CERTIFIED DIGITAL PRACTITIONER: GOVERNANCE, RISK AND COMPLIANCE

SAQA ID: 1303

Module 1: Governance

NAVIGATE COMPLIANCE
COMPLIANCE RE-IMAGINED

Table of Contents:

Learning Outcomes

By the end of this module, learners should be able to:

1. Explain the purpose and importance of corporate governance in South Africa.
2. Distinguish between the Companies Act, King V and JSE Listings Requirements.
3. Describe the 12 principles of King V and apply the Disclosure Template.
4. Discuss IT, AI, Cybersecurity, and Privacy Governance frameworks.
5. Integrate GRC (Governance, Risk, and Compliance) concepts into digital governance.
6. Evaluate how Joint Standards and AI regulations impact governance in practice.

1. Introduction to Governance

1.1 Key Terms:

- **Governance:** The system of rules, processes, and relationships through which organisations are directed and controlled. It defines how decisions are made, risks are managed, and accountability is ensured.

- **Accountability:** The obligation of leaders and employees to take responsibility for their decisions, actions, and their impact on stakeholders.

- **Transparency:** The practice of openness and honesty in communication, reporting, and decision-making. It builds stakeholder trust and prevents misconduct.

- **Ethics:** The moral compass that guides behaviour — doing the right thing, even when no one is watching.

- **Compliance:** Adhering to laws, regulations, standards, and internal policies that govern the organisation’s operations.

1.2 What is Governance?

Governance provides the structure for setting objectives, achieving results, and monitoring performance responsibly. It ensures that leadership, processes, and technology align to serve the organisation's purpose ethically and sustainably.

📘 Imagine a company as a ship. Governance is its navigation system — steering direction, balancing power, and preventing ethical or operational shipwrecks.

1.2.1 Corporate Governance

Corporate governance focuses on **how a company is led, managed, and held accountable**. It defines the roles of the board, management, and stakeholders to ensure integrity, fairness, and responsible decision-making. Furthermore it:

- Promotes ethical leadership and long-term sustainability.
- Protects shareholder and stakeholder interests.
- Aligns business goals with legal and ethical obligations.

1.2.2 Risk Governance

Risk governance ensures that the organisation **identifies, evaluates, and manages risks** that could affect strategic objectives. It integrates risk oversight into every level of decision-making, supports proactive risk-based decision-making, links enterprise risk management (ERM) with strategy, and enables resilience against financial, operational, IT, and reputational risks.

1.2.3 Compliance Governance

Compliance governance ensures the organisation **operates within the law and regulatory frameworks** — such as the Companies Act, FICA and POPIA. The following are key activities:

- Establishes policies, controls, and reporting mechanisms.
- Prevents misconduct, fraud, and regulatory breaches.
- Promotes a "compliance culture" — where everyone understands their obligations.

1.2.4 IT & Data Governance

IT and Data Governance ensure that technology and information are **used securely, efficiently, and ethically**. They align digital systems with business goals while safeguarding data privacy and cybersecurity. In essence they ensure accountability for data accuracy, protection, and accessibility, reduces technology and cyber risks, and demonstrate compliance with King V’s **Principle 9** on Technology and Information Governance.

1.2.5 AI Governance

AI governance establishes **ethical, transparent, and accountable oversight** of artificial intelligence systems. It ensures that algorithms are explainable, fair, and aligned with human values and laws. This in turn:

- Promotes responsible innovation and human oversight.
- Manages AI risks such as bias, privacy breaches, and misinformation.
- Links directly to ethical leadership under **King V Principles 1, 2, and 9**.

Governance matters because it forms the foundation for ethical leadership, accountability, and sustainable success. Without proper governance — whether corporate, risk, compliance, IT, or AI — organizations face mismanagement, ethical misconduct, financial and reputational loss, and breaches of legal or data protection requirements. Strong governance, on the other hand, builds stakeholder trust, ensures ethical and accountable leadership, and promotes proactive management of risk and compliance. It also enables technology and data to be used responsibly, driving innovation that aligns with legal and ethical standards.

📝Apply & Explain Activity

Reflect on an organisation you know. Identify one strong governance practice (corporate, risk, compliance, IT, or AI) and one area where poor governance could expose it to ethical, financial, or reputational risk.

2. The Companies Act (No. 71 of 2008)

2.1 Key Terms

Directors: Individuals elected or appointed to the board who are legally responsible for directing and controlling the company’s affairs. They act as custodians of the organisation’s resources, make strategic decisions, and ensure that management aligns operations with the company’s objectives, laws, and stakeholder expectations.

Fiduciary Duties: The legal and ethical obligations of directors to act in the best interests of the company, exercising care, skill, and diligence. Fiduciary duties include loyalty, honesty, avoiding conflicts of interest, and ensuring decisions are made in good faith for the benefit of the organisation, not for personal gain.

Reckless Trading: When a company continues to operate or incur debt knowing it cannot meet its financial obligations, or when directors act with gross negligence or disregard for consequences. Under **Section 22 of the Companies Act,** reckless trading is prohibited and can result in personal liability for directors.

Committees: Specialised groups appointed by the board to focus on key areas such as **Audit, Risk, Social & Ethics, and Remuneration. Committees** enable deeper oversight, promote independence, and ensure that governance, risk, compliance, and ethics are monitored effectively.

Accountability: The obligation of the board and management to answer for decisions, actions, and performance outcomes. Accountability ensures transparency and trust between the organisation and its stakeholders — a cornerstone of corporate and digital governance under **King V**.

