MAY 2026 EDITION

SkillWeed

THE MODERN CYBERSECURITY GUIDE

THE GRC PULSE: NAVIGATING THE FUTURE OF CYBER GOVERNANCE

TABLE OF CONTENTS

EDITOR'S NOTE

There's a quiet shift happening in cybersecurity right now and if you pay attention, you will notice it's no longer just about **compliance checklists or passing audits.** May is revealing something deeper: **Cyber GRC is evolving into a strategic, intelligence-driven function.**

Everywhere you look, the conversation is changing. AI is introducing new kinds of risks. Organizations are demanding **real-time visibility, not periodic reports**. And professionals are no longer just asking *"how do I stay compliant?"* rather they're asking *"how do I stay relevant?"*

That shift matters.

Because the future of Cyber GRC belongs to those who can **connect risk to real business impact**, understand **emerging technologies like AI**, and move from simply following frameworks to actually **thinking like decision-makers**.

At Skillweed, we are paying close attention to this evolution and more importantly, we are building with it in mind.

This edition is designed to give you clarity on what's happening right now:

- The rise of **AI Governance**
- The move toward **continuous compliance**
- The growing importance of **identity, third-party risk, and digital trust**
- And what all of this means for your **career and positioning**

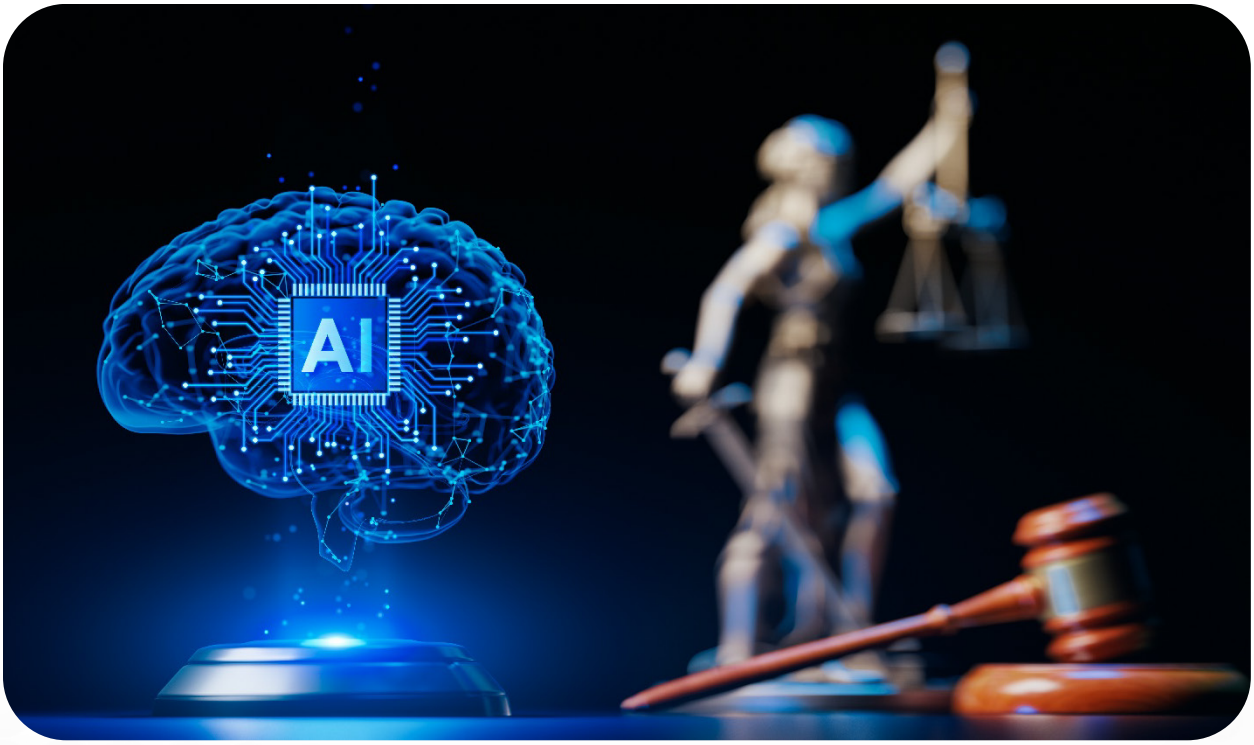
If you are just starting out or already in the field, one thing is clear: **This is not the time to stay static.**

It is the time to learn smarter, position strategically, and align yourself with where the industry is going, not where it has been.

We are glad you are here. Let's grow together.

Akingbade Akinfenwa

CHAPTER 1:
AI GOVERNANCE TAKES CENTER STAGE



Artificial Intelligence is no longer on the horizon, it is here, embedded in how organizations make decisions, automate processes, and deliver value.

But as adoption accelerates, so does uncertainty.

Across industries, leaders are asking a new question: **"How do we control what we don't fully understand?"**

This is where **AI Governance** steps in and why it has quickly become one of the most critical conversations in Cyber GRC today.

UNDERSTANDING AI GOVERNANCE

At its core, AI Governance is about **bringing structure, accountability, and control** to how AI systems are developed and used.

It ensures that AI is:

- **Safe** — minimizing unintended harm
- **Fair** — reducing bias and discrimination
- **Transparent** — enabling explainable outcomes
- **Compliant** — aligning with evolving regulations
- **Accountable** — assigning clear responsibility

In many ways, it is the natural evolution of GRC; **extending traditional risk and compliance principles into intelligent systems.**

WHY IT MATTERS NOW

The urgency around AI Governance is not theoretical, it is driven by real, emerging risks:

- AI systems making **biased or flawed decisions**
- Limited visibility into how models arrive at outcomes
- Increased exposure to **data privacy violations**
- The rise of **"Shadow AI"** — unsanctioned use of AI tools within organizations
- AI being leveraged for **cyber threats**, including deepfakes and automated phishing

These challenges are reshaping the risk landscape, forcing organizations to rethink how they approach governance entirely.

