UC UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha

Cybersecurity Strategy

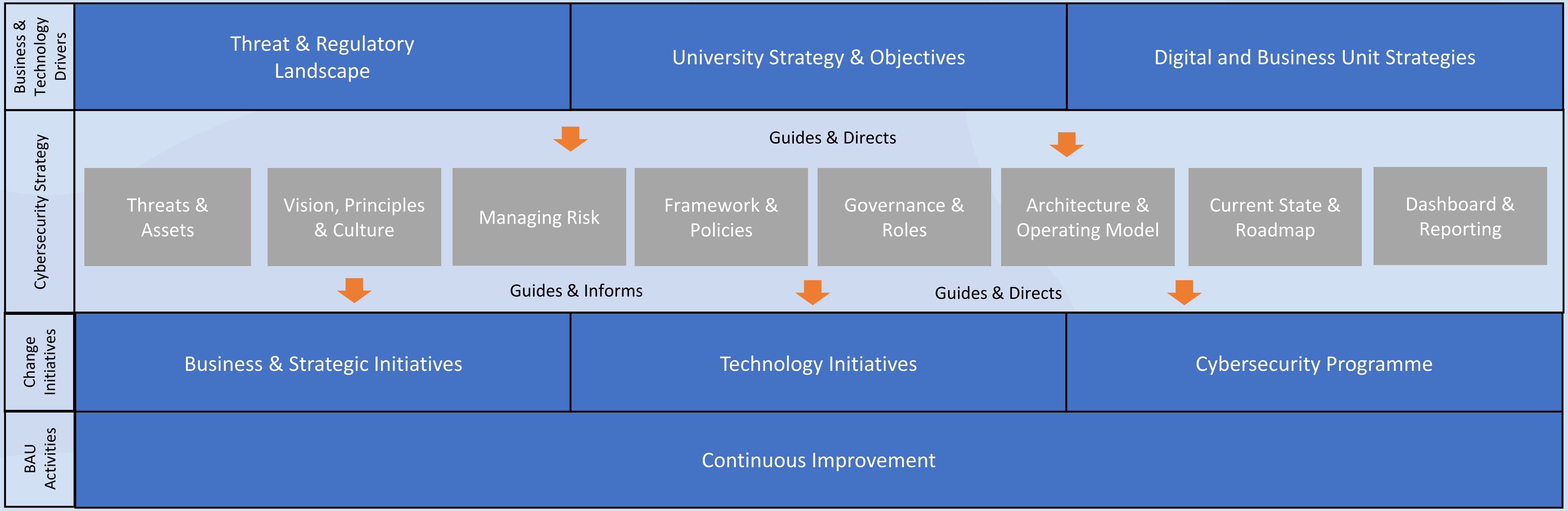
UC UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha
CHRISTCHURCH NEW ZEALAND

Introduction

The UC Cybersecurity Strategy has been created to translate the direction, guidance and intent of the University into clearly defined principles, governance, frameworks and a roadmap that ensures the investments made in cybersecurity improves the cyber resilience and enable the strategic goals of the University.

Cybersecurity Strategy Context

The Cybersecurity Strategy provides a clear line of sight from the University goals and objectives and ensures alignment with any improvement initiatives delivered through the Cybersecurity Programme. Improving and maintaining the cybersecurity of UC is a challenge for the entire organisation and not just IT or the security team. This is reflected in the fact that the Cybersecurity Strategy informs not just security initiatives but also wider technology and organisation activities.