2.2 Director Conduct, Accountability, and Transparency in South African Companies

The **Companies Act (No. 71 of 2008)** establishes the legal and ethical foundation for how directors should conduct themselves in managing a company. It recognises directors as **fiduciaries** — individuals entrusted with the stewardship of company resources, responsible for protecting shareholder and stakeholder interests while ensuring sustainable value creation. The following provides a comprehensive overview of key aspects.

1. **Director Conduct**
   The Act prescribes that directors must act:

   - **With care, skill, and diligence** — applying the same standard expected of a reasonably prudent person in similar circumstances **(Section 76).**
   - **In good faith and for a proper purpose** — decisions must be made honestly and in the best interests of the company, not for personal benefit.
   - **Free of conflicts of interest** — directors must disclose any personal or financial interests in matters before the board **(Section 75)**.
   - **Lawfully and responsibly** — ensuring the company complies with the Act, other applicable laws, and good governance practices.

2. **Accountability**
   Accountability under the Act means that directors are **personally answerable** for their actions and omissions. They cannot hide behind collective board decisions.

   - **Personal Liability (Section 77):** Directors can be held individually liable for losses, damages, or costs suffered by the company due to negligence, fraud, or breach of duty.

- **Board Oversight:** Directors are expected to establish internal controls, approve financial statements, and oversee executive management performance.
- **Ethical Responsibility:** Accountability extends beyond legal compliance — directors must also uphold ethical standards consistent with **King V's Principle 1 (Ethical Leadership)**.

3. **Transparency**
   Transparency ensures that the company operates **openly, fairly, and with integrity** in its dealings with regulators, shareholders, and the public.
   - **Disclosure Requirements:** The Act mandates accurate and timely disclosure of financial information, director remuneration, shareholdings, and conflicts of interest.
   - **Record-Keeping (Section 24):** Companies must maintain accessible, accurate records of board decisions, minutes, and financial statements.
   - **Stakeholder Confidence:** Transparent governance builds trust with investors, regulators, employees, and society — a critical element of **King V's outcome of Legitimacy**.

The **Companies Act** defines the role of directors through three key principles: **ethical and competent leadership, accountability for corporate decisions, and transparency in dealings with stakeholders.** Collectively, these principles form the foundation of corporate governance in South Africa, fostering integrity, fairness, and long-term organizational sustainability.

2.3 Board Committees

This section covers the establishment of **board committees** such as Audit, Risk, and Social & Ethics Committees.

2.3.1 Audit Committee

The **Audit Committee** is a statutory requirement for certain companies under **Section 94 of the Companies Act, 2008**. It plays a crucial role in maintaining the **integrity of financial reporting**, **internal controls**, and **risk management**. Additionally, under **King V**, the Audit Committee also supports *governance outcomes* such as **Effective Control** and **Legitimacy** by ensuring transparency and accountability in all financial matters.

Key Responsibilities

Area	**Description**
Financial Reporting Oversight	Reviews the integrity, accuracy, and fairness of financial statements and disclosures.
External Audit	Recommends the appointment of external auditors; ensures their independence; reviews audit findings.
Internal Audit and Controls	Oversees the internal audit function, internal control environment, and compliance with applicable standards.
Risk and Compliance	Coordinates with the risk committee to identify financial and operational risks.
Whistleblowing and Ethics	Reviews reports on fraud, irregularities, and ensures safe whistleblower channels.

Reporting

The Audit Committee provides an **Audit Committee Report** in the Annual Financial Statements (AFS), which must outline:

- Auditor independence and performance
- Key audit findings
- Oversight of internal control systems

2.3.2 Social & Ethics Committee (SEC)

The Social and Ethics Committee (SEC) is established under Regulation 43 of the Companies Regulations, 2011, read with the Companies Act. Its purpose is to ensure that the company operates responsibly and ethically toward its stakeholders, employees, society, and the environment. In the context of King V, this committee directly supports the governance outcomes of Ethical Culture, Performance, and Legitimacy.

Composition

- At least **three directors or prescribed officers**, with one being a **non-executive director**.
- Members should have experience in social, ethical, environmental, and human rights matters.
- The chairperson must report to the board and shareholders annually.

Key Responsibilities

Focus Area	**Duties**
Ethics Management	Monitors organisational ethics, anti-bribery measures, and conflicts of interest.

Focus Area	**Duties**
Corporate Citizenship	Reviews the company's impact on communities and compliance with human rights principles.
Environment and Sustainability (ESG)	Ensures the company's activities are environmentally sustainable and aligned to ESG commitments.
Labour and Employment Practices	Oversees fair treatment, diversity, transformation, and employee wellness.
Consumer Relationships	Monitors consumer protection compliance and complaint-handling practices.
Public Health and Safety	Ensures compliance with safety, product quality, and social responsibility standards.

2.3.3 Risk Committee

The **Risk Committee** (also referred to as the **Board Risk Committee**) assists the board in ensuring that all **strategic, financial, operational, IT, and compliance risks** are properly identified, evaluated, and managed. While not a statutory requirement under the Companies Act, it is strongly recommended under **King V** and is **mandatory for JSE-listed companies**. It supports the governance outcomes of **Effective Control** and **Good Performance**, ensuring resilience and value creation.

Composition

- Comprised mainly of **independent non-executive directors**.
- May include executive members such as the CFO, CRO, or CIO (by invitation).

- Chaired by a director with experience in enterprise risk management (ERM) and corporate governance.

Key Responsibilities

Focus Area	**Duties**
Risk Governance Framework	Recommends and monitors the risk management policy and framework to the board.
Enterprise Risk Management (ERM)	Oversees the identification, assessment, and mitigation of key business risks.
IT, Cyber, and AI Risks	Ensures digital, privacy, and cybersecurity risks are managed in alignment with King V.
Business Continuity and Resilience	Reviews crisis management plans, incident response, and business continuity measures.
Compliance and Assurance Integration	Works with the audit and compliance teams to ensure integrated reporting of risks.