FRAMEWORKS GUIDING THE SHIFT

To respond, global standards and regulatory frameworks are evolving rapidly. Among the most influential are:

- **NIST AI Risk Management Framework (AI RMF)**
- **ISO/IEC 42001 – AI Management Systems**
- **EU AI Act and emerging global regulations**

These frameworks provide a foundation for organizations to **identify, assess, and manage AI-related risks** — not just once, but continuously.

For Cyber GRC professionals, this shift represents more than a trend; it is a **career inflection point**.

Those who build competence in AI Governance are uniquely positioned to:

- Lead **AI risk and impact assessments**
- Develop **governance policies for intelligent systems**
- Support **regulatory and compliance initiatives**
- Advise leadership on **AI-related business risks**

The role is evolving from enforcing compliance to **shaping strategy**.

THE BIGGER PICTURE

Traditional GRC operated within structured, predictable environments.
AI introduces systems that **learn, adapt, and evolve** often in ways that are difficult to fully anticipate.

This marks a fundamental shift:

- From **static controls** → to **dynamic oversight**
- From **known risks** → to **emerging, adaptive risks**
- From **operational roles** → to **strategic influence**

LOOKING AHEAD

AI Governance is not a niche specialization, it is fast becoming a **core capability** in modern cybersecurity and risk management.

For professionals and organizations alike, the message is clear:

The future belongs to those who can govern intelligence, not just infrastructure.

As the lines between technology, risk, and decision-making continue to blur, one thing is certain: **AI Governance is no longer optiognal. It is foundational.**

CHAPTER 2:
RISE OF CONTINUOUS COMPLIANCE

FROM PERIODIC AUDITS TO ALWAYS-ON ASSURANCE

For years, compliance followed a familiar rhythm; prepare for the audit, gather evidence, pass the assessment, and repeat the cycle.

But that model is quickly becoming outdated.

In today's fast-moving digital environment, risk doesn't wait for audit cycles and neither can compliance. This is driving a major shift toward **Continuous Compliance**: a model where organizations maintain a constant state of readiness, visibility, and control.

WHAT IS CONTINUOUS COMPLIANCE?

Continuous Compliance is the practice of **monitoring, validating, and enforcing controls in real time** rather than relying on periodic reviews.

Instead of asking: *"Were we compliant last quarter?"* Organizations are now asking: **"Are we compliant right now?"** It's a shift from **point-in-time assurance → ongoing assurance**.

WHY THE SHIFT IS HAPPENING

Several forces are accelerating this transition:

- **Rapid system changes** in cloud and hybrid environments
- Increasing **regulatory expectations** for real-time accountability
- The growing complexity of **third-party ecosystems**
- Rising cyber threats that exploit even short windows of vulnerability

In this environment, a control that was valid yesterday may already be **ineffective today**.

HOW IT WORKS IN PRACTICE

Continuous Compliance is powered by:

- **Automation tools** that track controls in real time
- **Continuous Control Monitoring (CCM)** systems
- **Integrated dashboards** providing live risk visibility
- **Alerts and triggers** for immediate remediation

This allows organizations to move from reactive responses to **proactive risk management**.

WHAT CHANGES FOR GRC TEAMS

The role of GRC professionals is evolving significantly:

- From **manual evidence gathering** → to **system-driven validation**
- From **audit preparation** → to **always audit-ready environments**
- From **static reporting** → to **real-time insights and decision support**

GRC is no longer just about documentation, it's about **visibility and action**.

BUSINESS IMPACT

Organizations adopting Continuous Compliance are seeing:

- Faster identification and remediation of risks
- Reduced audit fatigue and operational burden
- Improved trust with regulators and stakeholders
- Stronger alignment between **risk, compliance, and business operations**

In essence, compliance becomes **embedded into daily operations**, not treated as a separate function.

WHAT THIS MEANS FOR YOU

For Cyber GRC professionals, this shift is critical:

- You need to understand **automation and GRC tools**
- Develop skills in **data interpretation and dashboards**
- Think beyond frameworks, focus on **real-time control effectiveness**
- Position yourself as someone who can **translate risk into actionable insights**

THE BOTTOM LINE

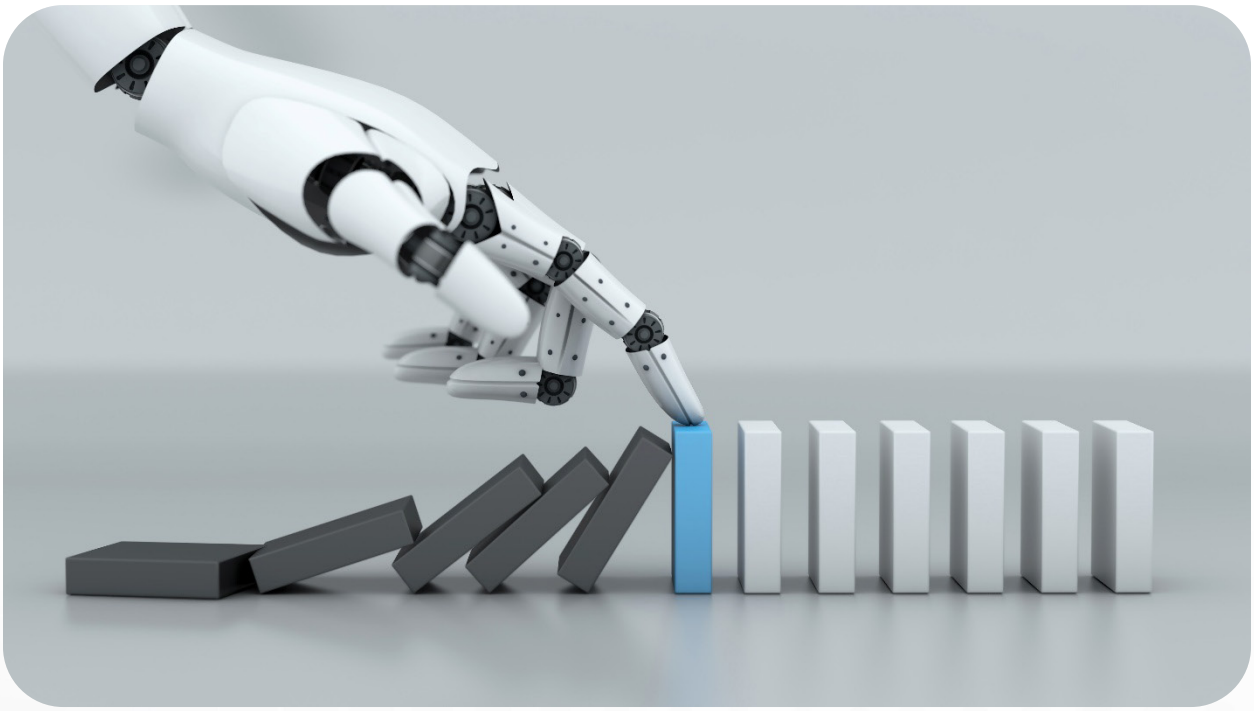
Compliance is no longer an event, **it's a continuous state.**