Business & Technology Drivers

Threat & Regulatory Landscape

University Strategy & Objectives

Digital and Business Unit Strategies

Cybersecurity Strategy

Guides & Directs

Threats & Assets

Vision, Principles & Culture

Managing Risk

Framework & Policies

Governance & Roles

Architecture & Operating Model

Current State & Roadmap

Dashboard & Reporting

Guides & Informs

Guides & Directs

Change Initiatives

Business & Strategic Initiatives

Technology Initiatives

Cybersecurity Programme

BAU Activities

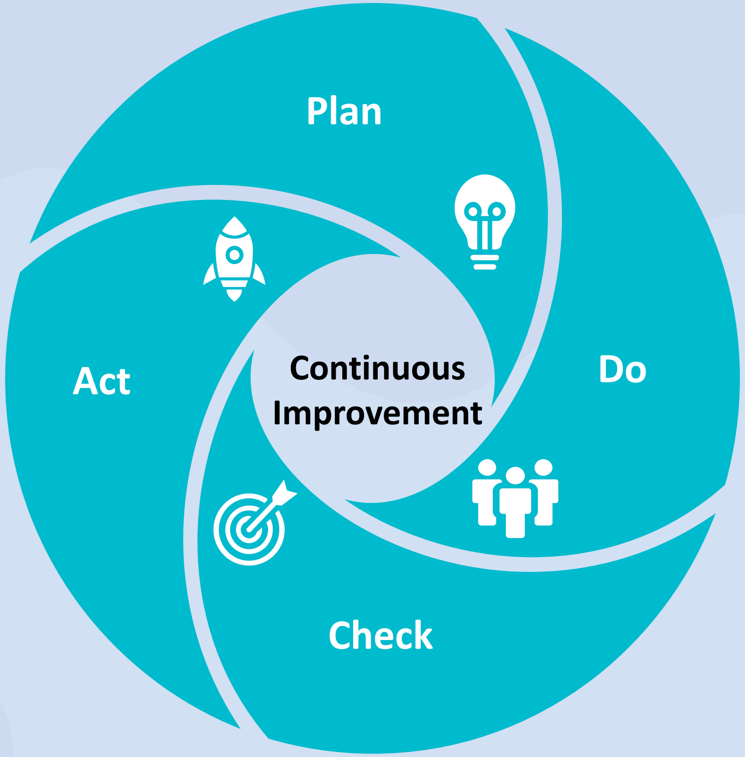
Continuous Improvement

Cybersecurity Continuous Improvement

The technology, organisational and threat landscape continually evolves.

This likewise means that cybersecurity needs to evolve and align to enable the University. This needs a cycle of continuous improvement and validation.

UC will maintain its commitment to continuous cybersecurity improvement and not consider this a problem that can be "fixed" and then focus on other issues. With the speed of change within the organisation and the threat landscape, UC cannot and will not lose focus on cybersecurity.



Plan, Do, Check, Act Cycle

01 ALIGNED PLANNING

We will continually review our strategy and our programme to ensure it aligns to the University and the threats that we face.

02 FLEXIBLE MODEL

We will adjust and change our operating model to enable the best outcomes for UC and leverage the expertise of our people and partners.

03 ADJUST THE BASELINE

As our cyber resilience improves, we will evaluate and adjust our baseline to an agreed compliance standard.

04 IMPROVE CONTROLS

We will measure our controls and ensure we are continually refining and improving their effectiveness.

UC Strategy

What is important to UC?

UC Strategic Goals

- Engagement
- Research
- Education
- People
- Efficacy
- Internationalisation
- Sustainability

