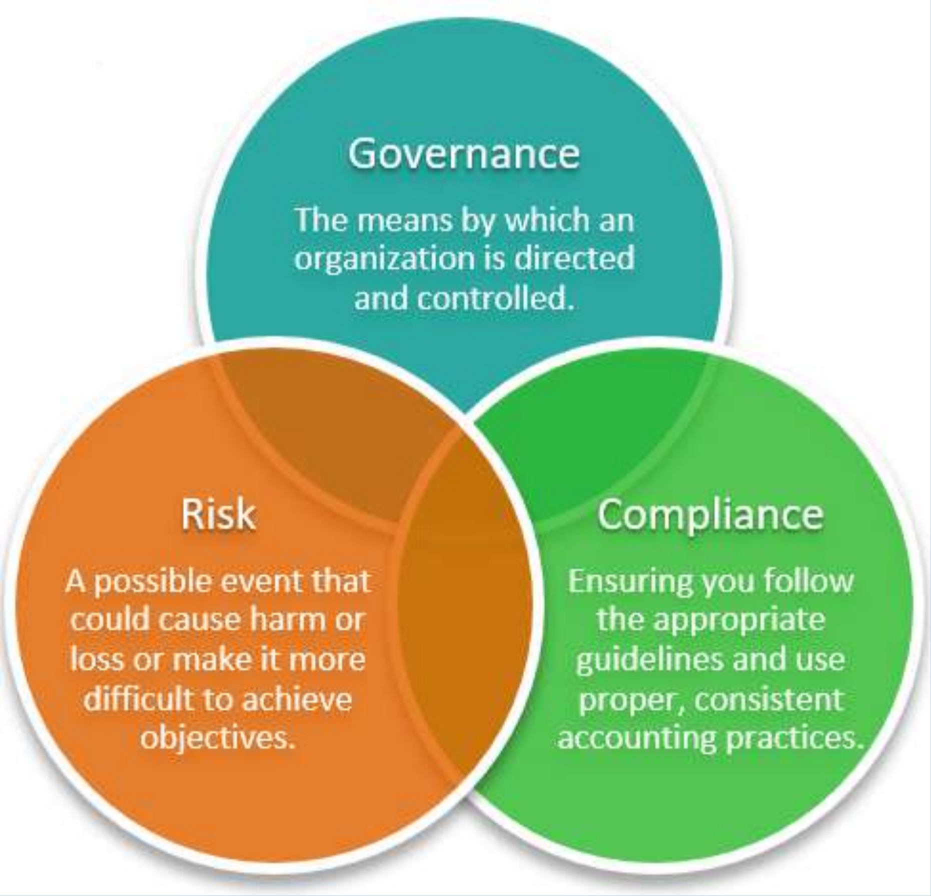
GRC
01010
11001
00101
62%
26%
24%
12%
8%
14%
20%
51%
45%

SkillToPro

GRC



Governance

The means by which an organization is directed and controlled.

