CYBERSECURITY READINESS PODCAST SERIES Episode 107

Compliant but Exposed: Rethinking GRC for Real Security
with Richa Kaul, Founder and CEO, Complyance

Host	Dr. Dave Chatterjee, Duke University
Guest	Richa Kaul, Founder and Chief Executive Officer, Complyance
Topic Focus	Intelligent GRC Automation and the Compliance-Security Gap
Podcast Portal	https://www.cybersecurityreadinesspodcast.com/

Summary

In Episode 107 of the Cybersecurity Readiness Podcast Series, Dr. Dave Chatterjee is joined by Richa Kaul — Founder and Chief Executive Officer of Complyance and a former public sector technology policy leader — to address one of the most consequential misunderstandings in enterprise security governance: the assumption that compliance equals security.

Opening with two recent and high-profile incidents — the May 2025 ransomware attack on Marks & Spencer, which halted online operations for weeks and generated estimated losses exceeding £300 million, and a concurrent third-party support provider compromise that exposed customer data across multiple platforms including Discord — Dr. Chatterjee establishes the episode's central premise: organizations that invest heavily in GRC platforms, generate dashboards full of green indicators, and maintain formal compliance certifications can still be catastrophically breached. The gap between being compliant and being secure is not theoretical. It is structural, and it is where attackers operate.

Kaul explains the root cause with precision. Traditional GRC tools were built to centralize data and automate workflow notifications — functions that reduce administrative burden but do not reduce risk. The result is a compliance theater dynamic in which organizations check boxes, pass periodic audits, and receive certifications that say little about their actual security posture. The Complyance platform is built on a different philosophy: compliance with standards should be a byproduct of genuinely good security practices, not the objective in its own right.

The episode explores the architecture of intelligent GRC: continuous monitoring across all integrated source-of-truth systems, agentic AI that automates evidence collection and remediation guidance, tiered third-party risk programs that apply scrutiny proportional to vendor criticality, and risk quantification frameworks that translate security signals into board-level governance decisions. Kaul is equally precise about what GRC platforms cannot do: they cannot substitute for operational security teams, and no platform — however sophisticated — can protect an organization whose leadership has not committed to genuine risk reduction as the governing objective.

Analyzed through Dr. Chatterjee's Commitment–Preparedness–Discipline (CPD) framework, the conversation reframes GRC from a compliance function into a governance discipline. The episode's central message is neither technical nor vendor-specific: the organizations that will withstand the next breach are not those with the most compliance certifications — they are those that have claimed ownership of the problem, built the continuous processes to address it, and institutionalized the discipline to keep those processes operating after the audit is over.

Discussion Highlights

The Opening Incidents: When Compliance Fails in Practice

Dr. Chatterjee opens with two concurrent third-party-originating breaches that illustrate the compliance-security gap at operational scale. In May 2025, Marks & Spencer — one of the United Kingdom's most iconic retailers — suffered a cyber attack that brought its online operations to a halt for weeks. Customers could not place orders. Gift cards stopped working. New hire onboarding was suspended. Estimated losses surpassed £300 million. The

attackers' entry point was a contractor — a third party with legitimate, vetted access — whose credentials were socially engineered. No dashboard had flagged the exposure.

At roughly the same time, a compromise of a third-party support provider gave attackers access to customer data across multiple platforms, including Discord. The breach did not originate inside the primary organizations. It arrived through vendor relationships that were on file, vetted at onboarding, and largely unsupervised thereafter. Both organizations were, by formal compliance measures, in order.

> *"These are not edge cases — they are illustrations of a pattern. Organizations investing heavily in GRC platforms, building out compliance programs, generating dashboards full of green indicators, and still facing catastrophic breaches that those tools never saw coming. The gap between being compliant and being secure is not abstract. It is where attackers live."*
>
> **— Dr. Dave Chatterjee**

What GRC Platforms Were Built to Do — and Why That Is Not Enough

Kaul identifies the structural limitation of legacy GRC platforms with directness: at minimum, they were glorified data repositories — centralized storage for compliance documentation. At best, they automated parts of existing workflows — sending notifications to evidence owners, accelerating audit preparation. Neither function reduces risk. The gap between "centralizing data" and "reducing risk" is precisely where Complyance is built to operate.

The next generation of GRC, as Kaul describes it, does the manual work on behalf of the security team — with appropriate guardrails — so that the GRC team's time is freed for the strategic, human-judgment-intensive work of genuine risk reduction. This is, she notes, the work that GRC teams want to do but consistently cannot, because they are perpetually consumed by chasing the next audit, the next policy approval cycle, the next evidence request.