And the professionals who understand how to operate in this model will be the ones who move from supporting the business to **driving it forward**.

As organizations demand more speed, transparency, and accountability, one thing is clear: **Continuous Compliance is not the future, it is the new standard.**

CHAPTER 3:
THIRD-PARTY RISK MAKING HEADLINES

WHY YOUR BIGGEST THREAT MAY NOT BE INSIDE YOUR ORGANIZATION



Today's world is interconnected. This means no organization operates alone. From cloud providers and payment processors to SaaS platforms and external consultants, businesses now rely heavily on **third-party vendors** to function and scale.

But with this dependence comes a growing reality: **your organization's security is only as strong as your weakest vendor.** And increasingly, that's where the risk lies.

UNDERSTANDING THIRD-PARTY RISK

Third-party risk refers to the potential threats introduced by external vendors, partners, or service providers who have access to your systems, data, or operations.

These risks can include:

- **Data breaches** through vendor systems
- **Operational disruptions** due to vendor failure
- **Compliance violations** inherited from third parties
- **Unauthorized access** to sensitive information

In many cases, organizations are secure internally but exposed externally.

RECENT THIRD-PARTY RISK HEADLINES (2025-2026)

Third-party and supply chain risks are surging, with attacks doubling since April 2025 and costing millions per incident. Here's a summary of major headlines:

Incident	Date	Details
Crunchyroll Breach	March 2026	Hackers compromised Telus International vendor, exposing 6.8M customer support tickets via stolen Okta SSO.
HackerOne Data Leak	Dec 2025-Jan 2026	Navia partner breach leaked employee data; disclosed March 2026.
Chain IQ Group AG	June 2025	Ransomware hit procurement vendors, leaking client data to the dark web using novel tactics.
Toronto School Board / PowerSchool	May-June 2025	Student platform breach led to extortion; ransom paid but attacks continued.
National Defense Corp	March 2025	Interlock ransomware stole 3M files from a defense supplier, disrupting military logistics.

WHY IT'S DOMINATING HEADLINES

Recent trends show a clear pattern: cyber incidents are increasingly originating from **supply chain vulnerabilities**.

Why?

- Organizations now manage **hundreds of vendors**, often without full visibility
- Vendors themselves rely on **sub-vendors**, creating layered risk
- Rapid onboarding processes often **skip deep risk assessments**
- Continuous monitoring is still **limited or nonexistent** in many environments

This creates a complex web of dependencies and a wider attack surface.

THE EXPANDING ATTACK SURFACE

What makes third-party risk particularly dangerous is its **indirect nature**.

Unlike internal threats, vendor risks are:

- Harder to detect
- More difficult to control
- Often outside direct authority

Yet, they can have **direct and severe consequences** on operations, reputation, and compliance.

WHAT EFFECTIVE THIRD-PARTY RISK MANAGEMENT LOOKS LIKE

Organizations are shifting toward more structured approaches, including:

- **Vendor risk assessments** before onboarding
- **Risk tiering** based on access and criticality
- **Ongoing monitoring** instead of one-time reviews
- **Contractual controls** and security requirements
- Integration with broader **GRC frameworks and tools**

This approach is commonly known as **Third-Party Risk Management (TPRM)** and it is quickly becoming a core GRC function.

As third-party ecosystems expand, so does the demand for professionals who can manage them effectively. Cyber GRC professionals are now expected to:

- Evaluate and classify vendor risks
- Design and enforce **TPRM frameworks**
- Monitor vendor compliance continuously
- Bridge the gap between **security, legal, and procurement teams**

This is no longer a support function, it's a **business-critical role**.

Organizations are beginning to understand that third-party risk is not just a technical issue, It's a **business risk**.

- A vendor outage can halt operations
- A vendor breach can damage trust
- A vendor compliance failure can trigger regulatory penalties

This is pushing third-party risk from the background to the **boardroom**.

THE BOTTOM LINE

You can secure your systems, enforce your policies, and strengthen your controls but if your vendors are exposed, so are you.

Third-party risk is no longer secondary. It is central.

With digital ecosystems expanding, one thing is clear: The organizations that thrive will be those that **treat vendor risk with the same urgency as internal risk** and the professionals who can lead that effort will be in high demand.

CHAPTER 4:
MANAGING "SHADOW AI" IN THE WORKPLACE

While organizations are busy rolling out official AI strategies, another reality is unfolding quietly in the background: **Employees are already using AI on their own terms.**

From drafting emails with ChatGPT to analyzing data with AI-powered tools, "unofficial" AI usage is rapidly becoming part of everyday workflows. This phenomenon is known as **Shadow AI** and it is one of the fastest-growing, least visible risks in modern organizations.