Reporting

The committee reports to the board on:

- Risk exposures and emerging threats
- Effectiveness of internal control systems
- Recommendations for mitigation and resilience strategies

2.4 Integration Between Committees

While each committee has distinct responsibilities, **King V** encourages **cross-functional collaboration** to ensure an integrated approach to governance:

Committee	**Collaborates With**	**Integration Focus**
Audit Committee	Risk Committee	Overlap in financial and operational risk oversight
Risk Committee	IT/Cyber/AI Governance Teams	Technology and data risk management
Social & Ethics Committee	Sustainability and HR Teams	ESG, transformation, and stakeholder impact
All Committees	Board of Directors	Integrated reporting and holistic governance assurance

2.5 Evidence for King V Compliance

To demonstrate compliance under **King V's "apply and explain" approach**, organisations should maintain:

- Approved **Committee Charters/Terms of Reference**
- **Minutes** of committee meetings showing discussion and oversight
- **Annual reports** from each committee tabled at board and shareholder meetings
- **Integrated Report Disclosures** summarising committee work, findings, and governance outcomes

2.6. Summary Table

Committee	**Primary Focus**	**Legal Basis**	**Key Governance Outcome**
Audit Committee	Financial reporting, controls, and assurance	Section 94, Companies Act	Effective Control
Social & Ethics Committee	Ethics, ESG, stakeholder impact	Regulation 43, Companies Regulations	Ethical Culture & Legitimacy
Risk Committee	Enterprise and operational risk	King V / JSE Requirements	Good Performance & Conformance

3. What Are the JSE Listing Requirements?

The **JSE Listing Requirements** are a set of rules issued by the **Johannesburg Stock Exchange (JSE)** that companies must comply with if they want to list their securities (shares, debt instruments, etc.) on the exchange. These rules ensure that listed companies maintain **transparency, good governance, and fair disclosure** to protect investors and promote confidence in South Africa's capital markets. Think of the JSE Listing Requirements as the **"rulebook for being publicly listed"** — similar to how the King Code governs corporate governance but specifically focused on listing and trading standards.

3.1 Purpose of the Listing Requirements

The main objectives are to:

- ✅ **Protect investors** by ensuring full, accurate, and timely disclosure of financial and operational information.
- 🧭 **Promote good governance and ethical leadership** in line with the King IV and soon King V corporate governance principles.

- 💡 **Ensure fair, efficient, and transparent trading** on the exchange.
- 📊 **Maintain the integrity of the JSE** and the reputation of South Africa’s capital markets.
- 🏢 **Support market stability** by regulating how companies issue and manage their securities

---

3.2 Structure of the Listing Requirements

The JSE Listing Requirements are divided into several **sections** that cover different aspects of a company’s obligations before and after listing.

Section	**Focus Area**	**Purpose**
Section 1	Definitions and Principles	Establishes terminology and general provisions.
Section 3	Continuing Obligations	Covers what companies must do after listing — reporting, disclosures, governance, etc.
Section 4	Financial Information	Sets accounting, auditing, and reporting standards.
Section 8	Corporate Governance	Aligns with King IV (and now King V) principles; requires independent boards, audit committees, etc.
Section 9	Related Party Transactions	Regulates deals between the company and connected persons (to avoid conflicts of interest).
Section 10	Disclosures and Announcements	Ensures timely market disclosures through the Stock Exchange News Service (**SENS**).
Section 11–13	Takeovers, Mergers & Circulars	Regulates corporate actions that affect shareholders.

3.3 Governance and King V Alignment

The JSE Listing Requirements explicitly reference the **King Code on Corporate Governance**. This means that all listed companies must:

- Apply and explain how they implement King principles.
- Disclose governance practices in integrated annual reports.
- Demonstrate ethical culture, responsible leadership, and stakeholder inclusivity.

With **King V**, boards will need to also evidence **AI governance, digital ethics, and sustainability (ESG)** — areas that will likely be incorporated into future JSE updates.

3.3.1 Compliance Implications

For compliance and GRC professionals, the JSE Listing Requirements mean:

- **Continuous Disclosure Oversight** – Monitoring all company announcements for accuracy and timing.
- **Governance Alignment** – Ensuring board structures meet independence and diversity requirements.
- **Risk Reporting** – Integrating ESG, cyber, and technology risks into board and investor reports.
- **Ethical Conduct** – Ensuring directors and officers act with integrity, avoid insider trading, and prevent market manipulation.

4. The King Code on Corporate Governance

The **King Code** promotes ethical, effective, and sustainable leadership. It’s voluntary but forms the cornerstone of governance excellence in South Africa.

Governance Outcomes:

1. Ethical Culture
2. Good Performance
3. Effective Control
4. Legitimacy

4.1 The 12 Principles of King V

Principle	Focus	What it Means	Application & Link to Governance Outcome
1. Ethical and Effective Leadership	Integrity, Competence, Responsibility	The governing body must lead ethically and effectively, setting the tone for a culture of integrity, fairness, and accountability.	Leaders act with moral courage, apply sound judgment, and ensure ethical decision-making. **Outcome:** *Ethical Culture & Good Performance*
2. Organisational Ethics	Values and Ethical Conduct	The organisation must embed ethical principles and behaviours into policies, systems, and daily operations.	Implement a Code of Ethics, whistleblowing mechanisms, and conduct ethics training. **Outcome:** *Ethical Culture & Legitimacy*
3. Responsible Corporate Citizenship	Sustainability & Societal Impact	The organisation should act as a responsible citizen, considering its economic, environmental, and social impact.	Integrate ESG, transformation, and sustainability into corporate strategy. **Outcome:** *Legitimacy & Good Performance*
4. Strategy and Value Creation	Purpose, Risk, and Sustainability	Strategy must integrate risk, performance, and sustainability to create long-term value.	Develop a strategic plan that links financial and non-financial objectives; align risk appetite with purpose. **Outcome:** *Good Performance & Effective Control*