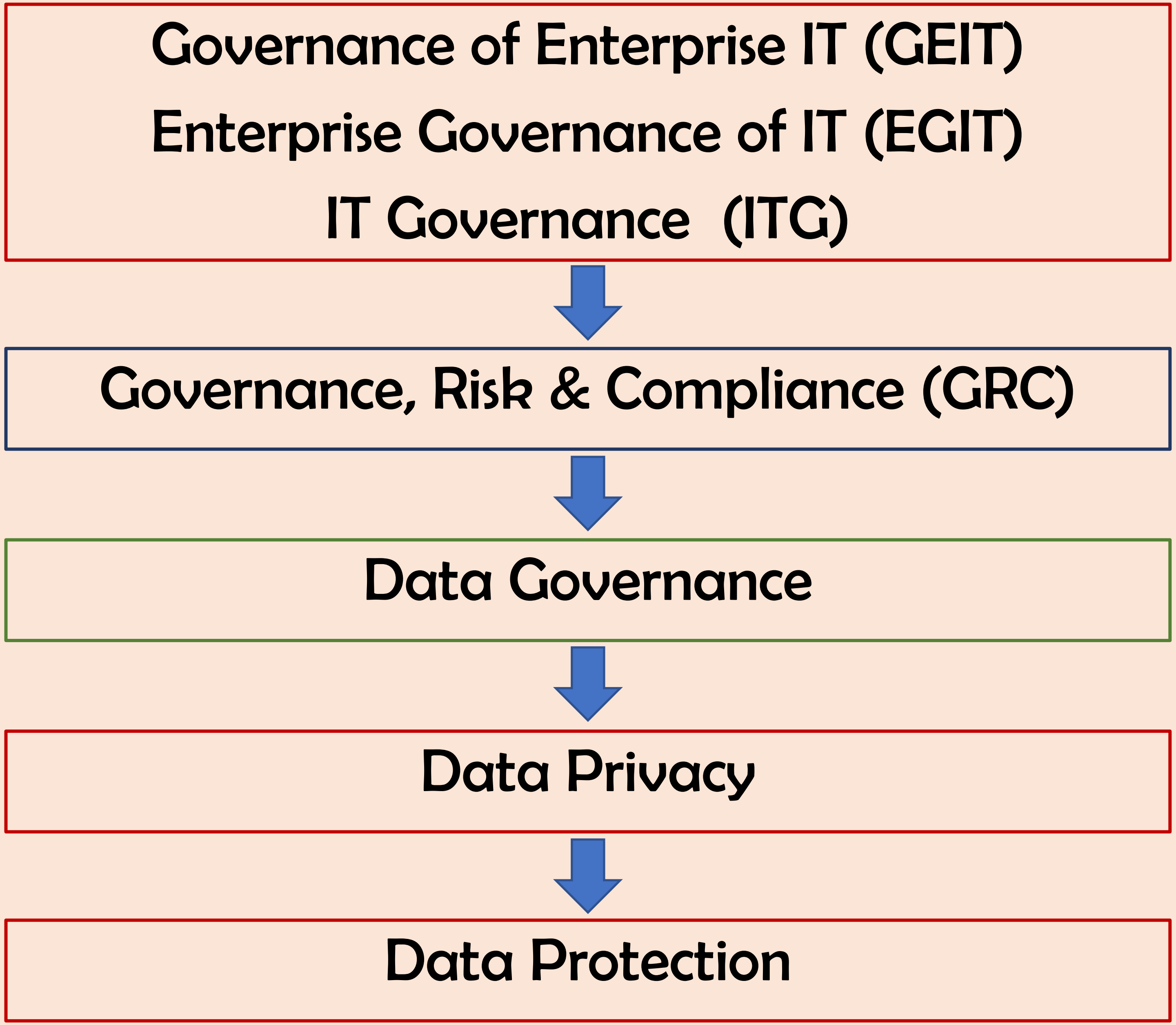
Risk

A possible event that could cause harm or loss or make it more difficult to achieve objectives.

Compliance

Ensuring you follow the appropriate guidelines and use proper, consistent accounting practices.

IT/IS GOVERNANCE IMPLEMENTATION TRACK



Governance of Enterprise IT (GEIT)

Enterprise Governance of IT (EGIT)

IT Governance (ITG)

Governance, Risk & Compliance (GRC)

Data Governance

Data Privacy

Data Protection

SkillToPro

GOVERNANCE, RISK & COMPLIANCE

GRC, short for **Governance, Risk And Compliance**, is a system that can make or break modern corporations. Organizations with effective GRC tools synchronize their risk management and regulatory compliance processes; organizations without may struggle with board effectiveness and overall corporate performance.

Entities across industries can benefit from a well-planned GRC strategy. GRC can help you align performance activities to business goals, manage enterprise risk and meet compliance regulations, all of which are make-or-break functions for corporations today.

GOVERNANCE, RISK & COMPLIANCE

In this chapter, we'll answer the following questions:

- What is GRC?
- What are the objectives of GRC
- Why does your organization need GRC?
- What does a strong GRC strategy look like?
- What does a weak GRC strategy look like?
- How can the right tools help your GRC strategy?
- What are GRC Frameworks?
- What is a GRC Solution?
- What is OCEG Capability Maturity Model?
- What are GRC Use Cases?

GOVERNANCE, RISK & COMPLIANCE

What is GRC?

GRC stands for governance, risk and compliance. GRC is a system that organizations use to structure governance, risk management, and regulatory compliance. **The concept is to unify an organization's approach to risk management and regulatory compliance**. Strengthening and rationalizing these processes can help improve business performance and enhance decision-making within corporate governance boards.

"GRC today must look across the risk and regulatory landscape to give boards centralized oversight of the most pressing challenges their organizations face. Would risk management be simpler if you had a unified view of governance, risk and compliance? Over the 17 years within the GRC industry, I've seen this be a game-changer for organizations." **Renee Murphy, Distinguished Evangelist**

GOVERNANCE, RISK & COMPLIANCE

The Open Compliance and Ethics Group (OCEG) coined the term GRC and formally defined it in 2007 as ***“the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity.”*** As the name suggests, the discipline has three main components: governance, risk management and compliance. Before we dive into what makes a GRC strategy effective, we’ll define and explain each of these three components individually.

GOVERNANCE, RISK & COMPLIANCE

GRC - Governance

Governance is the process of ensuring that all organizational activities (IT operations, training, etc.) align to support and advance the organization's overall goals and objectives. Governance typically involves the organization's key decision-makers, such as board members or high-level executives. It defines and enforces activities like:

- Board composition
- Corporate disclosure
- Executive compensation

How executives gather data, make strategic decisions, communicate with key stakeholders and determine who joins the board, all depend on governance. An example of poor governance in an organization might be a group of executives engaging in insider trading or a director whose business decisions and strategies consistently reflect a lack of interest in environmental, social or legal guidelines.

GOVERNANCE, RISK & COMPLIANCE

Effective governance uses data, information, and hard evidence to develop strategies and make decisions. Key data sources include:

- Internal audits
- Assurance reports
- Compliance monitoring results
- Risk assessments

Robust governance helps keep the organization on track and aligned with defined objectives.

GOVERNANCE, RISK & COMPLIANCE

GRC - Risk Management

Risk management involves identifying, assessing and controlling threats and risks to the organization. These threats could be financial pitfalls, legal consequences, cybersecurity threats, commercial liabilities, management errors, natural disasters, and other accidents.

Risk management processes typically rely on **internal audits and risk assessments** to identify critical gaps and areas of significant uncertainty. Risks can arise internally, within essential business operations and processes, or externally, out on the broader market.

Organizations often task many individuals with various elements of risk management, including IT security leaders, business analysts, finance officers and the governance board. A robust GRC framework can help ensure all risk management activities align with the organization’s ultimate goals and objectives.

GOVERNANCE, RISK & COMPLIANCE

GRC COMPLIANCE

GRC compliance involves aligning organizational activities with the laws and regulations that impact them. These regulations could be legal mandates, like privacy or environmental laws, or voluntarily established company policies and procedures.

For example, a compliance officer at a software company might work to ensure that their systems abide by regulations like GDPR. In contrast, an environmental inspector might search a construction site for environmental code violations and take the necessary steps to address them.

GRC frameworks encourage organizations to centralize compliance monitoring and stay on top of any laws or regulations that could affect their processes. Breaking compliance could result in devastating financial, legal and reputational consequences. These could include fines, time and money spent in court, and a tarnished reputation.

