Introduction to Governance

Module 1

Lesson Overview

- Module 1 Lesson (Touchbase)
- Assessment
- Attendance register (on the chat – select Module 1)
- Corporate Governance
- JSE Listing Requirements
- Companies Act
- King V
- Debrief on King V: Technology
- Guest Speaker: Adv Beulah Rhode

Lecturer

- Seasoned GRC professional, entrepreneur and Board Advisor
- +- 17 years experience in GRC
- Project Manager
- Pioneered SA’s first IT-Compliance professional pathway (NQF 4-8)
- Qualified lecturer
- Certified Anti-Money Laundering Specialist
- Certified Global Sanctions Specialist
- Certified Artificial Intelligence Governance Professional
- Chartered IT Compliance Officer (CITCO)
- Licensed Compliance Officer – FIC and FSCA

Lesson Outcomes

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. Discuss the technology principles of King V and apply the Disclosure Template.
4. Discuss IT, AI, Cybersecurity, and Privacy Governance frameworks.

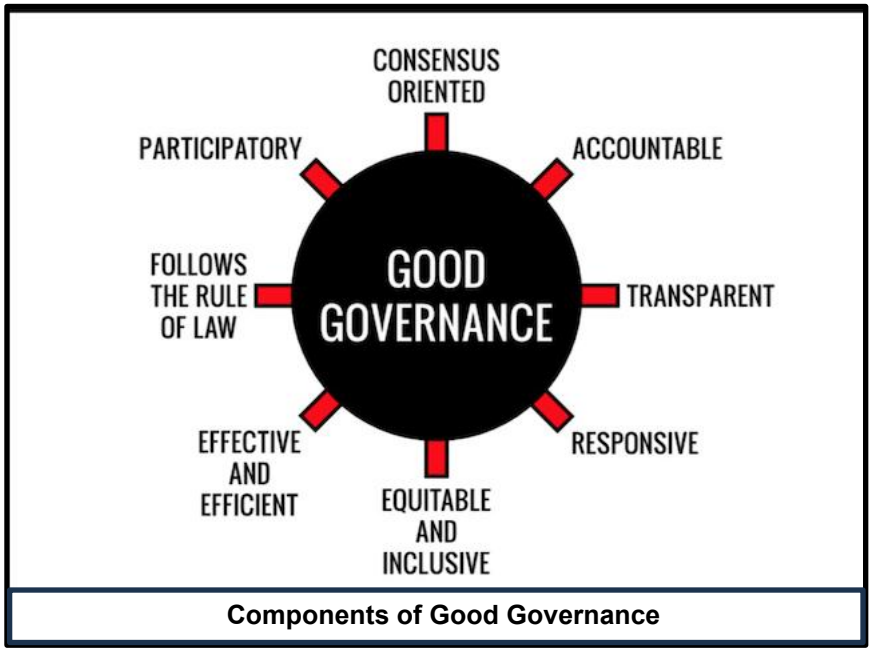
CORPORATE GOVERNANCE

Section 1

What Is Corporate Governance?

Good Governance

Governance isn't bureaucracy—it's intentional design.
It provides structure that sharpens strategy, strengthens ethical leadership, and supports sound, responsible decision-making.



Components of Good Governance

It's leadership with accountability, rules with purpose, and compliance with conscience.

Weak Governance

- Costly fines
- Reputational damage
- Regulatory scrutiny
- Loss of trust that can take years to rebuild.

Case Study: Eskom

Eskom (South Africa, ongoing since ~2010)

What happened:
State capture, corruption, inflated contracts, mismanagement, and operational failures.

Governance failures:
•Political interference in executive appointments
•Fraudulent procurement processes
•Lack of internal audit independence
•Board instability and poor oversight

Outcome:
Rolling blackouts, billions in losses, multiple commissions of inquiry.

What does good governance look like in your day-to-day work?