Principle	**Focus**	**What it Means**	**Application & Link to Governance Outcome**
5. Reporting and Transparency	Disclosure & Integrated Reporting	Reports must enable stakeholders to assess the organisation's performance, governance, and prospects.	Produce accurate, balanced integrated reports covering financial, ESG, and governance data. **Outcome:** *Legitimacy & Good Performance*
6. Governing Body as Custodian	Accountability & Oversight	The board is the ultimate custodian of corporate governance and responsible for effective control.	Approve governance frameworks, policies, and delegate authority responsibly. **Outcome:** *Effective Control & Ethical Culture*
7. Composition of the Governing Body	Diversity & Independence	The governing body must have an appropriate mix of knowledge, skills, experience, and independence.	Maintain a balanced board with diverse expertise and demographics; perform annual board evaluations. **Outcome:** *Effective Control & Good Performance*
8. Delegation and Committees	Roles and Responsibilities	The board should delegate appropriately	

📝Apply & Explain Activity:

> Select one principle and describe how your organization could evidence compliance.

Answer:

5. IT Governance

IT Governance refers to the framework of structures, processes, and decision-making mechanisms that ensure an organisation's **technology, information, and digital assets** support its strategic objectives, deliver business value, and manage risk effectively. It determines **who makes technology decisions**, **how those decisions are made**, and **how performance and risk are monitored**. In essence, IT governance is how leadership ensures that **technology enables — not endangers — the organisation's success.**

5.1 Why It Matters:

Technology is no longer a back-office function — it is a **strategic enabler of performance, innovation, and resilience.**
Under **King V Principle 9 (Governance of Risk, Technology and Information)**, boards are expected to:

- Treat information and technology as **strategic assets**.
- Oversee **data governance, cybersecurity, and AI ethics** with the same rigour as financial oversight.
- Ensure IT decisions align with the organisation's **purpose, strategy, and risk appetite.**

- Demonstrate evidence of governance through approved frameworks, reporting, and assurance activities.

Without effective IT governance, organisations risk:

- **Cyberattacks or data breaches** damaging stakeholder trust.
- **Wasted investments** in misaligned or duplicated technologies.
- **Regulatory non-compliance**, particularly with laws such as POPIA and the Cybercrimes Act

5.2 IT Governance Frameworks

Framework	**Purpose**	**Core Focus & Contribution to King V**
COBIT 2019 (Control Objectives for Information and Related Technologies)	Provides an enterprise-wide IT governance and management framework.	Defines clear roles, decision rights, and performance objectives for IT. Ensures technology aligns with business strategy and stakeholder needs. *Supports ethical leadership, effective control, and performance (Principles 1, 4, 9).*
ISO/IEC 27001	Establishes an Information Security Management System (ISMS).	Focuses on **confidentiality, integrity, and availability** of information through 114 security controls. Demonstrates compliance and assurance under **Principles 9, 10, 12**.
NIST Cybersecurity Framework (CSF)	Provides a risk-based model for managing cybersecurity threats.	Builds cyber resilience through five key functions — **Identify, Protect, Detect, Respond, and Recover** — aligning directly to **Principles 9 and 12** of King V.

5.3 How IT Governance Links to King V

Strong IT governance demonstrates compliance with **Principle 9**, ensuring that boards:

- Exercise oversight over technology strategy and cyber risk.
- Receive regular reports from CIOs or technology committees.
- Integrate IT risk into enterprise risk management (ERM).
- Protect stakeholder information through secure and ethical use of data and systems.

📝Apply & Explain Activity:

How can adopting frameworks such as COBIT, ISO 27001, or NIST help an organisation evidence compliance with King V Principle 9 on Technology and Information Governance?

Answer:

🧠Reflection Box:

List **two major risks** that poor IT governance could create for a financial institution and explain how they could affect **performance** and **stakeholder trust**.

Answer:

6. Cybersecurity Joint Standards & GRC Integration

6.1 Key Terms:

1. **Joint Standards:** Regulatory instruments jointly issued by the Financial Sector Conduct Authority (FSCA) and the Prudential Authority (PA) that prescribe how financial institutions must manage information technology (IT) and cybersecurity risks.

2. **FSCA:** The Financial Sector Conduct Authority, responsible for market conduct and consumer protection in South Africa's financial sector.

3. **Cyber Resilience:** An organisation's ability to **anticipate, withstand, respond to, and recover** from cyber incidents while continuing to deliver critical services.

4. **GRC (Governance, Risk, and Compliance):** The integrated framework through which organisations ensure that governance decisions, risk management, and regulatory compliance align to strategic objectives.

5. **Compliance:** Adherence to applicable laws, regulatory standards, and internal policies designed to ensure ethical and secure business operations.

6.2 Overview

Between **2023 and 2024**, the **FSCA** and **Prudential Authority** introduced two major **Joint Standards** for the financial sector:

- **Joint Standard 1 of 2023** – *Information Technology Governance and Risk Management*
- **Joint Standard 2 of 2024** – *Cybersecurity and Cyber Resilience Requirements*

These standards require financial institutions — including banks, insurers, and investment firms — to establish **formal, board-approved frameworks** for IT and cybersecurity governance. They aim to ensure that **technology risks are managed as core business risks**, not merely technical issues. This aligns directly with **King V Principle 9**, which calls for governing bodies to oversee **Technology and Information Governance** with the same diligence as finance and ethics.

