Information Security Strategy Processes

Planning Under Uncertainty

Robert Coles

GSK brands


SENSODYNE
Panadol
FOR COLD RELIEF


Ventolin
Evohaler


GlaxoSmithKline
Seroxat™ CR
paroxetine hydrochloride
30 controlled release tablets
12.5 mg


Horlicks
LIGHT
JUST ADD WATER
Aquafresh
CAVITY PROTECTION +


Augmentin DUO


Flixotide
Diskus
100


IMIGRAN
50
tablets for migraine
2 tablets


Nicorette
MINT
ENO
ENO
ENO
Scott's
EMULSION


Zantac™ injection
25mg/ml
Each 2ml contains
50mg ranitidine (as the hydrochloride)
(25mg/ml)
5x2ml
GlaxoSmithKline

Knowns and unknowns

- There are known knowns. These are things we know that we know. There are known unkowns. This is to say, there are things that we know we don’t know. But there are also unknown unknowns. These are thinks we don’t know we don’t know.
- Donald Rumsfeld

Incidents & Cyber Threat Actors

Hacktivists

Nation-State

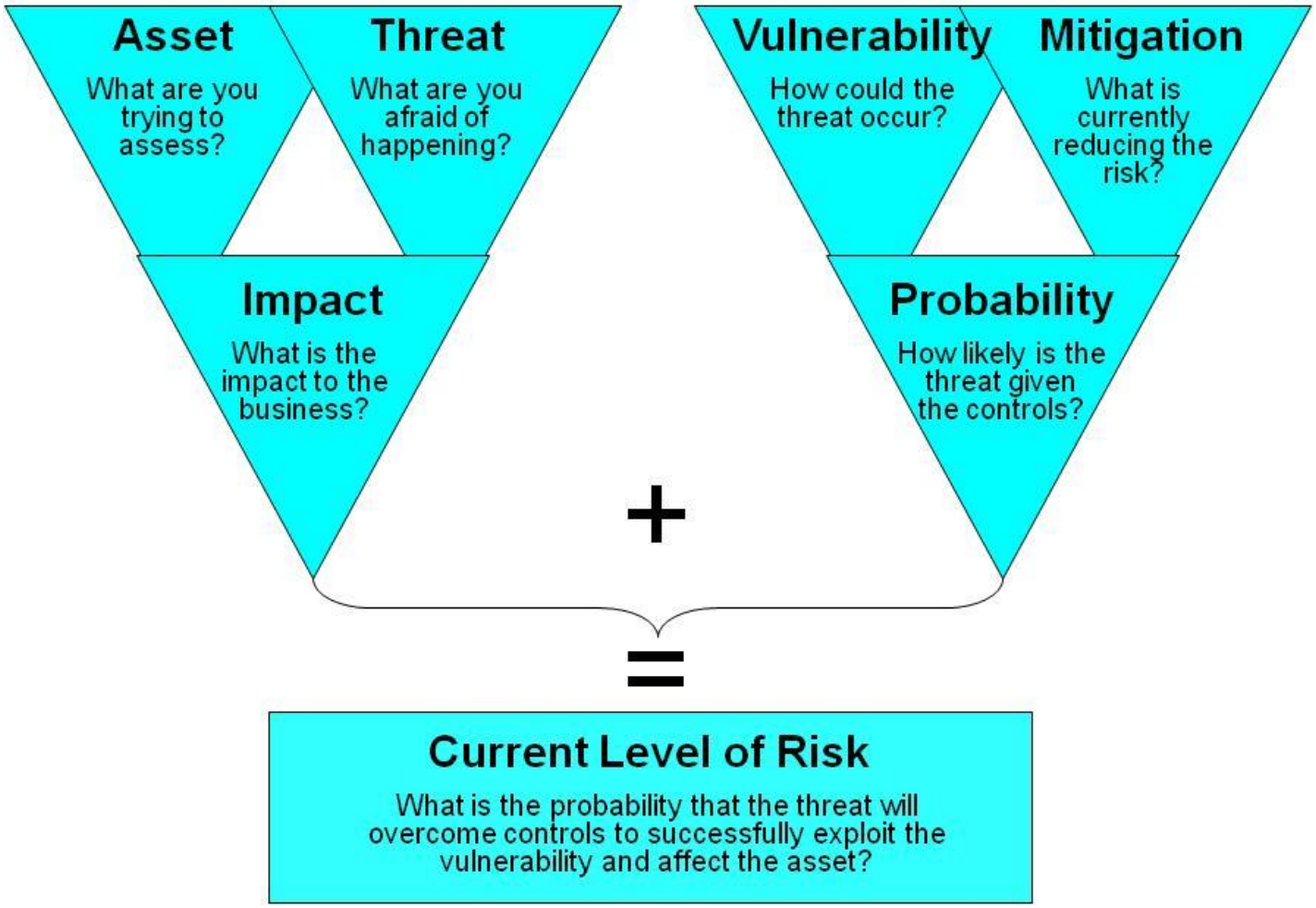
Cyber Terrorism

Organised Crime

Careless Insider

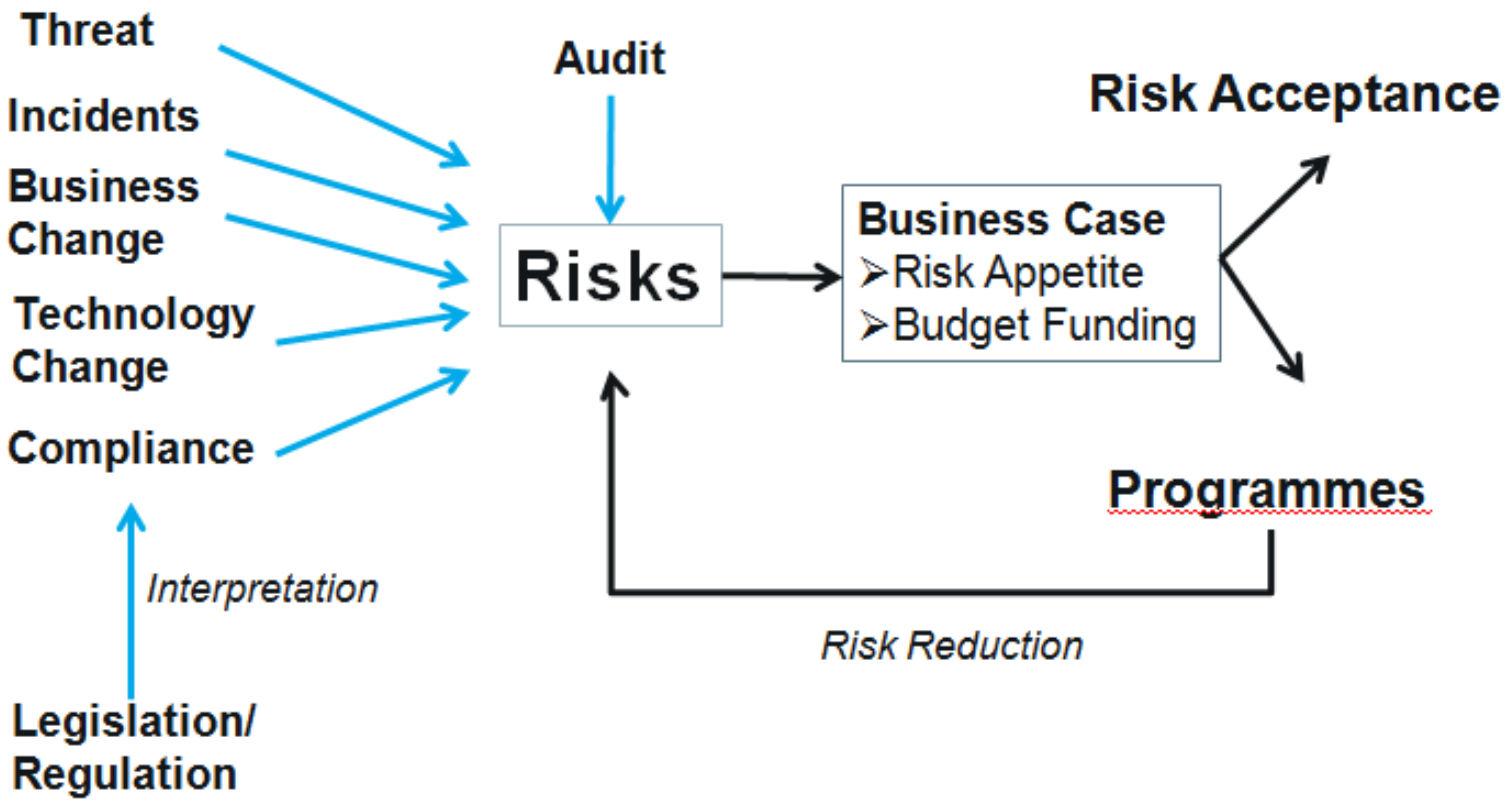
Malicious Insider

Approach – Planning Under Uncertainty



GAISP, ISO27001, COBIT, NIST800-12, SARA, ISRAM, OCTAVE, FRAP, CRAMM, NSA IAM etc

How secure are we?



