confidence.

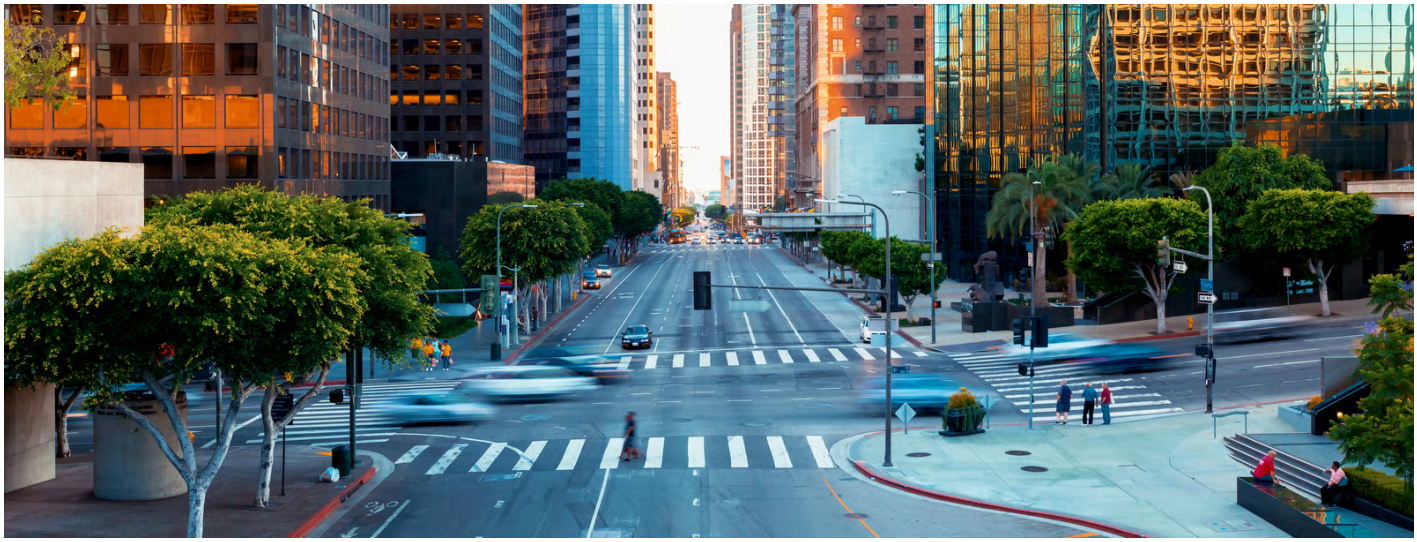
Principle 4

Risk Should Drive Priorities

Every organisation faces a unique combination of risks, business objectives, and regulatory requirements. Effective governance is therefore not about treating every issue equally—it is about understanding which risks have the greatest potential impact and prioritising resources accordingly.

Risk assessments provide the foundation for informed decision-making. By identifying and evaluating risks, organisations can focus their efforts where controls are most needed, allocate resources effectively, and address the issues that present the greatest threat to their objectives.

A risk-based approach enables organisations to move beyond checklist compliance and make decisions that strengthen security, support business objectives, and improve long-term resilience.



Principle 5

Automation Should Reduce Administrative Work

Effective governance relies on people making informed decisions, but many governance activities remain repetitive, manual, and time-consuming. Collecting evidence, tracking tasks, sending reminders, maintaining documentation, and preparing for audits often consume valuable time that could be spent managing risk and improving security.

Automation should support governance by reducing administrative effort rather than replacing human judgement. Routine activities can be streamlined, allowing organisations to work more efficiently while maintaining visibility, accountability, and control.

By reducing manual work, organisations can focus on what matters most, understanding risk, strengthening security, and making better decisions.

Principle 6

Governance Requires Visibility

Effective governance depends on accurate, timely, and accessible information. Without a clear understanding of risks, controls, assets, policies, and compliance activities, organisations cannot make informed decisions or respond effectively to changing circumstances.

Visibility is more than reporting, it is about creating a shared understanding of the organisation's security and compliance posture. When information is centralised and continuously maintained, decision-makers can identify emerging risks, monitor progress, and take action with confidence.

Better visibility leads to better decisions. By providing a clear view of governance activities, organisations can strengthen accountability, improve collaboration, and maintain compliance more effectively.

