CiO Espresso
Fueling your digital transformation, one sip at a time
#26
2024

TOP 5 POLICY MAKING DECISIONS *for CIOs*

What to consider in establishing a strong, secure and pragmatic program of GRC controls?

(Governance, Risk and Compliance)

Risk Management Framework

An engaged *army is formidable*

Safety *through role clarity*

Define a risk management framework that outlines the risk appetite and tolerance levels, risk assessment methodologies, and risk treatment strategies to prioritise and manage risks effectively.

Bottom line: Organisations commonly fail in one key area: **cultural integration and employee engagement.** Companies with highly engaged employees have 21% higher profitability and 41% lower absenteeism (Gallup). Engaged employees are more likely to be vigilant, adhere to risk management protocols, and contribute to a culture that prioritises governance, risk, and compliance.

Information Security Policies

Human creativity *is never more on display*

Than when *circumventing the rules*

Develop comprehensive information security policies and standards that address areas such as access controls, data encryption, incident response, business continuity, vendor management and industry compliance.

Bottom line: As often cited here, security policies should be tight enough to protect but flexible enough to enable productivity. 83% of employees admit to using non-approved software and tools for work purposes, primarily because the approved tools are too restrictive.

Compliance Management Program

If it's ingrained in what you do, *you'll do it*

Without even knowing— *and do it more often*

Implement a compliance management program to ensure that the organisation adheres to relevant laws, regulations, and industry standards applicable to IT operations.

Bottom line: By embedding compliance into daily workflows, organisations can more effectively anticipate and mitigate risks, creating a culture where compliance is naturally upheld. Those with integrated compliance programs experience 50% fewer compliance breaches compared to others with siloed programs.

> *After 30+ years of experience...*
> CIOs need to make GRC part of their everyday *ingrained* business. Define clear roles, keep a close watch, and build a culture of accountability. As Dolly Parton said "You can't just wing it. You need a plan, and the dedication to stick to it".

Third-party Risk Management

The difference between the *tool shop and the tools*

Is that the tool shop is *where you go to get everything*

Establish policies and procedures for third-party risk management while also conducting due diligence assessments, contractually enforce security requirements, and implement ongoing monitoring and oversight mechanisms to mitigate third-party risks effectively.

Bottom line: The Ponemon Institute cites "58% of companies have experienced a data breach caused by one of their vendors, and 42% of companies have terminated a vendor due to security concerns". Instead of improving their due diligence and monitoring processes, many organisations resort to adding more commercial terms and requirements, which can lead to higher costs without effectively mitigating risks.

Governance and Accountability

Do the check, not tick the box— *when ownership is clear*

It'll probably get done: *quality depends on the check*

Define roles, responsibilities, and accountability structures for GRC within the organisation, including oversight committees, steering groups, and designated risk owners. Establish clear lines of authority, decision-making processes, and escalation procedures to ensure effective governance, transparency, and accountability for GRC actions.

Bottom line: Is your reputation, trust and credibility worth it? Without clearly defined roles and accountabilities, you risk operational inefficiencies, increased vulnerabilities, and regulatory non-compliance, ultimately impacting your organisation's bottom line.

Like to delve into, dissect or draw on my experience over a coffee—let's set up a time... E L