# Cyber Security Issues and Plans

Ian Keller
ian@thereef.co.za
0714925765

# Discussion topics

Cyber Threat Management - Pros and Cons of Outsourcing

Information Security Roadmap Implementation

What are the top 10 Desktop, Server & Network Quick Fixes for Dramatically Increasing Security Across an Organisation

# Cyber Threat Management
# What can be outsourced?

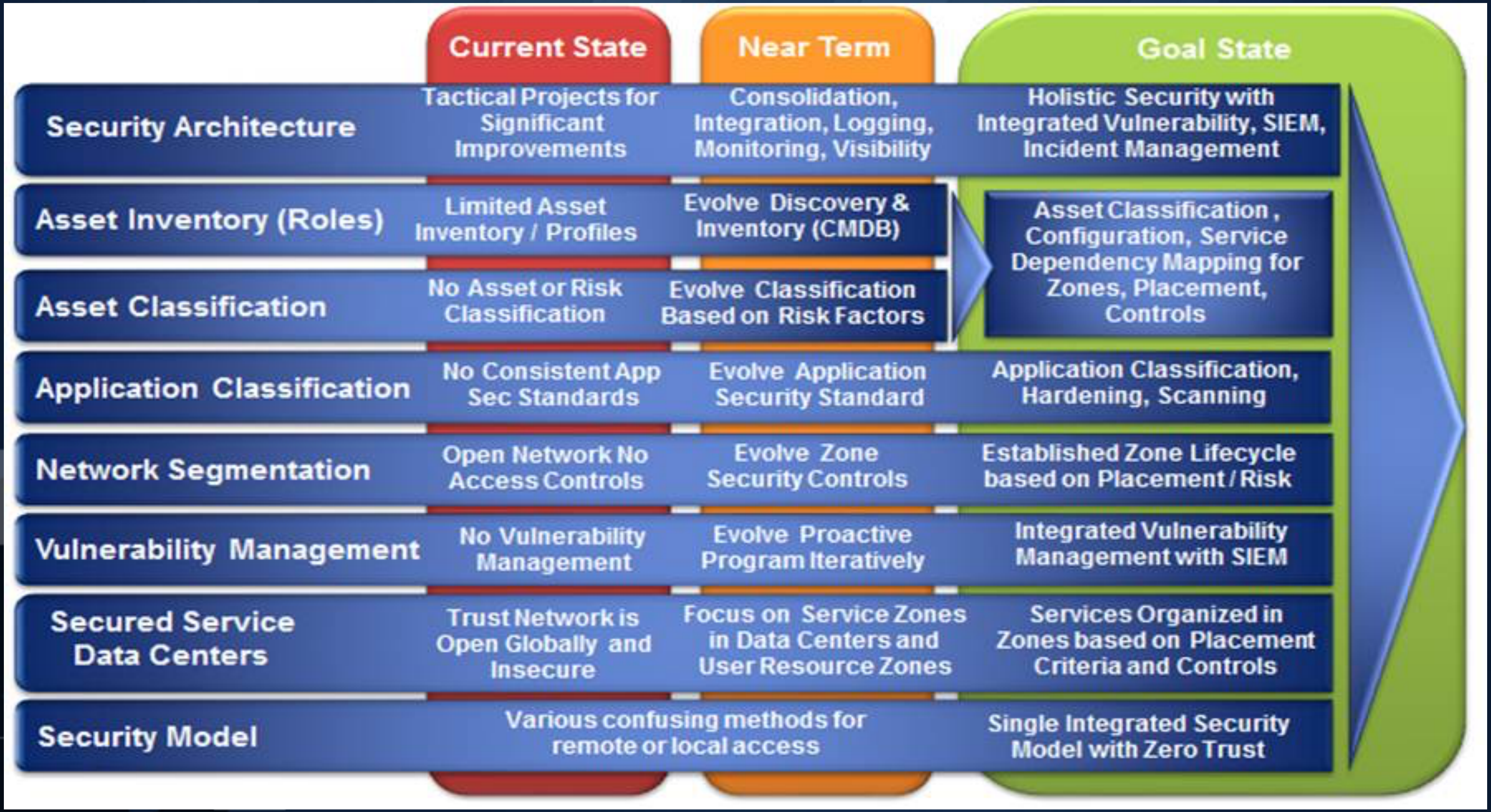
- Penetration Testing & Vulnerability Assessments
- Cyber Threat Intelligence
- Public Key Infrastructure (PKI)
- Firewall Management
- DDOS Protection
- Security Event Monitoring (SIEM / SOC)
- Cloud / Web Security
- eMail Security
- Log Management and Retention
- Authentication
- Vulnerability Scanning