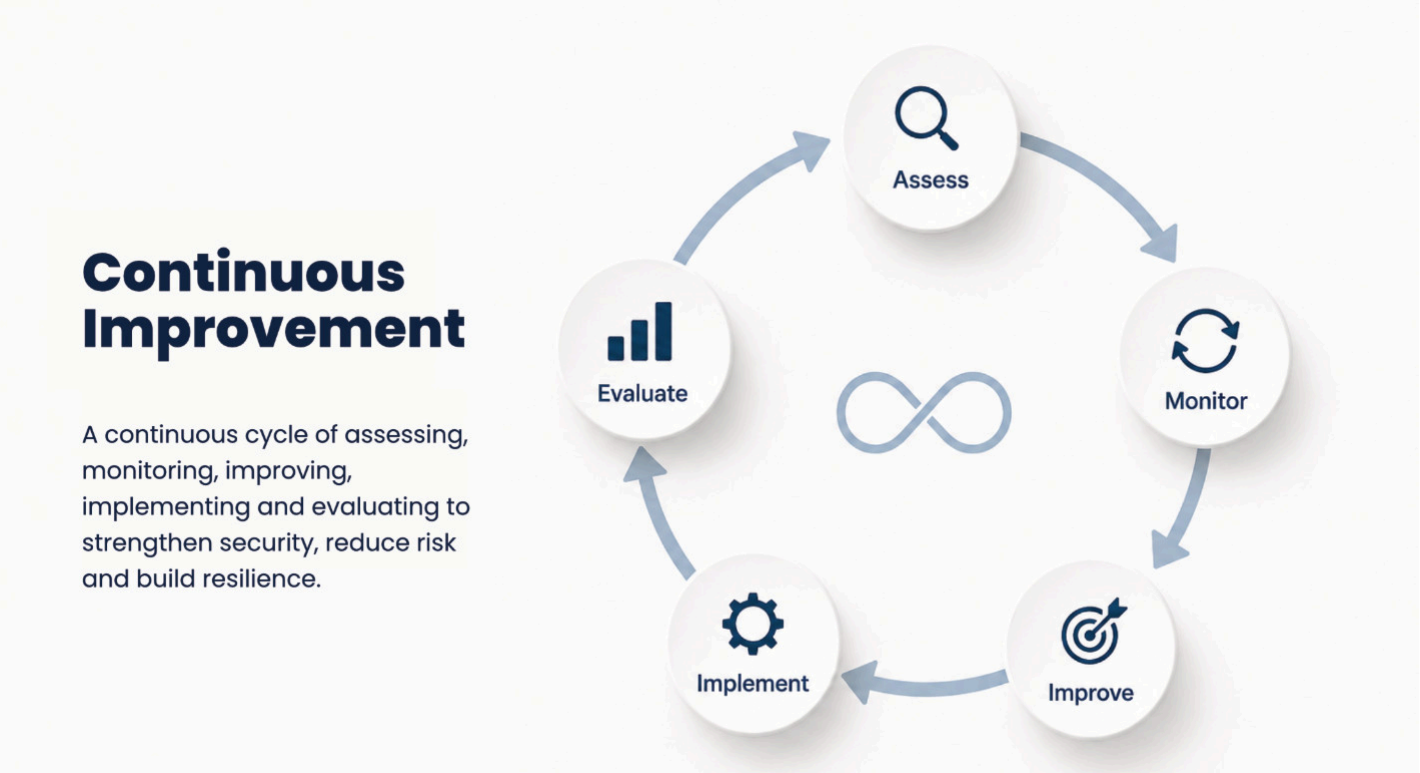
Principle 7

Continuous Improvement

Governance, risk, and compliance are not projects with a defined end point. Organisations evolve, technologies change, regulations develop, and new risks emerge. Maintaining an effective governance programme therefore requires continuous review, adaptation, and improvement.

Continuous improvement encourages organisations to regularly evaluate risks, measure the effectiveness of controls, learn from incidents, and identify opportunities to strengthen their security posture. Small, consistent improvements over time are often more effective than infrequent, large-scale initiatives.

Organisations that embrace continuous improvement are better prepared to adapt to change, respond to emerging challenges, and build lasting resilience. Governance should not be viewed as a destination, but as an ongoing commitment to improving security, reducing risk, and supporting long-term business success.



The Compeas Philosophy is built on a simple belief: governance should strengthen organisations, not slow them down. By focusing on security, simplicity, risk, visibility, automation, and continuous improvement, organisations can create governance programmes that are not only compliant, but resilient, efficient, and sustainable.

