ExecIA LLP

Excellence in Information Assurance

The Cynic's Guide to Information Security

Jeremy Ward
ExecIA LLP

The Cynic’s Guide to Information Security

Technology:

- Technology is more likely to be part of the problem than part of the solution.
- There is no such thing as a “quick technology fix”.
- All technology will eventually be abused.

People:

- All instructions will be misunderstood, or ignored.
- People do the easiest thing, even if they suspect it’s wrong.
- No one reports the whole truth, and nothing but the truth, to a survey or audit.

Failure:

- Stage 1: deny it happened.
- Stage 2: blame someone else.
- Stage 3: find an excuse.

General:

- “Unknown unknowns” will happen.
- If you weren’t looking, how do you know what really happened?

Technology Implementation

- Why?
  - Does it address a risk?
  - Does it meet a business need?
  - Is it required by an auditor?
  - Or is it just a neat idea?
- How?
  - Can it be done in-house?
  - Can it be outsourced?
  - Will it impact on existing technologies?
  - Can it be maintained?
  - Will it last?
- When?
  - Bleeding edge or catch-up?
  - Or can existing technology do the job?

Uses and Abuses of Technology

- Marketing v. Reality:
  - “Threats” are often marketing opportunities
  - Solutions are often technology in search of a problem
  - Vendors are often economical with the truth.
- Any new technology is a “niche” to be exploited
  - Think of: floppy discs; email; online banking; social networking etc.
- Any existing technology will be abused:
  - Security protections circumvented
  - Used for non-authorised purposes
  - “Tested” to destruction.

People Issues

- Culture and Experience
- Principles versus Rules
- Understanding versus Coercion
- Realism versus Idealism
- Measurement versus Guesswork
- Strategy versus Tactics

ExecIA Survey

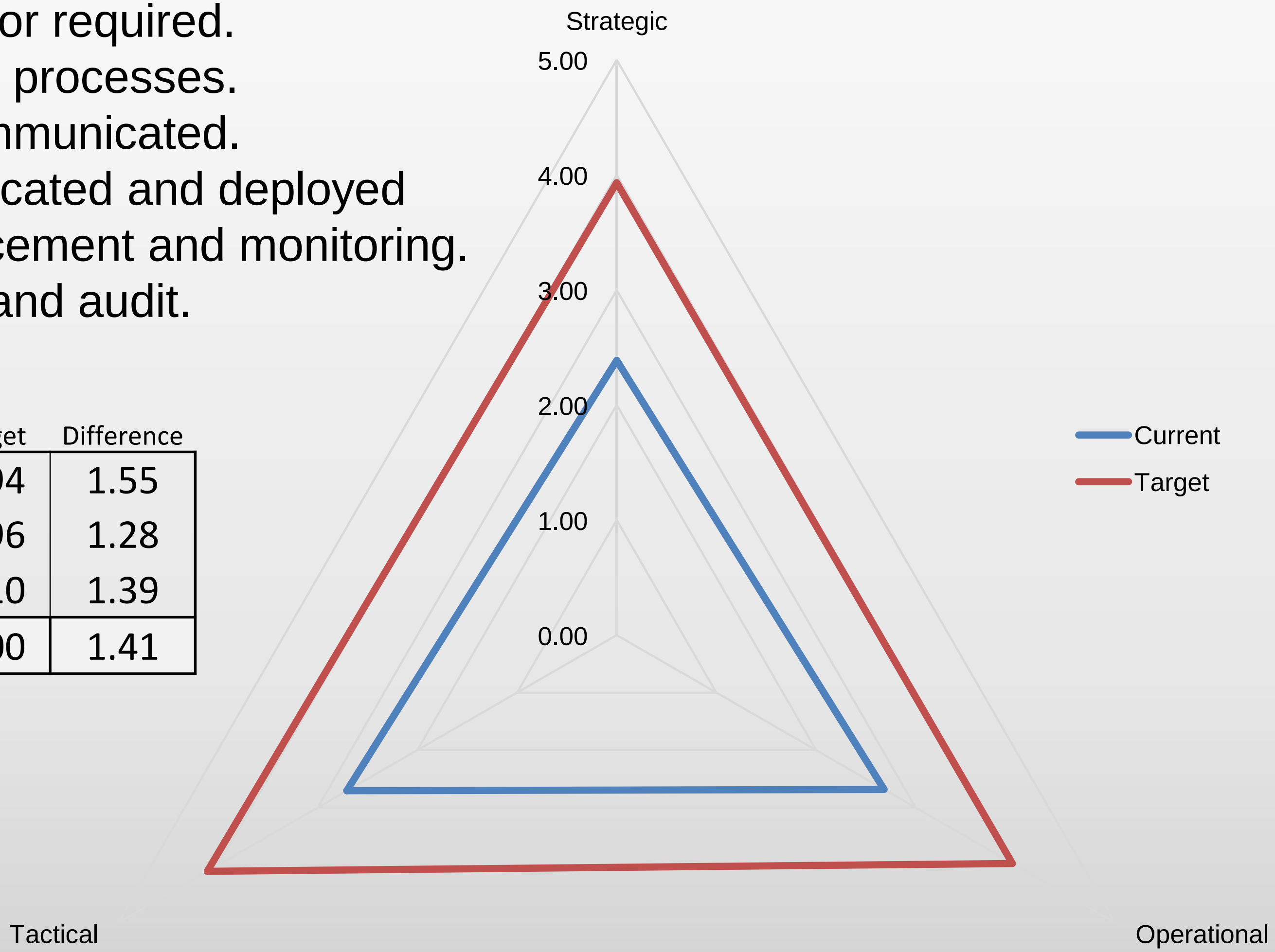
- December 2010
- 20 UK companies (large or very large)
- Banking and finance, retail, transport, IT services and government.
- 31 control areas self-assessed
- 3 control groups:
  - Strategic (alignment with GRC)
  - Operational (delivery of efficiency and effectiveness)
  - Tactical (technical building-blocks)
- Current and Target Capability Maturity
- 5-level Capability Maturity

