INFORMATION SECURITY CONFERENCE 2025
Future-Proofing Cybersecurity: Next-Gen Strategies

ISC25 .. ... -.-. ..--- .....

BEYOND GRC: How governance of enterprise risk can transform the security and resilience of modern organizations.”

Virginia Information Security (IS) Conference 2025

Future-Proofing Cybersecurity: Next-Gen Strategies

BEYOND GRC

Personal Story

I wasn't born this way.

- I started as a very technical ISDN operator.
- I did not adjust the message for the audience.
- I had no business in the boardroom.

BEYOND GRC

Horror Story

Doing everything "right" does not guarantee that things will not go horribly wrong.

- **Information Security Management System**
- **Cyber Liability Insurance**
- **Threat and Vulnerability Management**
- **Out of Business**

BEYOND GRC

What is GRC supposed to do for me?

According to OECG, “Governance, Risk, and Compliance (GRC) produces “principled performance.””

BEYOND GRC

What do people usually use GRC for?

Used incorrectly, GRC = CRG

- Compliance monitoring (checklists)
- Risk reporting (not risk management)
- Management reporting (tactical, not strategic)

BEYOND GRC

Why bother moving beyond GRC?

Compliance is the weakest risk management driver.

- **Regulator resources are limited.**
- **Most companies suffer consequences only after a problem occurs.**

BEYOND GRC

But . . . governance is part of GRC!

Governance only exists when there is active engagement from executive leadership. Apathy and disengagement from leadership is not governance.

BEYOND GRC

Does governance affect risk psychology?

Risk culture, influenced by governance, determines whether organizations prioritize compliance (pain avoidance) or value generation (pleasure maximization).

BEYOND GRC

How should governance work?

Governance practices that work well in one organization could be disastrous when applied to another organization.

BEYOND GRC

What is governance of enterprise risk?

Risk governance refers to the rules, processes, culture, and guidelines by which decisions about risks are taken and implemented.

BEYOND GRC

How is risk governance done in practice?

Established risk boundaries move people from making "gut" decisions based on feelings to making informed decisions based on data.

BEYOND GRC

Who sets the boundaries for risk?

The board of directors in partnership with the CEO should establish the acceptable risk boundaries for the company.

BEYOND GRC

What are the key risk areas?

Cybersecurity affects key risks but is not a key risk itself.

- Revenue
- Operations
- Regulations
- Reputation
- Safety

BEYOND GRC

Who is ultimately responsible?

The board is responsible for strategy, and the CEO is responsible for execution that creates value. Both roles are responsible for enterprise risk, which cybersecurity influences.

BEYOND GRC

What does everyone else do?

The entire company operates within the risk boundaries established by leadership and provides notice when problems are identified.

BEYOND GRC

How do we confirm risk governance works?

Performance measurement is the best tool to direct resources and adjust strategies to produce desired outcomes.

BEYOND GRC

What if we get risk governance wrong?

The business judgement rule protects boards from liability as long as the duty of loyalty and the duty of care are satisfied.

BEYOND GRC

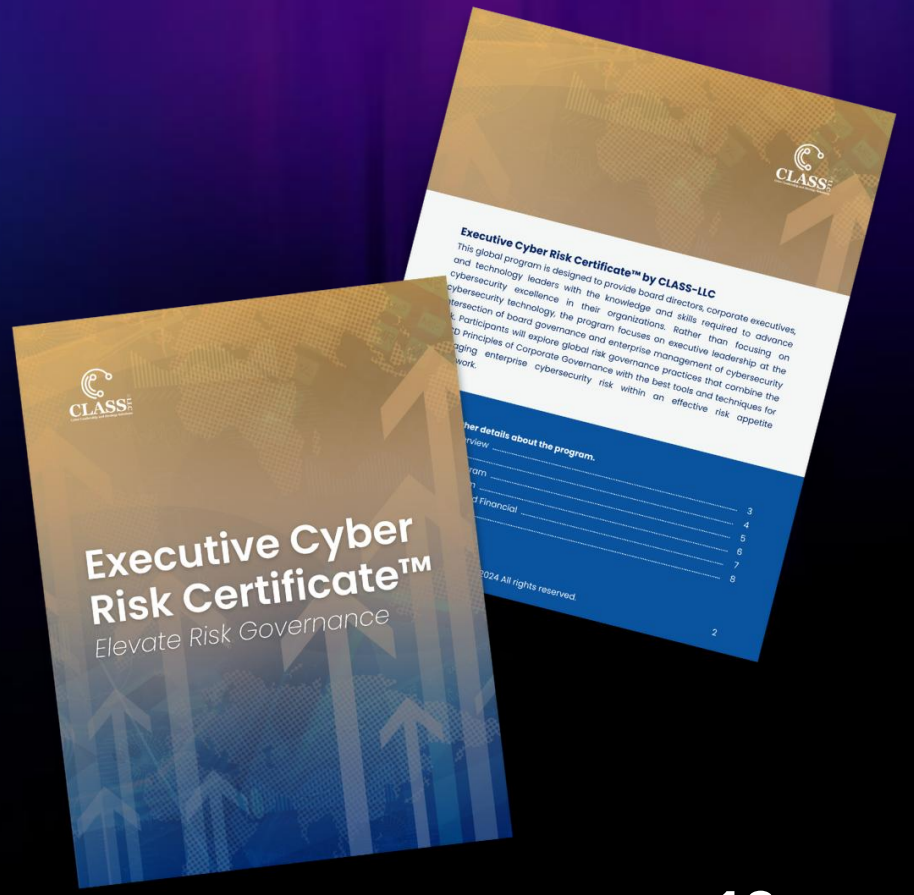
What are the fundamental resources?

- Corporate Governance Matters, 3rd Edition
- Essentials of Risk Management, 3rd Edition
- NIST IR 8286 (Plus Appendix A-D)
- NIST SP 800-221
- ISO 37000

BEYOND GRC

What if I need more help?

- Email ecrc@class-llc.com to learn more about our executive education program.
- Follow or connect with Keyaan Williams on LinkedIn.



BEYOND GRC

Thank you!