The Compeas Platform

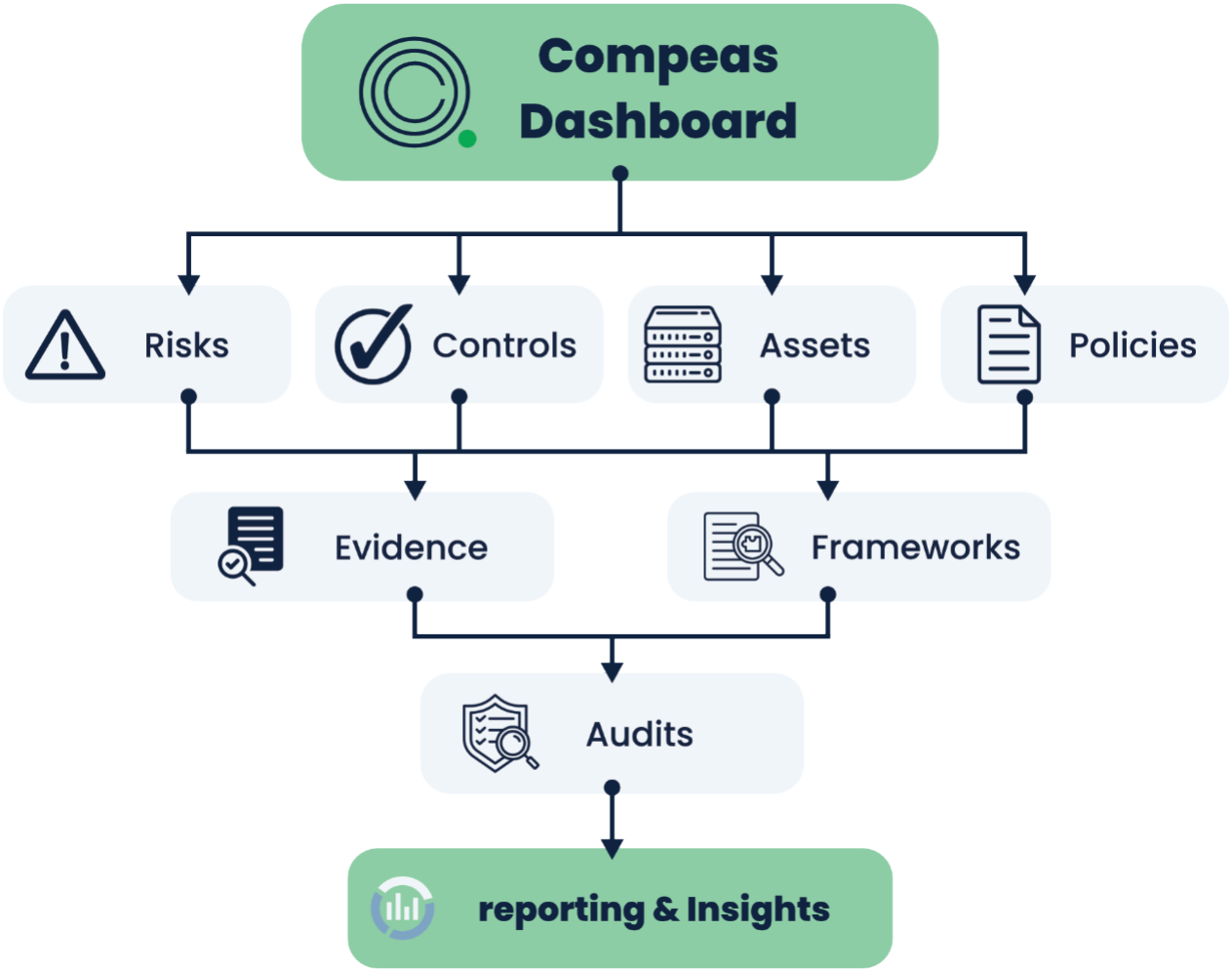
Technology should support good governance, not define it.

The Compeas platform has been designed around the principles presented in the previous chapter, helping organisations simplify governance, risk, and compliance while strengthening their information security.

Compeas brings together the core components of a modern governance programme into a single platform. Rather than managing risks, controls, policies, evidence, audits, and compliance activities across multiple systems, organisations gain a centralised workspace that supports collaboration, accountability, and continuous improvement.