Survey Findings – Overall Results

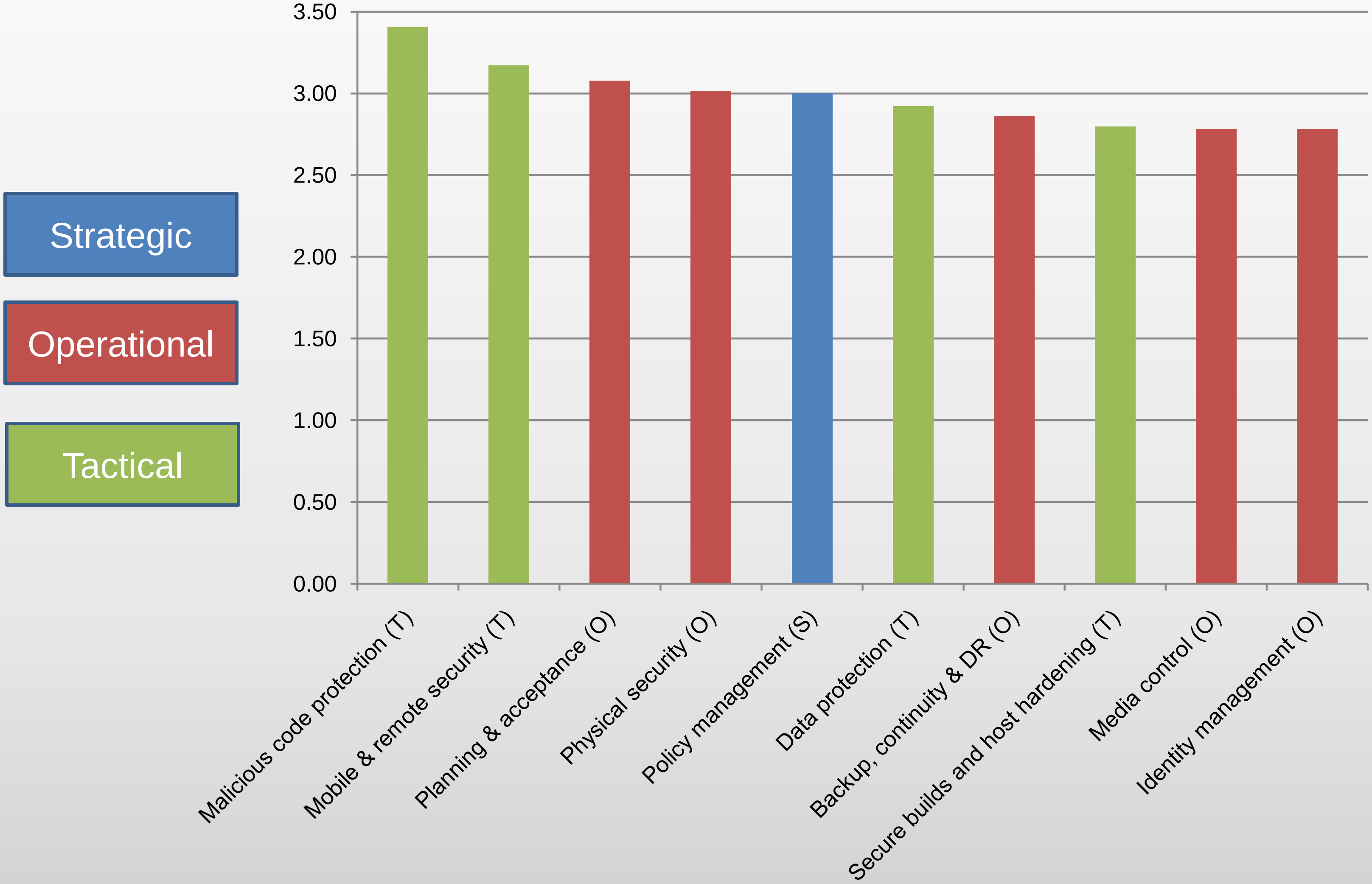
Maturity Levels:

0. Processes not present or required.
1. Ad-hoc, undocumented processes.
2. Processes not fully communicated.
3. Documented, communicated and deployed
4. Regular training, enforcement and monitoring.
5. Automated monitoring and audit.