> *"The whole idea of Complyance is to get to the reasons behind compliance — the why behind compliance — and to help enterprises automate the busy work and the admin manual tasks, and really focus on risk reduction, which is the core of what every GRC team really cares about: protecting the business."*
>
> **— Richa Kaul, Founder and CEO, Complyance**

The Audit Paradox: Does Compliance Assure Security?

Dr. Chatterjee poses the question directly: if an organization has passed its audits, isn't it reasonable to assume a baseline level of security readiness? Kaul's answer is segmented and unsparing. For large enterprises with stringent auditors, deep subject matter expertise, and mature security teams, compliance and security posture are more likely to be correlated — not because the frameworks guarantee security, but because the organizational infrastructure that produces genuine compliance tends to produce genuine security practice as well.

For startups and smaller organizations, the correlation largely breaks down. Cheaper auditors, less stringent checks, limited in-house expertise, and higher risk tolerance create conditions in which compliance certifications can be obtained without substantive security improvement. Kaul's framing is precise: the smaller the company, the less compliance even assures a baseline level of security.

The deeper problem, as Dr. Chatterjee notes, is temporal: audits are point-in-time assessments of point-in-time samples. Even the most rigorous annual audit does not assess continuous security posture. In an AI-enabled threat environment where attack vectors evolve daily, a clean audit report from three months ago provides no assurance about today.

> *"When we're doing audits, it's not even like you're doing a complete assessment at that point in time — you're doing a fraction of the assessment that you technically should be doing to see visibility across your organization. Once a year checking the anti-malware settings of 10 of your devices across 500 employees is not giving you the picture that you actually need."*
>
> **— Richa Kaul, Founder and CEO, Complyance**

The Green Dashboard Problem: Why Good GRC Should Surface Risk, Not Hide It

Dr. Chatterjee asks the question that challenges the fundamental value proposition of most GRC platforms: when the dashboard shows green, is that a sign of security — or a sign of insufficient monitoring? Kaul's answer is categorical. A perpetually green GRC dashboard is a governance warning sign, not a success indicator. Real organizations face real risk. If the platform never flags anything at orange or red, one of two things is true: the monitoring coverage is insufficient, or the risk thresholds are set so low as to be meaningless.

The paradigm shift Kaul describes is from reactive risk response — managing risk after it materializes or after an audit forces a review — to proactive risk reduction, in which continuous monitoring automatically surfaces potential risk, and the GRC team's entire workday is structured around addressing those outputs before they become incidents.

> *"I hope you're never looking at a green dashboard, because it's almost always going to be nonsense if that's what you're really seeing. That's not realistic for any business today."*
>
> **— Richa Kaul, Founder and CEO, Complyance**

GRC as Architecture: Cameras, Locks, and Lines of Sight

Kaul draws a precise boundary between the GRC function and the broader security function — a distinction that prevents both overestimation and underestimation of what GRC can accomplish. The security team is larger than the GRC motion. It operationalizes the controls that GRC monitors: vulnerability management, threat intelligence, identity and access management, endpoint protection. These are the locks on the doors, the safe walkways, the physical security of the enterprise.

The GRC team's role, if done well, is to maintain line of sight across the entire risk profile of the business — the cameras watching the house. A well-functioning GRC platform integrates signals from all source-of-truth systems, establishes risk thresholds, and automatically flags when any control breaks threshold. The board-level value is not technical; it is decisional: where do we put money, where do we focus time, where does the risk actually lie?

> *"Your GRC should be the cameras watching the house — that roof over the security and compliance risk architecture across the organization that says: I need to have eyes on everything, I need to be making good decisions about where we put our money, about where we focus our time, all based on where the risk really lies."*
>
> **— Richa Kaul, Founder and CEO, Complyance**

Third-Party Risk: The Hardest GRC Problem

Kaul identifies three sources of risk that a genuine GRC program must have visibility across: control gaps within the organization's own systems and practices; third-party vendor relationships; and risks raised from within the business itself — a category that requires training and organizational culture to produce reliable signal. Of these three, third-party risk is the hardest, because so much is outside the organization's direct control, and because trust is inherent to the vendor relationship.

Kaul's recommended approach is tiered and AI-enabled. Tier 1 vendors — those with access to customer PII, employee PII, or critical business infrastructure — must be treated as extensions of the organization itself. Every data interaction point must be traced and assessed. Every gap must be closed before or during onboarding. Tier 2 and Tier 3 vendors receive proportionally less rigorous scrutiny. Tier 4 vendors with access only to public information require essentially none.

For large organizations managing hundreds of vendor relationships, this tiered approach is what makes third-party risk management tractable. AI is not optional; it is the only mechanism that allows questionnaire distribution, evidence review, and continuous vendor monitoring to operate at the scale that modern supply chains require.