6.2.1 Objectives of the Joint Standards

1. **Embed Cyber Risk into Corporate Governance:** Elevate cybersecurity to a **board-level responsibility**, ensuring executive oversight and accountability.
2. **Integrate Cyber Risk within GRC Frameworks:** Link cyber risk management to enterprise risk, audit, compliance, and assurance processes.
3. **Enhance Industry Cyber Resilience:** Strengthen the ability of financial institutions to prevent, detect, respond to, and recover from cyber incidents.
4. **Promote Regulatory Consistency:** Align South African cybersecurity expectations with global standards such as **ISO 27001** and the **NIST Cybersecurity Framework**.

6.3 Domains of Cybersecurity

Domain	**Regulatory Requirement**	**GRC Integration**
Governance	The **Board** must approve and oversee a cybersecurity strategy and policy framework. Roles, responsibilities, and reporting lines must be clearly defined.	**Governance:** Demonstrates leadership accountability and oversight.
Risk Management	Cyber risk must be incorporated into the **Enterprise Risk Management (ERM)** process, including risk appetite statements and regular assessments.	**Risk:** Integrates digital risk with operational and strategic risk management.
Controls & Operations	Institutions must maintain **incident response plans**, manage **third-party (vendor) risks**, and implement robust **technical and procedural controls**.	**Compliance:** Ensures adherence to regulatory and internal control standards.
Reporting & Assurance	Significant cyber incidents must be reported to the **Regulator**. The board must receive **assurance reports** confirming the effectiveness of cyber controls.	**Monitoring & Assurance:** Provides transparency, continuous improvement, and regulatory accountability.

6.4 How Joint Standards Strengthen Governance

- **Ethical Responsibility:** They hold boards accountable for protecting customers' data and trust — connecting technology governance to ethical leadership (**King V Principles 1 & 2**).
- **Integrated Oversight:** They embed cybersecurity into overall **GRC frameworks**, aligning with the outcomes of *Effective Control* and *Legitimacy*.
- **Transparency and Assurance:** Require documented evidence — policies, incident reports, risk registers, and third-party assurance — to demonstrate compliance.
- **Resilience by Design:** Encourage proactive, not reactive, cybersecurity planning.

📝Apply & Explain Activity

Identify one cyber governance control (such as incident response testing, vendor due diligence, or board cyber briefings) that demonstrates **board accountability** under the Joint Standards. Explain how this supports King V's outcomes of *Effective Control* and *Ethical Culture.*

Answer:

7. AI & Emerging Technologies Governance

7.1 What is AI Governance?

AI governance refers to the frameworks, policies, processes, standards and oversight mechanisms that guide the development, deployment and use of artificial intelligence (AI) systems in a manner that is safe, ethical, lawful and aligned with human values.
In a compliance context, AI governance sits at multiple levels:

- At the **environmental** level: laws, regulations, public policy, national/international standards.
- At the **organisational** level: how a company/government body organises its AI risk assessment, assignment of roles, internal controls, oversight, reporting.
- At the **system (AI) lifecycle** level: how an individual AI system is designed, tested, validated, deployed, monitored, decommissioned, including data governance, bias mitigation, human oversight, etc.

Why is this important? Because AI systems are increasingly embedded in decision-making (credit scoring, recruitment, healthcare, public services) and if not governed well they can lead to harms: discrimination, unfairness, privacy breaches, lack of transparency, undermined trust, unintended consequences. Good governance helps align AI with ethical, legal and social norms.

7.2 The South African AI Policy Landscape

Where South Africa stands:

The South Africa National Artificial Intelligence Policy Framework was published in late 2024 by the Department of Communications and Digital Technologies (DCDT). The framework is **not yet** a fully-fledged AI Act/regulation (i.e., legally enforceable rules specific to AI) but rather a policy blueprint.

7.2.1 Key objectives & pillars of the South African policy

According to various sources the policy strives to:

- Harness AI for economic growth, social equity and innovation (i.e., "AI for good" in the South African context)
- Develop talent, build infrastructure, invest in research & development, create a dynamic AI ecosystem in South Africa.
- Promote ethical design, transparency, explainability, fairness, mitigating bias and ensuring data protection.

Strategic pillars

The policy identifies a number of strategic pillars. For example:

- Talent development / capacity building.
- Digital infrastructure (enabling environment for AI)
- Research, development and innovation.
- Ethical & safe deployment of AI (including transparency, explainability, bias mitigation)
- Public sector adoption / government usage of AI systems.

7.3 Implications for Compliance Professionals in South Africa

Organisations will need frameworks to assess whether their AI systems meet the “ethical, safe, transparent” criteria; so, knowing the key principles (see below) will be a differentiator. Moreover, despite the policy framework not yet fully enforced as regulation, aligning now with its objectives gives organisations a “first-mover” advantage and prepares them for future regulation. South Africa’s policy draws on international models (including the EU), therefore you will also need to understand how global standards impact local operations (see section on EU below).

7.3.1 The EU AI Act – Key Principles & Structure

7.3.1.1 What is the EU AI Act?

The EU AI Act (Regulation (EU) 2024/1689) is the world’s first **comprehensive** horizontal legal framework for AI systems. It entered into force on 1 August 2024, with many key provisions becoming enforceable from 2 August 2026 (and some earlier). It applies not only to AI providers in the EU but also broadly to AI systems whose output is used in the EU (so it has **extraterritorial** effects).

7.3.1.2 Key features:

- **Risk-based approach**: It categorises AI systems into levels of risk (unacceptable risk / high risk / limited risk / minimal risk) and imposes different obligations accordingly.

- **Prohibited Practices**: Some AI uses are banned (e.g., biometric surveillance for certain uses, social scoring by public authorities) in the EU context.