How much security is enough?

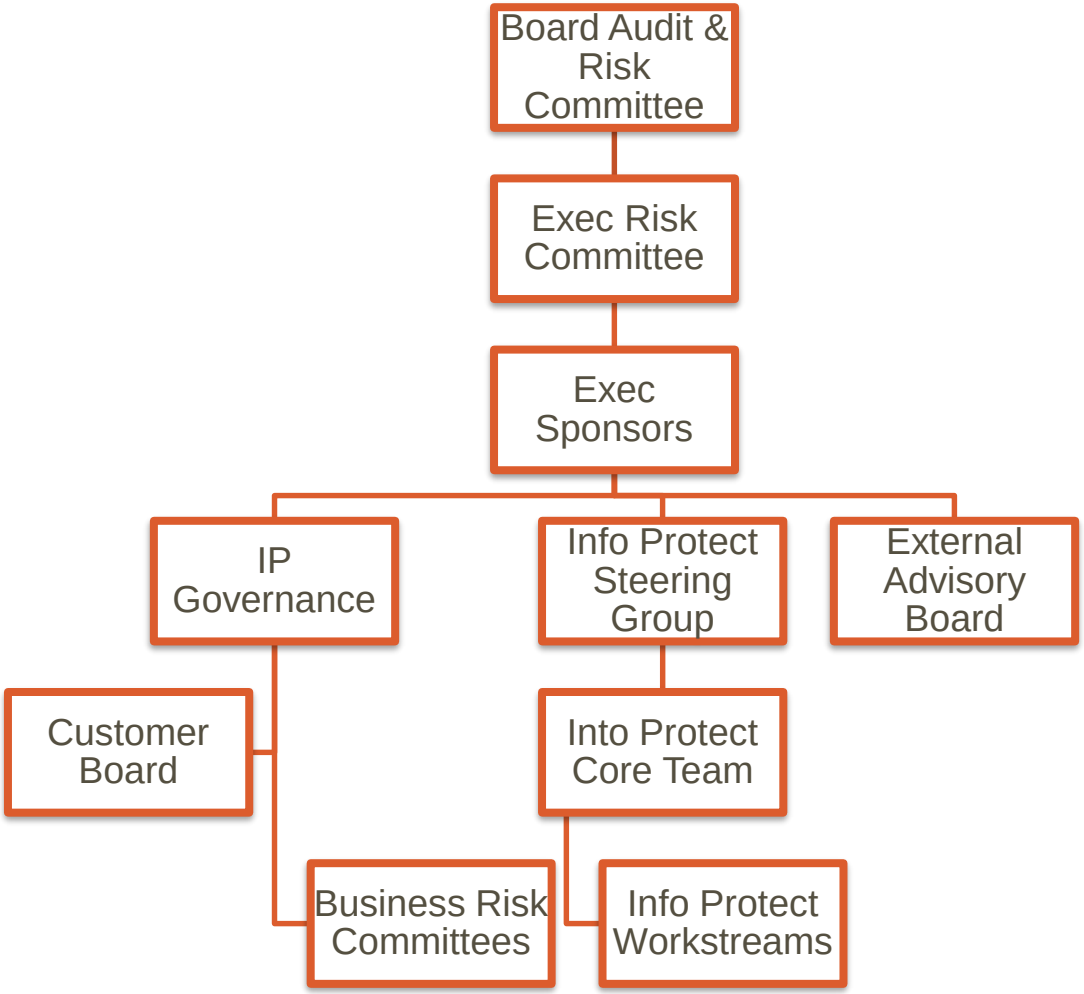
- Acceptability of a risk is proportional to the real and perceived benefits of the activity
- Voluntary risks (eg skiing) roughly 1000 x more acceptable than involuntary risks (eg natural disasters)
- Acceptable level of risk is inversely related to number of persons participating in the activity

- Starr C 1969 “Social Benefit versus Technological Risk”