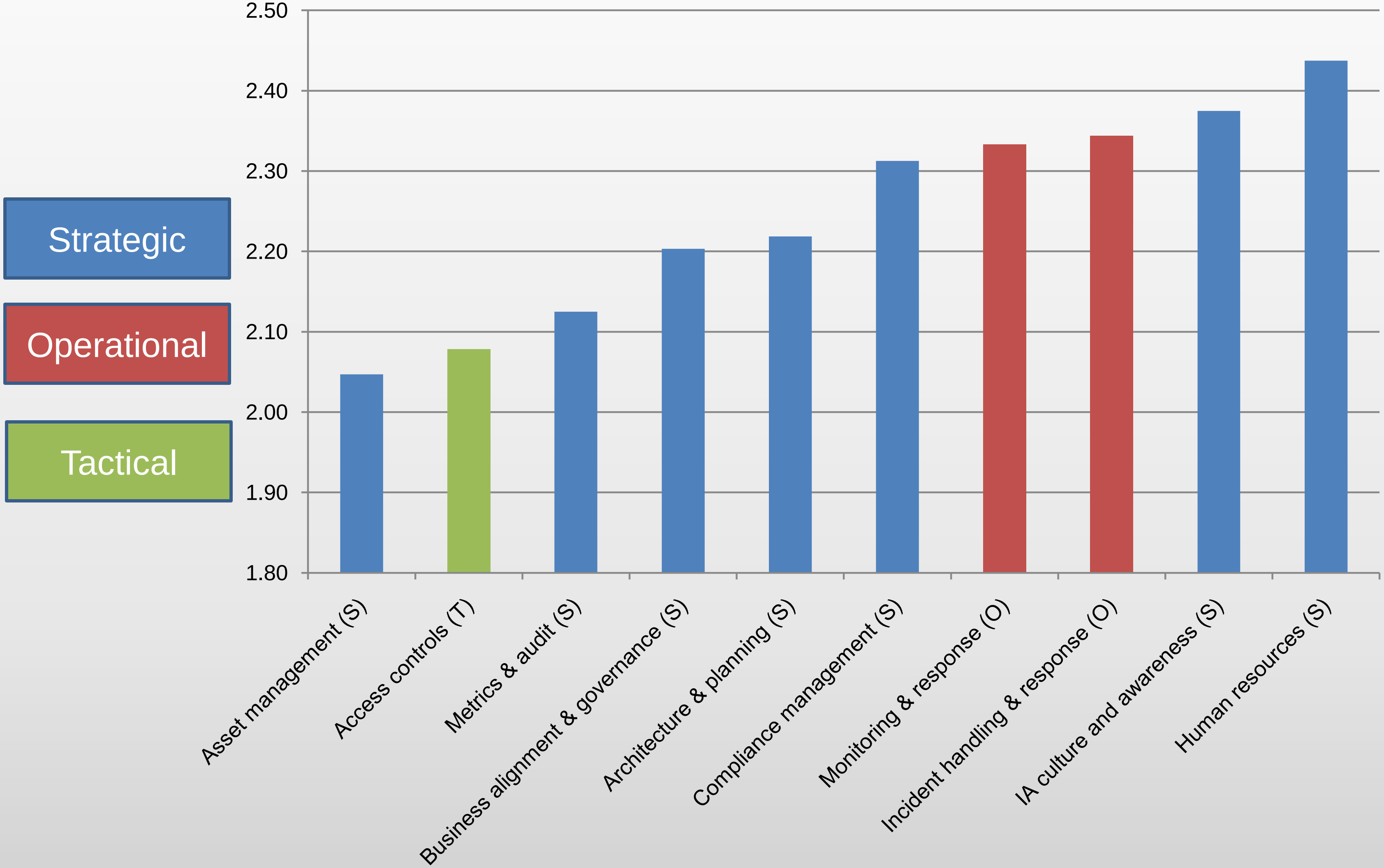
	Current	Target	Difference
Strategic	2.39	3.94	1.55
Operational	2.68	3.96	1.28
Tactical	2.71	4.10	1.39
Overall	2.59	4.00	1.41