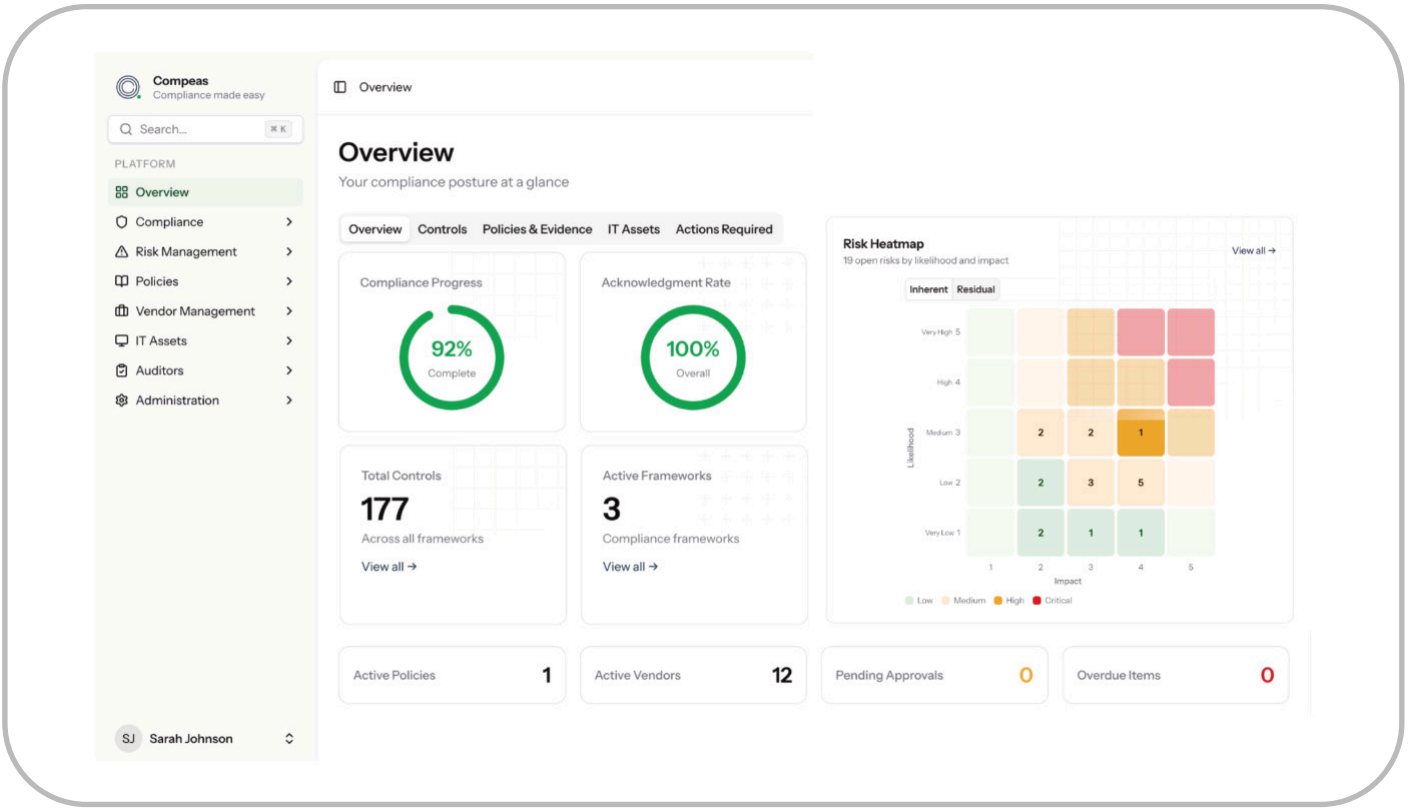
Whether your organisation is implementing its first compliance framework or managing multiple regulatory requirements across several business units, Compeas provides the tools needed to build, maintain, and continuously improve your governance programme.

The following pages introduce the platform's core capabilities and demonstrate how they work together to support modern governance, risk, compliance, and information security.



The Dashboard

The Dashboard, referred to as Overview within the Compeas platform, provides a central view of your organisation's governance, risk, and compliance programme. Designed to present the most important information in a clear and intuitive way, it enables you to quickly understand the organisation's current security and compliance posture and identify areas that require attention.



Key Benefits

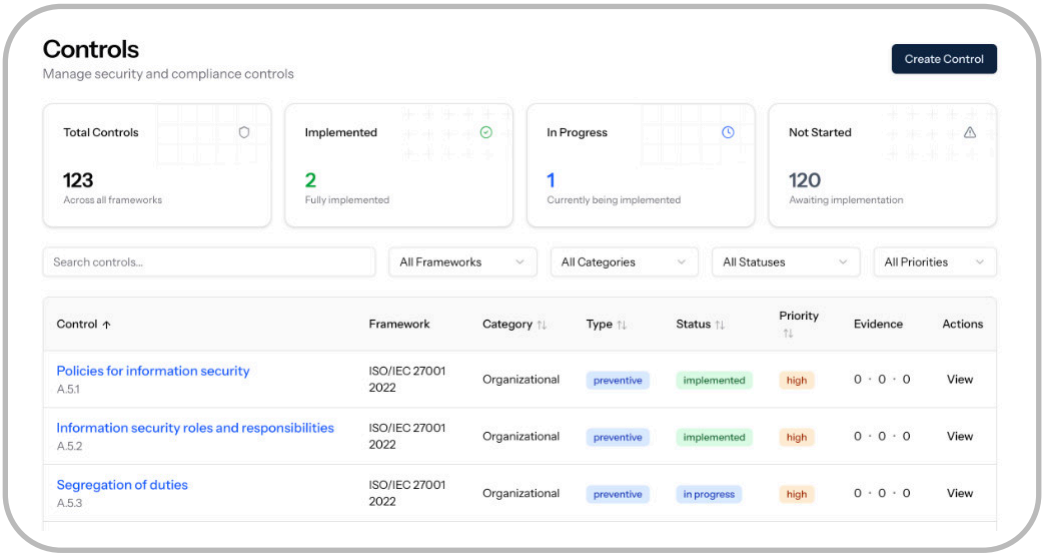
- Gain an immediate overview of governance, risk, and compliance activities.
- Monitor key metrics, outstanding tasks, and upcoming reviews.
- Identify high-priority risks and compliance activities.
- Improve visibility across teams through a single source of truth.
- Support informed decision-making with real-time information.

