Governance, Risk & Compliance

I bet you didn’t even know you loved it!!

Andrew Morgan
Ex-CISO
Future Consultant &
lover of GRC

GR&C

3 minutes for your email and insta before I convince you this stuff is super sexy

Did you know that Governance, Risk & Compliance (GRC) is the super sexy discipline that some of us don’t even know we need.

We love shiny and new technologies, but does the rest of business see the same sparkle?

Cyber is all about managing a risk that can shut down your company if you stuff it up.

Ok – here is the boring bit. If you have to check your email, Insta or Tik Toc – you’ve got about 3 minutes ok!

- GRC plays a pivotal role in the field of cyber security. It provides a framework that enables organisations to effectively manage their IT systems, mitigate risks, and ensure compliance with regulatory standards.
- Without a robust Governance, Risk, and Compliance strategy, organisations are more susceptible to cyber threats, which can lead to significant financial and reputational damage.

GR&C

What are they… blah blah blah

Governance

Blah etc etc….

Governance is the cornerstone of any effective Governance, Risk, and Compliance strategy. It involves establishing policies and procedures that guide the management and use of an organisation's people, processes and technology – not just it's IT systems.

In the context of cyber security, effective governance ensures that people, processes and technology systems are secure and that they align with the organisation's business objectives.

Governance

Blah etc etc….

Governance involves setting up a framework for decision-making. This includes defining strategy and making sure there is alignment with organisational strategy, roles and responsibilities, establishing reporting lines, and setting performance metrics.

By doing so, governance ensures that the organisation’s IT systems are managed in a transparent and accountable manner.

Risk

Blah etc etc….

Risk management is another critical component of GRC. It involves identifying potential threats to an organisation’s people, processes and technology and taking measures to mitigate them.

In the context of cyber security, risk management helps organisations to protect their people, their processes, their data and technology systems from cyber threats.

Risk management involves:

- effective monitoring of the threat landscape
- understanding and implementing processes according to:
  - o organisational risk appetite
  - o in line with the overall enterprise risk management framework
  - o approach to conducting risk assessments
  - o implementing risk mitigation strategies
  - o monitoring the effectiveness of these strategies.

Risk

Blah etc etc....

This Photo by Unknown Author is licensed under CC BY-SA

My personal mantra

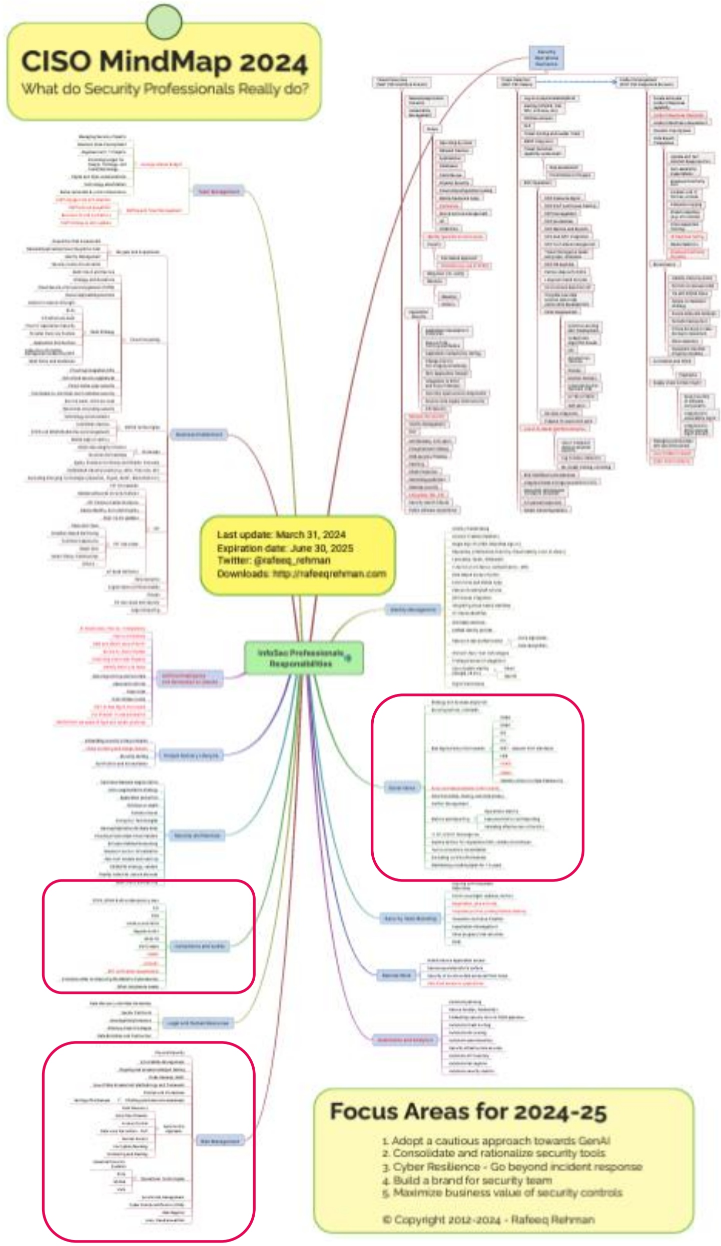
A cyber program is designed to protect the PEOPLE, ASSETS & REPUTATION of the business

