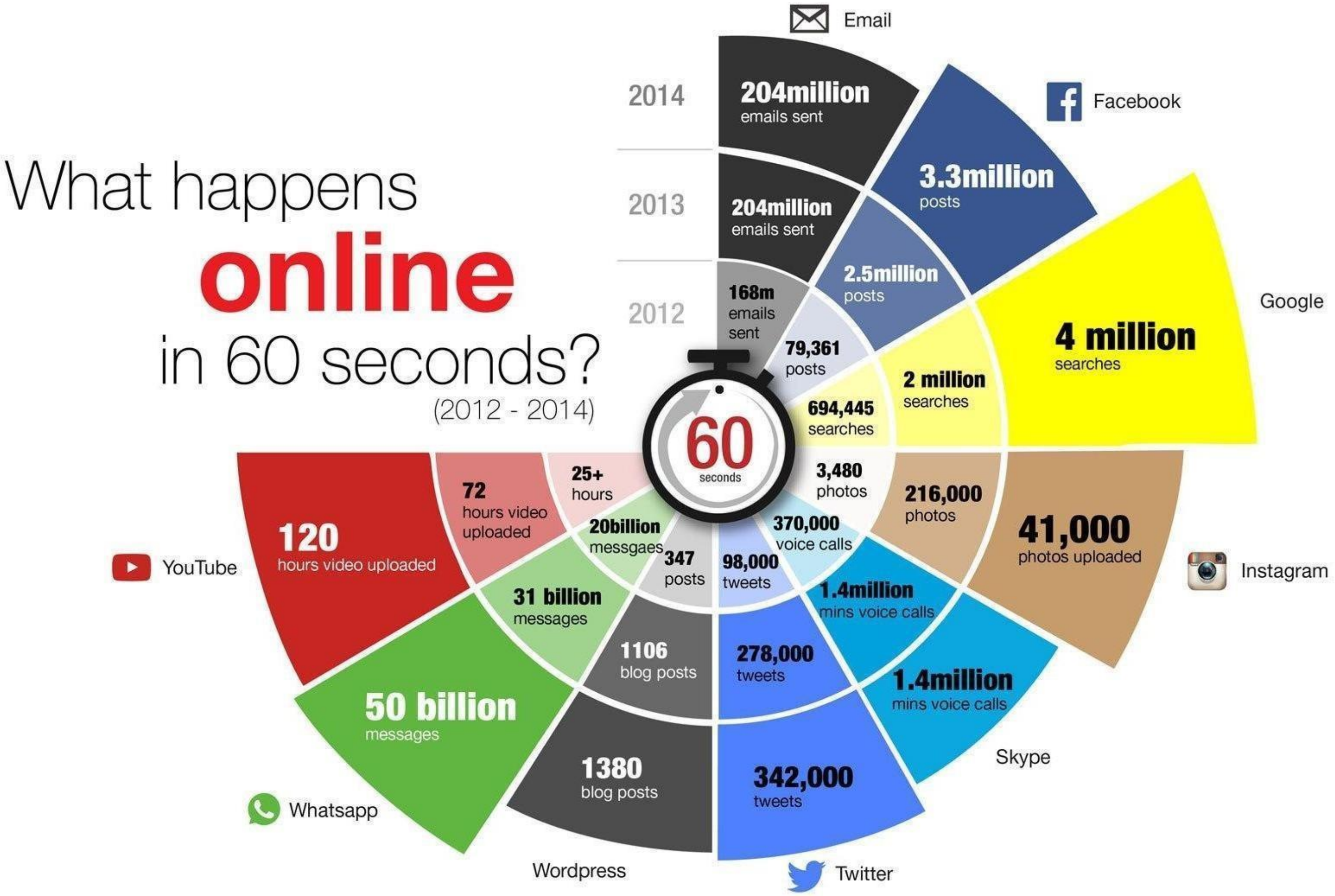
Information Security Model for Business

Tony Ventura

March 23, 2016

The New Style of IT

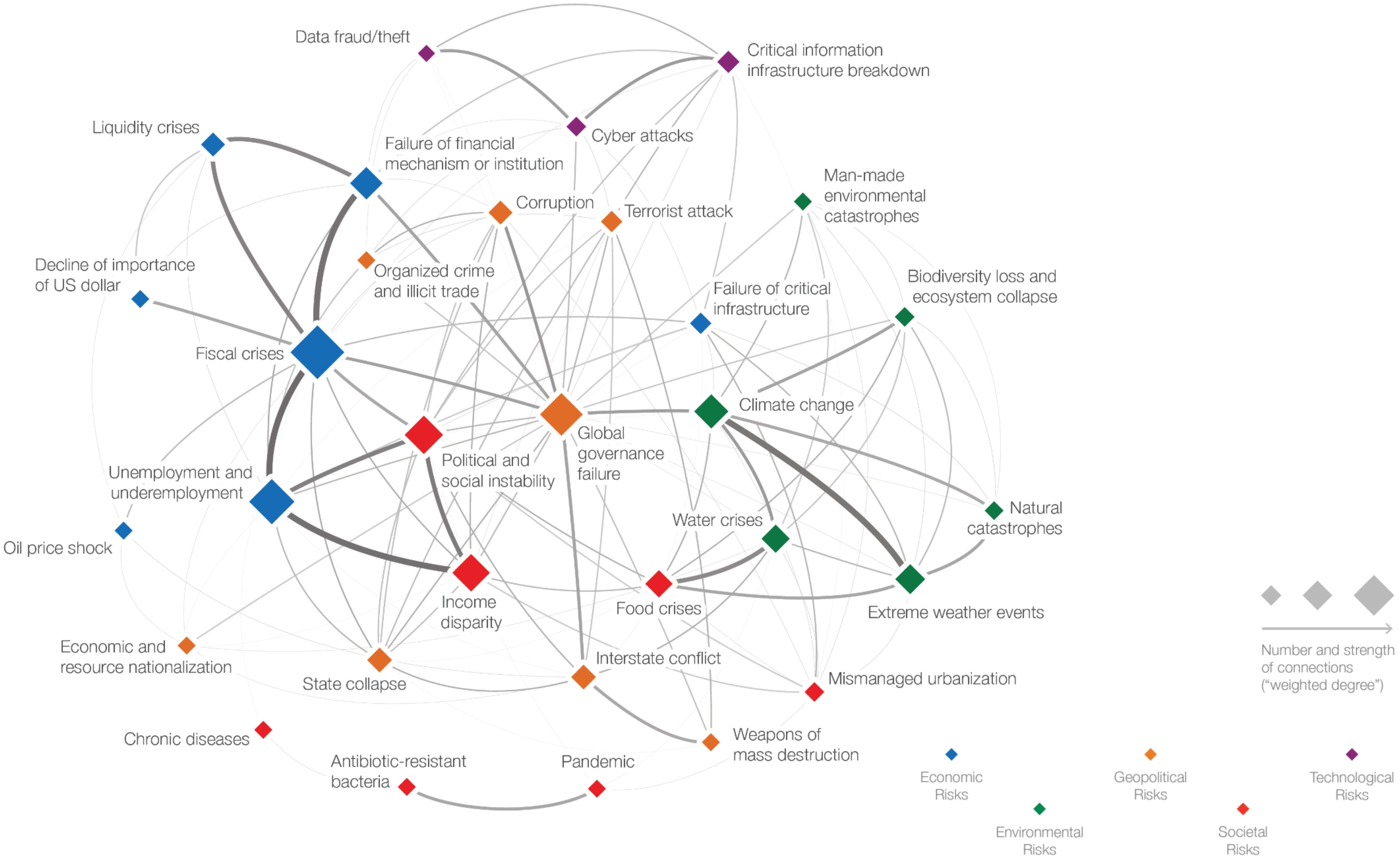
From a system of record to a system of engagement and constant interaction



Brings new business opportunities, but also new challenges and threats

Source: Forrester Research, Ponemon Institute, Coleman Parkes Research

Interconnected World means Interconnected Risks


Data fraud/theft
Critical information infrastructure breakdown
Liquidity crises
Failure of financial mechanism or institution
Cyber attacks
Corruption
Terrorist attack
Man-made environmental catastrophes
Decline of importance of US dollar
Organized crime and illicit trade
Failure of critical infrastructure
Biodiversity loss and ecosystem collapse
Fiscal crises
Climate change
Global governance failure
Political and social instability
Unemployment and underemployment
Natural catastrophes
Water crises
Oil price shock
Income disparity
Food crises
Extreme weather events
Economic and resource nationalization
State collapse
Interstate conflict
Mismanaged urbanization
Chronic diseases
Weapons of mass destruction
Antibiotic-resistant bacteria
Pandemic
Number and strength of connections ("weighted degree")
Economic Risks
Geopolitical Risks
Technological Risks
Environmental Risks
Societal Risks