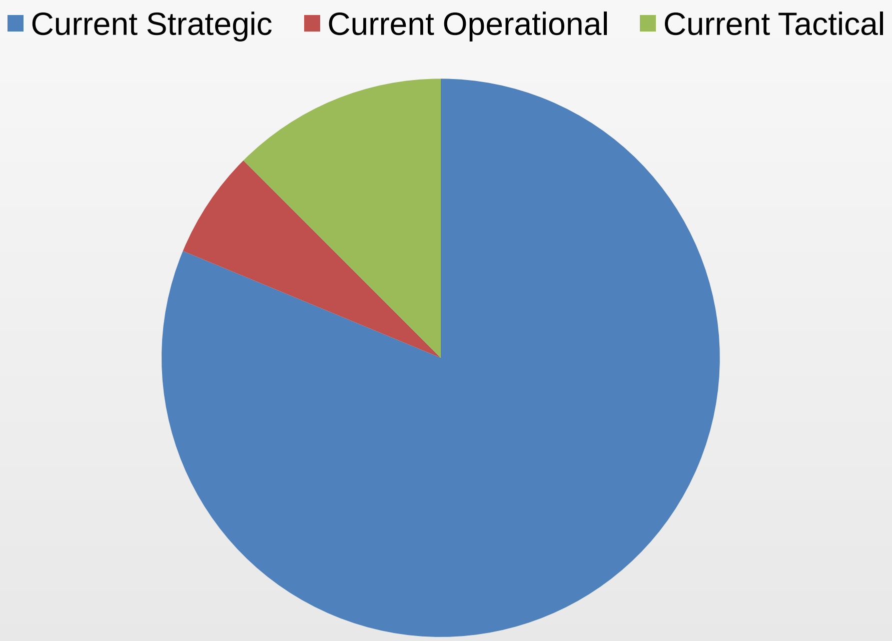
Top 10 Most Mature Controls

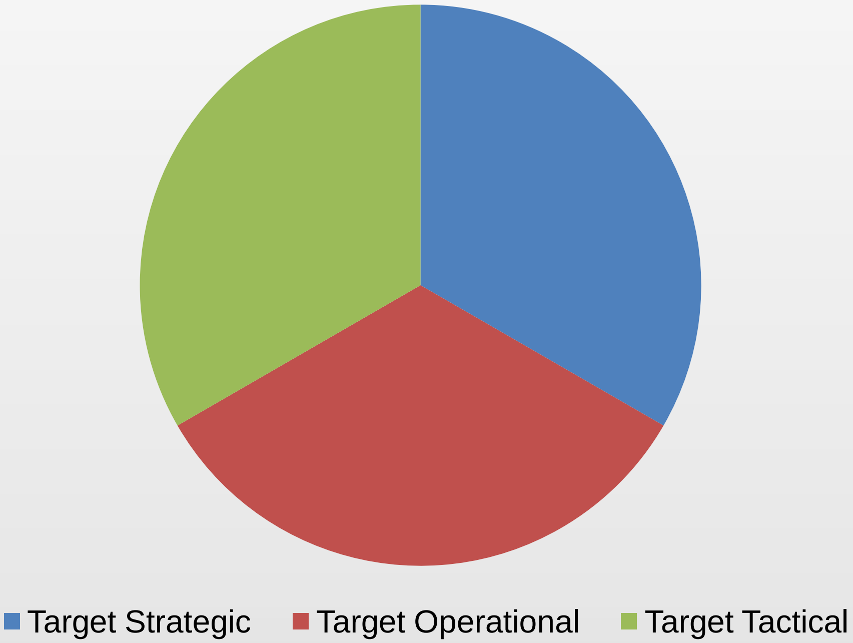


10 Least Mature Controls



Hope over Experience – Development of Strategy

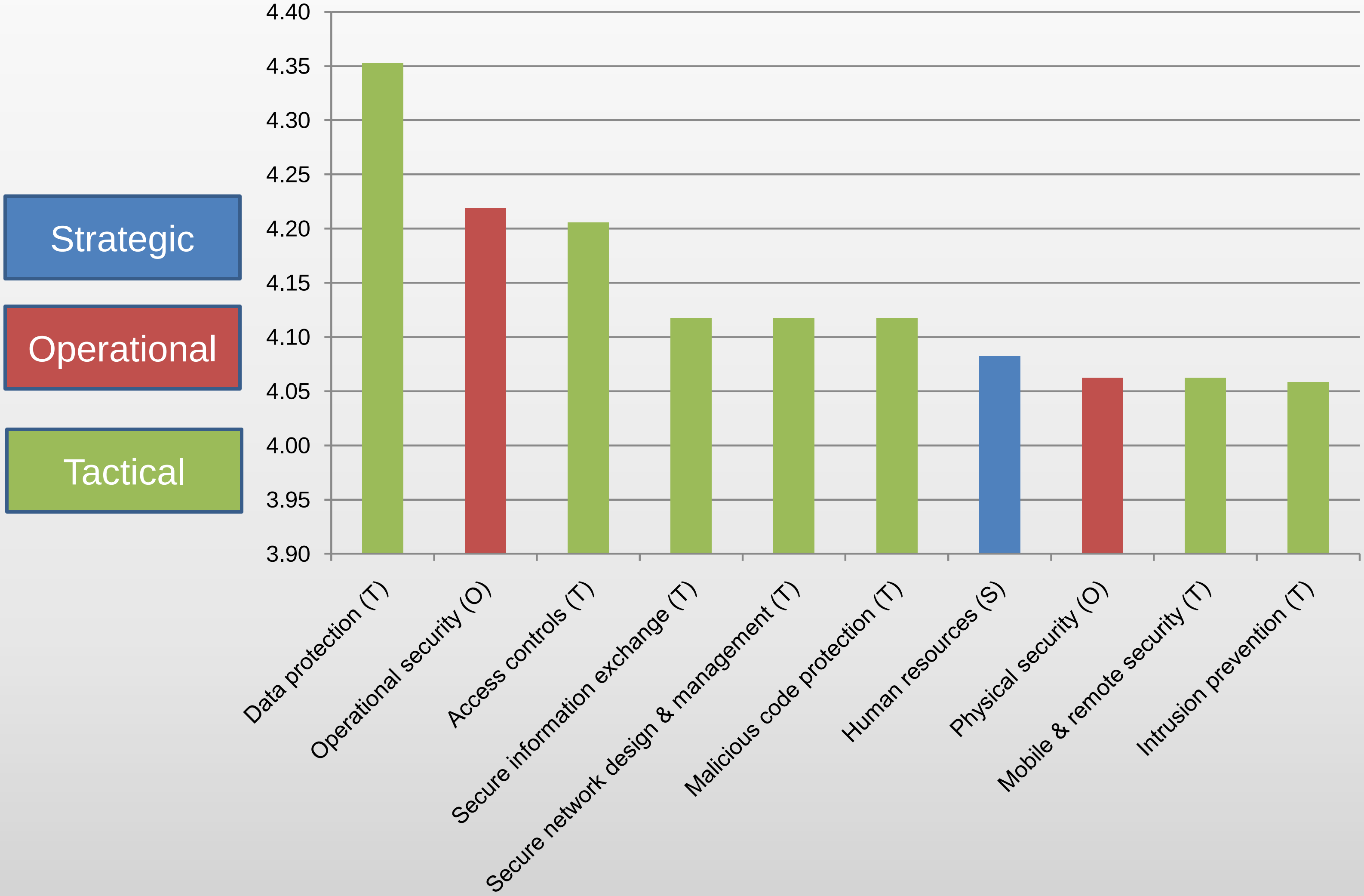




Number of respondents where relevant control group is assessed as **least** mature

Number of respondents where relevant control group is targeted to be **most** mature