# Cyber Threat Management - Pros and Cons of Outsourcing

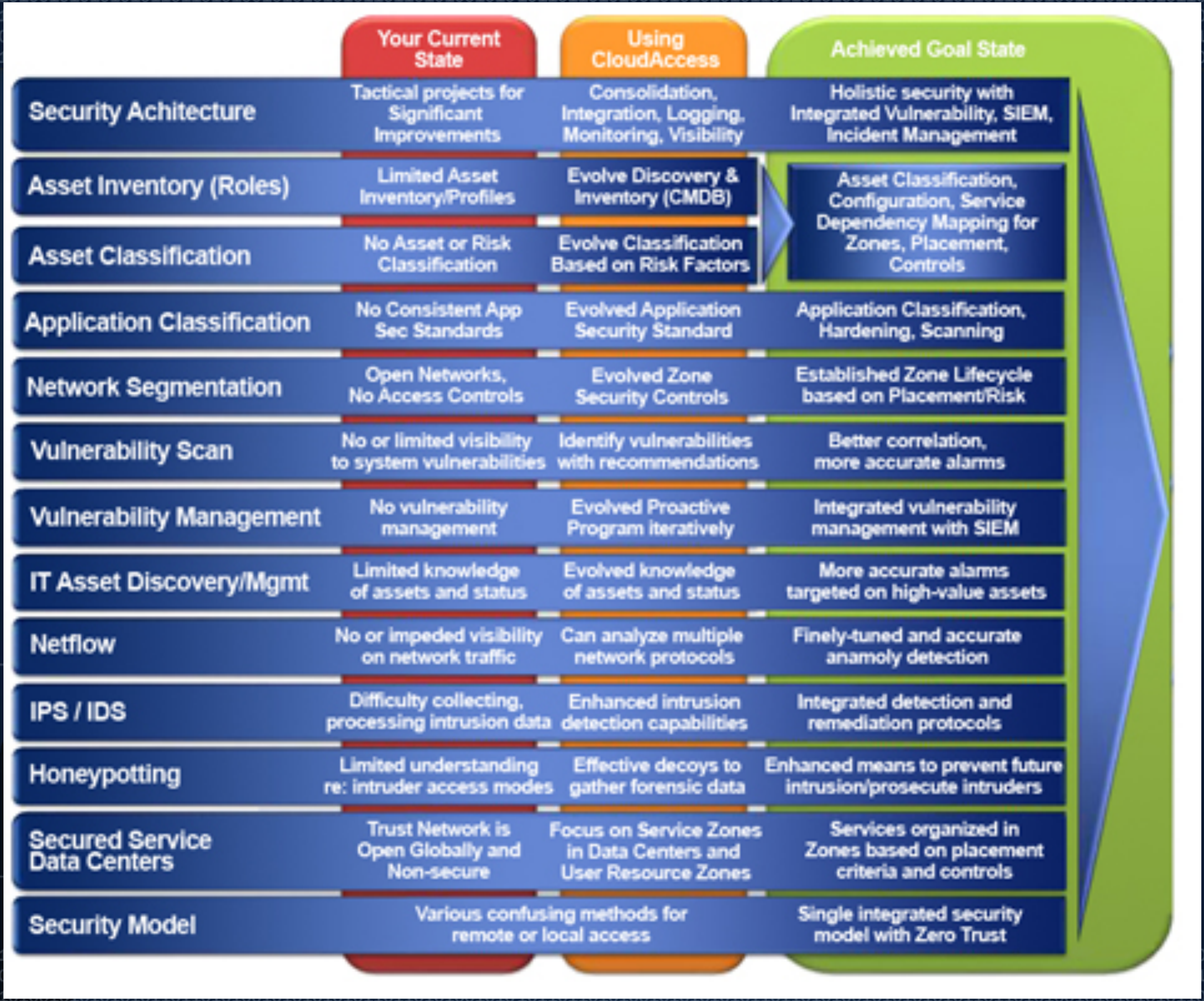
- Pro's
  - Access to Advanced Skills and Expertise
  - 24*7*365 Monitoring and staffing
  - Proactive vs reactive approach
  - Cost Savings
  - Access to updated knowledge base
  - Actionable *localized* Threat Intelligence

