Compliance

Introduction & Overview

Compliance??

Compliance Dictionary definition

Compliance [k*uh*m-**plahy**-*uh*ns]

the act of obeying an order, rule, or request

Also

the act of conforming, acquiescing, or yielding.

a tendency to yield readily to others, especially in a weak and subservient way.

conformity; accordance: *in compliance with orders.*

cooperation or obedience: *Compliance with the law is expected of all.*

Adherence ?

Adherence ?

adherence

noun [U]

formal

/ədˈhɪərəns/ **US**

the act of doing something according to a particular rule, standard, agreement, etc.

Regulations ?

Regulation

the rules or systems that are used by a person or organization to control an activity or process, or the action of controlling the activity or process

Risk ?

Risk

verb [T]

UK

/rɪsk/

to do something although there is a chance of a bad result

noun [C/U]

US

/rɪsk/

danger, or the possibility of danger, defeat, or loss

Governance ?

What is Governance ?

governance

noun [U]

UK

/ˈgʌv.ən.əns/ **US**

/ˈgʌv.ɚ.nəns/

the way that organizations or countries are managed at the highest level, and the systems for doing this

What is GRC ?

GRC ?

Governance, Risk and Compliance

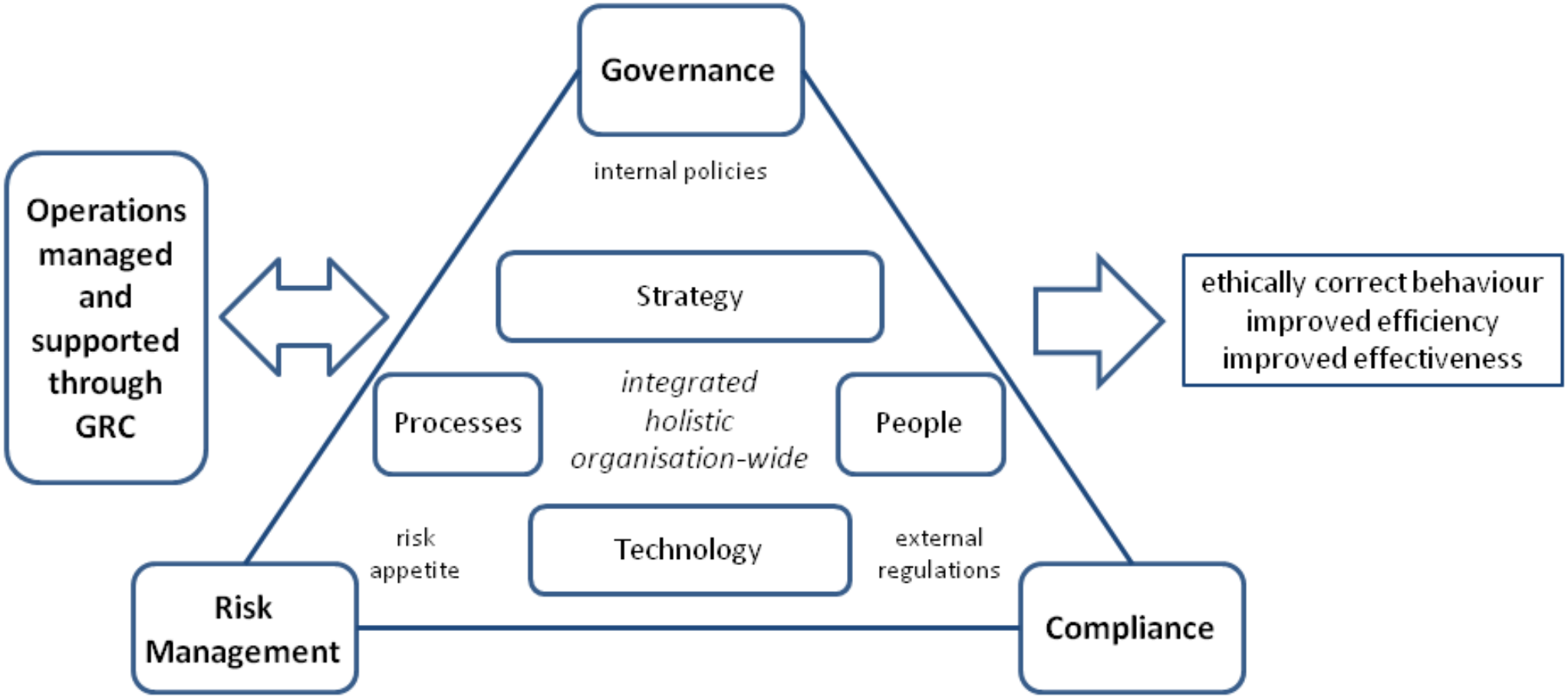
Governance, Risk and Compliance (**GRC**) refers to a strategy for managing an organization's overall governance, enterprise risk management and compliance with regulations.