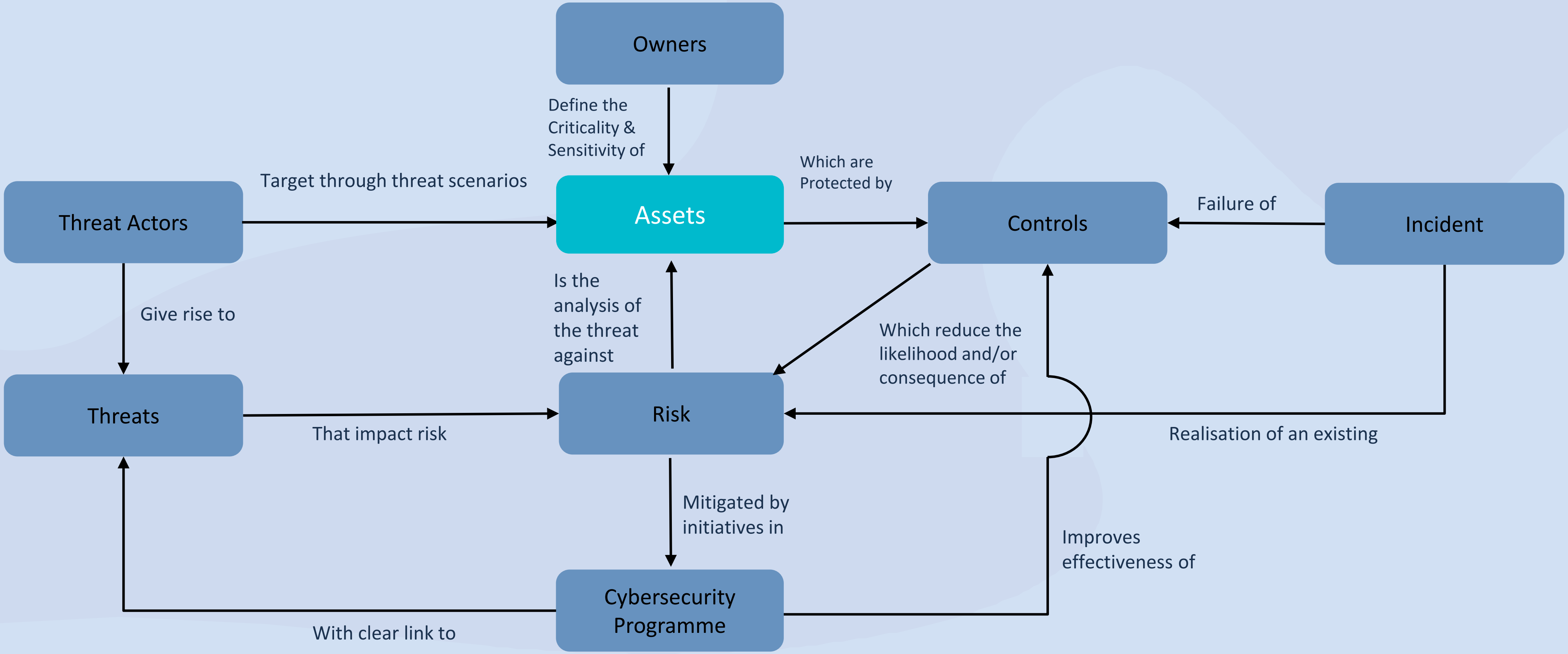
What are the strategic outcomes of cybersecurity?

- Enable and empower UC to deliver its Strategic plans through collaboration, engagement and proactive stewardship of cybersecurity.
- Support the management of UC's cyber risk exposure through cost-effective measures.
- Demonstrate trust and confidence in Digital services by continuously protecting UC from harm against evolving cyber risks and threats.
- To be recognised as an industry leader in the development of cybersecurity talent.

What are the strategic objectives of cybersecurity?

- Mature the cybersecurity capabilities of UC whilst ensuring a frictionless security experience.
- Deliver UC solutions and capabilities in line with cybersecurity best practices and industry standards.
- Embed cybersecurity into UC’s culture by cultivating a collaborative approach that brings together the University community.
- Safeguard UC’s operational resilience.

Risk & Security Relationship Model


Owners
Define the Criticality & Sensitivity of
Threat Actors
Target through threat scenarios
Assets
Which are Protected by
Controls
Failure of
Incident
Give rise to
Is the analysis of the threat against
Which reduce the likelihood and/or consequence of
Threats
That impact risk
Risk
Realisation of an existing
Mitigated by initiatives in
Improves effectiveness of
Cybersecurity Programme
With clear link to

Cybersecurity Vision

"**Enable** UC to support its teaching, learning and research outcomes and vision by embedding a positive **security culture** in everything we do and safely guide business decisions to protect us from cyber threats"

Cybersecurity Principles

1

Breadth Before Depth

We will establish visibility and understanding of the organisational and threat landscape to ensure that decisions are prioritised in context.

2

Risk Informed, Threat Aligned

All investments will be made with an awareness of the threats faced by the business and the risks being mitigated.

3

Defence in Depth

All controls should support effective defence in depth and must be aligned to identified threats with measurable outcomes.

4

Ensure Compliance

Compliance requirements will be identified and included in any new capabilities, systems or services.