- Con's
  - Massive skills shortage;
  - Large number of staff required to run (SIEM / SOC requires 3 to 4 shifts)
  - Will take a long time to entrench and mature process.
  - Cost Prohibitive
  - Retaining skilled staff

# The Security Roadmap

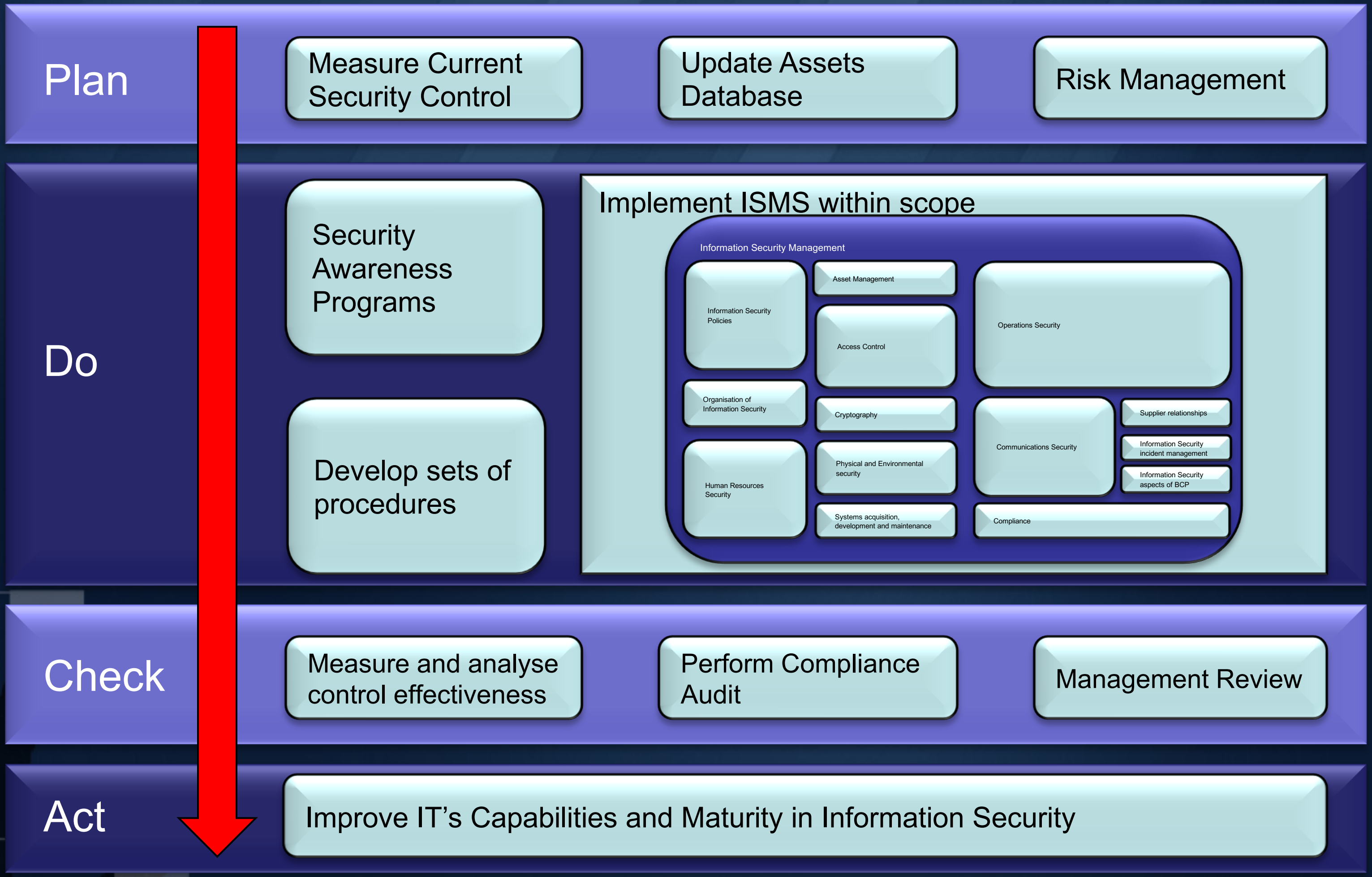


| | Current State | Near Term | Goal State |
|---|---|---|---|
| Security Architecture | Tactical Projects for Significant Improvements | Consolidation, Integration, Logging, Monitoring, Visibility | Holistic Security with Integrated Vulnerability, SIEM, Incident Management |
| Asset Inventory (Roles) | Limited Asset Inventory / Profiles | Evolve Discovery & Inventory (CMDB) | Asset Classification, Configuration, Service Dependency Mapping for Zones, Placement, Controls |
| Asset Classification | No Asset or Risk Classification | Evolve Classification Based on Risk Factors | |
| Application Classification | No Consistent App Sec Standards | Evolve Application Security Standard | Application Classification, Hardening, Scanning |
| Network Segmentation | Open Network No Access Controls | Evolve Zone Security Controls | Established Zone Lifecycle based on Placement / Risk |
| Vulnerability Management | No Vulnerability Management | Evolve Proactive Program Iteratively | Integrated Vulnerability Management with SIEM |
| Secured Service Data Centers | Trust Network is Open Globally and Insecure | Focus on Service Zones in Data Centers and User Resource Zones | Services Organized in Zones based on Placement Criteria and Controls |
| Security Model | Various confusing methods for remote or local access | | Single Integrated Security Model with Zero Trust |



| | Your Current State | Using CloudAccess | Achieved Goal State |
|---|---|---|---|
| Security Achitecture | Tactical projects for Significant Improvements | Consolidation, Integration, Logging, Monitoring, Visibility | Holistic security with Integrated Vulnerability, SIEM, Incident Management |
| Asset Inventory (Roles) | Limited Asset Inventory/Profiles | Evolve Discovery & Inventory (CMDB) | Asset Classification, Configuration, Service Dependency Mapping for Zones, Placement, Controls |
| Asset Classification | No Asset or Risk Classification | Evolve Classification Based on Risk Factors | |