WHAT IS SHADOW AI?

Shadow AI refers to the **use of artificial intelligence tools without formal approval, oversight, or governance** by an organization. It mirrors the concept of Shadow IT but with far greater implications.

Examples include:

- Uploading sensitive company data into public AI tools
- Using AI to generate reports, code, or decisions without validation
- Integrating AI tools into workflows without security review

In most cases, employees are not acting maliciously; they are simply trying to **work faster and smarter**.

WHY IT'S A SERIOUS RISK

The challenge with Shadow AI is not just its existence, it's its **lack of visibility and control**.

Key risks include:

- **Data leakage** — confidential information exposed to external AI models
- **Compliance violations** — especially with data protection regulations
- **Inaccurate outputs** — decisions based on unverified AI results
- **Security vulnerabilities** — unknown integrations and access points
- **Loss of accountability** — unclear ownership of AI-driven outcomes

Because these activities happen outside formal systems, they often go **undetected until damage is done**.

Shadow AI is accelerating due to:

- Easy access to powerful, user-friendly AI tools
- Pressure on employees to **increase productivity**
- Lack of clear organizational policies around AI usage
- Slow adoption of formal AI governance structures

In many workplaces, the tools are already ahead of the policies.

FROM RESTRICTION TO GOVERNANCE

A common mistake organizations make is trying to **ban AI tools outright**. In reality, that approach rarely works.

Instead, leading organizations are shifting toward:

- **Establishing clear AI usage policies**
- Providing **approved, secure AI tools** for employees
- Educating staff on **safe and responsible AI use**
- Implementing **monitoring and visibility mechanisms**
- Embedding AI into existing **GRC frameworks**

The goal is not to eliminate AI usage but to **bring it under control**.

THE ROLE OF CYBER GRC PROFESSIONALS

Managing Shadow AI is quickly becoming a core responsibility for Cyber GRC teams.

Professionals in this space are expected to:

- Identify and assess Shadow AI risks
- Develop and enforce **AI governance policies**
- Collaborate with IT and security teams for visibility
- Align AI usage with **regulatory and compliance requirements**
- Educate the workforce on responsible AI practices

This is where **AI Governance and GRC intersect in real time**.

A NEW REALITY OF WORK

Shadow AI highlights a broader shift:

Technology adoption is no longer top-down, it is **employee-driven**.

This means governance models must evolve from being **reactive and restrictive** to being **proactive and enabling**.

THE BOTTOM LINE

Shadow AI is not a future risk but it is already here, operating quietly across organizations.

Ignoring it creates exposure. Over-restricting it creates resistance.

The real solution lies in **visibility, education, and structured governance**.

As AI becomes embedded in daily work, one thing is clear: The organizations that succeed will not be those that avoid AI but those that **understand, manage, and govern it effectively.**

CHAPTER 5:
TOOLS ENABLING CONTINUOUS CONTROL MONITORING (CCM)

POWERING REAL-TIME ASSURANCE IN A DYNAMIC RISK ENVIRONMENT

Organizations are shifting towards **Continuous Compliance** and one capability that sits at the center of it all is **Continuous Control Monitoring (CCM).**

CCM is what transforms compliance from a manual, periodic task into a **real-time, automated system of assurance**. And at the heart of CCM are the tools that make it possible.

Continuous Control Monitoring is the practice of **automatically tracking and validating the effectiveness of security and compliance controls in real time**.

Instead of manually checking whether controls are working, CCM tools continuously answer: **"Is this control functioning as expected right now?"**

Modern CCM is powered by a combination of technologies working together to provide visibility and control:

1. GRC PLATFORMS

Centralize risk, compliance, and control management.

- Track control frameworks (ISO, NIST, SOC 2, etc.)
- Map controls to regulatory requirements
- Provide audit-ready documentation

2. SIEM & SECURITY MONITORING TOOLS

Analyze security events and detect anomalies in real time.

- Monitor logs and system activities
- Identify control failures or suspicious behavior
- Trigger alerts for immediate action

3. CLOUD SECURITY POSTURE MANAGEMENT (CSPM)

Ensure cloud environments remain compliant and secure.

- Detect misconfigurations
- Enforce cloud security policies
- Continuously scan for risks

4. IDENTITY & ACCESS MANAGEMENT (IAM) TOOLS

Control and monitor user access across systems.

- Enforce least privilege access
- Detect unauthorized access attempts
- Validate access-related controls

5. AUTOMATION & INTEGRATION TOOLS

Connect systems and eliminate manual processes.

- Automate evidence collection
- Sync data across platforms
- Enable real-time reporting dashboards

WHAT THESE TOOLS ENABLE

When effectively integrated, CCM tools provide:

- **Real-time visibility** into control effectiveness
- **Automated evidence collection** for audits
- **Instant alerts** when controls fail
- **Reduced manual workload** for GRC teams
- **Continuous audit readiness**

This is what allows organizations to move from reactive compliance → to **proactive assurance**.

With the rise of CCM tools, the role of Cyber GRC professionals is evolving:

- From **manual testers** → to **tool-enabled analysts**
- From **documentation-heavy roles** → to **insight-driven roles**
- From **after-the-fact reporting** → to **real-time decision support**

Understanding how these tools work and how they connect is becoming a **core competency**.

While CCM tools are powerful, implementation is not without challenges:

- Tool fragmentation and lack of integration
- High volume of alerts (noise vs. signal)
- Misconfigured controls leading to false confidence
- Skill gaps in interpreting tool outputs

Success depends not just on the tools but on **how they are configured and used**.

CCM tools are not just about compliance; they are about **trust, speed, and resilience**.