Think of **GRC** as a structured approach to aligning IT with business objectives, while effectively managing risk and meeting compliance requirements.

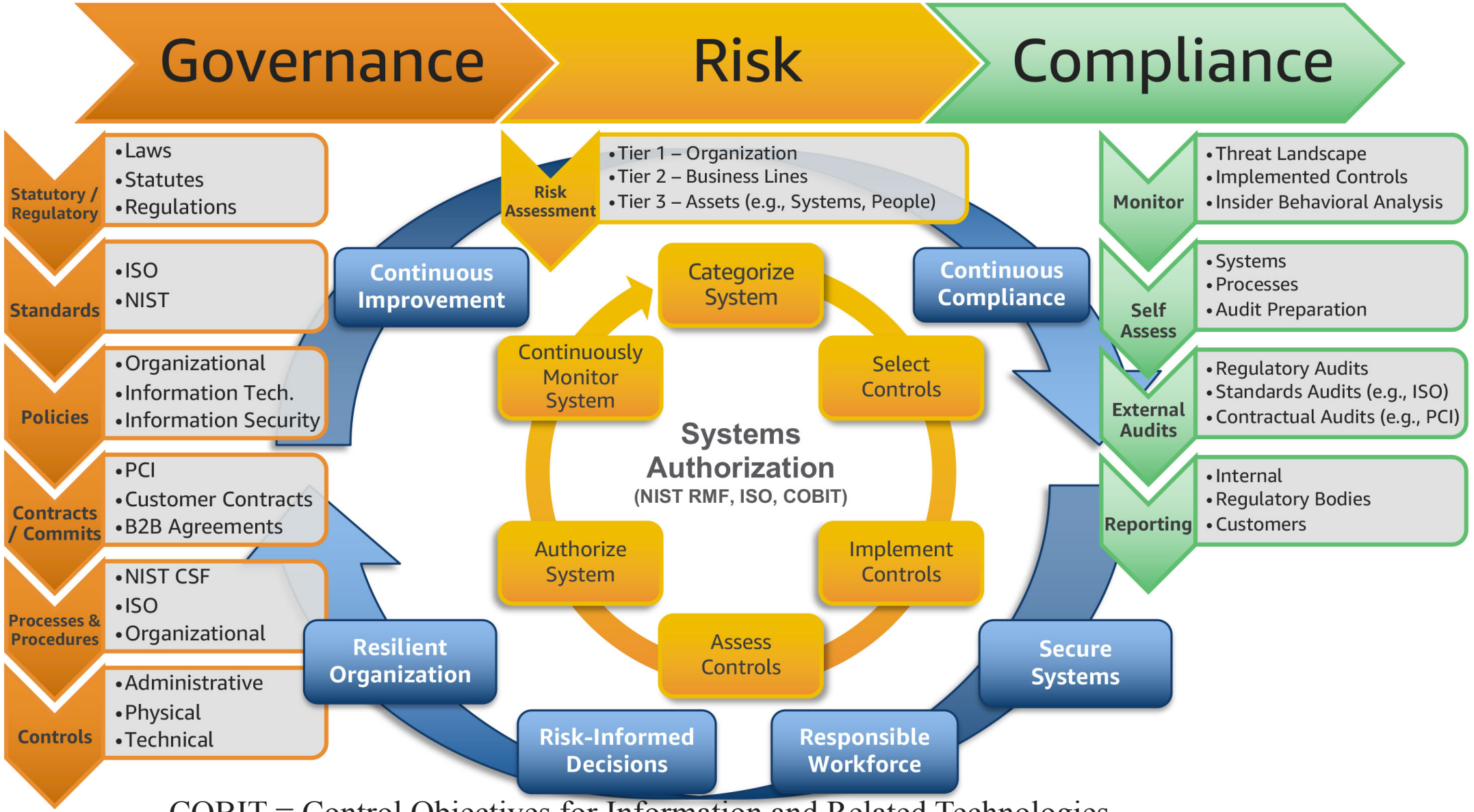

Governance
The means by which an organization is directed and controlled.
Risk
A possible event that could cause harm or loss or make it more difficult to achieve objectives.
Compliance
Ensuring you follow the appropriate guidelines and use proper, consistent accounting practices.