> *"When you're onboarding third parties, there's an entire third-party security review process and workflow that should be happening — with all potential risks identified and closed out based on the criticality of the vendor. For Tier 1 vendors, the process has to be really tight, because you should see it as an extension of your own business."*
>
> **— Richa Kaul, Founder and CEO, Complyance**

The CPD Framework Applied to GRC Governance

Dr. Chatterjee applies the Commitment–Preparedness–Discipline (CPD) framework to GRC governance, observing that as Kaul described the conditions for genuine GRC effectiveness, each CPD pillar came alive in turn:

CPD PILLAR	APPLICATION TO GRC GOVERNANCE
COMMITMENT	GRC excellence begins with senior leadership claiming explicit ownership of security governance — not just compliance. Commitment means treating GRC not as an audit-prep exercise but as a continuous risk reduction mission. It requires a named leader who ensures the platform is configured to the organization's actual risk profile, not a generic framework checklist, and who holds the function accountable for genuine security improvement rather than dashboard optics.
PREPAREDNESS	Preparedness in GRC means having the operational infrastructure to identify, monitor, and respond to risk before it materializes into a breach. This includes integrating all source-of-truth systems into a single pane of glass, establishing continuous monitoring controls (not point-in-time sampling), conducting tiered vendor risk assessments with particular rigor for Tier 1 vendors, and building agentic AI workflows that surface risk signals automatically — freeing the GRC team for the strategic work that dashboards alone cannot do.
DISCIPLINE	Discipline is the difference between a GRC program that works on paper and one that actually reduces risk. It means continuously executing the monitoring, remediation, and review processes established under Preparedness — not just in response to audits or incidents. It means periodic access reviews, ongoing vendor monitoring, contextualized employee training, and verifying that the controls in place are producing signal (orange and red alerts) rather than the false comfort of a perpetually green dashboard.

> *"As I'm listening to you, I literally can hear these three pillars of security governance come alive. Commitment — somebody who takes ownership of the effectiveness of this platform. Preparedness — the operational capability to identify, assess, and respond to the different types of risks and threats. Discipline — sustenance, systematic execution that is embedded in and institutionalized within the organizational processes."*
>
> **— Dr. Dave Chatterjee**

How to Evaluate a GRC Platform: Three Non-Negotiables

Kaul closes with a three-point evaluation framework for organizations selecting or renewing a GRC platform investment. First, configurability: a non-configurable platform will shoehorn the organization into the platform's processes, fields, and metadata — the inverse of what genuine risk reduction requires. The platform must be adaptable to the organization's specific risk profile, not the other way around.

Second, agentic AI capability: the shift in GRC is already underway. Organizations that select platforms capable of deploying AI agents to handle evidence collection, control gap remediation, task assignment, and vendor monitoring will free their GRC teams for the strategic risk work that cannot be automated. Organizations that do not will remain trapped in the compliance-theater dynamic.

Third, implementation partnership: software is only as effective as its implementation. Change management — ensuring the platform is actually used, and used well — is consistently overlooked in platform selection processes. A platform that the team does not know how to use provides neither compliance nor security.

> *"Don't let perfect be the enemy of done. Progress is still progress. Working towards a state of true automation and risk visibility brings you so much closer to those things than not doing it — and so*

even if it feels a little idealistic, the realities of organizations can get closer and closer to what we're talking about, with that effort and focus."

— Richa Kaul, Founder and CEO, Complyance

Actionable Recommendations

RECOMMENDATION	DETAIL
Reframe Your GRC Mission Statement	Stop measuring GRC success by audit pass rates. Define success as demonstrated, continuous risk reduction. If your program cannot show that risk levels have declined over time, the program is not working — regardless of compliance status.
Commission a Compliance Gap Assessment	Assess whether your current GRC platform is configured to monitor your organization's actual risk profile, or whether it is merely tracking standard framework requirements. The gap between the two is where most breaches originate.
Tier Your Vendor Risk Program	Identify your Tier 1 vendors — those with access to customer PII, sensitive company data, or critical infrastructure. For those vendors, trace every data interaction point and close gaps with the same rigor you apply to internal systems. Compliance questionnaires alone are insufficient.
Demand Continuous Monitoring, Not Periodic Sampling	Replace point-in-time audit sampling with continuous, integrated monitoring across all source-of-truth systems. A single pane of glass across controls is only valuable if the signals it surfaces are continuous, not quarterly.
Evaluate Platforms for Configurability and Agentic AI	When selecting or renewing a GRC platform, prioritize configurability over pre-built frameworks. The platform must reflect your organization's specific risk profile, not a generic SOC 2 or ISO 27001 template. Evaluate whether agentic AI capabilities free your team for strategic risk work.
Invest in the Implementation Partnership	Software is only as effective as its implementation. Allocate resources for change management and implementation support. A well-implemented platform with moderate features outperforms a feature-rich platform that the team does not know how to use.
Expect Orange and Red on Your Dashboard	A perpetually green GRC dashboard is a governance warning sign, not a success indicator. Real organizations face real risk. If your platform never flags anything, either the monitoring is insufficient or the thresholds are set too low to be meaningful.
For Boards: Request a Risk Trend Report	Board members should ask for trend data: Is the number of unresolved high-priority risks going up or down quarter over quarter? This is a governance signal that does not require technical expertise to interpret and cannot be gamed by compliance status alone.