Global Risks 2014, World Economic Forum, Switzerland, 2014

Security Threats & Implications

Cyber threat	**56%** of organizations have been the target of a cyber attack
Extended supply chain	**44%** of all data breach involved third-party mistakes
Financial loss	**$8.6M** average cost associated with data breach
Reputation damage	**30%** market cap reduction due to recent events
Cost of protection	**8%** of total IT budget spent on security
Reactive vs. proactive	**60%** of enterprises spend more time and money on reactive measures vs. proactive risk mgmt

Key Points

- Security is under immense pressure
- Need for greater visibility of business risks and to make sound security investment choices

Source: Forrester Research, Ponemon Institute, Coleman Parkes Research

Security challenges of a modern organization

Triggered by the New Style of IT and the new Threat Landscape

Security aligned with business objectives, acting as business enabler;

Provide End-to-End Security to critical assets and employees that now operate in a highly interconnected and perimeter-less environment;

Avoid complexity and accountability gap in Cyber Security;

Follow a Risk based approach for IT security that is aligned with the overall Risk Appetite;

Continuously measure Compliance, IT Risk Level and return on Security Investments;

Keep up with the increasing level of IT Security Laws, Regulations and Standards at a global scale;

Full Cyber Situational Awareness – See the Big Picture with no surprises or blind spots;

Deal with the new threat landscape (APTs, BYOD, state sponsored Cyber attacks, etc.);

Benchmark with Industry peers.

Security Strategy and Risk Management

What should business consider?

A. A holistic Risk and Security strategy and transformation roadmap

- Holistic strategy development to address the new threat landscape (e.g. APTs, BYOD, state sponsored Cyber attacks) to reduce complexity uncertainty and lack of visibility;
- A 360^{o} view of all interconnected people, data and systems involved in risk and cyber security to avoid a silo based approach.

B. Understand and measure IT Security Risk

- Measure the level of IT Security Risk and to assess whether is it aligned with the overall risk appetite;
- Benchmark the level of IT security risk with peers in the Industry;
- Understand whether security is enabling or restricting the Business;
- Visibility of the trade off between risk reduction and security spend.

What are the key factors to consider?

1. The ability to advise, transform, manage, complex, integrated security solutions*

- Deliver less complexity, less risk, cost and faster outcomes to the Business;
- Advise, implement and manage the security strategy and transformation roadmap avoiding the accountability gap in a multi-vendor environment;
- Provide security vision and strategy but also provide advice and implementation direction.