Top 10 Target Controls

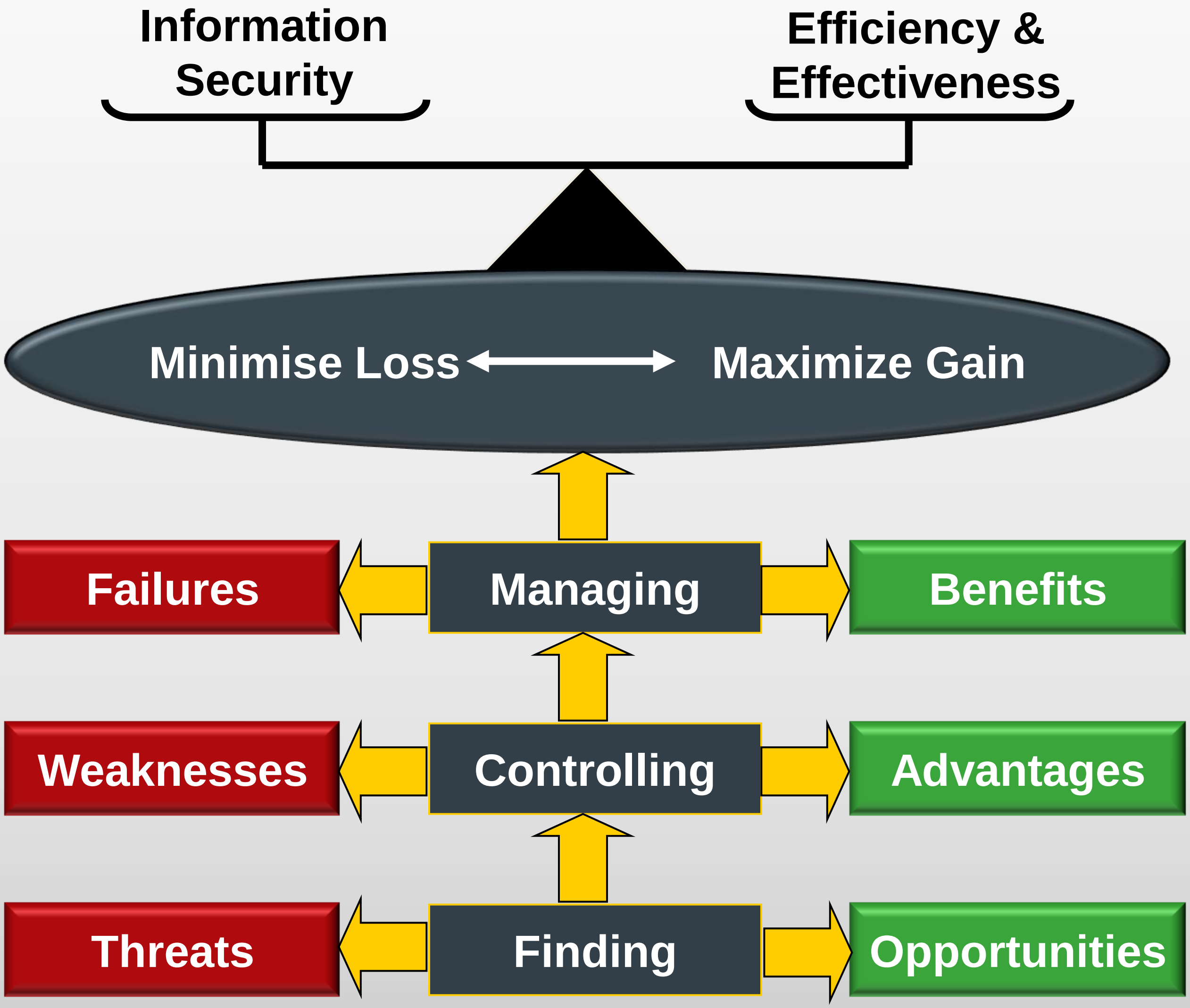


Top 10 Maturity Issues

Rank	Control Area	Average Current Maturity	Average Target Maturity	Difference
1	Access controls (T)	2.08	4.21	2.13
2	Asset management (S)	2.05	3.97	1.92
3	Metrics & audit (S)	2.13	3.97	1.85
4	Incident handling & response (O)	2.34	4.03	1.69
5	Architecture & planning (S)	2.22	3.88	1.66
6	Human resources (S)	2.44	4.08	1.64
7	Compliance management (S)	2.31	3.94	1.63
8	Operational security (O)	2.59	4.22	1.63
9	Intrusion prevention (T)	2.44	4.06	1.62
10	Remote & extranet coverage (T)	2.45	4.06	1.61