GRC OBJECTIVES

A successful GRC implementation leads to these key outcomes. Here's a more detailed breakdown of these outcomes:

1. **Strategic Alignment:** Information security governance ensures that security practices are aligned with the overall business strategy and objectives, supporting organizational goals.
2. **Risk Management:** By implementing a robust governance framework, organizations can effectively identify, assess, and mitigate security risks, reducing potential impacts on information resources.
3. **Value Delivery:** Effective information security governance optimizes investments in security, ensuring that security measures contribute to the overall value and performance of the organization.

GRC OBJECTIVES

4. **Resource Optimization:** A well-governed security program ensures that resources (personnel, budget, and technology) are used efficiently and effectively to achieve security objectives.
5. **Performance Measurement:** Information security governance enables organizations to measure, monitor, and report on the effectiveness of their security programs, ensuring that objectives are being met.
6. **Assurance Process Integration:** A robust governance framework integrates security assurance processes, ensuring that security controls are implemented and maintained effectively, providing confidence in the security posture.

GRC TERMINOLOGIES

- ❑ **Values** are prescribed and adopted by the company board of directors and form the foundation by which the company works. For example ***"Customer Obsession", "Care", "Agility",*** etc. These are often brief and punchy for maximum impact. Take a look at Centrica's corporate values. Values are usually accompanied by a mission statement to clearly articulate the company's priority and focus.
- ❑ **Principles** are statements of thought or belief which form the fundamental basis about attitudes and the way to behave. These may be company-wide or may be business unit or function-specific. Take a look at ***Amazon's Leadership Principles*** and at ***Microsoft's Ten Design Principles for Azure Applications***.
- ❑ **Tenets** are principles or beliefs that provide decision-making guidance in order to deliver the best value to customers. They are signposts that suggest not that way, this way. An example might be ***"We prioritize ease of use over performance".*** A good tenet is a tie-breaker or directive that influences actions and decisions through alignment with corporate, team, or project level values.

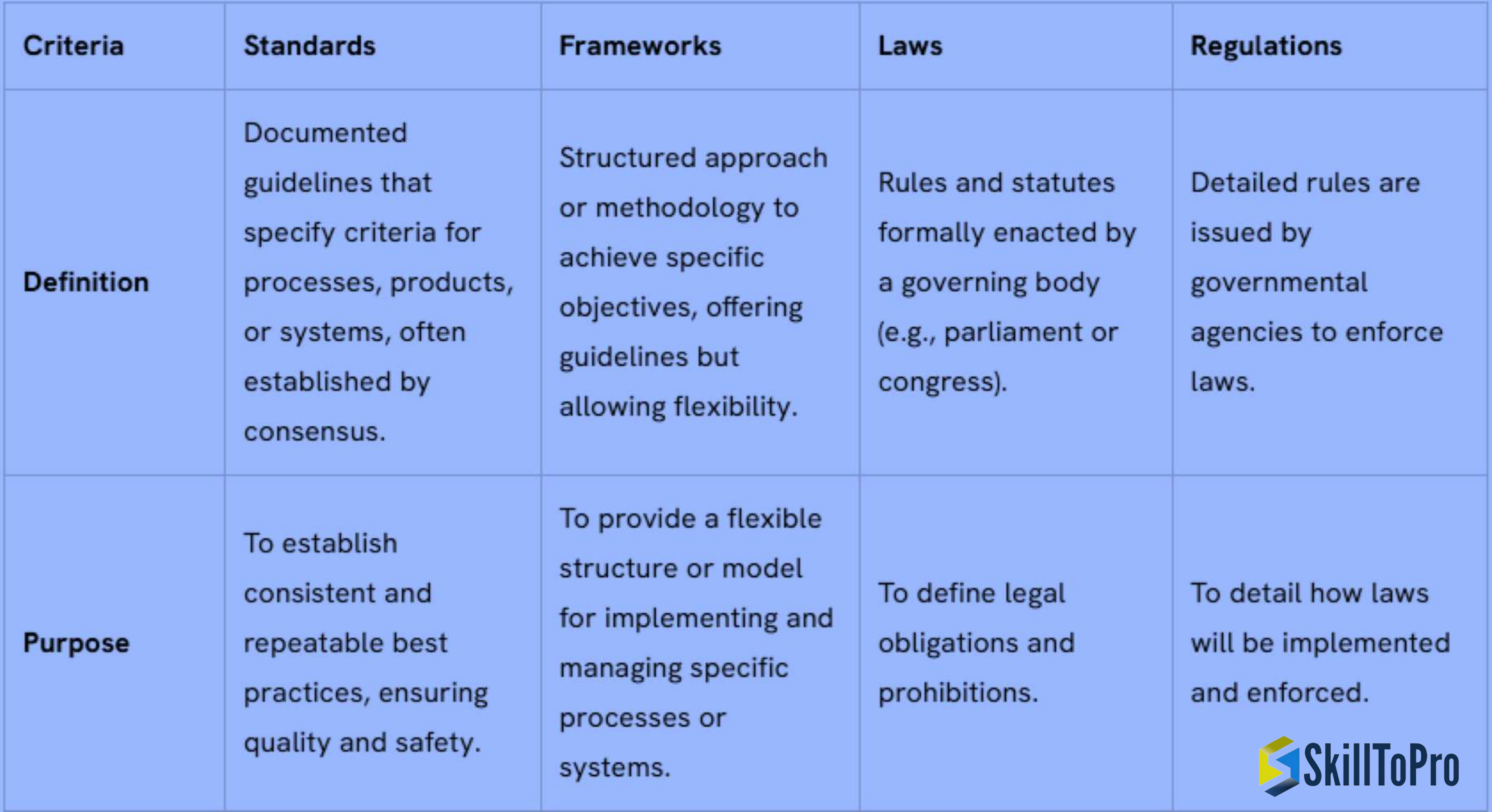
GRC TERMINOLOGIES

- ❑ **Policies** are formal, brief, high-level statements that typically includes declarations to require compliance with associated standards and regulatory requirements with a focus on the desired results and not the means of implementation. A policy statement might be ***"We will vigilantly protect customer data".*** In most cases, policies and principles are published together. Take a look at ***IBM's Corporate Policies and Principles***.
- ❑ **Procedures** describe respective processes: who does what, when they do it, and under what criteria. A procedure may contain multiple ways to achieve the associated objective and may or may not be mandatory, depending on what is stated in the related standards document.
- ❑ **Guidelines** provide the general statements, recommendations, and administrative instructions designed to achieve policy objectives and conform to standards by providing a framework within which to implement procedures. Guidelines are not generally prescriptive and often provide best practices for the company.