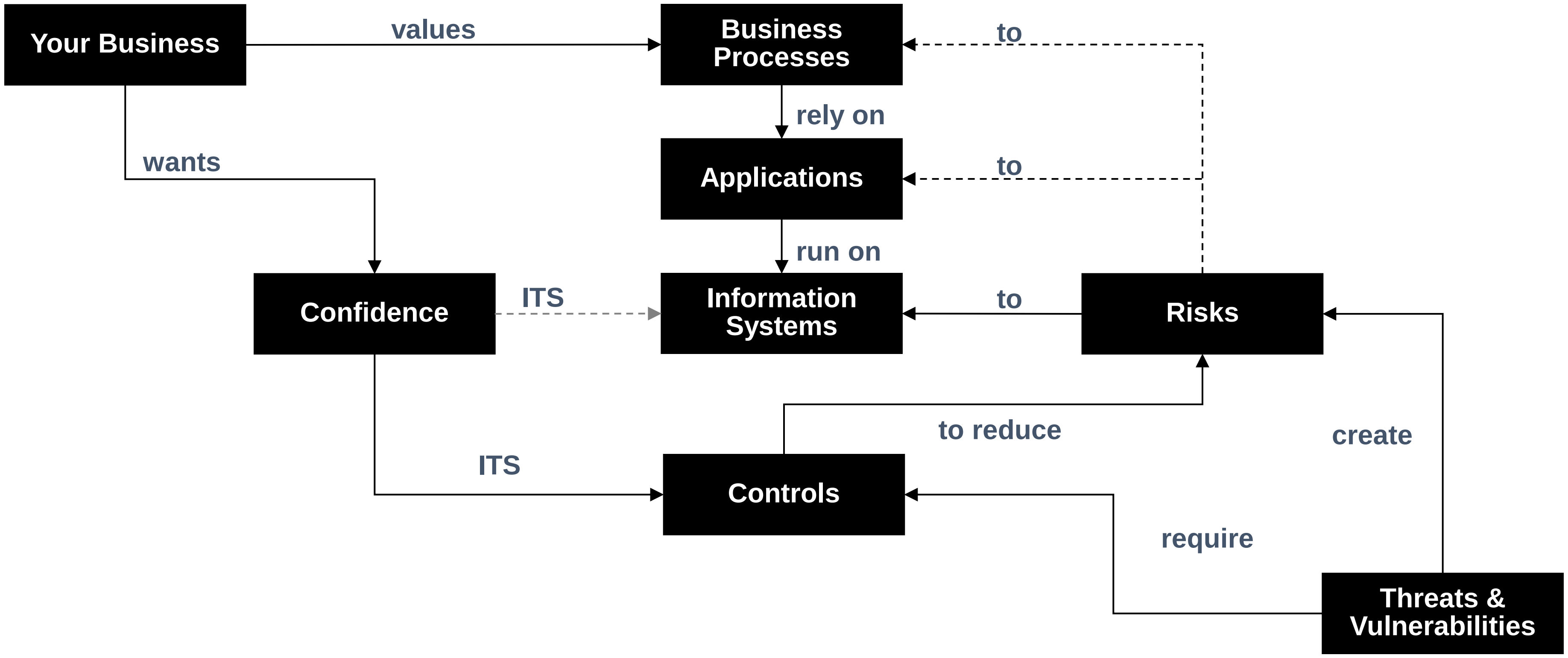
2. Approach to Security is driven from Business Risk down to controls (not by security governed controls up)

- Recommend security controls that are in sync with the Business risk appetite;
- Manage and measure risk and security controls effectiveness, continuously and across the entire organization & 3rd party ecosystem.

