

Secure Business by Design

Cybersecurity breaches don't happen by accident

Neither do secure businesses



Good cybersecurity is a decision worth making

Business
Risk
Focus

Cyber Risk

Cybersecurity influences every aspect of your business

Understanding how well cybersecurity risk is managed today is an essential business function.

The decision to make your business SECURE BY DESIGN will never be an accident.

We use our in-depth cyber risk assessment experience and understanding to ensure that your business is SECURE BY DESIGN.

Making the right business decisions is never easy, but some decisions are much simpler to make than others.

Good cybersecurity is a decision worth making

Business
Strategy
Focus

Cyber Attack

How will your business manage the impact of an active cyber attack?

Cybersecurity is potentially the most damaging risk that your business faces.

For your business to address cybersecurity properly it needs to be managed to both support and enable business objectives regardless of the impact of an attack.

Many security programs are only created reactively in response to detected breaches or the assumption that what happened to another company can happen to yours.

Our Secure Business by Design model allows you to address what matters most to your business so that you are prepared for any eventuality, and always have effective options regardless of which threat may materialize.

Good cybersecurity is a decision worth making

Cyber-
security
Focus

Cyber Resilience


This must be an active part of your business design.
Resilient business does not happen by accident.

Resilient businesses must answer these questions.


- Is our cybersecurity sufficient for our specific cyber risk posture?
- Can we prove this to our clients, stakeholders and our regulators?
- How fast can we deploy new business systems and remain secure?
- When we are attacked, can we continue to do business?



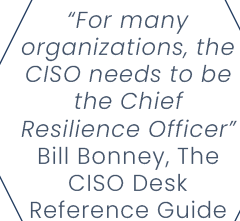
The Model



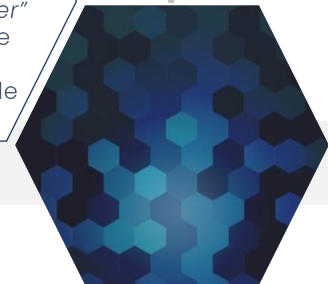
None of these questions are new but answering them today demands a different approach. Traditional responses resulting from post-compromise remediation, or to fulfil compliance requirements rarely reduce business risks as expected. Our Secure Business by Design model allows you to manage cybersecurity risk at the level your business needs to be successful. There are a multitude of superb cybersecurity frameworks available today [e.g., ISO 27000, NIST CSF, CIS v8] all of which contain very well directed and measurable cybersecurity technical and process controls.



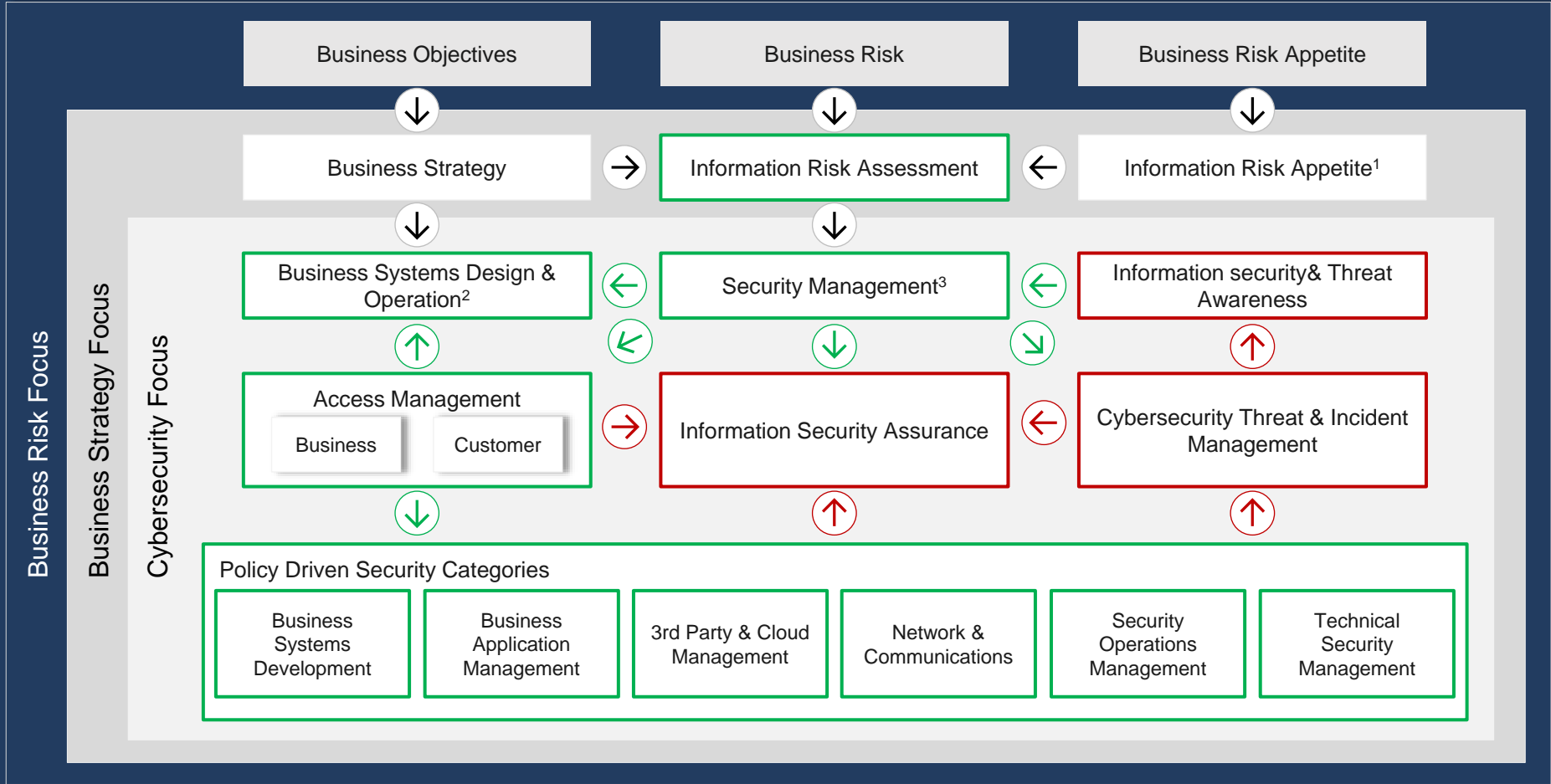
The *Secure Business by Design model* draws on these same frameworks. By ensuring that they are aligned to your actual business objectives and risk appetite, they embed value-adding functional security into all aspects of your business. This proactive approach enables clear communication of cybersecurity risk management aligned with a common business purpose. Business metrics highlight the value cybersecurity delivers to your organization.



"For many organizations, the CISO needs to be the Chief Resilience Officer"
Bill Bonney, The CISO Desk Reference Guide



The Model



⬇️ Business Objective and Risk Governance drivers

➡️ Security Policy & Control Driven

➡️ Business Objective and Risk Governance drivers

¹ Aligned with business strategy and value

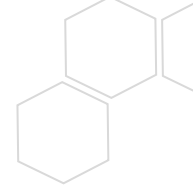
² Business Value Delivery

³ Security Policy and Information Security Management

The Four Steps to Secure Business by Design

The risk spectrum that any organization faces today is in constant flux, especially so with the acceleration of digital transformation, creating a need for constant enterprise-wide cyber risk re-evaluation. Every security program needs to be continuously reviewed and updated to address the specific threats to the business it protects, requiring access to experienced battle-hardened resources across a diverse, dynamic and appropriate skills set, with a continuous-learning ability and the necessary interpersonal skills to excel.





The Role of CISO
has changed
significantly over
the last 2-years

A CISO must understand today's business environment, how to manage inherent cyber risks and ensure that the necessary controls required for resilience also enable the value that supports business success.

That said, the CISO's role must change as any business does . This requires a CISO to grow their risk awareness faster than cyber risks to business evolve.

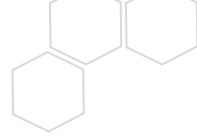
.....▶ One of the advantages that CISO's have is being part of a community willing to share experiences and advice.

As such, a CISO needs an always on go-to consulting partner to handle extended cyber threat identification and cyber risk management requirements even when your team is maxed out or otherwise fully committed.

We have sat in the CISOs seat, we know how to provide a fit-for-purpose cybersecurity service tailored to the needs of any CISO and security role, fitting both a business's risk appetite and budget.



Let's Talk



Patrick Evans
CEO

✉ pevans@slva-cs.com

☎ +1 (202)-288-2777

☎ +27 82 907 7027

📅 <https://calendly.com/pevans-slva>

🌐 [linkedin.com/in/llewellynpatrickevans](https://www.linkedin.com/in/llewellynpatrickevans)

🌐 www.slva-cs.com

🌐 <https://www.linkedin.com/company/slva-cs>

📍 **Headquarters**

4131 N Central Expressway
Suite 900 Dallas, TX 75204

Regional Office

31 Khyber Crescent, Khyber Rock
Sandton, Gauteng, 2191

Andrew Odendaal
COO / CISO

✉ aodendaal@slva-cs.com

☎ +1 (972) 672-3898

☎ +27 84 580 7057

🌐 [linkedin.com/in/andrew-o-3397292](https://www.linkedin.com/in/andrew-o-3397292)