GRC - coverage

Key Components of GRC

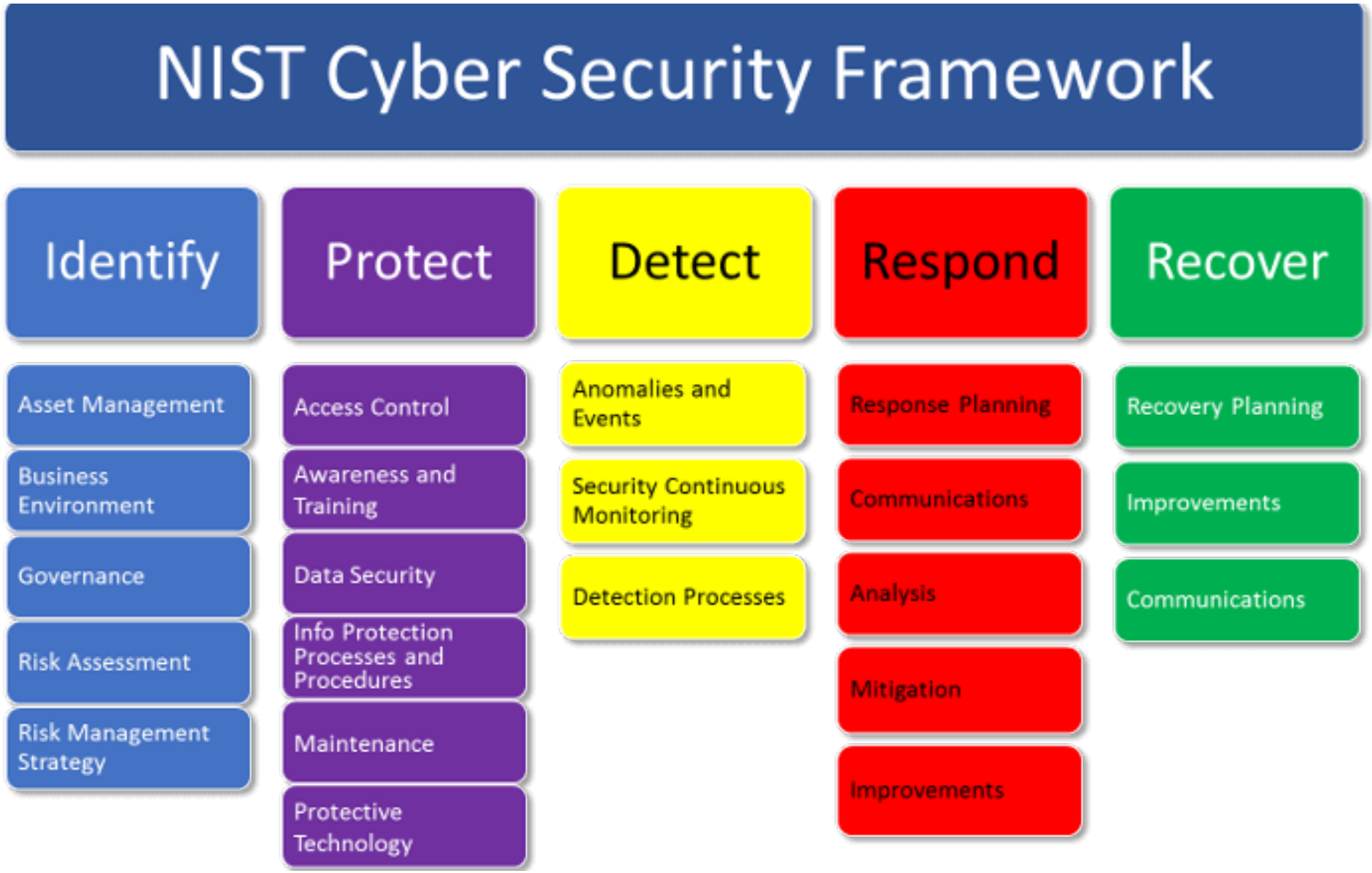


Detailed break-down



COBIT = Control Objectives for Information and Related Technologies

NIST CSF


NIST Cyber Security Framework
Identify
Asset Management
Business Environment
Governance
Risk Assessment
Risk Management Strategy
Protect
Access Control
Awareness and Training
Data Security
Info Protection Processes and Procedures
Maintenance
Protective Technology
Detect
Anomalies and Events
Security Continuous Monitoring
Detection Processes
Respond
Response Planning
Communications
Analysis
Mitigation
Improvements
Recover
Recovery Planning
Improvements
Communications

Compliance

Compliance means creating a program that establishes risk-based controls to protect the confidentiality, integrity, and availability of information stored, processed, or transferred

Compliance varies depending on industry vertical and not a stand-alone process

Cyber Security Controls

Management Security

Management security is the overall design of your controls. Providing the guidance, rules, and procedures for implementing a security environment.

Operational Security

Operational Security is the effectiveness of your controls. Includes access control, authentication, and security topologies after network installation is complete.

Physical Security

Physical security is the protection of personnel, data, hardware, etc., from physical threats that could harm, damage, or disrupt business operations or impact the confidentiality, integrity, or availability of systems and/or data.

Points of Cyber Security Compliance

- Require a Compliance team
- Plan for risk analysis based on industry vertical from risk team
  - Identify, Assess, Analyse and set risk appetite
- Set appropriate controls
- Create policies
- Monitor and react

Risk Management

Compliance Process

Cyber Due Diligence