3. Industry Aligned Security Strategy Advisory

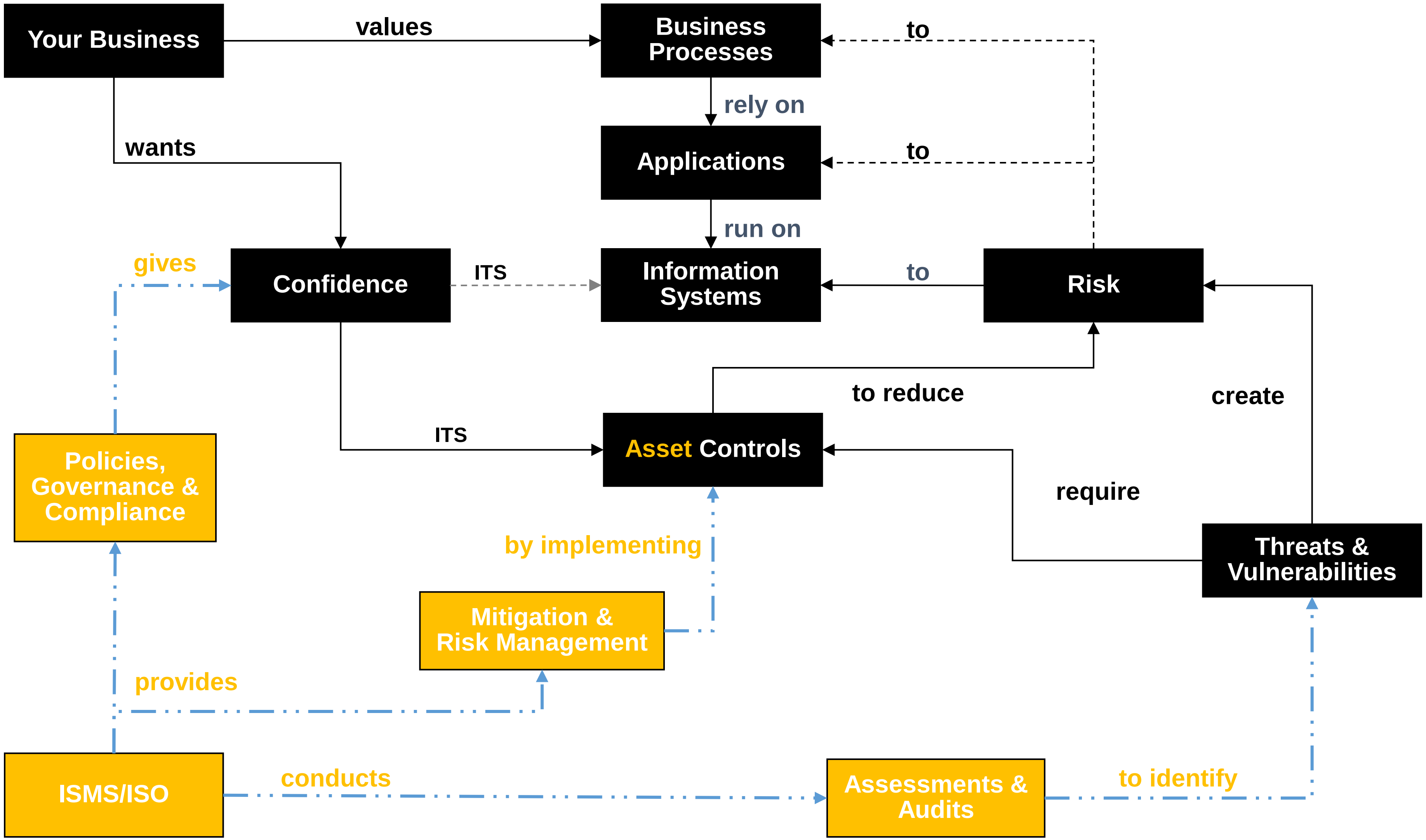
- Advisory by cyber security experts in the companies specific sector, with knowledge of regulation, compliance, and risk appetite for that vertical (e.g. Retail vs. Military vs. Energy vs … etc);

The goals of the security service: reduce risks and increase data confidentiality, integrity and availability of information…



Goals: Reduce risks and increase data confidentiality, integrity and availability

through asset management, policies, governance, compliance, risk management, assessments and audits



Security Maturity Targets

The changing threat landscape means that targets are moving, priorities change as do security budgets. Focus on delivering further maturity improvements in the key areas that reflect Asset Controls and Risk management:

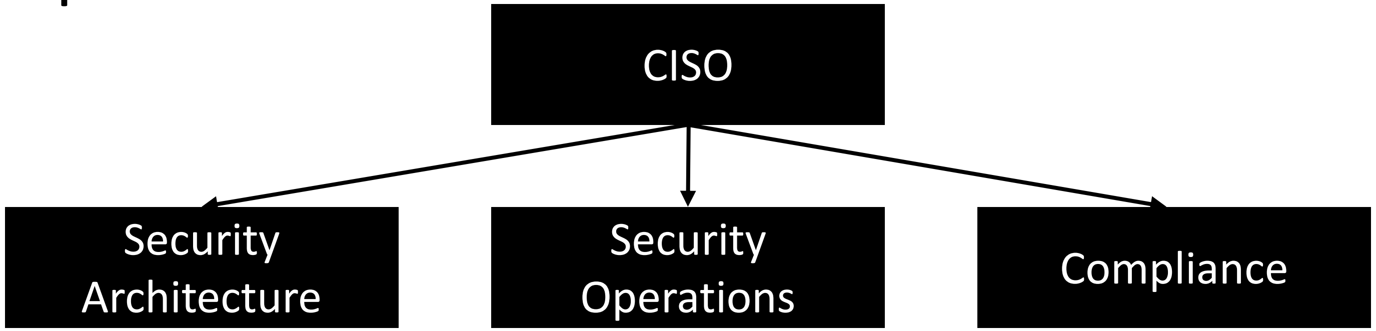
- **Risk Assessment and Treatment** – a key part of security maturity is aligning business benefits with risks. So this is targeted for continuous improvement.
- **Security Organisation** – a mature and focussed security organisation is key to staying one step ahead of the threats and risks posed by the new style of IT.
- **Incident Management** – assuming a "State of Compromise" means having to detect and respond to incidents as early as possible in the attack cycle. Absolutely key area.
- **Asset Management** – not all assets can, or indeed should, be protected to the same degree, so understanding critical assets is a key to responding to attacks.
- **Access Management** – ensuring that access is restricted to those that need access. Ensuring that access, especially privileged user access, is appropriate, monitored and managed. The insider threat is a growing one that cannot be ignored.