Organizations that leverage these tools effectively can:

- Respond to risks faster
- Build stronger relationships with regulators
- Operate with greater confidence in their control environment

THE BOTTOM LINE

Continuous Control Monitoring is the engine behind modern compliance and tools are the fuel that keeps it running.

But tools alone are not enough. The real advantage lies in professionals who can **translate tool outputs into meaningful risk insights and actions.**

As compliance continues to evolve, one thing is clear: **Mastering CCM tools is no longer optional, it is essential for staying relevant in modern Cyber GRC.**

CHAPTER 6:
GLOBAL COMPLIANCE UPDATES

NAVIGATING A RAPIDLY EVOLVING REGULATORY LANDSCAPE

Organizations now operate across borders and so do the regulations that govern them.

From data privacy laws to AI governance frameworks, the global compliance landscape is evolving faster than ever and Cyber GRC professionals are at the center of it all. Governments and regulatory bodies worldwide are tightening controls around:

- **Data privacy and protection**
- **Cybersecurity standards**
- **AI usage and governance**
- **Third-party and supply chain risks**

This is driven by increasing concerns around data misuse, cyber threats, and the ethical implications of emerging technologies.

KEY REGULATORY TRENDS TO WATCH

1. DATA PRIVACY IS EXPANDING BEYOND GDPR

While GDPR set the global benchmark, many regions are now introducing their own frameworks.

- Countries are adopting **localized data protection laws**
- Cross-border data transfer rules are becoming stricter
- Organizations must manage **multi-jurisdictional compliance**

Compliance is no longer "one framework fits all"

2. AI REGULATION IS TAKING CENTER STAGE

With the rise of AI, regulators are stepping in to define boundaries.

- New policies focus on **ethical AI use, transparency, and accountability**
- Organizations must assess **AI-related risks and biases**
- Documentation and explainability are becoming critical requirements

AI Governance is quickly becoming a core GRC function

3. CYBERSECURITY REGULATIONS ARE BECOMING MANDATORY

Cyber resilience is no longer optional.

- Governments are enforcing **minimum cybersecurity standards**
- Mandatory **breach reporting timelines** are tightening
- Industries like finance and healthcare face stricter oversight

Security is now a regulatory requirement, not just a best practice

4. THIRD-PARTY COMPLIANCE IS UNDER SCRUTINY

Regulators are extending responsibility beyond the organization.

- Companies are now accountable for **vendor compliance failures**
- Stronger requirements for **third-party risk management (TPRM)**
- Increased demand for **continuous monitoring and reporting**

Your vendors are now part of your compliance scope

WHAT DOES THIS MEAN FOR ORGANIZATIONS?

Operating globally now requires:

- Managing **multiple regulatory frameworks simultaneously**
- Aligning internal controls with **diverse compliance requirements**
- Maintaining **consistent documentation and reporting standards**
- Investing in tools and processes that support **continuous compliance**

The complexity is increasing but so is the need for structured GRC strategies.

Thanks to the regulations expanding, the importance of GRC expertise is also expanding and more necessary than others.

Professionals are expected to:

- Interpret and apply **global regulatory requirements**
- Align frameworks like **ISO, NIST, SOC 2** with regional laws
- Advise organizations on **compliance strategy and risk exposure**
- Stay ahead of emerging trends in **AI, privacy, and cybersecurity regulation**

This is no longer just a technical role; it is a **strategic, globally relevant function**.

While global compliance may seem overwhelming, it presents a unique opportunity:

- Organizations need **experts who understand multiple frameworks**
- There is growing demand for professionals who can **bridge regions and regulations**
- Specializing in areas like **AI governance or data privacy** can significantly boost career value

THE BOTTOM LINE

Compliance is no longer local: **it is global, dynamic, and constantly evolving.**

Organizations that succeed will be those that can **adapt quickly, stay informed, and integrate compliance into their core operations.**

As the regulatory landscape continues to shift, one thing is clear: The future belongs to Cyber GRC professionals who can **think globally, act strategically, and navigate complexity with confidence.**

CHAPTER 7:
SKILLWEED SPOTLIGHT

INSIDE THE EXPERIENCE EVERYONE'S TALKING ABOUT

There is a reason more people are quietly gravitating toward Skillweed.

Not because of loud promises…But because of **real experiences, real growth, and real results**.

This month, we are taking you inside what's actually happening within the community from our AI Internship to CRISC preparation through the lens of those living it.

INSIDE THE AI INTERNSHIP: LEARNING BY DOING

Most people *learn* AI. Here, you actually **work with it**.

Participants in the Skillweed AI Internship aren't just watching videos, they're:

- Breaking down real-world AI governance concepts
- Applying knowledge directly from structured content (starting with Chapter 1)
- Engaging in practical discussions that mirror real industry scenarios

But what stands out isn't just the content…

It's the experience.

"I thought it would be another course. But it actually feels like we're building something together."

There's a rhythm to it; You learn, you try, you ask questions, you improve.

No pressure. No perfection. Just progress.

CRISC PREP: A DIFFERENT KIND OF PREPARATION

If you've ever tried preparing for certifications alone, you already know:

It can feel overwhelming. Unstructured. And easy to give up on.

That's why Skillweed's CRISC Prep feels different.

Instead of guessing what matters, students are guided through:

- **Domain-focused breakdowns** that simplify complex topics
- **Past-question-heavy sessions** that reflect real exam patterns
- **On-demand access** for flexible learning
- **Live classes** for structure, accountability, and clarity

And for many, the biggest shift isn't just knowledge, it's confidence.

"I finally understand what the exam is about. That changed everything for me."

STUDENT WINS: PROGRESS YOU CAN SEE

Not every win is loud but they are happening every day.

- Someone who had no prior GRC knowledge now confidently explains risk frameworks
- Someone who struggled with consistency now shows up daily
- Someone who doubted themselves is now preparing to write their certification exam

These are the kinds of wins that don't always trend, but they **change careers**.