5

Secure By Design

Everything developed, designed or subscribed to will be securely architected, designed, implemented and operated.

6

Safety First

We will ensure that we prioritise investments that ensure the safety and security of our staff and our students.

7

Continuously Improve

Cyber resilience is a process of continuous improvement through layers of refinement and enhancement

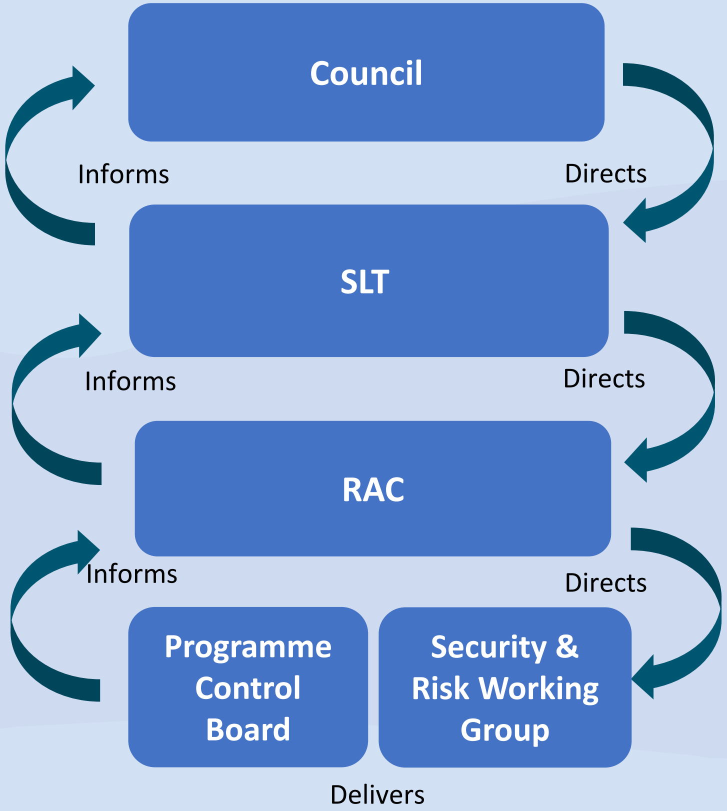
8

Zero Trust Journey

Ensure that alignment with the zero trust journey and the authentication and validation of every interaction.

Cybersecurity Governance

Effective linkage between operational activities and the cybersecurity programme are guided through effective governance. This is established through the key forums defined below.



COUNCIL

- + Endorses & sets the strategic cybersecurity direction of the University.
- + Endorse organisational risk appetite and tolerances.
- + Assist in prioritisation by helping to identify critical assets and highlight key risks.
- + Assess the effectiveness of the cybersecurity strategy.

SLT

- + Realise the board's cybersecurity strategy & ensure sufficient resourcing to execute the strategy
- + Define critical assets and highlight key risks.
- + Approve relevant policies & standards
- + Oversight of the overall cybersecurity budget and ensuring expenditure supports the strategy.
- + Oversight of the delivery of cybersecurity initiatives.
- + Monitor the effectiveness of the cybersecurity programme

RAC

- + Measure the effective reduction of cybersecurity risk via the cybersecurity strategy execution.
- + Define organisational risk appetite and tolerances.
- + Monitor & track key risks.

Programme Control Board

- + Oversight of the approved programme budget and delivery of programme initiatives.
- + Measure the effectiveness of the cybersecurity programme

Security and Risk Working Group

- + Develop & maintain the cybersecurity strategy, policies & standards, architecture & controls framework.
- + Ensure delivery of cybersecurity operational activities & programme.
- + Proactively manage cybersecurity operations and continuous improvement.
- + Coordinate and manage audit and assurance activities.

Cybersecurity Framework

UC has selected the NIST Cybersecurity Framework (CSF) to provide structure and context for the security controls deployed across the organisation.

The definition of controls is based on ISO27001 and where needed, NIST 800-53 and the NZ PSR.