Security Framework Development

Older Security Management Framework

Getting this right is absolutely critical if the organisation structure is to be developed that supports an asset centric security model.

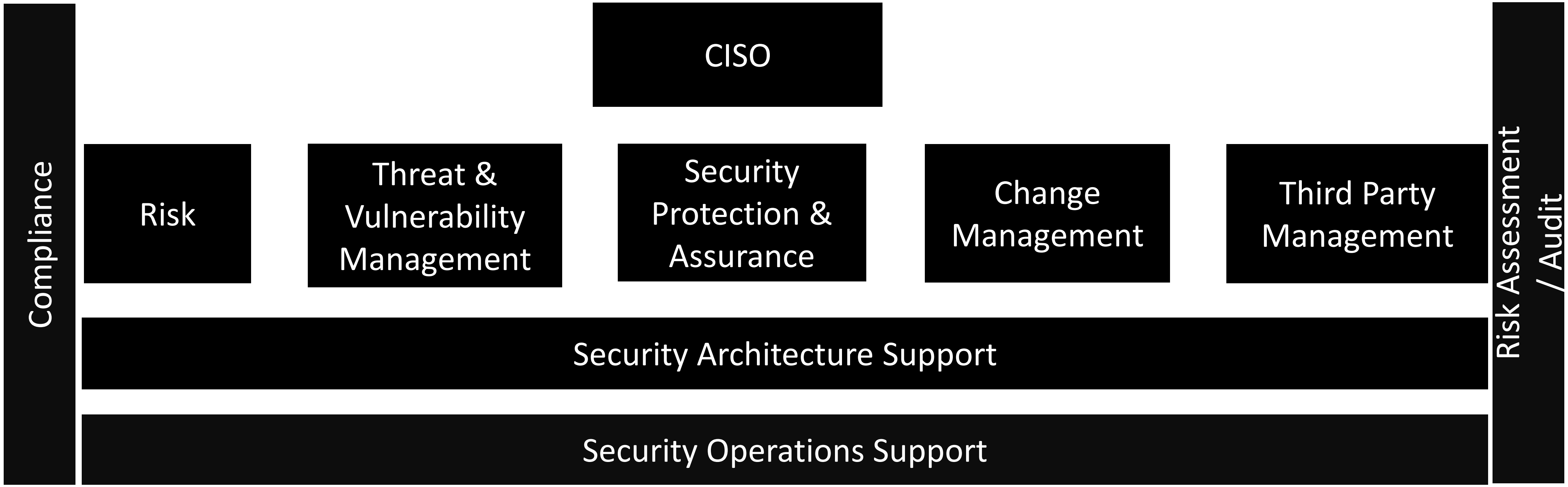
Currently many industries still have a very traditional security structure aligned across traditional operational disciplines:



This model does not really align responsibilities to business requirements but rather enforces (re-enforces) technological demarcation lines

Risk Based Security Management

New model of InfoSec frameworks is GRC managed



CISO
Compliance
Risk
Threat & Vulnerability Management
Security Protection & Assurance
Change Management
Third Party Management
Risk Assessment / Audit
Security Architecture Support
Security Operations Support

In this model, the key business requirements and protection strategies are defined by the central core functions. Architecture and operations support is pooled to support these core functions as required to deliver the strategy.

Risk Based Asset Framework

How information assets are classified, stored, used and deleted. Assessing their importance and the consequent risks.

This Framework aims to define what the key information assets are. This will involve:

- Identifying assets, their location and ownership
- Identifying the relative importance of assets so that risk can be measured and quantified
- Maintaining lifecycle information that could impact on the relative importance of those assets and hence the risk
- Conducting regular risk assessments to ensure that these are up to date and accurate
- Defining and maintaining classification levels

Threat & Vulnerability Management Framework

How threats to information assets are identified and managed

This Framework focuses on threat identification, mitigation, detection and response. This is the preventative, detective and responsive element to complement the protective measures in the Security Framework.