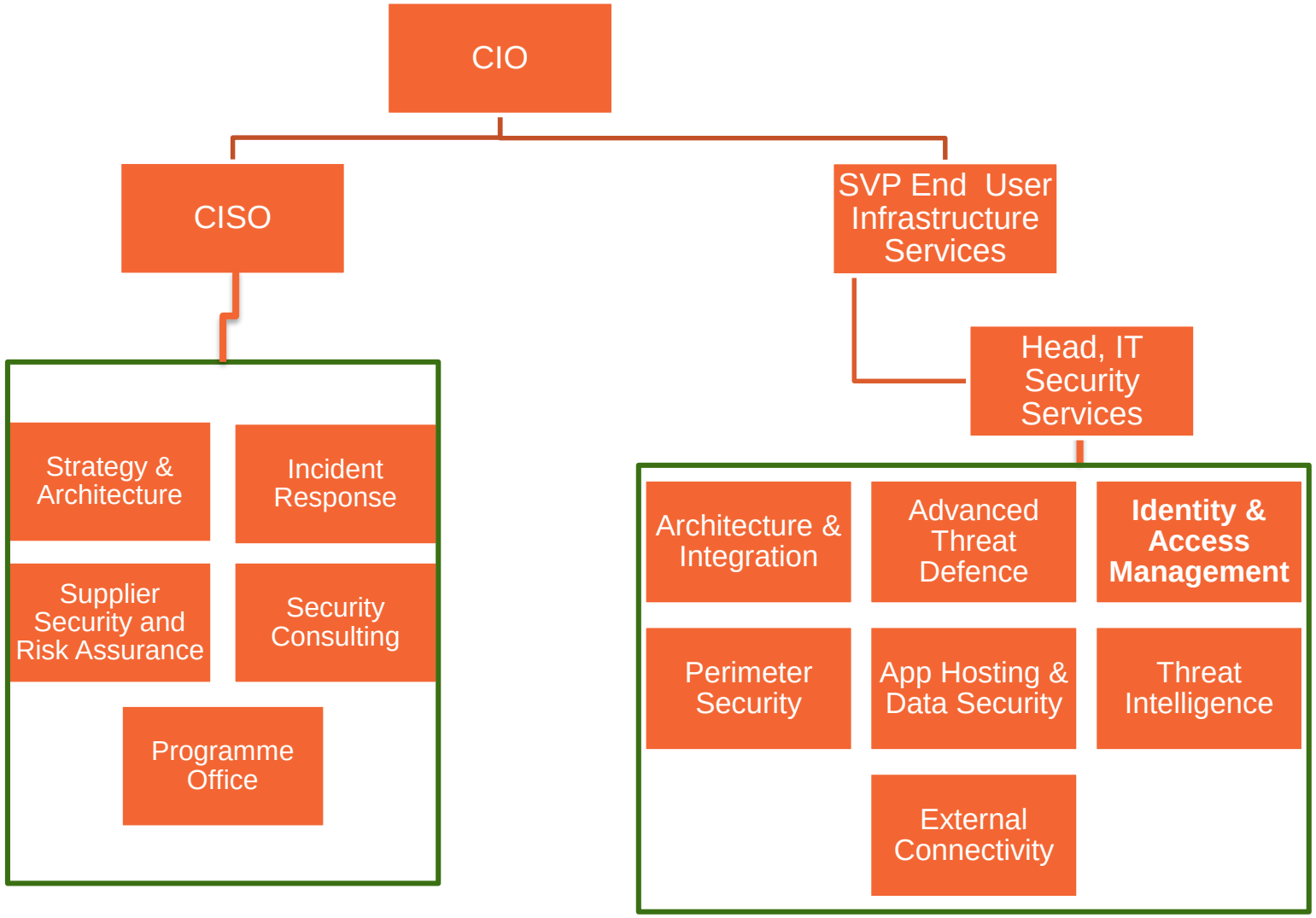
GSK: Strategy Inputs & Security Principles

- External consultants conducted an external and internal information security benchmark using ISO 27001 as the framework and organisational benchmark
- In March 2014, held a 3-day strategy session – 85 people, brainstormed threats using ISF categories and how to reduce risk/improve maturity
- Ran internal skills assessment using IISP skills competencies framework
- Ran 21 workshops covering key assets
- Three key principles for the information security strategy.
  - Right skills
  - Supply and demand
  - Tiering

Governance



Information Security Organisation



Cost vs Risk Ranking

Risk Index > 2	£
Access Management	x
Operational Technology	x

Risk Index > 1.5	£
Application Security	x
Technology	x

Foundational	£
Cultural Change	x
Governance	x

Unknown Unknowns

- Hacking the human
- Machine learning and AI to commoditise hacking
- Machine learning and AI to improve detection of hacks
- Intelligent machines attacking each other – humans as collateral damage
- Security gets so complex that we no longer know how to fix it when it goes wrong – Computer Says No
- Quantum computing will allow the breaking of all current encryption methods
- Sentient robots will reflect human society
- Obliteration of privacy – items of interest will be located, identified, monitored and remotely controlled (David Patraeus)