The Overview page serves as the starting point for the Compeas platform, providing quick access to every aspect of your governance programme and helping organisations maintain visibility, accountability, and continuous improvement.

Compliance

The Compliance capability provides a structured approach to managing security and compliance requirements across recognised standards and regulations. By bringing frameworks, controls, evidence, and testing together in a single workspace, organisations can demonstrate compliance while strengthening their overall security posture.

Rather than treating each framework independently, Compeas enables organisations to implement controls once and map them to multiple frameworks, reducing duplication and simplifying ongoing compliance activities.



How it helps

Manage multiple frameworks, including ISO 27001, NIS2, GDPR, and other recognised standards.

- Implement and maintain security controls from a central location.
- Map controls to multiple frameworks to reduce duplication.
- Collect and organise evidence to demonstrate compliance.
- Perform control testing to verify that controls operate effectively.
- Create repeatable test procedures to support continuous assurance and audit readiness.

By combining frameworks, controls, evidence, and testing within a single capability, organisations can move beyond periodic compliance exercises and establish a governance programme built on continuous improvement.

Risk Management

Effective risk management enables organisations to identify, assess, and reduce risks before they become incidents. The Risk Management capability provides a structured approach to documenting risks, prioritising remediation activities, and monitoring progress over time.

Each identified risk can be assessed based on its likelihood and impact, providing a clear understanding of the organisation's overall risk exposure. Risks can then be assigned to appropriate owners, linked to remediation activities, and monitored throughout their lifecycle to ensure they are addressed effectively.

Inherent Risk

Residual Risk

How it helps

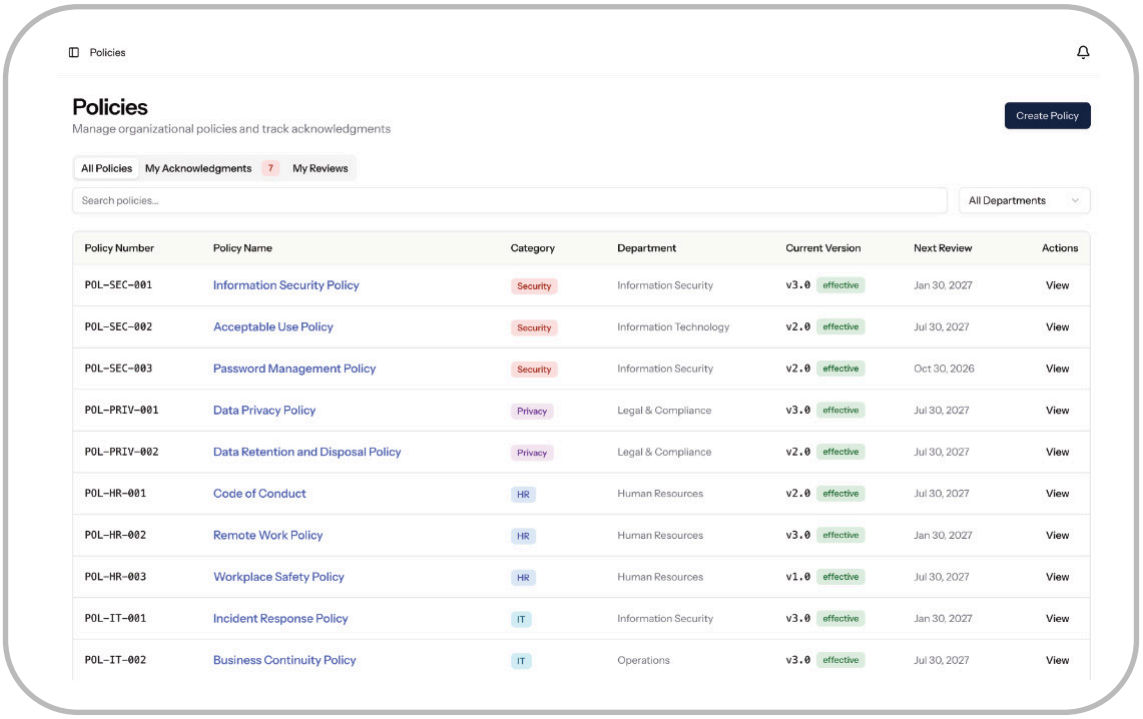
- Maintain a centralised register of organisational risks.
- Assess risks using likelihood and impact to support prioritisation.
- Visualise risk exposure through an interactive risk matrix.
- Track remediation activities and monitor their progress.
- Assign ownership and accountability for identified risks.
- Maintain visibility of organisational risk through the Overview page.

By providing a consistent approach to risk management, organisations can make informed decisions, prioritise resources effectively, and continuously improve their security posture.

Policies

Policies provide the foundation for effective governance by defining how an organisation manages information security, risk, and compliance. The Policies capability enables organisations to create, maintain, review, and approve policies through a structured and repeatable process.