GRC TERMINOLOGIES

- **Standards** contain the mandatory, recommended, and optional actions and rules to generally support and conform to a given policy. ***Each standards document is typically subject specific (e.g., "Identity and Access Management Standard").*** Mandatory statements should be specific and measurable. Take a look at the PCI Security Standards which are accompanied by the associated goal. Audits take place against published standards.
- **Controls** are specific safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical assets, information, computer systems, or other resources, typically designed to protect the confidentiality, integrity and availability of information. Controls specify the mechanisms to implement the requirements and recommendations set forth in Standards. A single control (such as deploying a firewall at every ingress point) often satisfies multiple security requirements. In open standards such as ISO/IEC 27002, controls may take the form of recommendations (e.g., "Security perimeters should be used to protect areas that contain information and information processing facilities.").

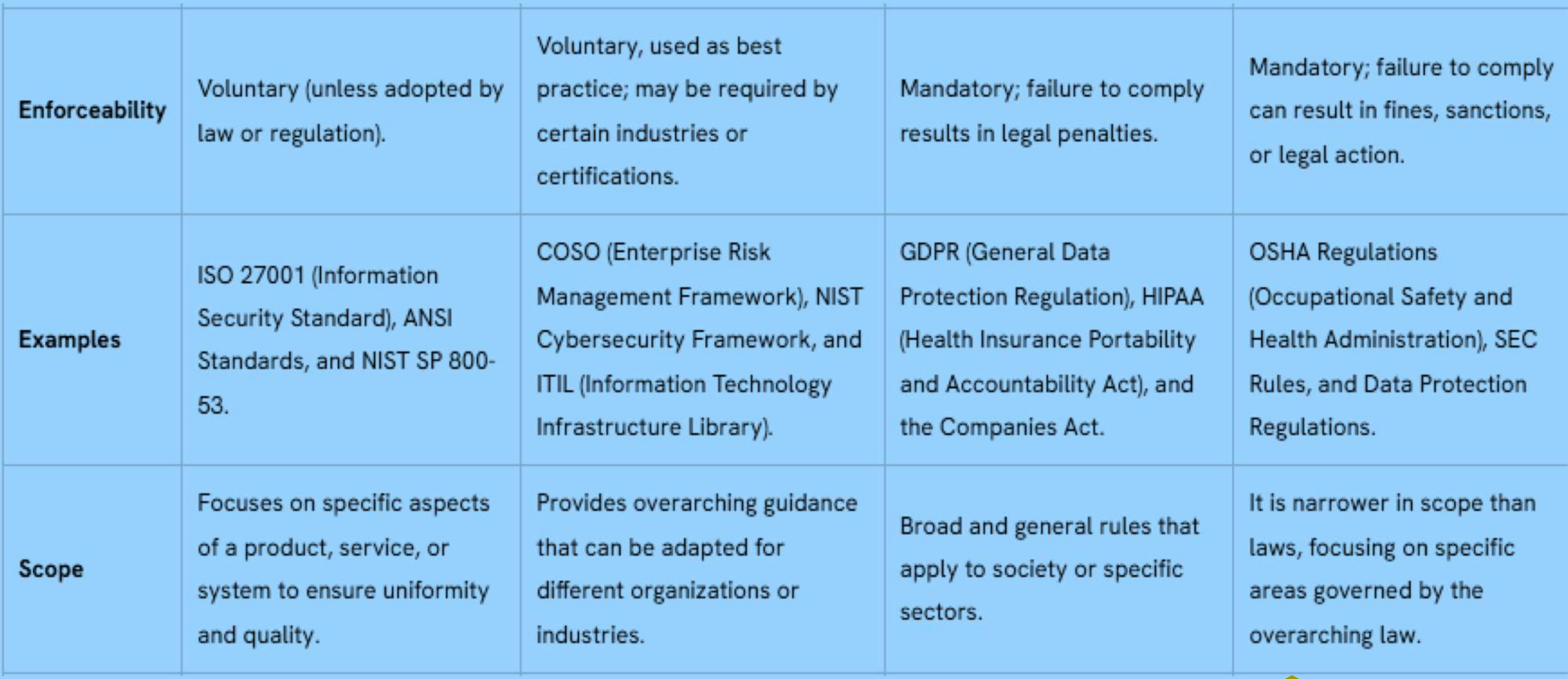
GRC TERMINOLOGIES



Criteria	Standards	Frameworks	Laws	Regulations
Definition	Documented guidelines that specify criteria for processes, products, or systems, often established by consensus.	Structured approach or methodology to achieve specific objectives, offering guidelines but allowing flexibility.	Rules and statutes formally enacted by a governing body (e.g., parliament or congress).	Detailed rules are issued by governmental agencies to enforce laws.
Purpose	To establish consistent and repeatable best practices, ensuring quality and safety.	To provide a flexible structure or model for implementing and managing specific processes or systems.	To define legal obligations and prohibitions.	To detail how laws will be implemented and enforced.