"The biggest thing I gained wasn't just knowledge. It was clarity."

WHAT PEOPLE ARE REALLY SAYING

Across the community, a few themes keep coming up:

- *"It doesn't feel like I'm learning alone."*
- *"The structure makes it easy to stay consistent."*
- *"You actually understand, not just memorize."*
- *"It's intense, but in a good way."*

And maybe the most telling one: *"I wish I joined earlier."*

MORE THAN A PROGRAM; A COMMUNITY

Skillweed isn't just about classes.

It's:

- The late-night questions that get answered
- The shared wins in the group chat
- The accountability you didn't know you needed
- The people who remind you why you started

It's structured enough to guide you and flexible enough to grow with you.

IF YOU'VE BEEN WATCHING FROM THE OUTSIDE...

You don't need to rush.
You don't need to be perfect.

But if you've been thinking about:

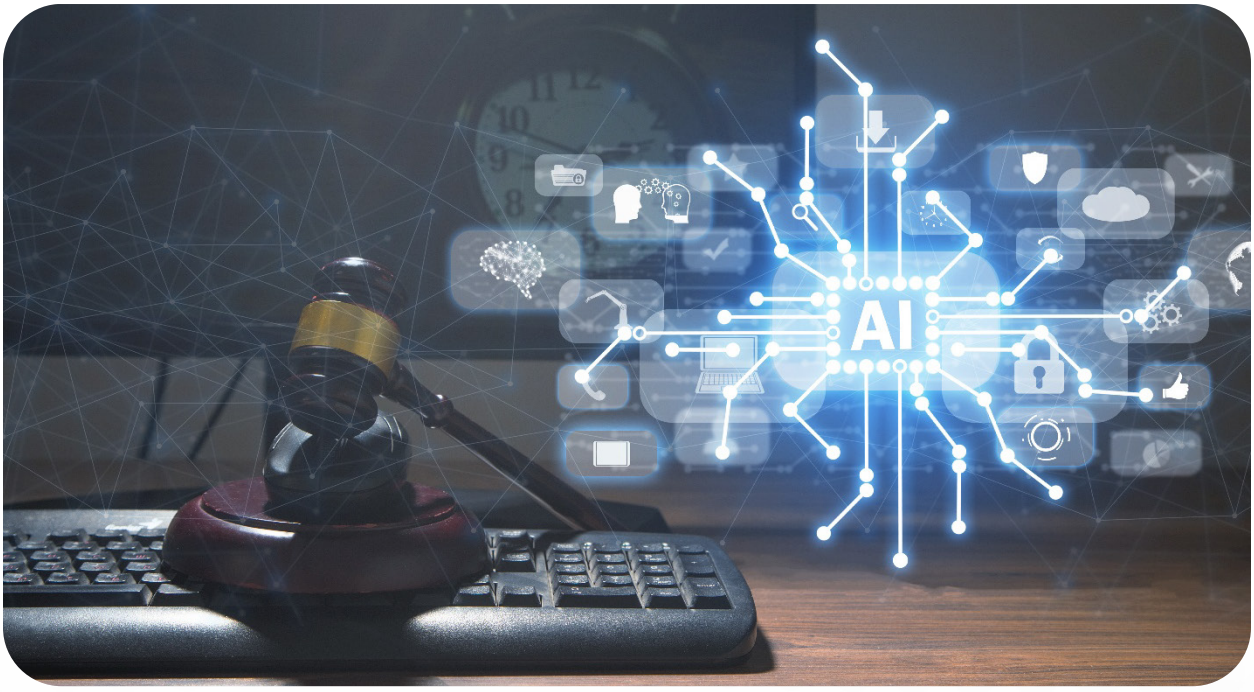
- Moving into Cyber GRC
- Getting certified (CRISC, CISA, CISM, Security+)
- Learning AI in a way that actually makes sense

Then maybe this is your sign to look a little closer. Because the people inside? They started exactly where you are.

And now... they're moving forward.

CHAPTER 8:
TOOL OF THE MONTH

VANTA – AUTOMATING COMPLIANCE, UNLOCKING SPEED



Speed, trust, and compliance define business success, one tool continues to stand out for modern Cyber GRC teams: **Vanta.**

Designed to simplify and automate compliance processes, Vanta is helping organizations move from **manual, time-consuming audits** to **continuous, real-time assurance**.

WHAT IS VANTA?

Vanta is a **compliance automation platform** that helps organizations achieve and maintain certifications like:

- SOC 2
- ISO 27001
- HIPAA
- GDPR

It connects directly to your systems and continuously monitors your controls, eliminating the need for scattered spreadsheets and last-minute audit scrambles.

WHY IT STANDS OUT

What makes Vanta particularly powerful is its ability to **automate the heavy lifting** of compliance.

Key capabilities include:

- **Automated evidence collection**
- **Real-time control monitoring**
- **Pre-built compliance frameworks**
- **Audit readiness dashboards**
- **Integrations with cloud providers and SaaS tools**

Instead of chasing documents, teams can focus on **understanding and managing risk**.

WHAT THIS MEANS FOR GRC PROFESSIONALS

For Cyber GRC professionals, tools like Vanta are changing the game:

- No more last-minute audit panic
- Reduced manual documentation work
- Increased visibility into control effectiveness
- Faster path to certifications

This shifts your role from **process-heavy → insight-driven**.

Vanta plays a critical role in:

- **Continuous Compliance** initiatives
- **Continuous Control Monitoring (CCM)**
- **Startup and scale-up environments** needing fast certification
- Organizations looking to build **trust with customers and regulators**

It's especially valuable for teams that need to **move fast without compromising security**.

While Vanta is powerful, it's not a "set it and forget it" solution.