I achieve this by building a program that is:

✓ Driven by culture.

✓ Informed by risk &

✓ Delivered through people, process and technology


CISO MindMap 2024
What do Security Professionals Really do?
Last update: March 31, 2024
Expiration date: June 30, 2025
Twitter: @rafeeq_rehman
Downloads: http://rafeeqrehman.com
InfoSec Professionals Responsibilities
Focus Areas for 2024-25
1. Adopt a cautious approach towards GenAI
2. Consolidate and rationalize security tools
3. Cyber Resilience - Go beyond incident response
4. Build a brand for security team
5. Maximize business value of security controls
© Copyright 2012-2024 - Rafeeq Rehman

Rafeek Rahman releases a wonderful document every year called the CISO MindMap (What do Security Professionals Really DO?).

This is the 2024 edition listing a comprehensive listing of key elements of any security program.

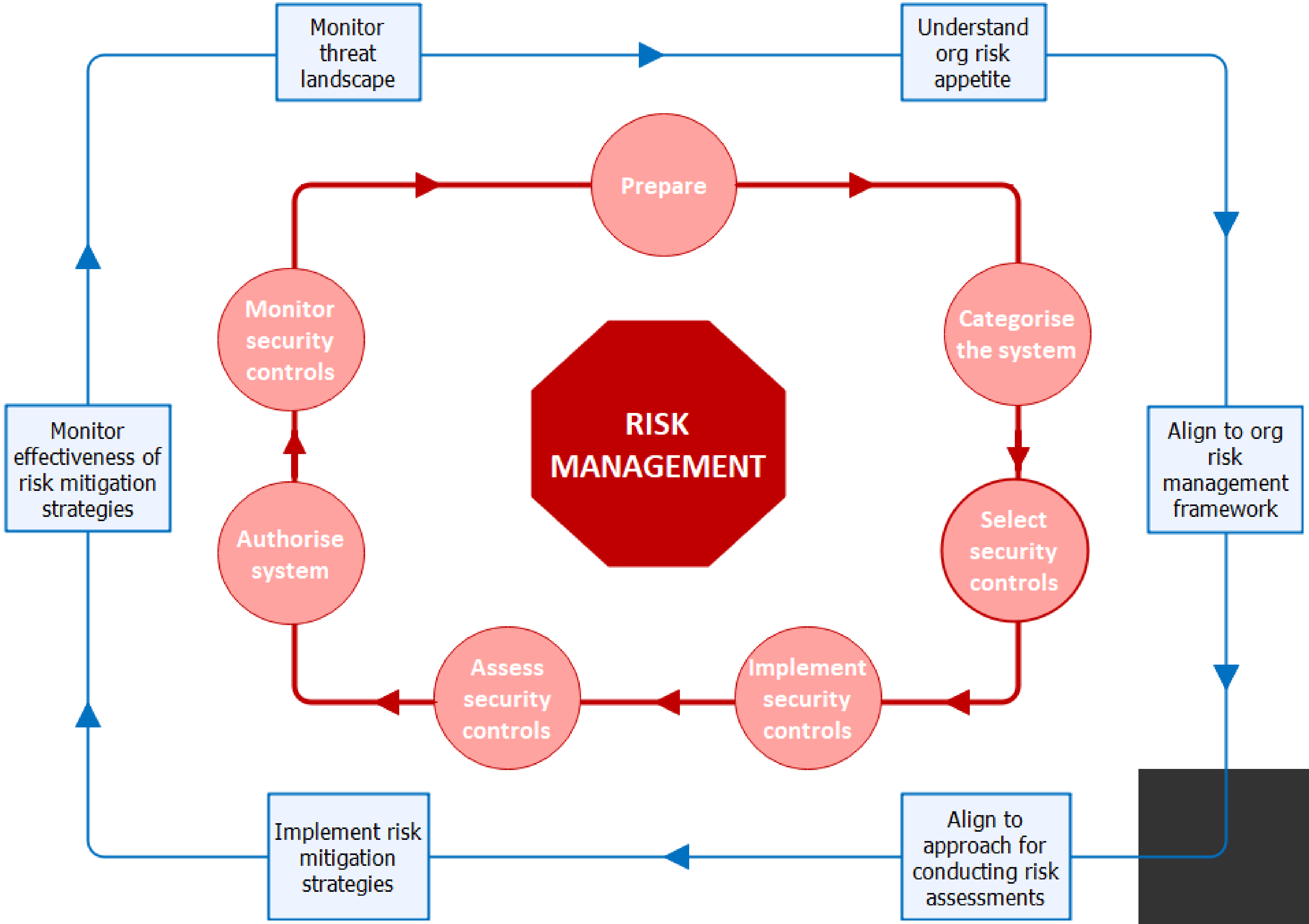
Rafeek suggests that the key elements of focus for 2024 should be:

- Adopt a cautious approach towards GenAI
- Consolidate and rationalize security tools
- Cyber Resilience - Go beyond incident response
- Build a brand for security team
- Maximize business value of security controls

GRC

Why I love it

(and you should too)


Monitor threat landscape
Understand org risk appetite
Align to org risk management framework
Align to approach for conducting risk assessments
Implement risk mitigation strategies
Monitor effectiveness of risk mitigation strategies
Prepare
Categorise the system
Select security controls
Implement security controls
Assess security controls
Authorise system
Monitor security controls
RISK MANAGEMENT

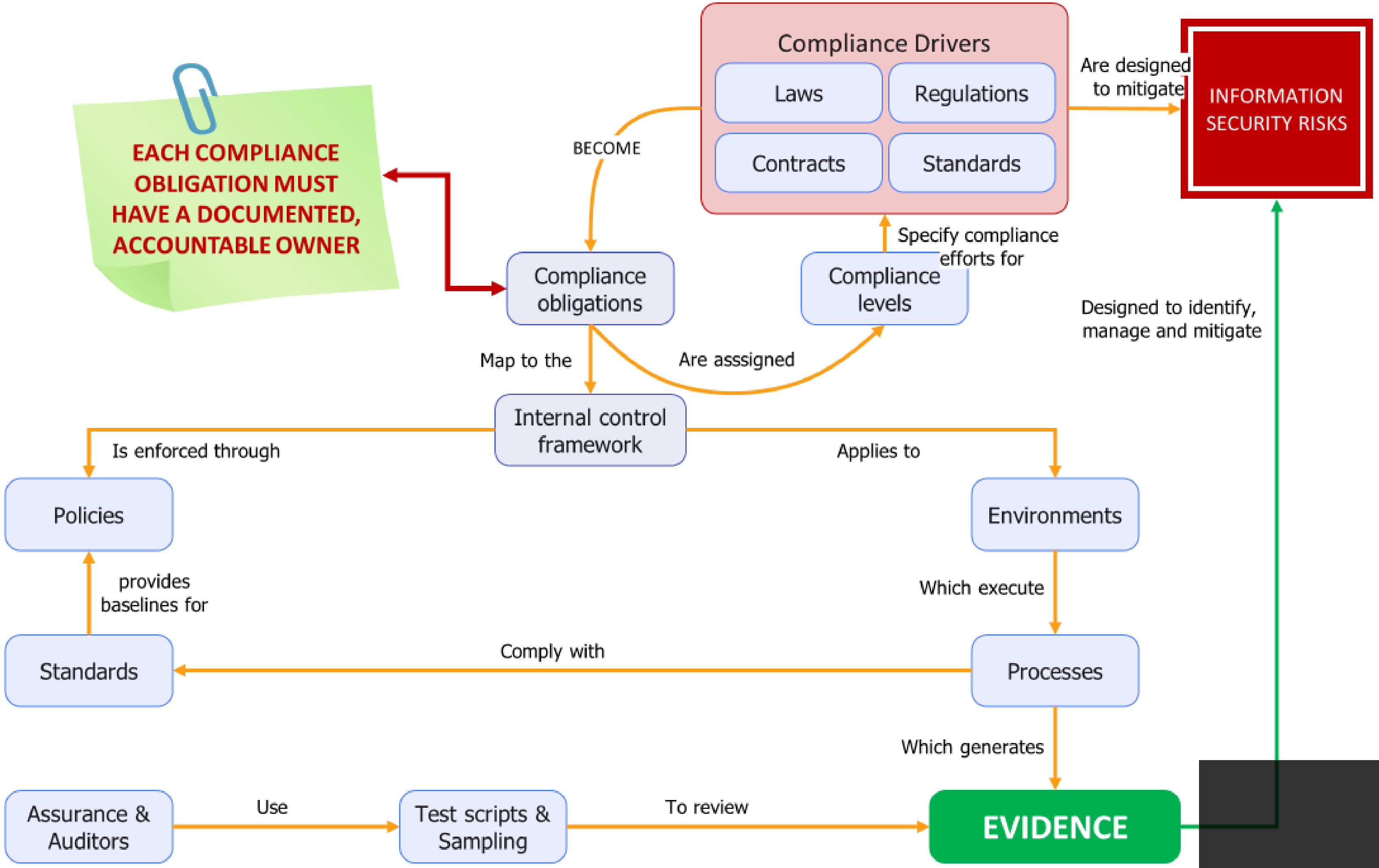
RED = NIST Risk Management Framework

Blue = Andrew Morgan approach to risk management

GRC

Why I love it

(and you should too)



The goal of security compliance management is to ensure a robust security system fit to meet industry standards while aligning with corporate policies, elected security models & frameworks and regulatory mandates.

GRC

Why I love it

(and you should too)

To govern and oversight an information security program and ensure that the program delivers its program of work, I favour a two-tier governance structure in place – an Information Security Governance Council (SGC) and an Information Security Management Committee (SMC).

Scope/ Responsibilities

1. Approve escalated exemptions involving high risks, with escalation to C-suite where appropriate
2. Foster and enhance a positive information security culture across the business
3. Establish long-term information security goals and objectives to continue to enhance the org’s information security capability
4. Monitor the org’s various security GRC strategies and plans, and oversight the management of risk
5. Consider outcomes of security, compliance and risk incidents and investigations
6. Facilitate information sharing for information security improvements
7. Provide information and participate in the prioritisation and co-ordination of information security related projects and funding through a Strategic Review Board
8. Governance of information security programs

Information Security Governance Council (SGC)

The Information Security Governance Council (SGC) is the business led information security and risk governance body responsible for providing oversight of the org’s information security programs. The group provides an integrated approach to managing information security risks and improving business capability and maturity for information security.

1 level below C-suite level membership from different areas within the business will ensure the necessary business focus and accountabilities. The SGC will be the business forum to:

1. Monitor and support the ongoing enhancement of the org’s information security performance and culture
2. Monitor the org’s information security risk profile
3. Assess escalated information security issues from the SMC and other sources
4. Prioritise information security activities, including information security funding; and
5. Informing relevant business stakeholders of key information security initiatives