On average, respondents shared 58% of the top 10 maturity issues

Balanced Risks


Information Security

Efficiency & Effectiveness

Minimise Loss ↔ Maximize Gain

Failures

Managing

Benefits

Weaknesses

Controlling

Advantages

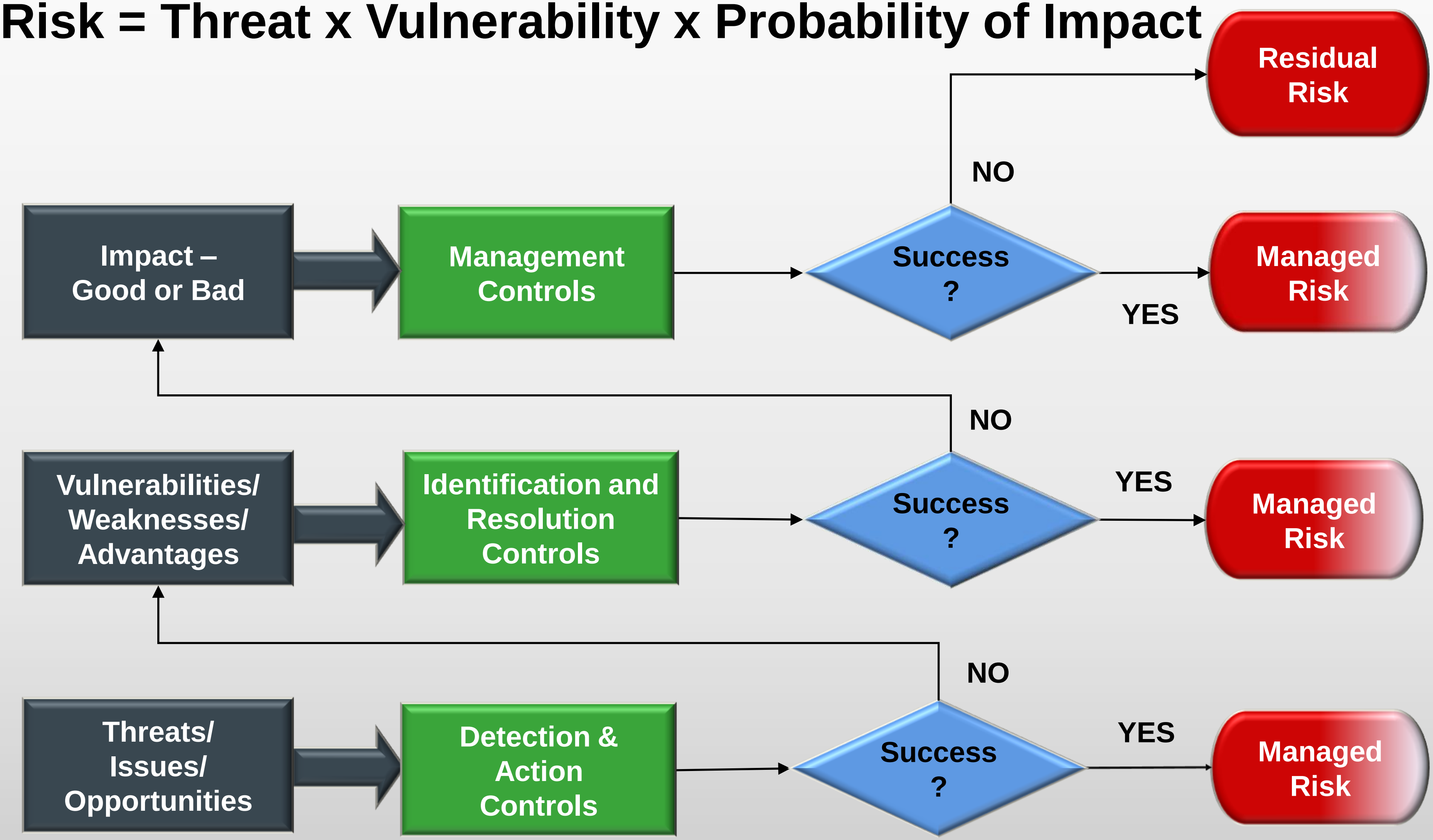
Threats

Finding

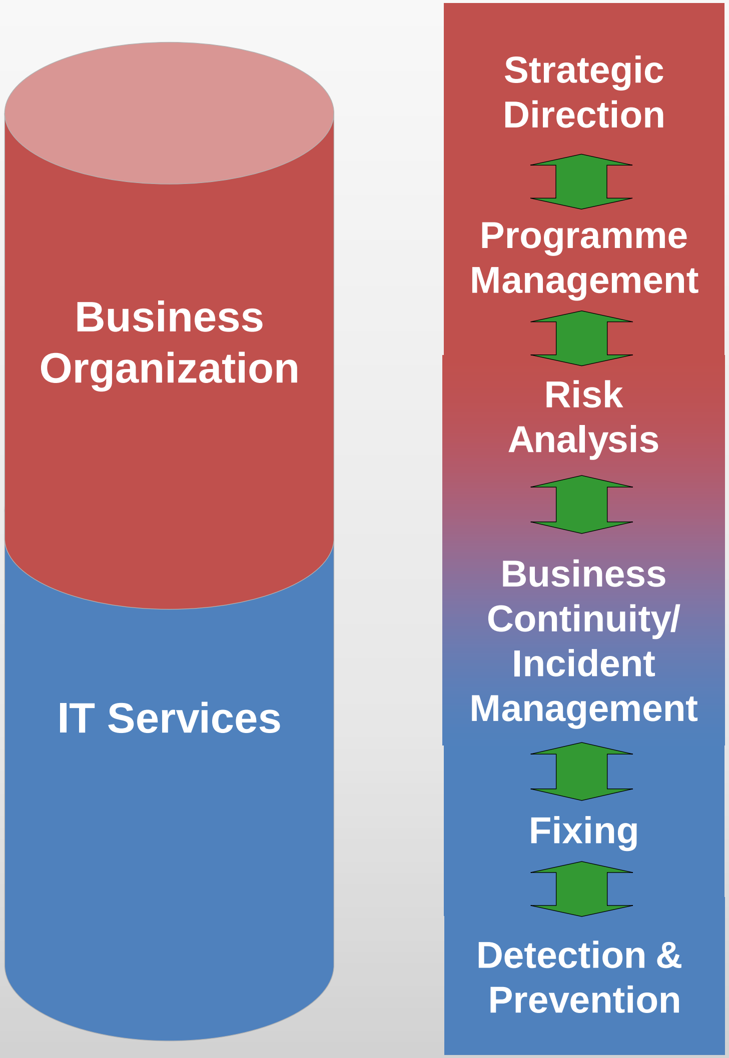
Opportunities

Managing Risk