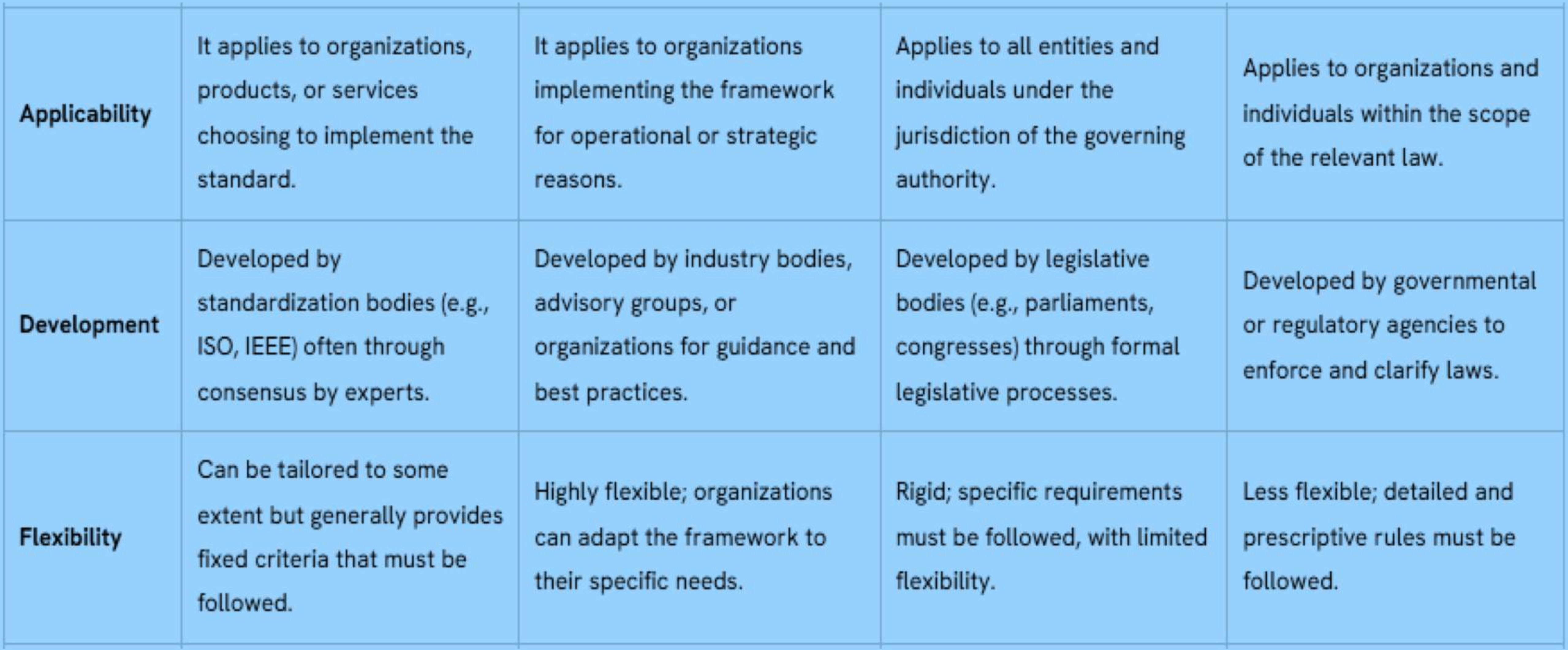
SkillToPro

GRC TERMINOLOGIES



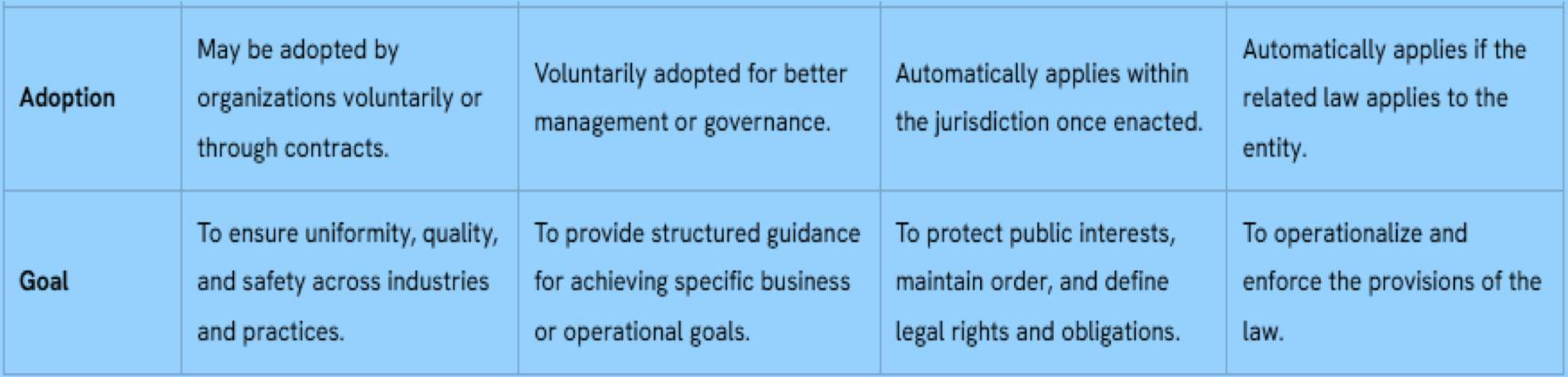
Enforceability	Voluntary (unless adopted by law or regulation).	Voluntary, used as best practice; may be required by certain industries or certifications.	Mandatory; failure to comply results in legal penalties.	Mandatory; failure to comply can result in fines, sanctions, or legal action.
Examples	ISO 27001 (Information Security Standard), ANSI Standards, and NIST SP 800-53.	COSO (Enterprise Risk Management Framework), NIST Cybersecurity Framework, and ITIL (Information Technology Infrastructure Library).	GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), and the Companies Act.	OSHA Regulations (Occupational Safety and Health Administration), SEC Rules, and Data Protection Regulations.
Scope	Focuses on specific aspects of a product, service, or system to ensure uniformity and quality.	Provides overarching guidance that can be adapted for different organizations or industries.	Broad and general rules that apply to society or specific sectors.	It is narrower in scope than laws, focusing on specific areas governed by the overarching law.