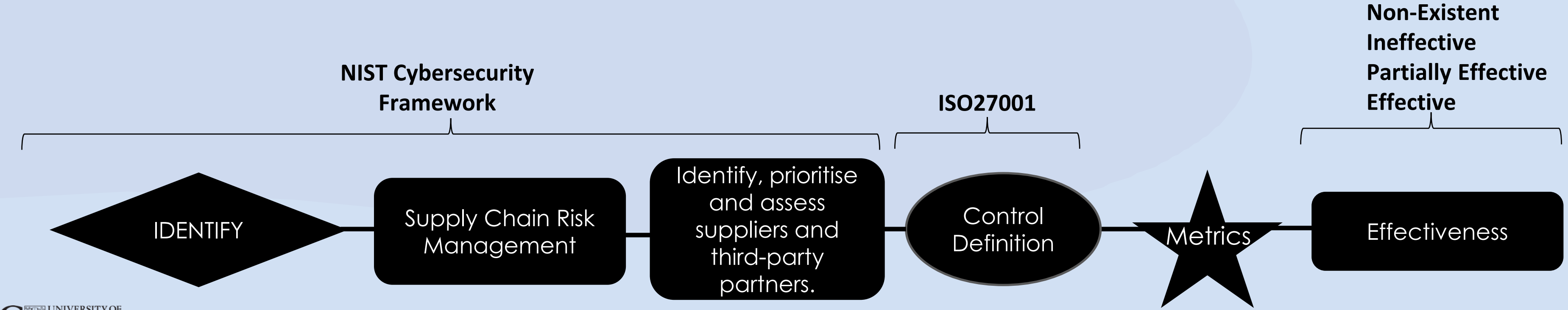
Policies
Standards
Guidelines

Our controls are explained and mandated through our policies, standards and guidelines

We will deliver our controls improvements and continually maintain them through our Cybersecurity Programme

Policies & Standards

1. Information Security Policy
2. Acceptable Use Policy
3. Asset Management Standard
4. Information Classification and Handling Standard
5. Vulnerability Management Standard
6. Secure Operations Standard
7. Third-Party Risk Management Standard
8. Sharing and Collaboration Standard
9. Cloud Services Standard
10. Encryption Standard
11. Identity and Access Management Standard
12. End User Device Management Standard
13. System Acquisition and Development Standard



NIST Cybersecurity Framework

ISO27001

Non-Existent
Ineffective
Partially Effective
Effective

IDENTIFY → Supply Chain Risk Management → Identify, prioritise and assess suppliers and third-party partners. → Control Definition → Metrics → Effectiveness