Risk = Threat x Vulnerability x Probability of Impact

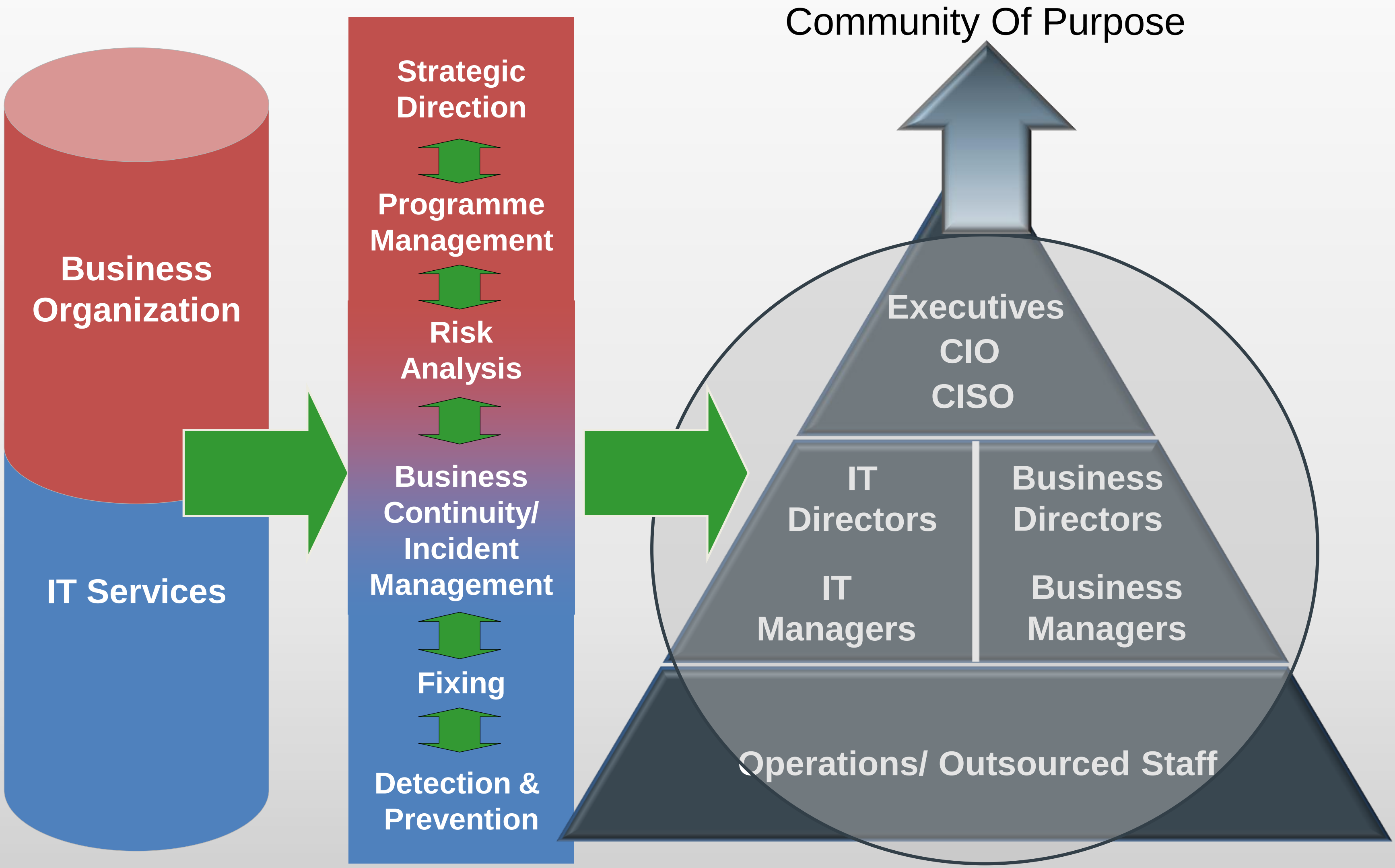

Residual Risk
NO
Impact – Good or Bad
Management Controls
Success ?
Managed Risk
YES
NO
Vulnerabilities/ Weaknesses/ Advantages
Identification and Resolution Controls
Success ?
YES
Managed Risk
NO
Threats/ Issues/ Opportunities
Detection & Action Controls
Success ?
YES
Managed Risk