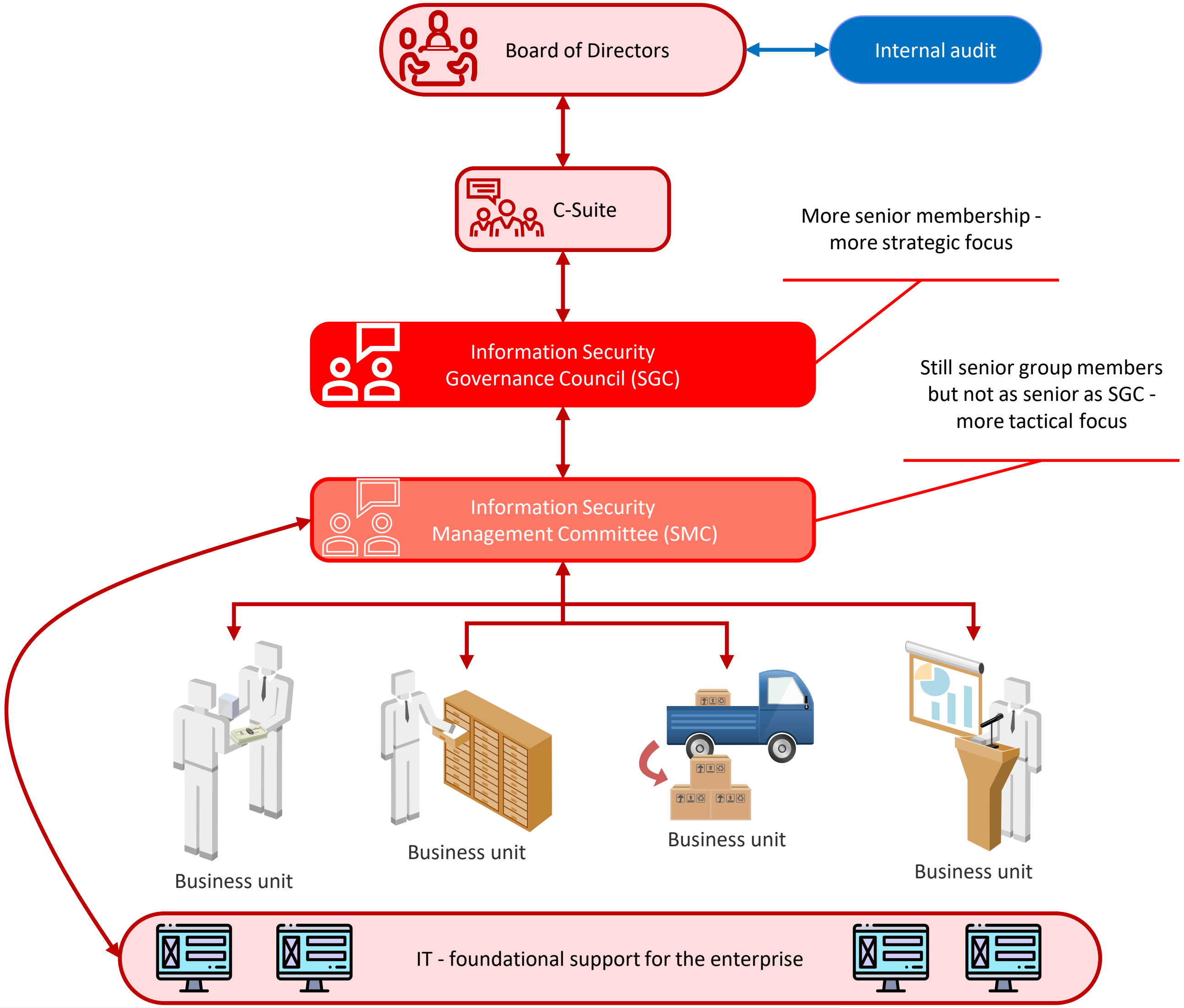
To govern and oversight an information security program and ensure that the program delivers its program of work, I favour a two-tier governance structure in place – an Information Security Governance Council (SGC) and an Information Security Management Committee (SMC).

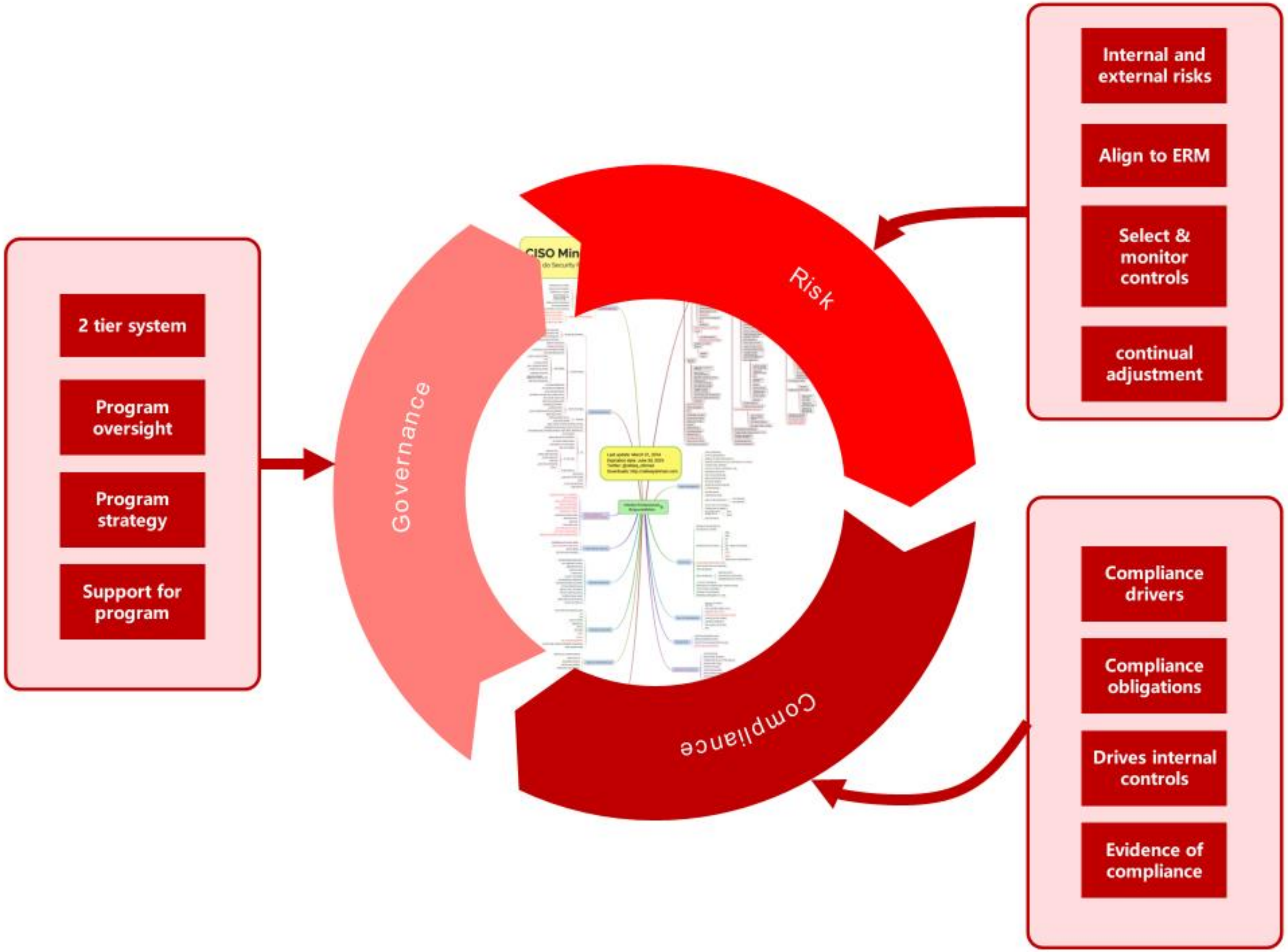
Information Security Managemen t Committee (SMC)

The Information Security Management Committee (SMC) is the governance body for information security risk and compliance activities at the org.

The SMC will:

1. Make decisions on prioritisation of activities and resources to address information security risks at a tactical level to ensure alignment with the information security strategy and regulatory requirements (in conjunction with the impacted lines of business)
2. Assign responsibilities and actions for information security projects and information security risk activities
3. Oversight delivery of the information security program in line with the org's risk appetite for information security and compliance related activity
4. Make determinations and decisions on escalated items from operational teams and lines of business
5. Escalate unresolved items to Information Security Governance Council (SGC)


Board of Directors
Internal audit
C-Suite
More senior membership - more strategic focus
Information Security Governance Council (SGC)
Still senior group members but not as senior as SGC - more tactical focus
Information Security Management Committee (SMC)
Business unit
Business unit
Business unit
Business unit
IT - foundational support for the enterprise



- 2 tier system
- Program oversight
- Program strategy
- Support for program

- Internal and external risks
- Align to ERM
- Select & monitor controls
- continual adjustment

- Compliance drivers
- Compliance obligations
- Drives internal controls
- Evidence of compliance

GRC

Why I love it

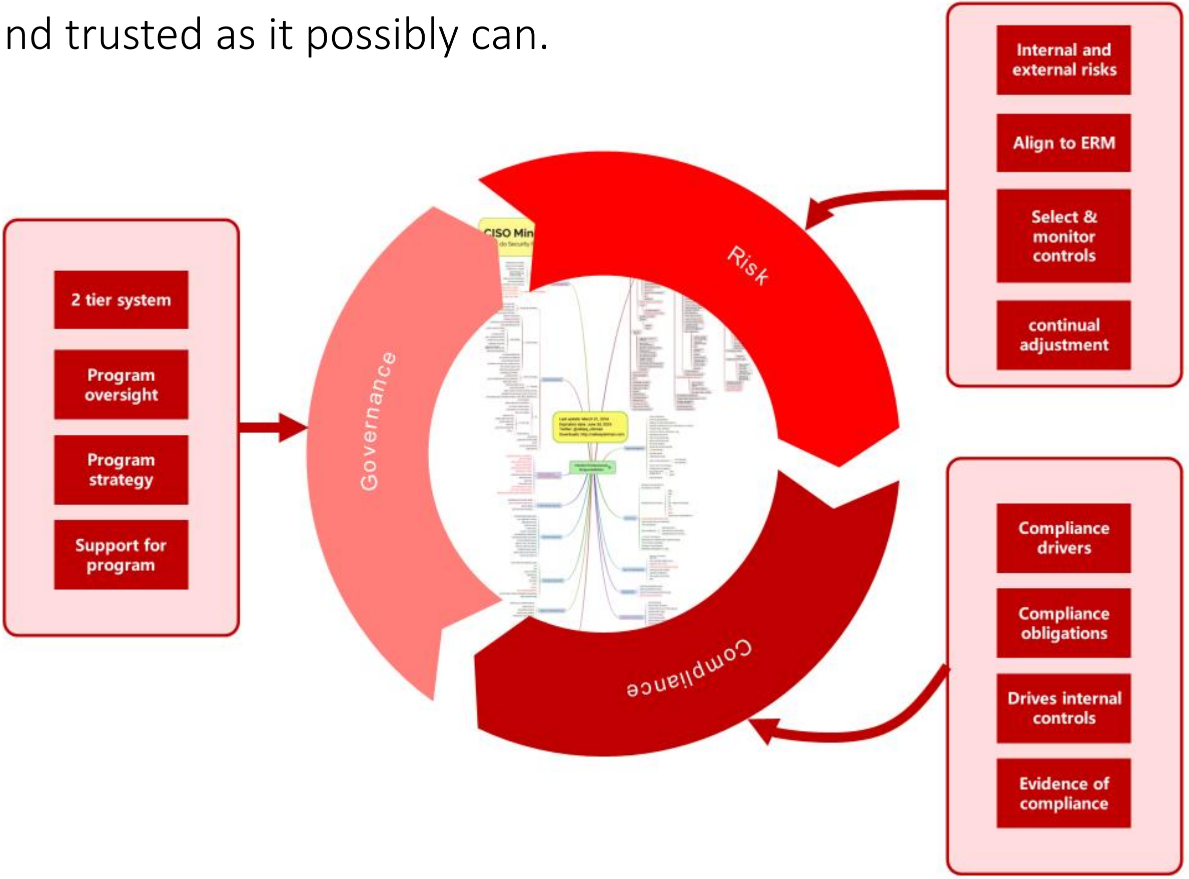
(and you should too)

GRC

Making beautiful butterflies out of small grubs

As we can see – GRC can turn your program into something beautiful that others envy and admire.

Lots of us naturally gravitate to Rafeek's model – doing 'all the things' but in my mind, a well thought out security model lets itself be safe within the cocoon of governance, risk and compliance so that it can emerge as safe, practical, relevant and trusted as it possibly can.


Internal and external risks
Align to ERM
Select & monitor controls
continual adjustment
Risk
2 tier system
Program oversight
Program strategy
Support for program
Governance
Compliance
Compliance drivers
Compliance obligations
Drives internal controls
Evidence of compliance