Security Architecture

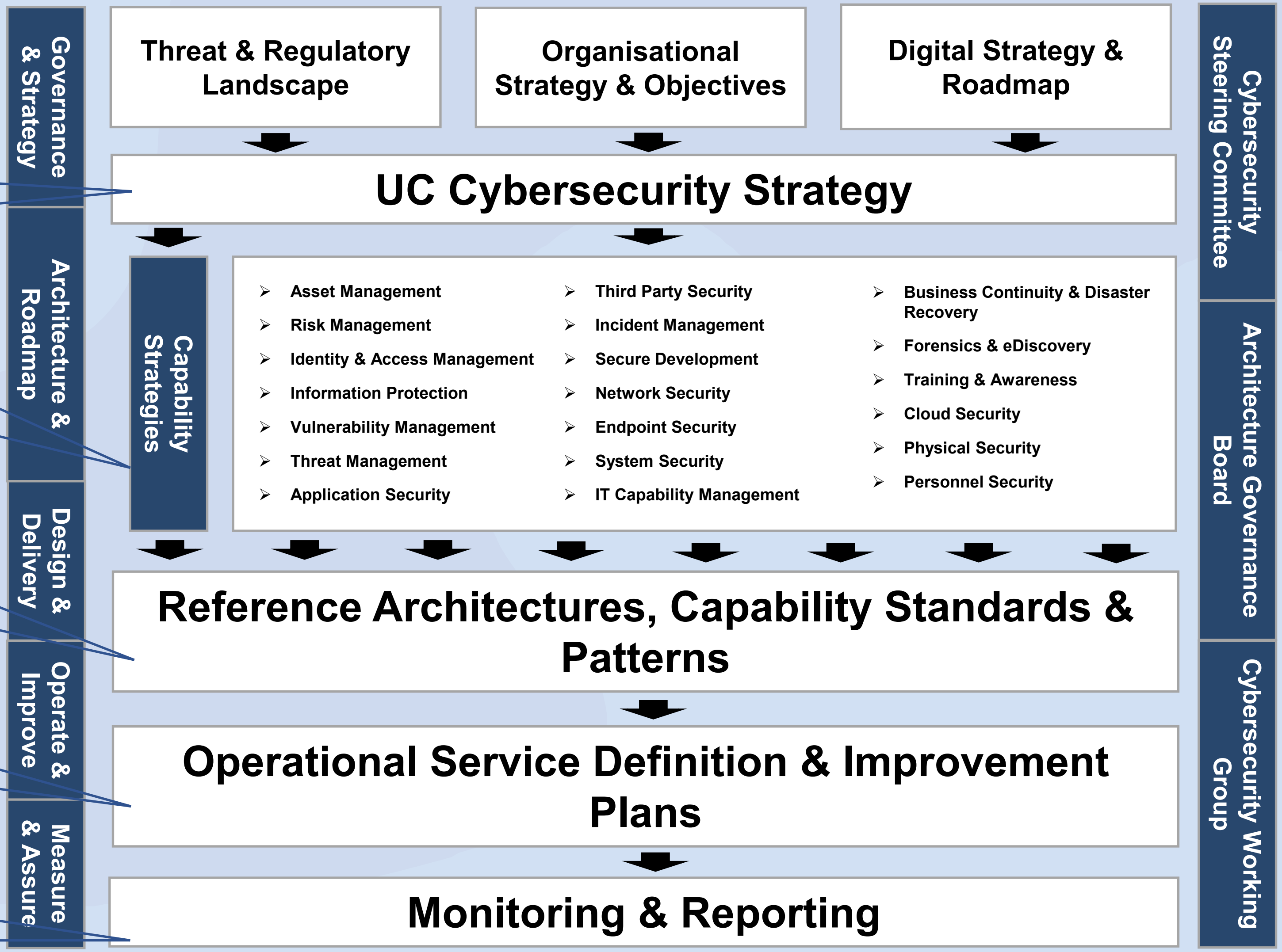
The ***Cybersecurity Strategy*** provides the interface between the business and threat landscape and establishes the required governance and approach as defined in the ***Cybersecurity Strategic Context***.

The ***Cybersecurity Strategy*** defines the Enterprise Architecture Domain for Cybersecurity. This domain is then interpreted through a series of ***Capability Strategies.*** Each capability has challenges and opportunities, defined objectives and outcomes, threat and controls alignment, current and target state as well as planned and future roadmap initiatives.

Capability Strategies can be supported through ***Reference Architectures***, ***Capability Standards*** & ***Patterns*** that support the ability for stakeholder groups and initiatives to align with and adopt the strategies of the Cybersecurity Strategy & Architecture Domain.

The Capability Strategies and supporting collateral guide and inform the ***Operational Service Definitions*** and ***Improvement Plans***. These address the operational implementation and continuous improvement of our services.

The monitoring and reporting as defined by our ***Assurance Framework*** provides the feedback and input to direct and update the strategy and capabilities to support continuous refinement and improvement.



Governance & Strategy

Architecture & Roadmap

Design & Delivery

Operate & Improve

Measure & Assure

Threat & Regulatory Landscape

Organisational Strategy & Objectives

Digital Strategy & Roadmap

UC Cybersecurity Strategy

Capability Strategies

- Asset Management
- Risk Management
- Identity & Access Management
- Information Protection
- Vulnerability Management
- Threat Management
- Application Security
- Third Party Security
- Incident Management
- Secure Development
- Network Security
- Endpoint Security
- System Security
- IT Capability Management
- Business Continuity & Disaster Recovery
- Forensics & eDiscovery
- Training & Awareness
- Cloud Security
- Physical Security
- Personnel Security