Time Stamps

TIME	CONTENT
0:00	Opening scenario — the May 2025 Marks & Spencer cyber attack and the Discord third-party breach
0:49	Host framing: the compliance-security gap — where attackers live
3:47	Richa Kaul welcome and introduction

4:16	Guest career journey — from public sector regulation (Commonwealth of Virginia) to Chief Strategy Officer at an AI company to founding Complyance
6:04	The founding motivation: GRC is suboptimal — it creates work, not insight
6:40	What is missing in existing GRC platforms: the evolution from data repository to intelligent agent
8:24	The compliance-first framing challenged: compliance with a why
9:01	The 100+ frameworks Complyance supports — and why framework coverage is not the starting point
10:33	The audit paradox: passing audits as a baseline for security readiness — myth or reality?
11:20	Segment-based answer: enterprises vs. startups and the differential assurance value of compliance
12:18	Point-in-time auditing and the continuous monitoring imperative
13:36	Why a perpetually green dashboard is a governance warning, not a success indicator
14:49	Single pane of glass: integrating all source-of-truth systems into the GRC platform
17:48	The paradigm shift: from reactive risk response to proactive risk reduction
19:39	GRC as the cameras around the house: line of sight vs. operational security
22:10	Does GRC support remediation? Yes — AI-guided remediation, task assignment, and risk treatment planning
24:39	Audit logging as legal and governance infrastructure — the evidentiary value of GRC records
25:50	Vendor risk as the hardest GRC problem: third-party access, social engineering, and trust boundaries
28:07	Vendor oversight as a continuous obligation: maintaining security parity with client organizations
28:30	When the vendor doesn't have a GRC platform: tiering and criticality-based prioritization
30:42	Using AI to make third-party risk management tractable at scale
31:05	The check-the-box mentality: why organizations settle for compliance theater
33:13	The GRC platform's role in preventing compliance theater: tools vs. enforcement
34:56	Dr. Chatterjee applies the CPD framework — Commitment, Preparedness, Discipline — to GRC governance
37:11	Evaluation criteria for selecting a GRC platform: configurability, agentic AI, and implementation partnership
38:38	Closing takeaways — don't let perfect be the enemy of done; progress is still progress
39:44	Episode wrap-up and listener call to action

Memorable Quotes

"A ransomware attack did not just disrupt a business — it cost one of the world's most recognized retailers over 300 million pounds in estimated losses. The attacker's entry point was not a zero-day exploit. It was a contractor credential. The organization was compliant. That is the gap we are exploring today."

— Dr. Dave Chatterjee

"The way that we're handling GRC today is suboptimal, to put it lightly. It creates a lot of work, it doesn't create a lot of insight. It checks a lot of boxes, it doesn't actually reduce risk."

— Richa Kaul, Founder and CEO, Complyance

"I believe that compliance with certain standards is a happy byproduct of really good security practices — not the other way around. The idea of the platform is not to check the box on the standards, but to centralize your security practices and controls, monitor them, address the risks —

and have the compliance be a happy byproduct of everything that is already working towards the bigger goals."

— Richa Kaul, Founder and CEO, Complyance

"67% of organizations address SAP security reactively. But this GRC dynamic is universal: if your GRC program only moves when an audit fires, your posture at the moment of the next breach is essentially zero. The controls were never running continuously. The signals were never being watched. The discipline was never there."

— Dr. Dave Chatterjee

"The GRC team of the future isn't going to be chasing evidence requests and policy approvals. They're going to be doing strategic risk reduction work — the work that actually matters, the work they always wanted to do — because the agents are doing everything else. That is a wonderful thing to watch."

— Richa Kaul, Founder and CEO, Complyance

"A green dashboard should not automatically mean everything is in order. Organizations must be proactive in threat and risk management — and a well-configured GRC platform will raise red flags if security controls are not being implemented or enforced effectively. The absence of signal is itself a signal worth investigating."

— Dr. Dave Chatterjee