It focusses on:

- Threat intelligence analysis and use case development for detection
- Detective technologies (SOC policy & operating procedures)
- Patch and vulnerability management
- Computer Security Incident Response
- Forensics analysis

Security Controls Framework

How information assets are protected (Compliance requirements)

This framework focuses on the pro-active, ongoing protection of assets. It takes note of:

- Risk assessments
- Compliance requirements (regulatory and legal)
- Contractual requirements

It is on the basis of those that people, process and technology can be aligned to build protective controls that are relevant to the business.

These are not necessarily “product” centric but will involve the requirements definition of products such as firewalls, WAF, NIPS/HIPS, DLP, anti-virus, messaging, web filtering controls, etc.

Also involves security policy, standards and operational procedures.

Change Management / SDLC Engagement

How changes to systems and applications handling information assets are managed

This Framework is all about security engagement in the ongoing lifecycle management of information assets. It addresses the risks posed by such changes and can include:

- Responsibility for all the Security aspects of System Development Lifecycle
- Security requirement definitions for IT projects that involve either new developments or changes to existing infrastructure.
- Security milestones for all IT projects that involve either new developments or changes to existing infrastructure.
- Ongoing engagement and security support for IT projects.
- Ensuring that appropriate risk assessment are commissioned and any required vulnerability assessments are conducted.
- Appropriate review and sign-off on system changes (Change Management)

Third Party Management Framework

How information assets are securely shared with others.

Outsourcing and co-operation agreements with third parties has meant that critical infrastructure and information assets are shared. This Framework addresses the management of the sharing of such information assets and infrastructure. This includes:

- Ensuring that contracts and other working documents clearly define the security controls expected from third parties, aligning with the risk profile of the assets concerned.
- Ensuring that appropriate classification policies are applied by third parties
- Conducting assessments/Audits as required of third party compliance
- Ensuring that risk/vulnerability assessments are conducted when there are changes
- Ensuring that appropriate security incident notification, response and reporting procedures are in place.

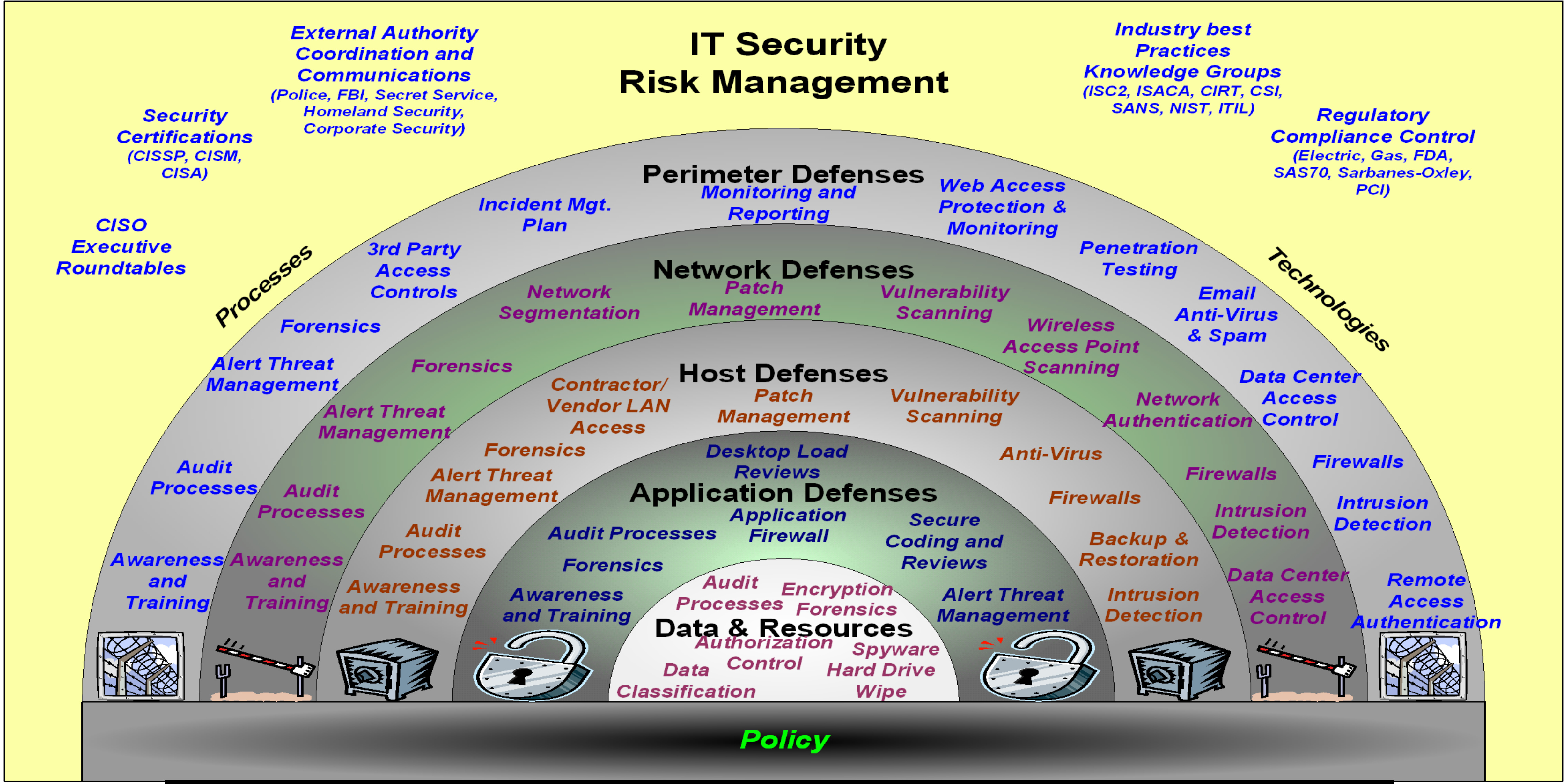
Compliance, Risk Assessment and Audit Framework