- **High-Risk AI Systems**: For systems classified as “high-risk”, there are stricter obligations: conformity assessment, risk management, human oversight, transparency, documentation.

- **Governance & Enforcement**: The Act creates new institutional architecture — e.g., the European Artificial Intelligence Board, the European AI Office, and national competent authorities for supervision.

7.3.1.3 Why the EU AI Act matters (for South Africa too)

South Africa’s AI policy acknowledges that the EU AI Act is the “first comprehensive prescriptive regulation” and that South Africa intends to align with global standards. Even if a South African company does not operate in the EU, if its AI system is used by EU customers or has EU market impact, the EU AI Act may apply (extraterritorial effect) — which means local entities must be aware of global regulatory trends. The EU’s regulation creates a “global benchmark” or “brussels effect” — namely, regulatory standards created in the EU often influence other jurisdictions and the expectations of multinational corporations.

For compliance professionals in South Africa, this means that aligning to EU-style obligations (transparency, accountability, risk management) is a good strategic move, even ahead of local binding regulation.

7.4 Core AI Governance Principles: Transparency, Accountability, Explainability (and others)

Below are the key principles you often see in AI governance frameworks and how they apply in practice.

7.4.1 Transparency

Definition / Purpose:

Transparency means that the design, logic, data (where appropriate), decision-making processes, assumptions and limitations of an AI system are sufficiently clear to stakeholders (users, affected individuals, auditors) so they can understand how the system arrived at a decision and what it can and cannot do. It helps build trust and allows for meaningful oversight and audit.

Application:

- Documenting the AI system’s purpose, scope, data provenance, model choices, validation results, known limitations and potential risks.
- Disclosing to users when they are interacting with an AI system (rather than a human) and informing them of how to get human review/appeal if a decision affects them.

- Providing “appropriate” explanations of system outputs in understandable form (not only to engineers).

📘 **In EU AI Act Example:**

The Act imposes transparency obligations for general-purpose AI models and high-risk systems — e.g., maintaining technical documentation, disclosing that a system is AI, informing users of limitations. This means organisations must embed transparency into their lifecycle processes: design, deployment, monitoring.

In South Africa context:

The South African AI policy also mentions transparency and explainability as one of the strategic pillars (ensuring that AI systems deployed in South Africa are understandable, auditable, accountable). Compliance roles will need to ensure that organisations have documentation and disclosures around AI systems — especially for public sector or regulated uses.

7.4.2 Accountability

Definition / Purpose:

Accountability means that there is a clear assignment of responsibility for the outcomes of AI systems (good and bad). Organisations must have governance mechanisms so that if something goes wrong (e.g., bias, incorrect decision, system failure) one can identify who did what, who is responsible, how to remediate, how to learn and improve. It also means there are audit trails, governance processes, and appropriate oversight structures.

Application:

- Defining roles such as “AI system owner”, “AI risk manager”, “independent reviewer”.
- Having audit logs, version control, model change management.
- Incident reporting: when the AI system causes a serious adverse effect, the organization must investigate and report.
- Remediation: If an AI system wrongly discriminates or harms individuals, there is a process for redress.

📘 **In EU AI Act Example:**

The Act requires providers and deployers of high-risk AI systems to set up risk-management systems, keep logs, conduct post-market monitoring, and cooperate with competent authorities. Governance and enforcement provisions ensure national authorities can investigate and sanction.

In South Africa context:

Though specific regulation is still evolving, the policy framework emphasises the need for governance, accountability and institutional readiness. For compliance professionals, it means encouraging organisations to build accountability into their AI project governance from the outset (not as an afterthought).

7.4.3 Explainability

Definition / Purpose:

Explainability (or interpretability) is about making the internal workings, decision-logic or output of AI systems understandable to humans in a meaningful way — especially in contexts where decisions materially affect rights, access, opportunities, fairness. It is often considered a key enabler of transparency and accountability: if you can't explain how the system came to a result, it is harder to hold anyone responsible or trust the outcome.

Application:

- For a credit scoring AI: being able to say "because you had these three factors, the model weighted them this way, hence this score" in plain language.
- Ensuring the model is auditable: logs plus explanation of reasons, plus ability to query/contest output.
- For more complex ("Blackbox") models: providing "proxy explanations", confidence metrics, documentation of training data and feature importance.
- Ensuring users/affected persons have access to understandable explanation and possibly make human review.

In AI Governance literature:

The EU AI Act emphasises the requirement of human oversight (see Article 14) and, implicitly, explainability so that humans can monitor, detect anomalies, intervene. Research highlights explainability as one of the most cited principles in governance frameworks.

In South Africa Context:

The policy mentions that AI systems must ensure transparency, explainability and fairness so that society trusts AI and that bias is mitigated.

7.4.4 Other Key Principles Include:

While the question asked for transparency, accountability, explainability, it’s useful in training content to highlight other commonly referenced principles in AI governance, because they contextually link. These include:

- **Fairness / Non-discrimination**: Ensuring AI systems do not unfairly treat individuals or groups on the basis of protected or sensitive attributes, and bias is identified and mitigated.
- **Safety & Robustness**: AI systems should be secure, resilient to attack or misuse, reliable and functioning as intended.
- **Human-Centric / Human Oversight**: Ensuring humans remain in control, can intervene, understand AI decision making, avoiding undue automation/delegation. The EU Act’s Article 14 addresses human oversight.
- **Privacy & Data Governance**: Good governance of the data used by AI systems: quality, provenance, bias, consent, data protection laws (important in SA under POPIA)
- **Sustainability / Social Impact**: Considering broader societal impacts of AI: employment, equity, inclusion, environmental impact.

7.5 How the EU AI Act Impacts South Africa

Here's how the EU regulation can have practical impacts for South Africa's compliance and governance environment.