- Tools don't replace **understanding of controls**
- Misconfigurations can lead to false confidence
- Human oversight is still critical

The real value comes when **tools + expertise** work together.

WHY DOES THIS TOOL MATTERS NOW?

As compliance expectations evolve, organizations can no longer rely on:

Manual tracking
Static reports
Periodic checks

They need:

Real-time visibility
Automated workflows
Continuous assurance

That's exactly what Vanta delivers.

THE BOTTOM LINE

Compliance is becoming faster, smarter, and more automated and tools like Vanta are leading that transformation.

But here's the real insight: The most valuable professionals are not those who just *use tools*... but those who understand **how to leverage them to drive real business impact**.

CHAPTER 9:
COMMUNITY HIGHLIGHTS

COMMUNITY SPOTLIGHT: CLINT IHEME

In this edition of our Skillweed Alumni Spotlight, we're featuring **Clint Iheme**, whose journey into Cyber GRC reflects exactly what's possible when clarity meets the right environment.

Q: Tell us a bit about yourself. What were you doing before joining Skillweed?

Clint: I came from a GovCloud Engineering role, but I knew I wanted something more aligned with where the industry was going.

Q: What made you start considering cybersecurity or GRC?

Clint: I realized that every industry needs people who can protect data and manage risk, so the demand wasn't going anywhere. GRC stood out because it's where tech meets strategy, and that felt like a career with real staying power. It's not optional anymore,it's essential.

Q: What was your biggest fear before starting?

Clint: I was worried about investing time and energy into something and not seeing results. That hesitation was real.

Q: Did you try learning on your own before Skillweed?

Clint: Yeah, I watched a few YouTube videos but it felt random and scattered. There was no clear path, so I never really got anywhere with it.

Q: How would you describe your first week in the Skillweed community?

Clint: It was a bit overwhelming at first, but everyone on the team was welcoming and engaging. The whole energy felt superb, and you could tell people actually wanted to see each other learn and win.

Q: What surprised you the most about the learning experience?

Clint: Everything was pure hands on with a real life scenarios from top fortune 10 companies, as though you were actually doing the work, and not just reading through slides. The Kahoot games was spot on.

Q: If you had to describe Skillweed in three words?

Clint: Structured. Supportive. Real exposure.

Q: What made the classes different from other programs?

Clint: The instructors didn't just teach, they broke things down in a way that actually made sense and made sure nobody got left behind. They made sure everyone participated.

Q: How did the community support impact your journey?

Clint: It made a huge difference. Whenever I got stuck on something, I could just drop a question on the chat and someone would help almost immediately. Everyone was active, engaged, and ready to help, including the instructors, which made learning feel less lonely. Everyone treated it like a workplace chat, which was fun.

Q: How did Skillweed simplify complex topics for you?

They use real world examples instead of textbook lingo. Once you can picture it in a real scenario, it just clicks

Q: What was your favorite moment during the program?

Clint: Seeing how the program builds your confidence from almost zero to a point where you can actually hold your own.

Q: How did the structure (live sessions, recordings, practice) help you?

Clint: The live sessions kept me accountable, and reviewing recordings helped reinforce everything. It made learning stick.

Q: What study habits helped you succeed?

Clint: I started reviewing recordings the same day and staying consistent. That made a big difference.

Q: What has changed for you since completing the program?

Clint: My mindset completely changed. I went from feeling lost to having clarity and direction.

Q: Did this experience impact your confidence?

Clint: Definitely. I can now hold real conversations about GRC confidently.

Q: Have you earned any certifications since joining?

Clint: Yes, I've completed CompTIA Security+ and a few others.

Q: How has Skillweed influenced your career direction?

Clint: I now have a clear path and the skills to pursue opportunities in GRC.

Q: What's one thing people wouldn't expect about Skillweed?

Clint: How much fun it actually is. You forget you're even learning sometimes.

Q: Did you ever feel like giving up?

Clint: Not at all. The team spirit keeps you going.

Q: What made the journey enjoyable?

Clint: The people. Learning alongside others from different backgrounds was powerful.

Q: Who was that one person (mentor/student) that made your experience better?

The instructors genuinely cared about every single person's progress.

Q: Who would you recommend Skillweed to?

Clint: Anyone who is serious about getting into cybersecurity or GRC.

Q: What would you say to someone thinking of joining?

Clint: Stop overthinking it and just sign up. You'll thank yourself later.

Q: If you could go back, would you still choose Skillweed?

Clint: Without a doubt. I'd do it all over again.

Q: What are you currently working on?

Clint: I'm focused on building my career in GRC and preparing for my CISA certification.

Q: Where can people connect with you?

Clint: LinkedIn

Q: Final advice for beginners in Cyber GRC?

Clint: Start before you feel ready. You will never know everything before you begin and that's okay.

Clint's journey is a reminder that clarity, structure, and the right community can completely transform your path in tech.

CHAPTER 10:
OPPORTUNITIES & NEXT STEPS

TURNING KNOWLEDGE INTO ACTION — YOUR PATH FORWARD STARTS HERE

You've explored the trends. You understand the shifts. Now comes the most important question:

WHAT ARE YOU GOING TO DO WITH THIS KNOWLEDGE?

At Skillweed, learning doesn't end with insight, it moves into **structured action, real opportunities, and measurable outcomes**.

UPCOMING PROGRAMS: LEARN WHAT THE MARKET DEMANDS

Skillweed is doubling down on what truly moves careers forward — **certifications and real-world, job-relevant skills.**

CERTIFICATION-FOCUSED PROGRAMS

- **CRISC (Risk & Control)**
- **CISA (Audit & Assurance)**
- **CISM (Security Management)**
- **CompTIA Security+ (Foundational Security)**

These programs are:

- **Exam-focused** (past questions heavy)
- **Structured for busy professionals**
- Delivered via **live classes + on-demand access**

The goal is simple: **Not just to learn but to pass and apply.**

The CRISC On-demand and live classes are **open for registration**. Visit www.skillweed.com to register.