Six Layers of Risk Management

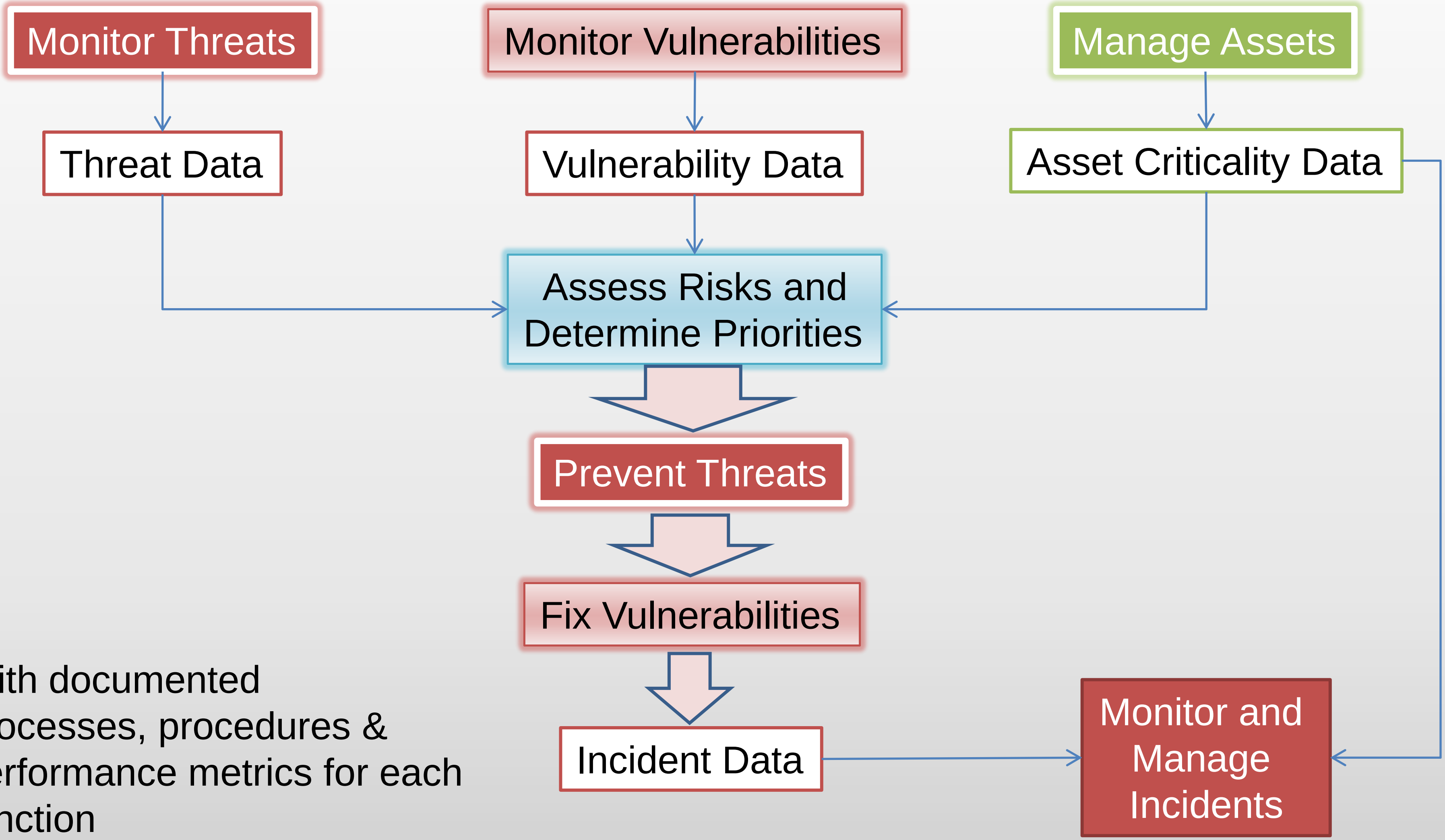


With ***information*** flow between the 6 layers

Effective Risk Management Delivers a "Community of Purpose"

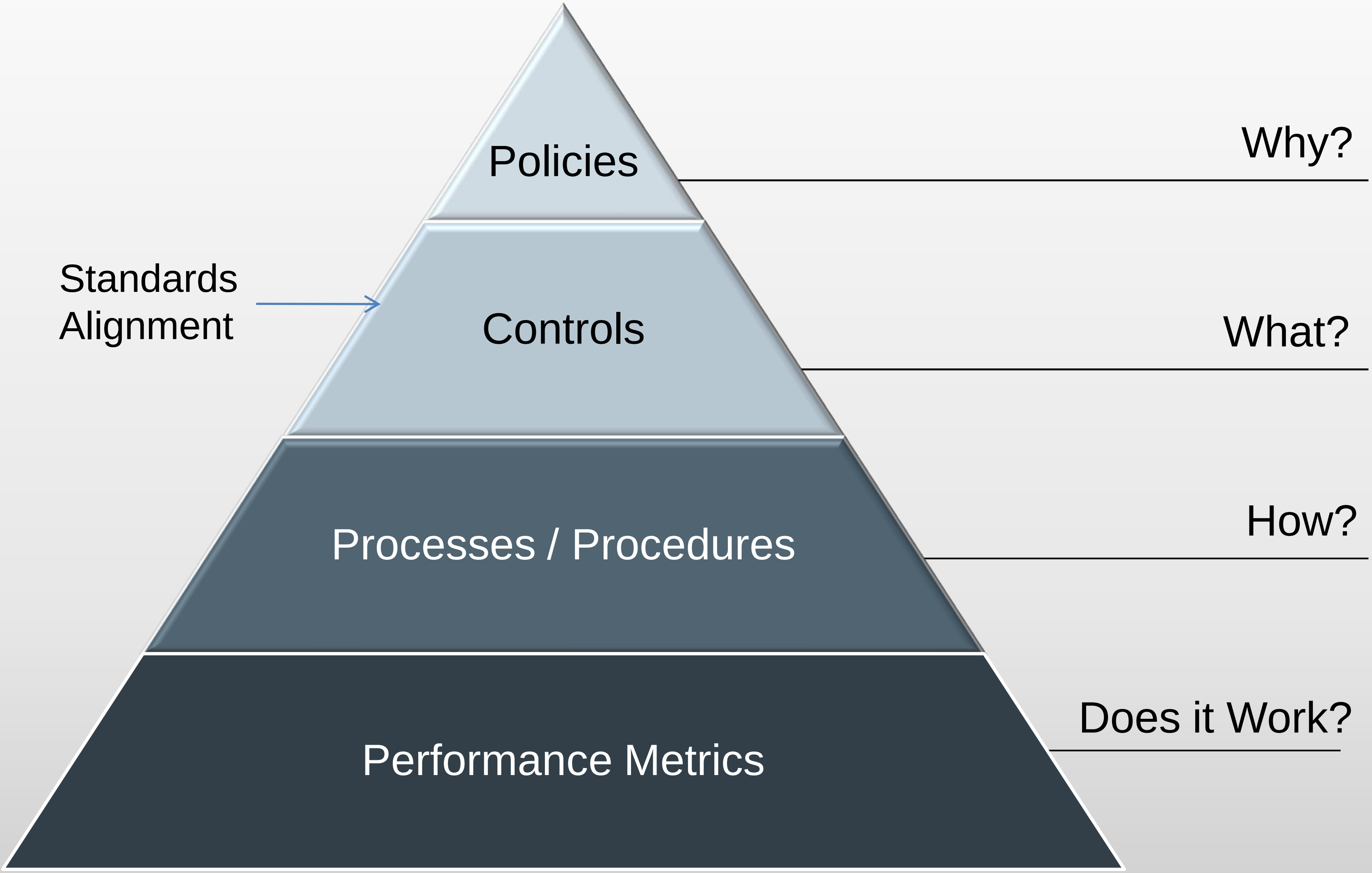


Security Operations – A functional model



With documented processes, procedures & performance metrics for each function

In a Clear Framework



Standards Alignment

Policies

Why?

Controls

What?

Processes / Procedures

How?

Performance Metrics

Does it Work?

The 3-Phase Solution

- Phase 1: Have a strategy.
- Phase 2: Measure the outcome.
- Phase 3: Make adjustments.

ExecIA LLP

Excellence in Information Assurance

Thank-You

jeremy.ward@execia.com