Reference Architectures, Capability Standards & Patterns

Operational Service Definition & Improvement Plans

Monitoring & Reporting

Cybersecurity Steering Committee

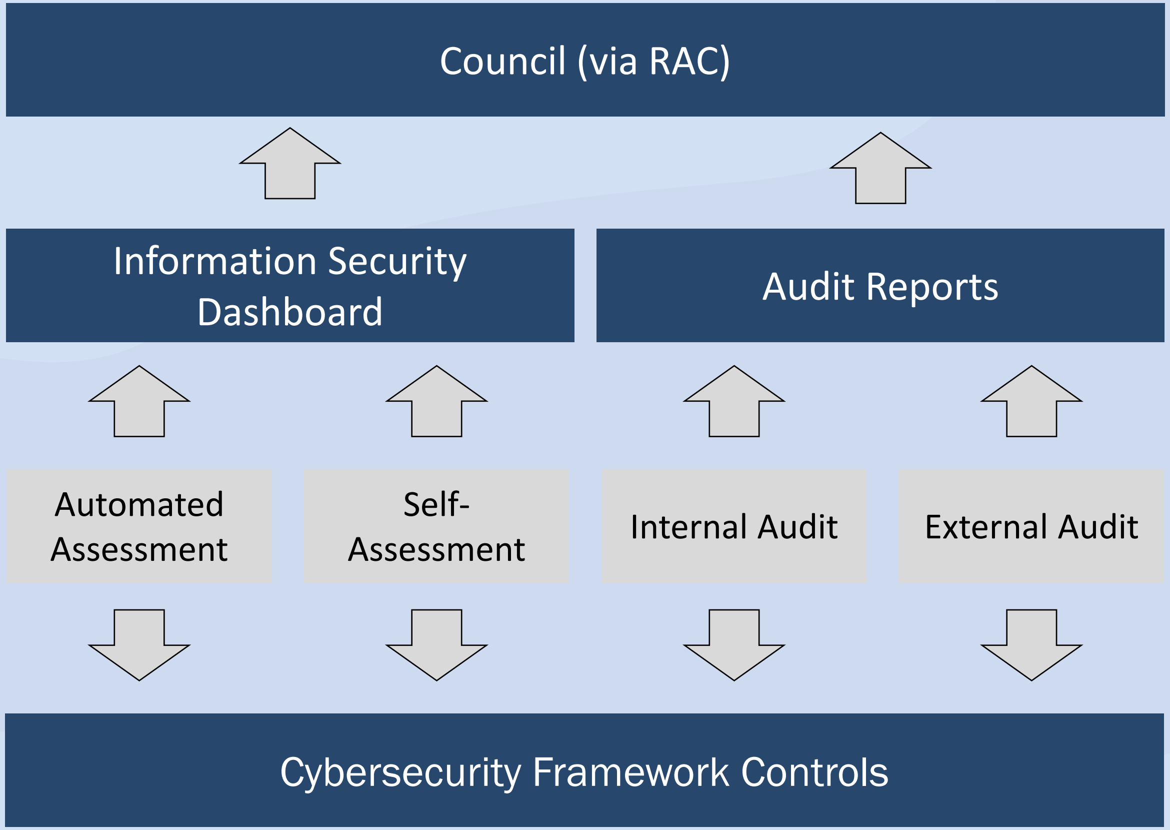
Architecture Governance Board

Cybersecurity Working Group

UC UNIVERSITY OF CANTERBURY Te Whare Wānanga o Waitaha

Assurance Framework

Having a consistent measurement of information security controls using a combination of internal and external assurance provides a clear measure of current performance.



Council (via RAC)

Information Security Dashboard

Audit Reports

Automated Assessment

Self-Assessment

Internal Audit

External Audit

Cybersecurity Framework Controls

- All assurance activity should be based on the agreed Cybersecurity Framework controls.
- This ensures consistent reporting and representation of compliance and maturity.
- Internal and external audit activity should be aligned to achieve maximum scope.
- Wherever possible assessment should be automated based on agreed metrics.
- Any audit and testing results should provide balanced input into the information security programme.