By managing policies within a centralised workspace, organisations can ensure that documentation remains current, responsibilities are clearly defined, and periodic reviews are completed on time. This helps demonstrate compliance while ensuring that policies continue to reflect the organisation's objectives, regulatory requirements, and evolving risk landscape.



How it helps

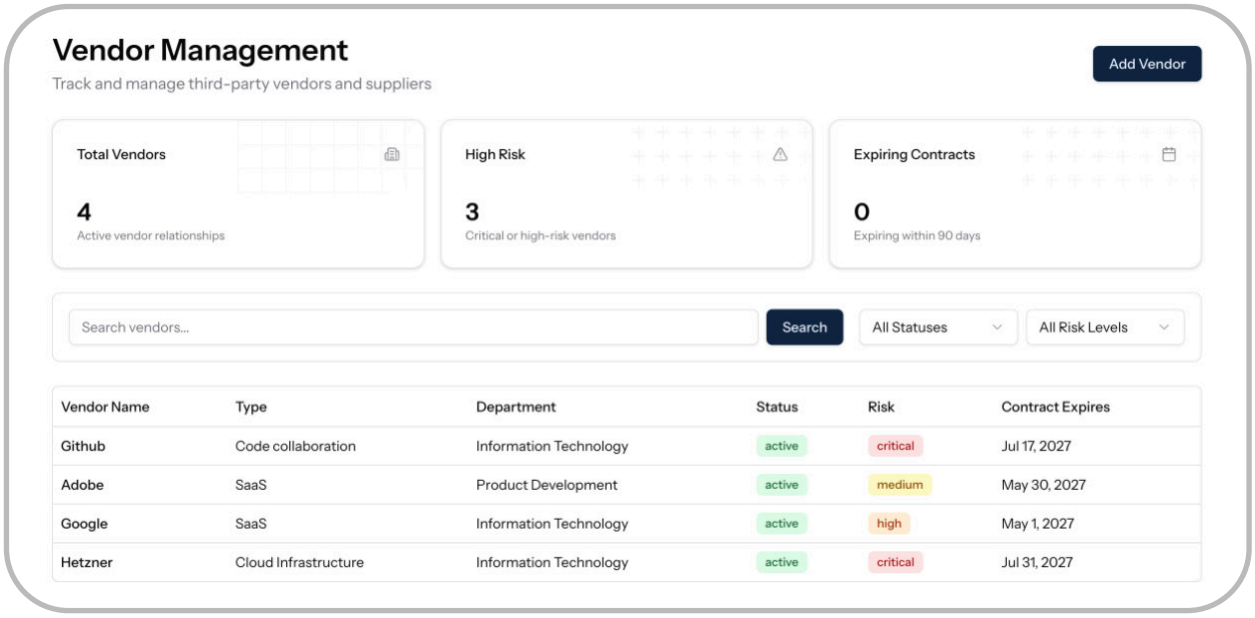
- Maintain a central repository for organisational policies.
- Manage policy reviews through a structured review process.
- Assign policy owners and review responsibilities.
- Track upcoming and completed policy reviews.
- Ensure policies remain current and aligned with business and regulatory requirements.

Effective policies are more than documents—they provide the foundation for consistent governance, informed decision-making, and continuous compliance.

Vendor Management

Third-party suppliers play an important role in modern organisations, but they can also introduce significant security, privacy, and operational risks. The Vendor Management capability provides a structured approach to maintaining oversight of suppliers throughout their lifecycle, helping organisations strengthen governance and reduce third-party risk.

By maintaining a central register of vendors, organisations can document supplier information, assess potential risks, assign ownership, and demonstrate appropriate oversight during audits and compliance assessments.