Control Risks has pioneered the intelligence and threat-led approach to cyber and data security with the aim of keeping you secure, compliant and resilient.

Cyber Threat Intelligence

Gain a clear picture of the cyber security capabilities of your partner, acquisition target or third party vendor and the potential risks they may present. Equally, if you are the seller, using Control Risks to conduct a self-cyber due diligence before going public will increase the value of your proposition.

Compliance Process (Contd)

Threat, Risk Assessments and Maturity Assessments

- Delivered through subscription service or bespoke projects, our cyber threat intelligence service provides:
- Strategic threat intelligence – Forward looking intelligence helps our clients understand global developments and trends in the cyber threat landscape. This informs their cyber security strategy and enables them to understand how cyber security threats can be contextualized within the broader threat landscape.
- Tactical threat intelligence – Actionable intelligence analyzing the tactics, techniques and procedures of cyber threat actors targeting organizations across the world.
- Operational threat intelligence – Understand and analyse the immediate threats to your organisation detected from a range of open and closed sources.

Cyber Security Training

To Avoid

- Risks and threats
- Fines and Penalties
- Embracement
- Business reputation
- Whereabouts of your organisation

Compliance Framework

- FISMA - Federal Information Security Management Act of 2002
- SOX - Sarbanes-Oxley
- HIPAA/HITECH - Health Insurance Portability and Accountability Act
- PCI DSS – Payment Card Industry – Data Security Standards
- NIST – National Institute of Standards and Technology
- ISO/IEC 27000 – International Standard Organisation/International Electrotechnical Commission