1. **Benchmarking & Standard-Setting**

The EU AI Act sets a global benchmark. South Africa's policy explicitly references the EU document as a "concrete regulatory prescript". For South African organisations, aligning with the EU's standards early can give strategic advantage (especially if dealing with EU partners or markets). For compliance professionals, it means "know the EU standard" even if local law has not yet fully caught up.

2. **Extraterrestrial Reach**

If a South African company develops/provides an AI system and the output is used in the EU market, the EU AI Act may apply (even if the provider is outside the EU). This means compliance teams in South Africa must assess whether their AI systems or services touch EU users/market and therefore whether they need to meet EU-AI-Act obligations.

3. **Preparing for Future Local Regulation**

Since South Africa's AI policy framework is the precursor to future regulation (potential AI Act) the evolution of the EU's regulation provides guidance on structure, obligations, governance models. Compliance systems built today with EU standards in mind will make future compliance with South African regulation less burdensome.

4. **Supply Chain & Partner Risk**

South African firms working with EU firms or supplying to them will likely face contractual/regulatory demands tied to the EU AI Act (e.g., documentation, audit, transparency). Compliance professionals must manage these upstream/downstream risks. Conversely, EU firms investing in or partnering with South African firms may demand that local partners align with EU-compliance standards.

5. **Global Reputation & Market Access**

As Africa aims to develop its AI ecosystem, having frameworks aligned with globally respected standards (like the EU's) boosts trust, investor confidence, cross-border partnerships. For South

Africa, being compliant or near-compliant helps position it as a credible AI hub on the continent. Compliance professionals in South Africa today can leverage this as a “value proposition”: your firm is AI-governance-ready.

---

8. Privacy & Cybersecurity Governance

shutterstock.com · 2195130533

Privacy Governance is the **framework of policies, roles, and controls** that ensure an organisation collects, uses, stores, shares, and deletes **personal information** in a way that is lawful, transparent, and respectful of individual rights. It is guided by privacy laws such as South Africa’s **Protection of Personal Information Act (POPIA)**, and international laws like the **EU General Data Protection Regulation (GDPR)**.

8.1 Objectives:

- ✅ Protect individuals' personal data and dignity.
- ✅ Demonstrate compliance with privacy laws (POPIA, GDPR, etc.).
- ✅ Embed privacy into corporate culture ("privacy by design and default").
- ✅ Build trust with customers, employees, and regulators.

8.2 Domains of Data Privacy Governance:

Domain	Governance Focus	Example
Policies & Frameworks	Establish privacy policy, consent, and data retention standards	POPIA manual, consent forms
Roles & Accountability	Appoint Information Officer / DPO with board oversight	CEO delegates privacy to compliance
Risk Management	Identify and mitigate data-protection risks	Data-mapping, DPIA, privacy risk register
Training & Awareness	Educate employees on data handling and breaches	Annual POPIA training
Reporting & Monitoring	Report and investigate data breaches	Notify Information Regulator within 72 hours

8.2.1 POPIA Governance Principles

1. **Accountability** – The responsible party must ensure lawful processing.
2. **Processing Limitation** – Collect only necessary data with consent.
3. **Purpose Specification** – Use data for a clear, lawful purpose.
4. **Information Quality** – Keep data accurate and updated.
5. **Openness** – Inform data subjects about processing.
6. **Security Safeguards** – Protect against loss or unauthorised access.
7. **Data Subject Participation** – Allow individuals to access or correct data

---

8.3 Cybersecurity Governance Explained

8.3.1 Definition

Cybersecurity Governance is the **system of leadership, strategy, and control** that ensures information systems are protected against cyber risks — such as hacking, ransomware, phishing, or insider threats — while enabling the organisation to achieve its business objectives. It forms part of **IT Governance** under King V Principle 9 and aligns with standards such as **ISO 27001 (Information Security Management)** and the **NIST Cybersecurity Framework**.

8.3.2 Objectives

- ⚙️ Protect information assets (confidentiality, integrity, availability).
- 🚨 Detect, respond, and recover from cyber incidents effectively.
- 🧩 Align cyber risk with enterprise-risk management (ERM).
- 🧭 Ensure board oversight and reporting on cyber resilience.

8.3.3 Key Governance Elements

Domain	Governance Focus	Example
Leadership & Strategy	Board approves cybersecurity strategy & policy	King V Board Committee oversight
Risk Management	Identify, assess, and treat cyber threats	Risk registers, penetration tests
Controls & Architecture	Implement layered defences (network, access, data)	Firewalls, encryption, MFA
Incident Response	Establish response plans, test and learn	Cyber drills, breach reporting
Third-Party Security	Manage vendor and supply-chain risks	Vendor due diligence, SLAs
Reporting & Assurance	Continuous monitoring, metrics, and audits	SOC 2, internal audit reports

9. The Intersection: Privacy × Cybersecurity Governance

9.1 Integration:

Privacy and cybersecurity are deeply interdependent disciplines that work together to protect an organisation’s information ecosystem. Privacy focuses on safeguarding individuals’ personal data, driven primarily by legal and regulatory requirements such as POPIA and the GDPR, with the Information Officer or Data Protection Officer typically providing oversight.

Its core risk is the misuse or unlawful processing of personal information, and the desired outcome is lawful, ethical, and transparent data use. Cybersecurity, on the other hand, is centred on protecting all digital assets—systems, networks, and information—from threats and compromise, guided by risk and resilience frameworks such as ISO and NIST.

Oversight typically sits with the CISO or IT Risk Committee, and its main objective is to ensure secure, resilient, and uninterrupted operations. Although their focus areas differ, privacy and cybersecurity must operate together to deliver holistic protection for the organisation.