How information assets are securely shared with others.

The means of providing assurance to the companies Executive and Governing boards, meeting Regulatory / Compliance groups and provide overall assurance.

- **Compliance;** defines the required awareness and controls as defined by regulatory and government agencies. Aligning to these requirements provide evidence of the companies adherence and assurance management to these controls.
- **Risk Assessment:** is a review and measurement based on the corporate defined controls or those base on best practices (eg, ISO27000 series). This provide a measure of where the company aligns to these standards and where gaps are identified potentially introducing risk to the organization.
- **Audit**

Overall Security Controls



IT Security Risk Management

Security Certifications (CISSP, CISM, CISA)

External Authority Coordination and Communications (Police, FBI, Secret Service, Homeland Security, Corporate Security)

Industry best Practices Knowledge Groups (ISC2, ISACA, CIRT, CSI, SANS, NIST, ITIL)

Regulatory Compliance Control (Electric, Gas, FDA, SAS70, Sarbanes-Oxley, PCI)

CISO Executive Roundtables

Processes

Technologies

Perimeter Defenses

Incident Mgt. Plan

Monitoring and Reporting

Web Access Protection & Monitoring

3rd Party Access Controls

Penetration Testing

Forensics

Email Anti-Virus & Spam

Alert Threat Management

Data Center Access Control

Audit Processes

Firewalls

Intrusion Detection

Awareness and Training

Remote Access Authentication

Network Defenses

Network Segmentation

Patch Management

Vulnerability Scanning

Wireless Access Point Scanning

Forensics

Network Authentication

Alert Threat Management

Firewalls

Audit Processes

Intrusion Detection

Awareness and Training

Data Center Access Control

Host Defenses

Contractor/ Vendor LAN Access

Patch Management

Vulnerability Scanning

Forensics

Anti-Virus

Alert Threat Management

Firewalls

Audit Processes

Backup & Restoration

Awareness and Training

Intrusion Detection

Application Defenses

Desktop Load Reviews

Application Firewall

Audit Processes

Secure Coding and Reviews

Forensics

Awareness and Training

Alert Threat Management

Data & Resources

Audit Processes

Encryption

Forensics

Authorization Control

Spyware

Data Classification

Hard Drive Wipe

Policy

Best Case Scenario

Thank you

Tony Ventura

t2905v@Hotmail.com

44 (0) 7836268193

CISM Certified Information Security Manager
An ISACA Certification

ISO

ISO 27001
Lead Auditor

CISSP Certified Information Systems Security Professional Expired

iisp The Institute of Information Security Professionals