INTERNSHIP PATHWAYS: FROM LEARNING TO DOING

Knowledge alone is no longer enough. Employers are looking for **proof of application**.

That's why Skillweed is introducing **hands-on internship pathways**, including:

- **AI Governance Internship (Live Use Cases)**
- Practical exposure using **real frameworks and scenarios**
- Collaborative learning with peers
- Opportunity to build **portfolio-ready experience**

This bridges the gap between: **"I've learned it" → "I've done it"**

CERTIFICATION ENROLLMENT: YOUR FAST-TRACK ADVANTAGE

If you're serious about breaking into or advancing in Cyber GRC, certifications are no longer optional, they are **signals of credibility**.

WHY SKILLWEED'S APPROACH WORKS:

- **95% success rate** across programs
- Focus on **what actually appears in exams**
- Simplified breakdown of complex domains
- Community-driven accountability (you don't do it alone)

AVAILABLE OPTIONS:

- **On-Demand Classes** → Learn at your pace
- **Live Classes** → Structured, guided, and interactive

A great place to start is CRISC certification. Both the On-demand and live prep classes are **open for registration**. Visit www.skillweed.com to register.

Best of both worlds — flexibility + support.

MORE THAN A PROGRAM — A GLOBAL COMMUNITY

Skillweed isn't just a place to learn. It's a **career ecosystem**.

- Students across **US, UK, Canada, Africa, Australia**
- Active communities (WhatsApp, live sessions, peer groups)
- Continuous support beyond the classroom

This is where:

- Beginners become professionals
- Learners become certified
- Individuals become part of something bigger

YOUR NEXT MOVE

You have three clear paths in front of you:

1. **Stay where you are**
2. Keep learning without direction
3. **Take structured action with Skillweed**

Only one of these leads to real outcomes. You can start by binge watching our past Free AI Internship. Visit academy.skillweed.com/courses/free-AI-internship to register.

THE BOTTOM LINE

Opportunities don't just appear, they are created through **intentional learning and execution**.

Skillweed gives you:

- The **knowledge**
- The **structure**
- The **community**
- And the **pathway**

All that's left... is your decision.

START WHERE IT MATTERS MOST

Join a program. Enter an internship. Get certified.

Because the difference between *wanting a tech career* and *having one* is **taking the next step.**

CHAPTER 11:
LANDZILLE —
INVESTING IN LAND, INVESTING IN PEOPLE

How a bold vision for educated land investment is reshaping the landscape of long-term wealth building in America one parcel at a time.

In an industry often clouded by opacity, high-pressure sales, and confusing fine print, Landzille arrived with a different proposition:***what if land investment could be transparent, educational, and genuinely empowering for the everyday investor?***

Landzille did not emerge in a vacuum. It was born from the ecosystem of **SKILLWEED**, a company already committed to building enterprises that solve real problems for real people. Within that culture of purposeful innovation, a gap became impossible to ignore: the land investment market was inaccessible to most people, not because of money alone, but because of knowledge. Everyday investors that were hardworking, ambitious, and financially motivated were being left out. Not because they lacked the desire to invest in land, but because the information, the guidance, and the trust simply weren't there. **Landzille was the answer.**

From day one, the mission has been clear; to demystify land investment, walk alongside every client through the process and ensure that no one ever feels alone in one of the most significant financial decisions of their life.

The Landzille experience includes:

- Deep-dive consultations to understand each investor's goals, timeline, and risk appetite
- Step-by-step education on land valuation, zoning, due diligence, and long-term appreciation
- Transparent walkthroughs of every parcel's potential, with no hidden details
- Ongoing support post-purchase, because the relationship doesn't end at signing

It is a model built on trust and trust, in the land investment world, is everything.

In a crowded market, Landzille's edge is not accidental, it is architectural. Here are the five models that set us apart from conventional land investing:

01	Ag Exemption Filing: We file Agricultural Exemptions on your behalf, legally reducing your property tax from day one.
02	Legacy Nutrient Deduction Service: We assess your land's soil nutrient profile and unlock tax deductions most investors never knew existed.
03	Farmer Leasing for Passive Income: You own the land. Farmers need it. We connect both. You earn regular lease income while your land sits, appreciates, and works.
04	Land as Collateral: Your land has financial weight. Use it to access funding for a business, development, or your next investment without selling a single square foot. This is how real wealth compounds.
05	ROI in High-Growth Corridors: We identify land where growth is already happening, infrastructure, expanding cities, development zones. By the time you're ready to sell or build, your land could be worth multiples of what you paid.

Roxton is one of Texas's most compelling land investment pockets today. Located in Lamar County, it's benefiting from infrastructure growth, rising rural demand, and population shifts. Landzille identified it early through data offering 13+ acre parcels selected for long-term value, with full transparency before you invest. ***Secure your spot early;reach out now to explore available parcels..***

Landzille's commitment goes beyond land;we invest in people. **Our Annual Summer Internship Program** equips high schoolers with real-world knowledge in land investment, financial literacy, entrepreneurship, and community impact, giving them a head start most adults never get.

Cybersecurity, at its core, is about protecting what matters most; assets, trust, and the systems people rely on. Landzille, in its own way, operates on the same principles. It protects investors from the risks of uninformed decisions. It safeguards trust through transparency. And it builds systems of education, community, and investment that people can rely on for the long term.

From Roxton, Texas to The Leonard Project, from its first investor conversation to its thousandth, Landzille is writing a story about what responsible, human-centered land investment looks like; one parcel, one investor, one community at a time.

The land has always been there. Landzille is simply making sure the right people have access to it.

CONNECT WITH LANDZILLE

www.landzille.com | +1 (214) 649-8495

Roxton project | The Leonard project | Summer Internship Program


SkillWeed