How it helps

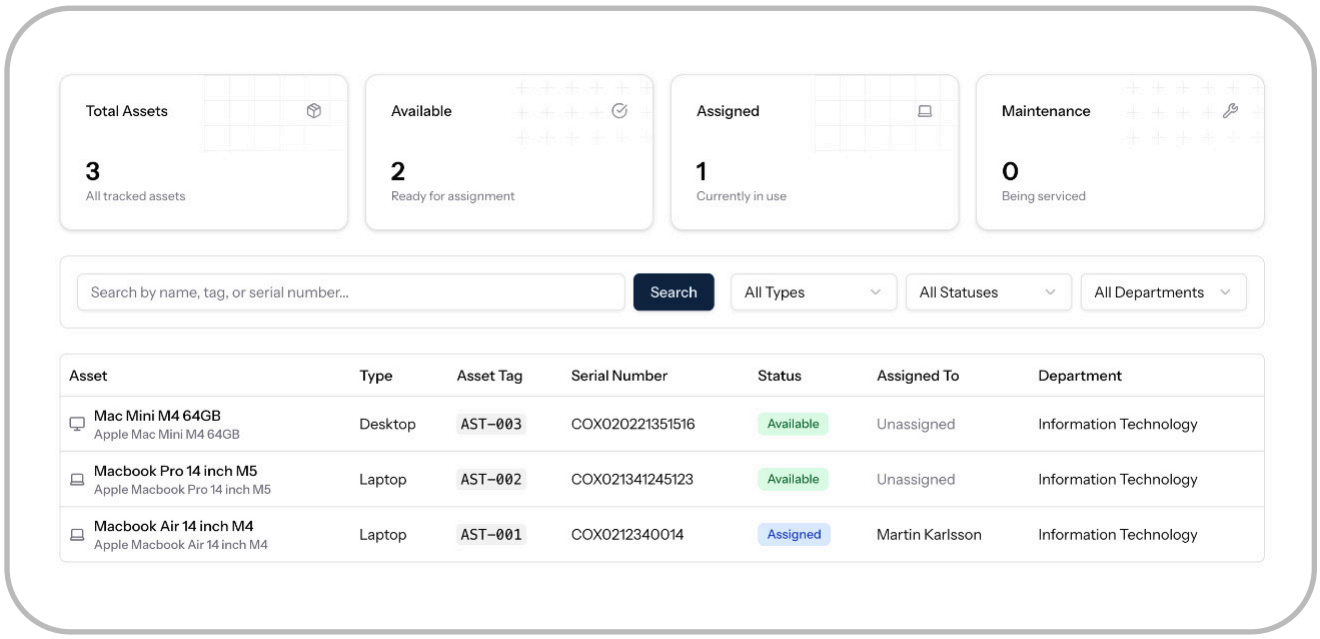
- Maintain a central register of suppliers and third-party vendors.
- Record key information relating to each vendor.
- Assess and monitor supplier-related risks.
- Assign ownership and accountability for vendor relationships.
- Support supplier due diligence and ongoing monitoring.
- Demonstrate effective third-party governance during audits and assessments.

Effective vendor management strengthens organisational resilience by helping organisations understand, manage, and reduce the risks associated with third-party suppliers.

IT Assets

Maintaining an accurate inventory of IT assets is fundamental to effective governance, risk management, and information security. The IT Assets capability enables organisations to maintain visibility of their hardware, software, and other technology assets, providing a solid foundation for managing risk and supporting compliance.

By centralising asset information, organisations gain a better understanding of what needs to be protected, who is responsible for each asset, and how assets relate to risks, controls, and compliance activities.



How it helps

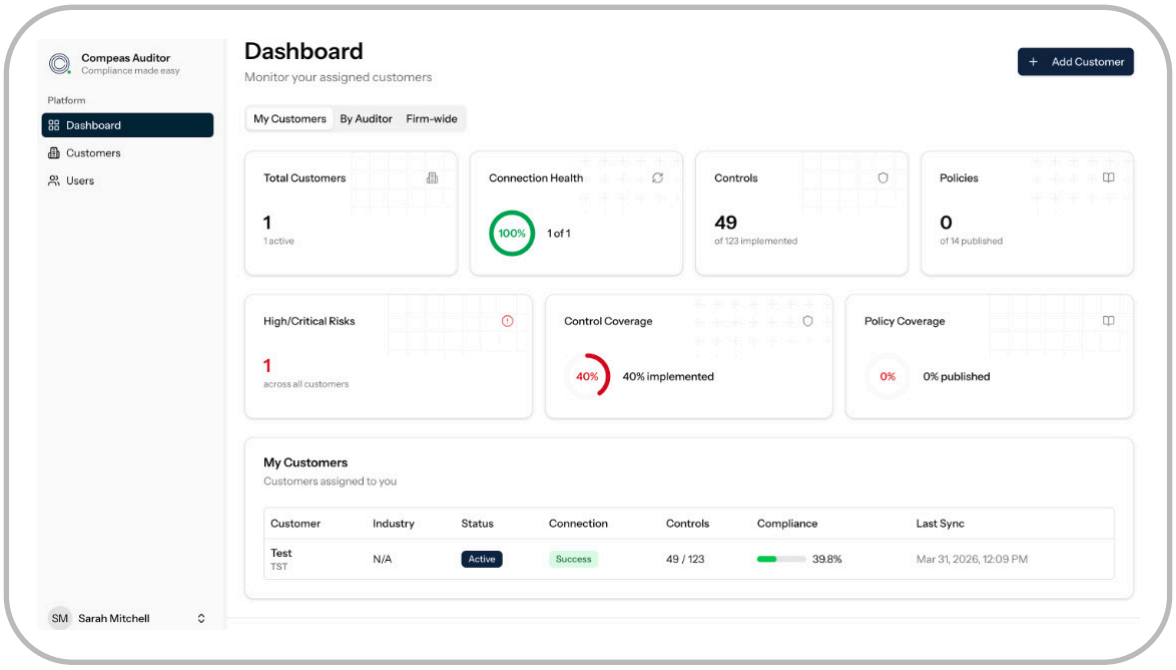
- Maintain a central inventory of IT assets and software.
- Record key information, including ownership and asset details.
- Improve visibility across the organisation's technology environment.
- Support risk assessments and security controls through accurate asset information.
- Strengthen governance by maintaining an up-to-date asset inventory.
- Demonstrate effective asset management during audits and compliance assessments.