- Clear Decision-Making
- Transparency in Actions
- Ethical Behaviour
- Respecting Policies and Controls
- Role Clarity
- Risk Awareness
- Accountability
- Collaboration and Respect
- Continuous Improvement

THE LEGAL FRAMEWORK

Section 2

The Companies Act

- **Companies Act = Road Code**
  Sets the rules for how companies must operate in South Africa.

- **Directors = Drivers**
  Must act with care, skill, honesty, and responsibility.

- **Record-Keeping = Mandatory**
  Accurate financials and documents must be maintained for compliance with CIPC and SARS.

- **Reckless Trading = Prohibited**
  Section 22: Directors cannot continue trading if the company is financially distressed.

- **Big Companies Need Committees**
  Audit Committee, Social & Ethics Committee, etc., to provide oversight and manage risk.


KING V

King Code on Corporate Governance

- The King Code is South Africa's **voluntary guide** for good corporate governance.
- It goes beyond legal compliance and promotes **ethical, responsible leadership**.
- Acts as a **compass**, not a rulebook—guiding organisations to act with integrity and transparency.
- Built on **four core governance outcomes**:
  - **Ethical Culture – Doing the right thing consistently**.
  - **Good Performance** – Achieving goals with purpose, not just profit.
  - **Effective Control** – Strong systems, controls, and risk management.
  - **Legitimacy** – Earning trust from investors, employees, and society.
- Focuses on sustainability, accountability, and long-term value creation.
- Uses an **"apply and explain"** approach instead of tick-box compliance.
- Encourages organisations of all sizes to adopt responsible, stakeholder-centred governance.

King Code Vs Companies Act

Feature	Companies Act	King Code
Type	Legislation (law)	Best Practice Code
Application	Mandatory	Voluntary (“Apply and Explain”)
Focus	Minimum legal duties	Ethical leadership, sustainability
Penalties	Legal consequences (fines, liability)	Reputational, market trust impact
Example	Directors must act with care and diligence (Section 76)	Boards should promote ethical culture and fair remuneration

The New King V

Modernisation of Principles

- King IV had **17 principles**; King V reduces this to **±12 clearer, streamlined principles**.

Enhanced Disclosure

- “Apply and Explain” remains.
- King V introduces a **standardised Disclosure Template** for governance reporting.
- Improves **transparency, comparability, and consistency** across organisations.

The New King V cont…

Focus on Emerging Risks

Strong emphasis on:

- **Technology & Information Governance** (AI, cybersecurity, data).
- **Sustainability & ESG** (environmental + social impact).
- **Impact & Materiality** (two-way effects between business and society).

The New King V cont…

Integrated Thinking

- Recognises interdependence of **people, planet, and performance**.
- Encourages decisions that consider broader ecosystem impact.

Digital Governance

- Technology is now central—not a support function.

- Boards must govern:
  - Data, AI, and digital systems
  - Cyber and privacy risks
  - Algorithmic fairness and ethics

- Organisations must **evidence digital governance** and treat tech risks like financial risks

JSE LISTING REQUIREMENTS

Section 3

Why Governance Matters for JSE-Listed Companies

- Listing on the JSE means operating in a **high-trust, high-transparency environment**.
- Companies must meet strict rules to **protect investors** and uphold market integrity.

Key Governance Expectations

- **Strong Board Structure**
  - Independent non-executive directors
  - Audit, Risk, Social & Ethics, and Remuneration Committees
- **Transparent Reporting**
  - Timely financial statements
  - Continuous disclosure of material information
- **Fair and Equal Treatment of Shareholders**
  - No selective disclosure
  - Voting rights respected
- **Robust Internal Controls & Risk Management**
  - Effective systems to manage financial, operational, and compliance risks
- **Compliance with King Code Principles**
  - Ethical leadership, accountability, internal controls, sustainability
- **Market Conduct & Disclosure**
  - Immediate reporting of price-sensitive information
  - Avoidance of insider trading
- **Fit and Proper Leadership**
  - Directors must be competent, ethical, and free of conflicts

Governance in Action

- **Are we acting ethically?**
- **Have we properly documented our decisions?**
- **Are we genuinely compliant—or simply assuming we are?**

What Does Good Governance Look Like?

Good governance means the board knows its role and doesn't interfere with operations—but it asks the tough questions. It means employees feel safe to speak up, because there's a whistleblowing policy that actually works. It's when financials are accurate, risks are well-managed, and stakeholders are engaged, not ignored.

In short?

- ✅ Decisions are ethical
- ✅ Roles are clear
- ✅ Risks are known
- ✅ Compliance is embedded
- ✅ Performance is tracked
- ✅ The culture encourages accountability—not blame

IT GOVERNANCE

Section 4

What IT Governance Ensures

- Alignment of technology decisions with organisational strategy
- Delivery of value through technology investments
- Effective management of IT and cyber risks
- Technology supporting—not hindering—business goals

King V Requirements for Technology & Information Governance

- Governing body must **oversee IT** as a strategic enabler
- IT must support achievement of organisational objectives
- Ethical, secure, and responsible use of technology
- Clear accountability for data, cybersecurity, and digital systems

Data, information and technology

PRINCIPLE 10: The governing body governs data, information and technology in a way that enables the organisation to sustain and optimise its strategy and objectives.

Examples of Evidence for King V Compliance

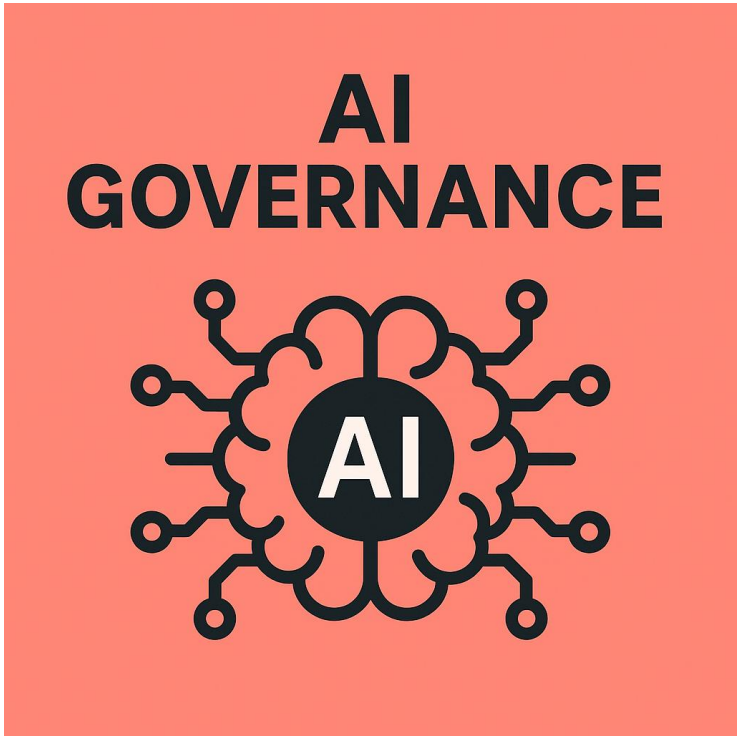
- Approved **IT Governance Framework or Policy**
- **IT Risk Register**, cyber risk dashboards, vulnerability reports
- Board or committee **minutes showing oversight** of key IT projects
- **Technology strategy** aligned to business objectives
- Records of cybersecurity training, incident response plans, or penetration testing
- Approved **Data Governance / Information Management Policy**
- Evidence of **IT spend reviews**, ROI assessments, or project prioritisation processes

AI GOVERNANCE

Section 5

What is AI Governance

- AI Governance ensures that artificial intelligence is developed and used in a way that is ethical, transparent, and aligned with organisational values.
- Under King V, the governing body must oversee how emerging technologies—including AI—are acquired, developed, implemented, and monitored.



109. The governing body should oversee that the organisation's acquisition, development, use and distribution of emerging, innovative and disruptive technologies result in:
    a. Investment and deployment that create sustainable value for the organisation within its economic, social and environmental context.
    b. Assessment, evaluation and responses to the risks and opportunities associated with emerging, innovative and disruptive technologies to ensure the alignment of current risk exposures with established risk appetite and tolerance levels.
    c. With respect to artificial intelligence:
        i. Adherence to the values of ethics, human centricity, accountability, transparency, explainability, security, privacy, fairness and trustworthiness.
        ii. Clear accountability for decisions, actions, outputs and outcomes – which includes subjecting the processes, data, models, algorithms, resources and tools used in the development, implementation, monitoring and management of automated technologies to human oversight and override mechanisms that are commensurate with the level of risk to the organisation and its stakeholders.
110. The governing body should consider periodic assurance on the effectiveness, compliance and ethics of the organisation's acquisition, development, use and distribution of technology.

King V Expectations for Emerging & Disruptive Technology

Organisations must ensure that innovative technologies — including AI — result in:

a) Sustainable Value Creation

- Investments in AI must support long-term economic, social, and environmental value
- AI projects must align with the organisation's strategic objectives

b) Risk & Opportunity Management

- AI risks must be assessed and managed within the organisation's risk appetite
- Boards must address risks relating to cybersecurity, privacy, bias, and model failure
- Opportunities must be evaluated to ensure responsible innovation

King V Expectations for Emerging & Disruptive Technology

c) Ethical Use of AI

AI must adhere to values of:

- **Ethics**
- **Human-centricity**
- **Accountability**
- **Transparency & Explainability**
- **Security & Privacy**
- **Fairness & Trustworthiness**

d) Human Oversight & Accountability

- Clear accountability for AI decisions, outputs, and impacts
- Human oversight must be built into AI processes, models, and algorithms
- Override mechanisms must exist proportionate to risk
- AI tools must be monitored continuously for accuracy, fairness, and safety

AI Governance Principles

Principle	Easy Explanation
Ethics	AI must do the right thing and not cause harm or break laws. *Just because AI can do something, doesn't mean it should.*
Human-Centricity	Humans stay in control and make final decisions. *AI helps people—people don't work for AI.*
Accountability	A human is always responsible for AI's actions and outcomes. *If AI makes a mistake, a human must fix it.*
Transparency & Explainability	AI decisions must be understandable, not hidden or mysterious. *No black boxes—AI should explain itself.*
Security & Privacy	AI must keep data safe and follow privacy laws like POPIA. *AI must lock the data door and never snoop.*
Fairness & Trustworthiness	AI must be unbiased and treat everyone fairly. *AI should act like a fair and trustworthy referee.*

PRIVACY & DATA GOVERNANCE

Section 6

What is Data Governance?

Data Governance protects personal information and ensures compliance with privacy laws such as **POPIA (South Africa)** and **GDPR (EU)**.

It also ensures that data handling aligns with King V's principles of **ethics, transparency, and legitimacy**.

- We know what data we have
- We know where it is stored
- We know who can access it
- We keep it safe and secure
- We use it ethically and legally (e.g., POPIA)
- We fix it when it's wrong
- We don't lose it or misuse it

PRINCIPLES	EXPLANATIONS AND DISCLOSURES
PRINCIPLE 10: The governing body governs data, information and technology in a way that enables the organisation to sustain and optimise its strategy and objectives.	**Exception declaration:** All the practices recommended in support of Principle 10 have been implemented, except for the following: › Recommended Practice No. [x] › Recommended Practice No. [x] *[ADDITIONALLY, THE ORGANISATION TO EXPLAIN WHY THE RECOMMENDED PRACTICES AS PER THE EXCEPTION DECLARATION HAVE NOT BEEN ADOPTED, AND WHICH COMPENSATING MEASURES HAVE BEEN IMPLEMENTED TO ENSURE ATTAINMENT OF THE OBJECTIVE SET BY PRINCIPLE 10.]* **Specific disclosures:** Disclosure in relation to **data and information**: › Whether the governing body is satisfied that the management and control (including acquisition, creation, use, dissemination and disposal) of data and information are effective, compliant and ethical. › Whether the governing body is satisfied that the arrangements for the prevention and detection of information privacy breaches are effective, and that significant incidents have been appropriately responded to, to manage consequences and prevent future occurrences. Disclosure in relation to **technology**: › Whether the governing body is satisfied that the acquisition, development, use and distribution of technology in and by the organisation are effective, compliant and ethical. › Whether the governing body is satisfied that the arrangements for the prevention and detection of cyber-attacks are effective, and that significant incidents have been appropriately responded to, to manage the consequences and prevent future occurrences. › Whether the governing body is satisfied that the ethical, legal and operational risks associated with the use of emerging, innovative and disruptive technologies are effectively managed and addressed. › With regards to AI, whether the governing body is satisfied that the accountability for decisions, actions, outputs and outcomes is clearly established – including that automated technologies are subject to human oversight and override mechanisms that are commensurate with their level of risk to the organisation and its stakeholders. *[ADDITIONALLY, OR ALTERNATIVELY, THE ORGANISATION TO INSERT LINKS TO WHERE IN OTHER EXTERNAL REPORT(S) THE REQUIRED DISCLOSURES ON THE APPLICATION OF PRINCIPLE 10 ARE MADE.]*

How to Evidence Data Governance

Element	Description / Example Practices
Data Lifecycle Management	Map how personal data is collected, used, stored, shared, and deleted.
Roles & Accountability	Appoint a Data Protection Officer or Information Officer.
Consent & Lawful Processing	Demonstrate lawful bases for processing (POPIA conditions).
Data Subject Rights	Procedures for access, correction, deletion, and objection.
Third-Party & Cross-Border Transfers	Contracts and safeguards for data shared with vendors or overseas.
Breach Management	Incident response process and notification timelines.

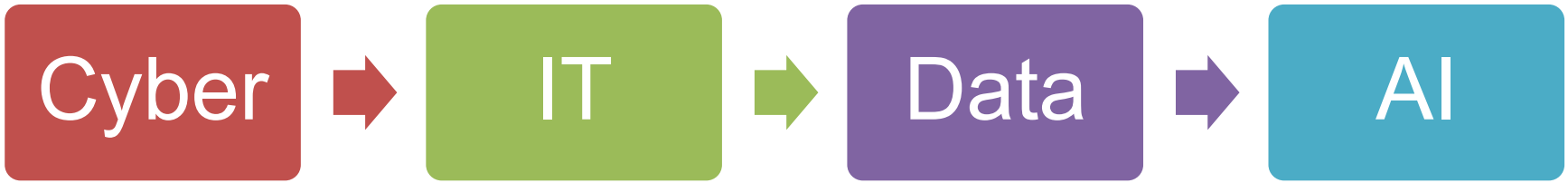
CYBERSECURITY GOVERNANCE

Section 7

What is Cyber Governance

Cyber governance is how an organisation makes sure its systems, data, and technology are **protected from cyber risks** such as hacking, fraud, data breaches, and ransomware.

- King V links technology risk to the **ethics and performance outcomes** of governance.
- Boards must evidence that they can **anticipate, withstand, respond to, and recover from** cyber incidents.



Oversight and monitoring

108. The governing body should oversee and monitor that the implementation and execution of policies, standards, and frameworks result in the realisation of the envisaged benefits from the organisation's technology strategies, investments, assets, resources, products and services. In particular, the following should be ensured:
    a. Compliance with laws and regulations.
    b. Arrangements for organisational resilience and disaster recovery planning and testing.
    c. Benefit to the organisation that is commensurate with significant investments in technology assets, resources, products and services.
    d. Responsible disposal of obsolete technology, including physical assets such as servers and computers, having regard to environmental impact as well as data and information security.
    e. Effective cyber security strategies and practices to protect technology assets, resources, products and services.
    f. Effective management of the risks associated with the acquisition and utilisation of outsourced technologies and services, including having minimum requirements for assurance to be provided by the service provider with respect to the effectiveness of the controls over significant risks.

How to Evidence Cyber Governance

Element	Description / Example Practices
Cyber Risk Management	Identify and rank critical systems and potential threat vectors.
Incident Response Plan	Step-by-step process for managing cyber incidents and data breaches.
Security Controls	Implement layered defences (firewalls, encryption, multi-factor authentication, SOC monitoring).
Awareness & Training	Conduct regular staff training and phishing simulations.
Testing & Assurance	Regular vulnerability scans, penetration testing, and cyber maturity assessments.
Reporting & Escalation	Cyber dashboards to EXCO/Board with key metrics and incidents.

Convergence of IT, Data, Cyber and AI Governance

All four frameworks should **link into one integrated Digital Governance Framework**, showing:

- **Alignment:** Each framework supports the organisation's purpose, strategy, and risk appetite.
- **Oversight:** A Board or sub-committee (e.g., IT, Risk, or Audit Committee) receives regular reports.
- **Accountability:** Roles and responsibilities are clearly defined between the CIO, CISO, Compliance Officer, and Board.
- **Assurance:** Internal audit or independent reviews test the effectiveness of controls.

Common Governance Frameworks

Framework	Primary Focus	King V Outcome Supported	Common Standards / References
IT Governance	Alignment of tech with strategy	Performance & Conformance	ISO 38500, COBIT 2019
AI Governance	Ethical, responsible AI use	Ethical Culture & Legitimacy	OECD AI Principles, EU AI Act
Privacy Governance	Data protection & rights	Legitimacy & Ethical Culture	POPIA, GDPR, ISO 27701
Cybersecurity Governance	Protection & resilience	Conformance & Performance	NIST CSF, ISO 27001, PA Joint Standard 1 of 2023

Module Summary Cont…

The Essence of Governance

Governance is the system that directs, controls, and protects an organisation. It ensures ethical leadership, clear accountability, responsible decision-making, and long-term value creation. Good governance prevents risk, builds trust, and strengthens performance.

Legal Backbone: Companies Act
The Companies Act sets the minimum legal standards for SA companies: director duties, record-keeping, financial responsibility, oversight committees, and prohibition of reckless trading.

Best Practice Compass: King Code (King IV → King V)
The King Code is voluntary but powerful — guiding organisations to act ethically, transparently, sustainably, and responsibly.
King V modernises governance with fewer principles, stronger disclosure, and a major focus on digital governance (data, cyber, AI, technology, ESG).

Module Summary

Governance for Listed Entities: JSE Requirements

JSE-listed companies operate in a high-trust environment requiring rigorous reporting, independent oversight, ethical conduct, and robust risk management.

Digital Governance Components

- **IT Governance:** Aligns tech with strategy and ensures value + control
- **Data Governance:** Protects data, ensures quality, ethics, and POPIA compliance
- **AI Governance:** Ensures responsible, ethical, transparent use of AI
- **Cyber Governance:** Protects systems and data from cyber threats

All four must converge into an **integrated digital governance framework** with clear accountability, oversight, and assurance.

Practical Take-Backs

1. Strengthen Ethical Decision-Making
•Pause before decisions: *Is it ethical? Is it legal? Is it documented?*

2. Improve Transparency & Documentation
•Record key decisions
•Maintain audit trails
•Communicate risks early

3. Apply Good Governance Daily
•Follow policies
•Escalate issues
•Respect delegations of authority
•Avoid shortcuts

4. Enhance Digital Awareness
•Understand how your work touches **IT, data, cyber, and AI governance**
•Follow privacy rules and cyber hygiene
•Question automated outputs — *don't blindly trust AI*

Practical Take-Backs

5. Encourage a Speak-Up Culture
•Use whistleblowing channels
•Raise concerns without fear
•Promote accountability — not finger-pointing

6. Align With King V Principles
•Lead ethically
•Focus on performance + purpose
•Strengthen control environments
•Build legitimacy with stakeholders

7. Build Risk Awareness
•Identify risks in your work area
•Take early action
•Don’t wait for audit or compliance to find issues

Guest Speaker

PRACTICAL INSIGHTS: WHAT GOOD AND BAD GOVERNANCE LOOKS LIKE IN PRACTICE.