GRC TERMINOLOGIES



Applicability	It applies to organizations, products, or services choosing to implement the standard.	It applies to organizations implementing the framework for operational or strategic reasons.	Applies to all entities and individuals under the jurisdiction of the governing authority.	Applies to organizations and individuals within the scope of the relevant law.
Development	Developed by standardization bodies (e.g., ISO, IEEE) often through consensus by experts.	Developed by industry bodies, advisory groups, or organizations for guidance and best practices.	Developed by legislative bodies (e.g., parliaments, congresses) through formal legislative processes.	Developed by governmental or regulatory agencies to enforce and clarify laws.
Flexibility	Can be tailored to some extent but generally provides fixed criteria that must be followed.	Highly flexible; organizations can adapt the framework to their specific needs.	Rigid; specific requirements must be followed, with limited flexibility.	Less flexible; detailed and prescriptive rules must be followed.

GRC TERMINOLOGIES



Adoption	May be adopted by organizations voluntarily or through contracts.	Voluntarily adopted for better management or governance.	Automatically applies within the jurisdiction once enacted.	Automatically applies if the related law applies to the entity.
Goal	To ensure uniformity, quality, and safety across industries and practices.	To provide structured guidance for achieving specific business or operational goals.	To protect public interests, maintain order, and define legal rights and obligations.	To operationalize and enforce the provisions of the law.

WHAT DOES A WEAK GRC STRATEGY LOOK LIKE?

Unfortunately, a suboptimal approach to GRC can cause many issues. A weak strategy is typically founded on a host of disjointed activities and poor processes, including:

- ❑ Unclear objectives
- ❑ Lack of effective oversight
- ❑ Lack of access to crucial information
- ❑ Organizational and functional silos
- ❑ High costs
- ❑ High rates of duplication
- ❑ Wasted resources, data and information
- ❑ Unnecessary complexity

THE NEED FOR GRC?

Organizations face a rapidly changing and increasingly complex business climate. Whether you're part of a large corporation, government agency, small business or nonprofit, you'll face numerous challenges, including:

❑ Constant **changes to regulations and enforcement** that severely impact business operations

❑ Stakeholder demand for s**trong performance outcomes, consistent growth and transparent processes**

❑ Growing costs of addressing **compliance requirements and managing risk**

❑ Increase of **third-party relationships** and associated governance challenges

❑ Potential **legal and financial consequences** resulting from lack of effective oversight and overlooking critical threats

SkillToPro

BENEFITS OF GRC MANAGEMENT AND STRATEGY

The standard components of a strong GRC strategy include, but are not limited to:

- ❑ Effective oversight
- ❑ Integrated reporting and analytics
- ❑ Organization-wide ethics and integrity requirements
- ❑ Integrated information, risk and control activities
- ❑ Unified vocabulary across departments and disciplines
- ❑ Standardized practices for core processes like hiring, training, investments, evaluation, etc.

GRC FRAMEWORKS

A governance, risk and compliance framework is a structured approach to implementing GRC processes. An effective framework offers a systematic way to identify, assess, prioritize, and mitigate risks, ensuring that business operations follow a consistent set of ethical and security standards and are in compliance with laws and regulations.

COSO Framework - The Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework is a reputable ERM framework businesses across industries use to create a more holistic view of risk. Integrating COSO principles into a GRC model helps corporations layer accepted risk management best practices over their governance and compliance objectives.

NIST Framework - The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a repeatable process for managing and improving cybersecurity. Within GRC, it offers a structure for identifying, responding to and recovering from cybersecurity threats — a must, given that cyber-attacks spiked in 2023.

GRC FRAMEWORKS

ISO Framework - The International Organization for Standardization (ISO) offers guidance on various business needs, including information security and risk management. These standards complement GRC by offering documented approaches organizations can leverage to improve risk management and compliance.

ISACA Framework - ISACA is a global professional association that develops frameworks for IT governance and risk management, including the Control Objectives for Information and Related Technologies (COBIT). These frameworks can guide how an organization's GRC model aligns IT governance practices with their overall objectives and regulatory landscape.

GRC SOLUTIONS

In order to address the needs of GRC, a lot of organizations are turning to technology solutions. These solutions enable the leadership to monitor GRC across the enterprise by ensuring business processes and information technology continue to align to the governance, risk and compliance requirements of the organization. Capabilities include:

- Risk management (logging, analysis, and management)
- Document management
- Audit management
- Reporting
- Analytics

However, having a GRC tool alone isn't enough to guarantee effective GRC. Technology doesn't have ethics—people do. Hence GRC must be addressed from a people and process perspective, even before technology is considered.

OECG GRC CAPABILITY MODEL

The OECG GRC capability model is a **comprehensive framework** offering a **unified approach to organizational management across risk, governance, audit, ethics, IT, and compliance.** Organizations can use the capability model to enhance any of the above frameworks to serve as their sole methodology for developing and improving GRC practices.

Developed from a study of nearly 300 large corporations, the model offers GRC best practices organized into four components:

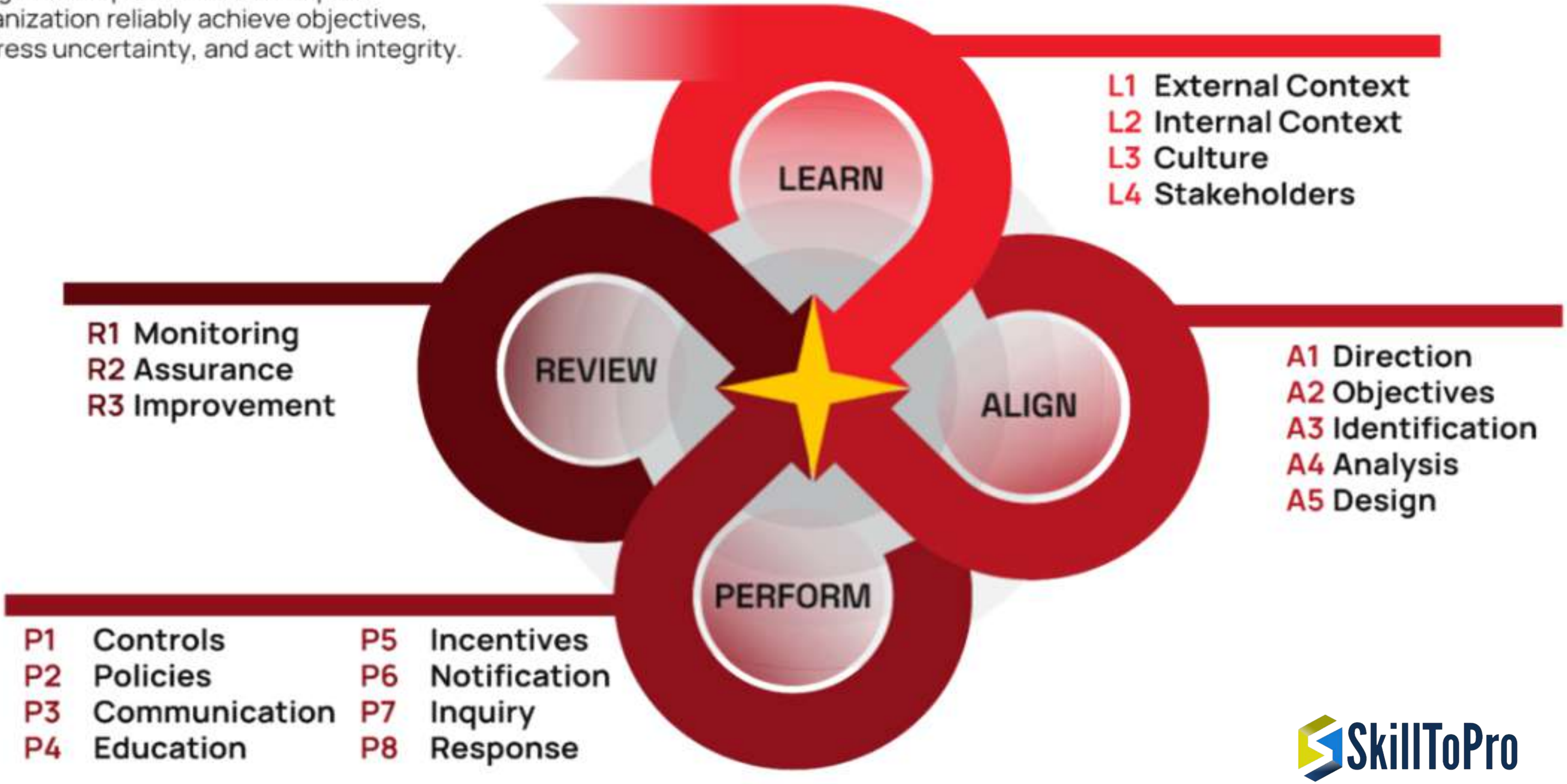
- **Learn:** This component involves building a deep understanding across the organization of GRC concepts, regulations and practices, including thorough education and training.
- **Align:** Organizations should build upon what they have learned by aligning GRC activities and strategic objectives and developing clear governance structures.
- **Perform:** The third component means executing GRC processes and activities to begin proactively managing risk, monitoring performance and maintaining compliance through audits, internal controls and more.
- **Evaluate:** Organizations must continuously assess the effectiveness of their GRC efforts through monitoring and measurement, which requires establishing performance metrics.

SkillToPro

OECG GRC CAPABILITY MODEL

GRC Capability Model 3.5

integrated capabilities that help an organization reliably achieve objectives, address uncertainty, and act with integrity.



LEARN

- L1 External Context
- L2 Internal Context
- L3 Culture
- L4 Stakeholders

ALIGN

- A1 Direction
- A2 Objectives
- A3 Identification
- A4 Analysis
- A5 Design

PERFORM

- P1 Controls
- P2 Policies
- P3 Communication
- P4 Education
- P5 Incentives
- P6 Notification
- P7 Inquiry
- P8 Response

REVIEW

- R1 Monitoring
- R2 Assurance
- R3 Improvement

GRC USE CASES

Organizations use GRC to integrate processes and tools to manage risks, meet compliance demands, and serve their own objectives. Here are typical examples of uses:

- ❑ **Establishing Policies and Practices**
  - A GRC framework helps organizations establish policies and practices to minimize compliance risk.
  - IT and security GRC solutions leverage timely information on data, infrastructure, and applications (virtual, mobile, cloud).
- ❑ **Improving Efficiency**
  - Centralizing issues into one framework eliminates duplicate efforts.
  - GRC creates a “single source of truth” to provide consistent and up-to-date information to everyone.

GRC USE CASES

- **Streamlining GRC Activities**
  - Monitoring compliance, risks, and governance can be automated to reduce manual work.
  - Many tasks can be systematized to save time and reduce errors.

- **Managing Financial and AI-Driven Models**
  - GRC guides model development, validation, and use.
  - It makes it easier to catalog and manage all models in use.
  - GRC ensures models are in compliance with applicable regulations.
  - GRC provides guidelines and standards for how organizations can use AI ethically.

GRC USE CASES

- **Risk Assessment and Reduction**
  - Organizations can get ahead with prevention, using the framework to identify risks.
  - GRC facilitates creating scenarios to analyze and formulating proactive protections to prevent problems.

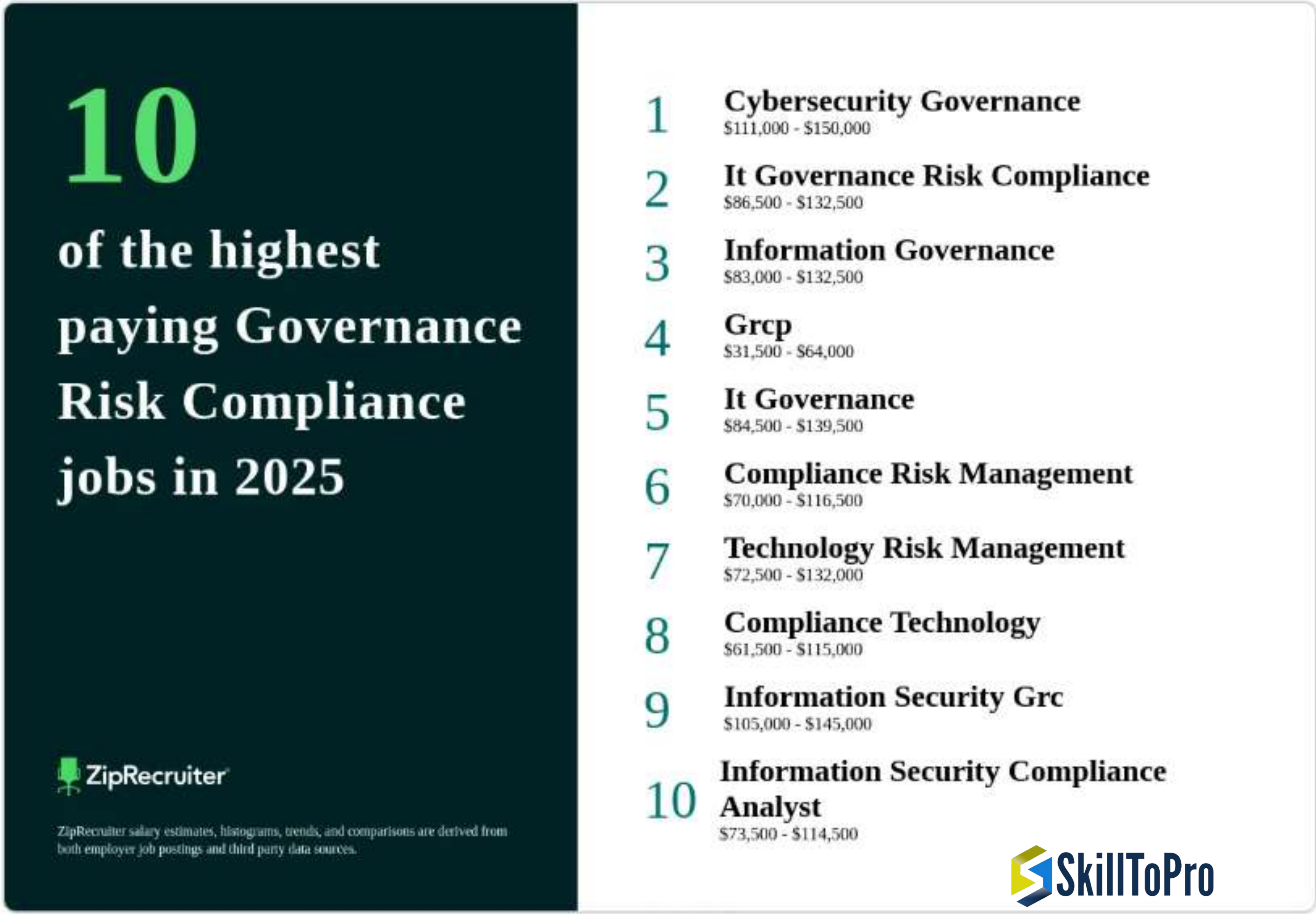
- **Support for Companies with Compliance Failures**
  - GRC can help organizations track and analyze incidents to identify root causes, and provides an audit trail.
  - The framework helps with impact assessments, incident response, and corrective actions.
  - GRC provides support in case of future failures.

GRC USE CASE

- ❑ **Improving Compliance**
  - GRC helps organizations identify areas where they are non-compliant and vulnerable.
  - It supports proactive reporting.
  - GRC contributes to creating a culture of compliance.

- ❑ **Better Policies and Management**
  - Organizations can standardize their policies and apply them consistently.
  - It is easier to respond to regulatory changes quickly, even automatically.
  - Companies can make faster, more informed decisions

Top GRC Job Titles



10

of the highest paying Governance Risk Compliance jobs in 2025

1	**Cybersecurity Governance**	$111,000 - $150,000
2	**It Governance Risk Compliance**	$86,500 - $132,500
3	**Information Governance**	$83,000 - $132,500
4	**Grcp**	$31,500 - $64,000
5	**It Governance**	$84,500 - $139,500
6	**Compliance Risk Management**	$70,000 - $116,500
7	**Technology Risk Management**	$72,500 - $132,000
8	**Compliance Technology**	$61,500 - $115,000
9	**Information Security Grc**	$105,000 - $145,000
10	**Information Security Compliance Analyst**	$73,500 - $114,500

ZipRecruiter

ZipRecruiter salary estimates, histograms, trends, and comparisons are derived from both employer job postings and third party data sources.

GRC JOB ROLES

- Senior Consultant – (IT GRC)
- Cyber Security GRC Operations Analyst
- InfoSec and GRC Officer
- Enterprise Risk Management Analyst
- Audit, Governance and Compliance Analyst
- GRC/ERM Technology Manager
- Security and Compliance Manager
- Senior Compliance Officer
- GRC IT Compliance Manager
- Security Advisor Senior - CGRC
- Internal Control and Compliance
- Compliance and Legal Officer
- Internal Audit Officer
- IT Strategy and Governance