An accurate asset inventory is the foundation of effective information security. Organisations cannot protect, monitor, or manage what they do not know exists.

Auditors

Preparing for audits should be a structured and collaborative process rather than a last-minute exercise. The Auditors capability provides a secure workspace where organisations can collaborate with external auditors, share evidence, respond to requests, and manage audit activities from a single location.

By centralising communication and evidence, organisations can improve transparency, reduce administrative effort, and maintain a clear record of audit-related activities throughout the engagement.



How it helps

- Connect securely with external auditors.
- Share evidence directly through the platform.
- Manage evidence requests and responses in one place.
- Review comments and audit feedback.
- Track review markers and audit progress.
- Create and manage secure auditor connections using API keys.

By bringing audit collaboration into the governance programme, organisations can simplify audit preparation, reduce duplication, and demonstrate compliance with greater confidence.

Why Organisations Choose Compeas

Organisations choose Compeas because it turns the principles of good governance into everyday practice. One platform replaces scattered spreadsheets, documents, and manual processes — giving you a single source of truth for risks, controls, policies, vendors, and audits. Here are six reasons why organisations across Europe build their governance programmes on Compeas.

1

One Platform

Manage governance, risk, compliance, policies, IT assets, vendors and audits from one platform, giving organisations one source of truth.

2

Built Around Recognised Frameworks

Support internationally regognised standards and regulations, including ISO 27001, NIS2, GDPR and many more

3

Implement Once Comply With Multiple Frameworks

Map a single control to multple frameworks, reducing duplication, simplify maintenance and improve consistency across the goveranance programme.

4

Continuous Compliance

Replace periodic compliance exercises with continuous monitoring, evidence collection, policy reviews, control testing and ongoing improvement.

5

Built for Collaboration

Bring management, compliance teams, IT, business stakeholders and external auditors togheter in a secure and collaborative workspace.

6

Compliance Made Easy

Designed to simplify compliance rather than complicate it, allowing organisations to spend less time on administration and more time improving security.

About Compeas

Compeas was founded in 2026 by former CISO and security professional Martin Karlsson, with the ambition of becoming the leading European Governance, Risk, and Compliance (GRC) platform.

From the very beginning, our mission has been simple: to make governance, risk, and compliance easier to understand, easier to manage, and easier to maintain.

We believe organisations should spend less time navigating complex processes and disconnected systems, and more time improving security, managing risk, and building trust. Technology should support good governance, not create additional complexity.

This philosophy is reflected in everything we build. From the way the platform is designed to the way we work with our customers, our focus remains the same: helping organisations establish practical, sustainable, and effective governance programmes.

Compliance Made Easy is more than our motto—it is the principle that guides our products, our services, and our commitment to helping organisations succeed.

Our Mission

Our mission is to help organisations simplify governance, strengthen information security, and build trust through modern compliance.

We believe that governance, risk, and compliance should empower organisations rather than slow them down. By reducing complexity, improving visibility, and supporting continuous compliance, we enable organisations to focus on what matters most, protecting their business, managing risk, and achieving their strategic objectives.

Every decision we make, every feature we develop, and every customer relationship we build is guided by a single principle:

Compliance Made Easy.

Our Vision

We envision a future where governance, risk, and compliance are no longer viewed as administrative obligations, but as strategic enablers of trust, resilience, and business success.

As regulatory requirements continue to evolve and organisations increasingly rely on digital technologies, governance must become more intelligent, collaborative, and continuous. Compliance should be embedded into everyday operations, supported by technology that provides visibility, automation, and confidence without adding unnecessary complexity.

At Compeas, we are committed to building a platform that helps organisations navigate this future. By combining modern technology with practical governance principles, we aim to make governance accessible, effective, and sustainable for organisations of every size.

Our vision is simple: to become Europe's leading Governance, Risk, and Compliance platform by helping organisations build stronger security, reduce risk, and make compliance easy.

Thank you

Thank you for taking the time to read our introductory book.

We hope this book has provided valuable insights into modern governance, risk, and compliance, and demonstrated how a simpler, more practical approach can help organisations strengthen security, manage risk, and build trust.

Whether your organisation is just beginning its compliance journey or managing multiple regulatory frameworks across the enterprise, Compeas is designed to help you move from complexity to clarity.

If you would like to learn more about the Compeas platform or arrange a personalised demonstration, we would be delighted to hear from you.

Compeas

Compliance Made Easy

www.compeas.com

info@compeas.com

linkedin.com/company/compeas

Scan the QR code below to get straight to our webpage: