

Developing a Successful Cyber Strategy

Charles Gillman

[https://www.linkedin.com/in/charles-gillman/
@fullstackciso](https://www.linkedin.com/in/charles-gillman/@fullstackciso)

How To Ensure Your Strategy Succeeds



Buy-In?

Budget?



Security?

Cyber Strategy Pitfalls



Security speaks a different language to the business

Reactive
Vendor or tool-led



Wrong Drivers



Success is difficult to quantify

Overly ambitious
Causes a drag on the business

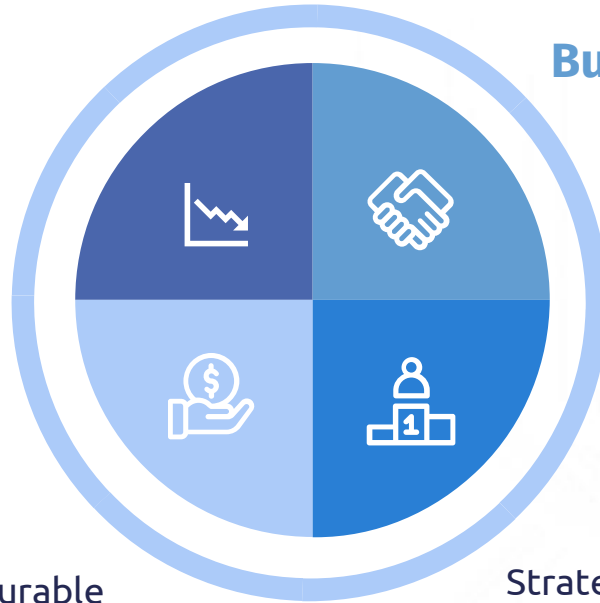


Not Implementable

Proven Benefits of a Successful Strategy

By using the right
drivers

Reduce Risk



Address what matters
to the business

Business Buy-In

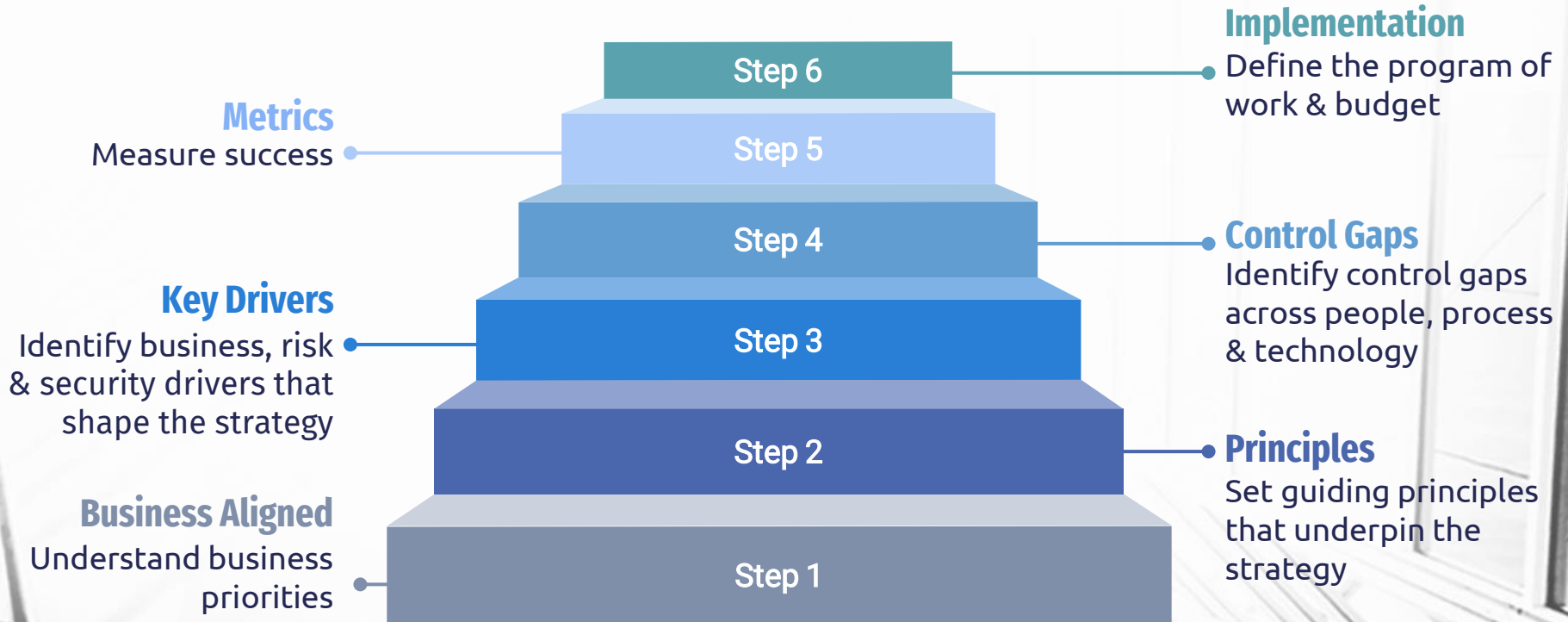
Show ROSI

Showing a measurable
Return on Security
Investment

Delivered

Strategy will be in lock-
step with the business
velocity

Six Steps to a Successful Cyber Strategy



Successful Strategy is Business Aligned

Aligned to business strategy

Aligns with the business strategy

Aligned to IT initiatives

Supports the technical direction of the business

Valued by the business

Valued by all the stakeholders



Revenue Streams

Protects the business revenues streams

Go-to-market

Understands the businesses go-to-market offerings

Growth

Supports the often rapid growth of the business

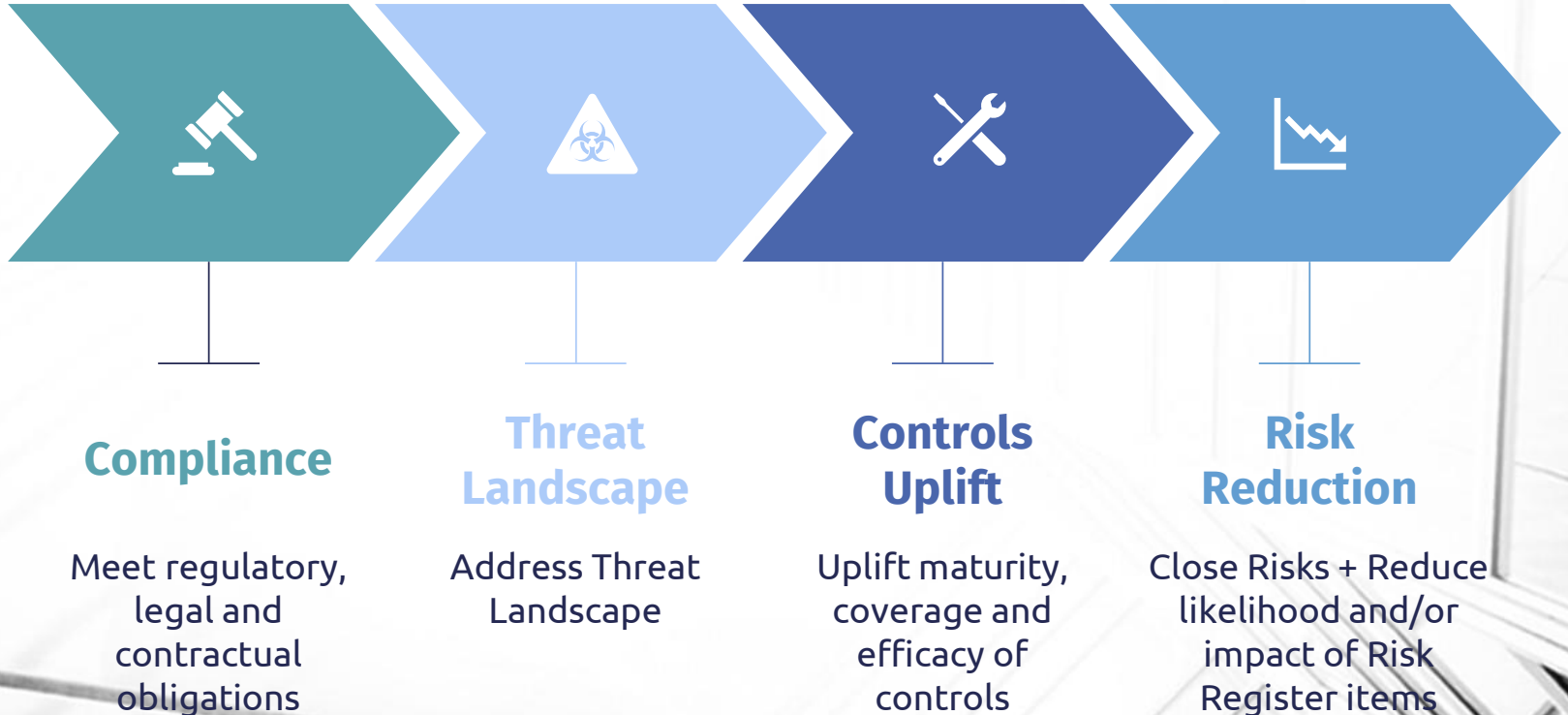
Cyber Strategy Principles

The guiding principles that underpin the strategy

Example:

- **Develop and Govern a Healthy Security Culture**
- **Manage Risk in the Language of Business**
- **Establish a Control Baseline**
- **Simplify and Rationalize IT and Security**
- **Control Access with Minimal Drag on the Business**
- **Institute Resilient Detection, Response and Recovery**

Key Cyber Strategy Drivers



Identifying Cyber Control Gaps



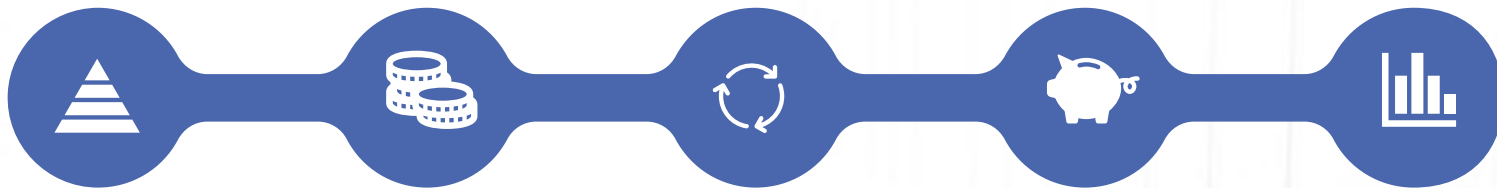
Avoiding Waste

**Investment =
Risk**

Security investment is commensurate with risk

**Low cost /
no cost**

Uplift of capabilities e.g. IR



**Leveraging
existing
investment**

Ensure existing investments are fully utilised

**Cost
containment**

Re-use of licences / lower cost vendors

**Return on
Security
Investment**

Show a ROSI through metrics

Effortlessly Measuring Success



Maturity Uplift

CMMi uplift against CSF or other framework

Risk reduction

Close or reduce likelihood or impact of risks in Risk Register

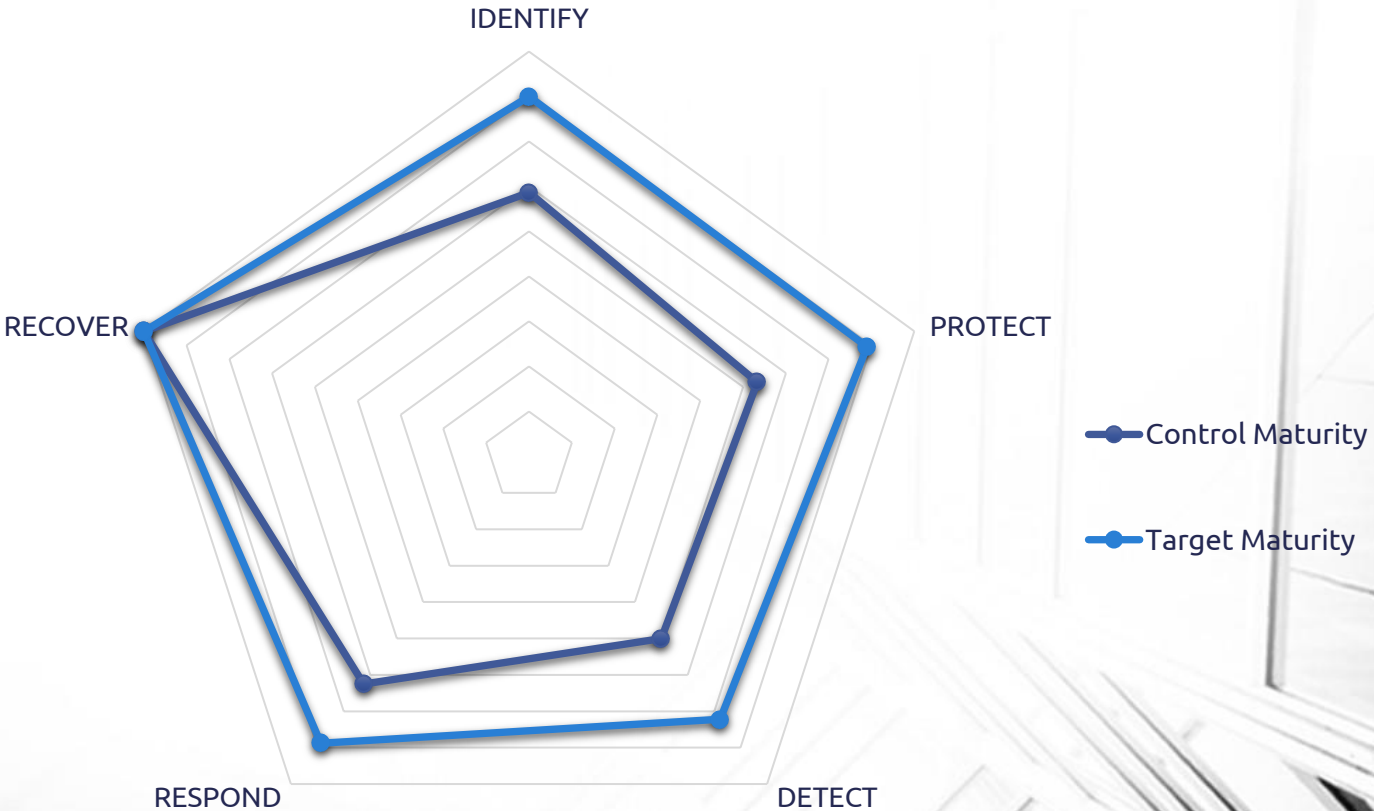
Balanced Scorecard

Financial, business, client and innovation perspectives

Objectives & Key Results

Measuring the results of the strategy objectives

Maturity Uplift Example – NIST CSF

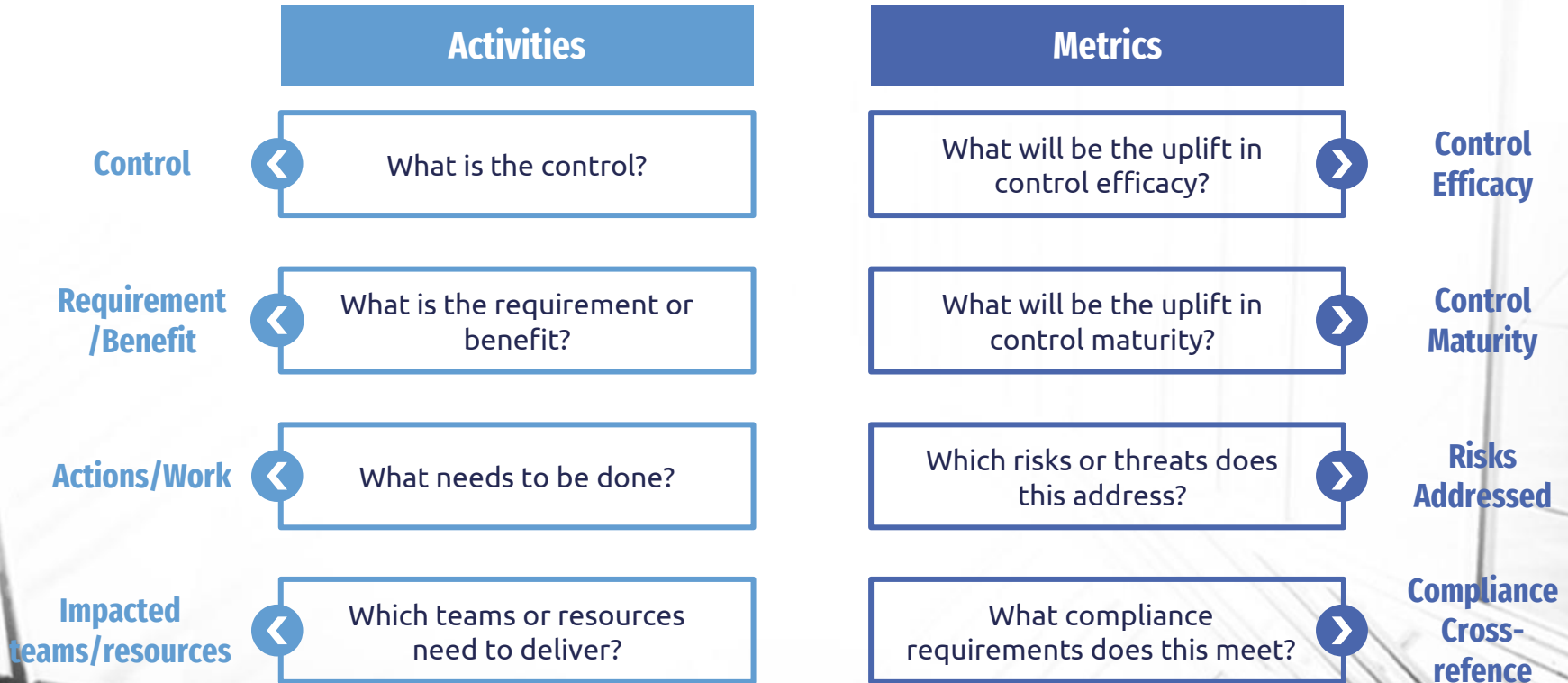


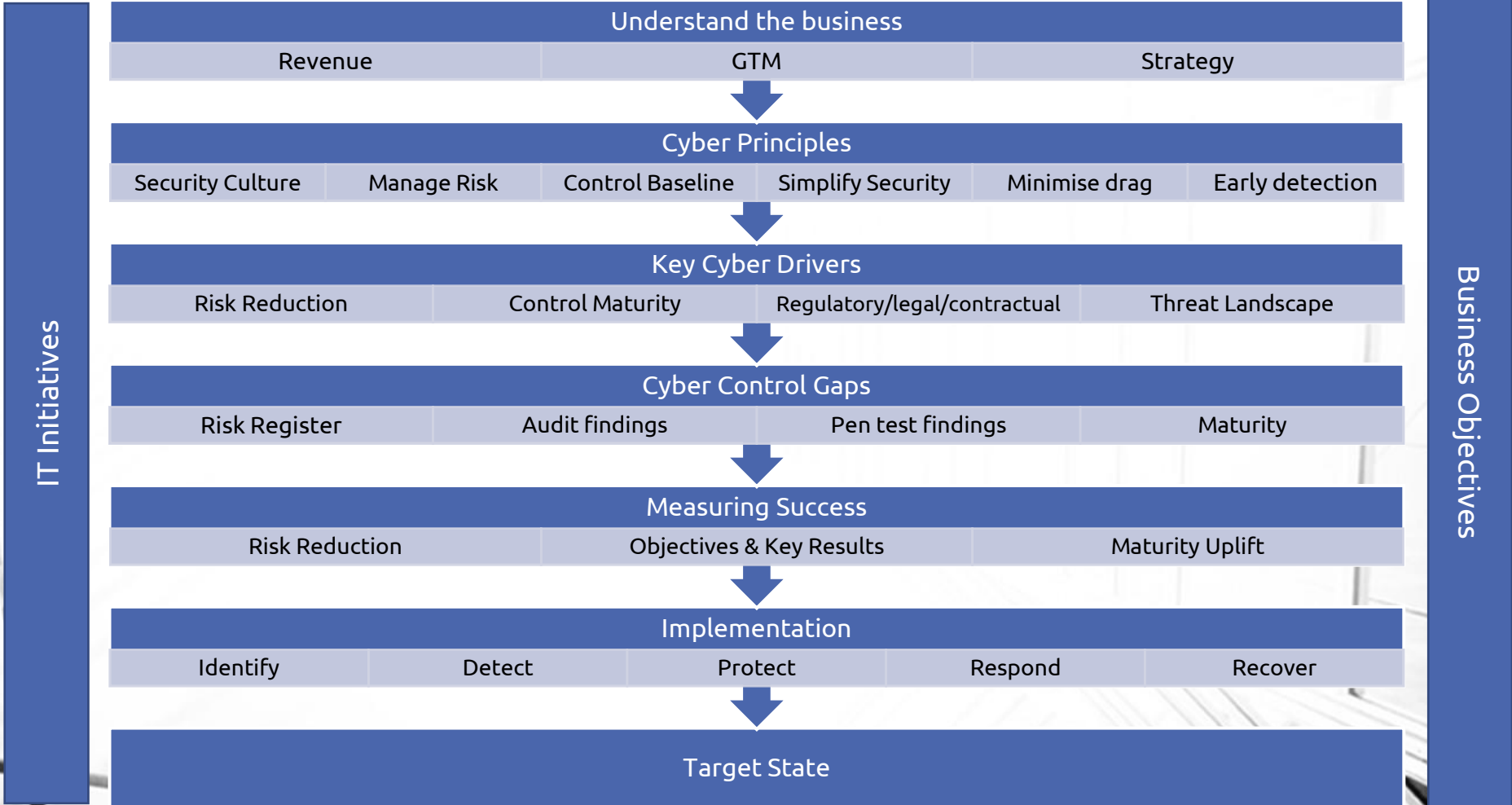
OKR Example

Objective: Reduce risk

- **Key Result 1:** Close existing risks through the implementation of compensating controls
- **Key Result 2:** Reduce either the Likelihood or Impact of Critical & High risks through the implementation of compensating controls

Tested Implementation Formula





Successful Cyber Strategy Takeaways

**Business Alignment
Increases Chance of
Success**

**Metrics
Measure
Success**

**Key Drivers Justify
the Investment**

**Risk &
Compliance
Define the
Controls**