9.2 Governance Frameworks & Standards

Framework	**Purpose / Focus**	**Relevance**
King V Principle 9	Governing technology and information	Board accountability for IT, privacy, and cyber risk
ISO 27001 / 27701	Information security & privacy extension	Technical and governance controls
NIST CSF	Identify–Protect–Detect–Respond–Recover	Used globally for cyber-risk governance
COBIT 2019	Governance of IT	Aligns IT processes with enterprise goals
POPIA / GDPR	Legal data-protection compliance	Privacy governance framework
Joint Standard 1 of 2023 (FSCA & PA)	Cyber and IT risk governance for financial institutions	Integrates cybersecurity into GRC

Module Summary: Corporate and Digital Governance

This module explored how **governance, risk and compliance (GRC)** intersect to form the foundation of ethical, transparent and sustainable leadership in the digital era, where learners gained an integrated understanding of **corporate governance frameworks**, regulatory obligations, and the evolving expectations of boards in managing technology, information, and emerging risks.

1. The Essence of Governance

Governance is the system of **rules, relationships, and processes** through which organisations are directed and controlled. It ensures that decisions are ethical, transparent, and aligned with long-term value creation. Across all frameworks, governance is built on four universal outcomes championed by **King V**:

- **Ethical Culture**
- **Good Performance**
- **Effective Control**
- **Legitimacy**

2. The Companies Act (No. 71 of 2008)

The **Companies Act** is South Africa’s legal backbone for corporate behaviour. It defines:

- The **fiduciary duties** of directors (care, skill, honesty, good faith).
- Requirements for **accountability, transparency, and record-keeping**.
- Prohibitions against **reckless or fraudulent trading**.
- The establishment of **board committees** such as Audit, Risk, and Social & Ethics Committees.

It embeds accountability by holding directors personally liable for misconduct or negligence, reinforcing the ethical leadership principles promoted by King V.

3. JSE Listings Requirements

For listed entities, the **JSE Listings Requirements** ensure market transparency, investor confidence, and adherence to best-practice governance standards. Listed companies must:

- Comply with the **Companies Act** and apply **King V principles**.
- Disclose governance performance, board composition, remuneration, and ESG metrics.
- Maintain independent **Audit, Risk, Remuneration, and Social & Ethics Committees**.
- Report material risks, price-sensitive information, and stakeholder engagement outcomes.

Together, the Act, King V, and JSE Rules form South Africa's **"governance triangle"** of legality, ethics, and accountability.

4. The King V Code of Corporate Governance

King V provides the *ethical compass* that complements the Companies Act's legal framework. It introduces 12 principles that guide boards to apply good governance voluntarily but transparently through the **"apply and explain"** philosophy. King V strengthens governance through:

- Simplified, outcome-based principles.
- Integration of **technology, ESG, and sustainability**.
- A **Disclosure Template** enabling consistent public reporting of governance practices.
- Alignment with global best practice and emerging risk contexts.

5. IT Governance

IT Governance ensures that **technology and information** are managed strategically, securely, and ethically. It aligns IT decisions with corporate objectives and risk appetite while ensuring compliance with King V Principle 9.

Key frameworks supporting IT governance include:

- **COBIT 2019** – defines governance and management of enterprise IT.
- **ISO 27001** – establishes an information security management system.
- **NIST CSF** – enhances cyber resilience through risk-based control functions.

Strong IT governance ensures technology delivers value, mitigates cyber and data risks, and supports organisational sustainability.

6. Cybersecurity Governance and the Joint Standards

The **FSCA & Prudential Authority's Joint Standards (2023–2024)** make cybersecurity a **board-level obligation**. They require financial institutions to integrate cyber risk into enterprise risk management, maintain incident-response plans, and ensure regulatory reporting and assurance. This reinforces King V's expectation that technology and information are governed as strategic assets — linking ethical responsibility with resilience and compliance.

7. AI and Emerging Technologies Governance

As artificial intelligence transforms business and society, boards must exercise **AI governance** to ensure technology is used responsibly and transparently. Under King V Principles 1, 2 and 9, boards must:

- Oversee **AI ethics**, transparency, and accountability.
- Address risks such as bias, explainability, and data privacy.
- Align with **South Africa's National AI Policy Framework (2024)** promoting ethical, inclusive innovation.
- Understand global influences like the **EU AI Act (2024)**, which introduces a **risk-based model** for AI compliance.

AI governance demonstrates ethical leadership in practice — balancing innovation with integrity.

8. Privacy and Data Governance

Data is now a strategic asset requiring ethical stewardship. Through **POPIA** and **GDPR**, organisations must protect personal information and ensure fairness, transparency, and consent in data processing. King V integrates privacy under ethical leadership and legitimacy — requiring boards to approve data governance frameworks, monitor compliance, and promote a culture of digital trust.

9. Governance, Risk & Compliance (GRC) Integration

Modern governance demands an **integrated approach**, linking risk, technology, ethics, and compliance into a single framework. Effective GRC ensures that:

- **Governance** provides direction and accountability.
- **Risk management** anticipates threats and builds resilience.

- **Compliance** ensures adherence to laws and standards.
- **Information and technology** are governed for sustainable value creation.

Integrated GRC delivers the ultimate King V outcomes: ethical culture, performance, effective control, and legitimacy.

---

10. The Big Picture

Strong governance is not paperwork — it's a **culture of responsibility and trust.**
When boards lead ethically, manage risks intelligently, and govern technology wisely, they create resilient organisations that protect stakeholders and contribute to a sustainable economy.

💡 **Key Insight:** In the digital era, good governance isn't about ticking boxes — it's about **integrity in action, accountability in data, and ethics in innovation.**