| Application Classification | No Consistent App Sec Standards | Evolved Application Security Standard | Application Classification, Hardening, Scanning |
| Network Segmentation | Open Networks, No Access Controls | Evolved Zone Security Controls | Established Zone Lifecycle based on Placement/Risk |
| Vulnerability Scan | No or limited visibility to system vulnerabilities | Identify vulnerabilities with recommendations | Better correlation, more accurate alarms |
| Vulnerability Management | No vulnerability management | Evolved Proactive Program iteratively | Integrated vulnerability management with SIEM |
| IT Asset Discovery/Mgmt | Limited knowledge of assets and status | Evolved knowledge of assets and status | More accurate alarms targeted on high-value assets |
| Netflow | No or impeded visibility on network traffic | Can analyze multiple network protocols | Finely-tuned and accurate anamoly detection |
| IPS / IDS | Difficulty collecting, processing intrusion data | Enhanced intrusion detection capabilities | Integrated detection and remediation protocols |
| Honeypotting | Limited understanding re: intruder access modes | Effective decoys to gather forensic data | Enhanced means to prevent future intrusion/prosecute intruders |
| Secured Service Data Centers | Trust Network is Open Globally and Non-secure | Focus on Service Zones in Data Centers and User Resource Zones | Services organized in Zones based on placement criteria and controls |
| Security Model | Various confusing methods for remote or local access | | Single integrated security model with Zero Trust |

# Information Security Roadmap Implementation



Plan

Measure Current Security Control

Update Assets Database

Risk Management

Do

Security Awareness Programs

Develop sets of procedures

Implement ISMS within scope

Information Security Management

Information Security Policies

Asset Management

Access Control

Operations Security

Organisation of Information Security

Cryptography

Communications Security

Supplier relationships

Information Security incident management

Information Security aspects of BCP

Human Resources Security

Physical and Environmental security

Systems acquisition, development and maintenance

Compliance

Check

Measure and analyse control effectiveness

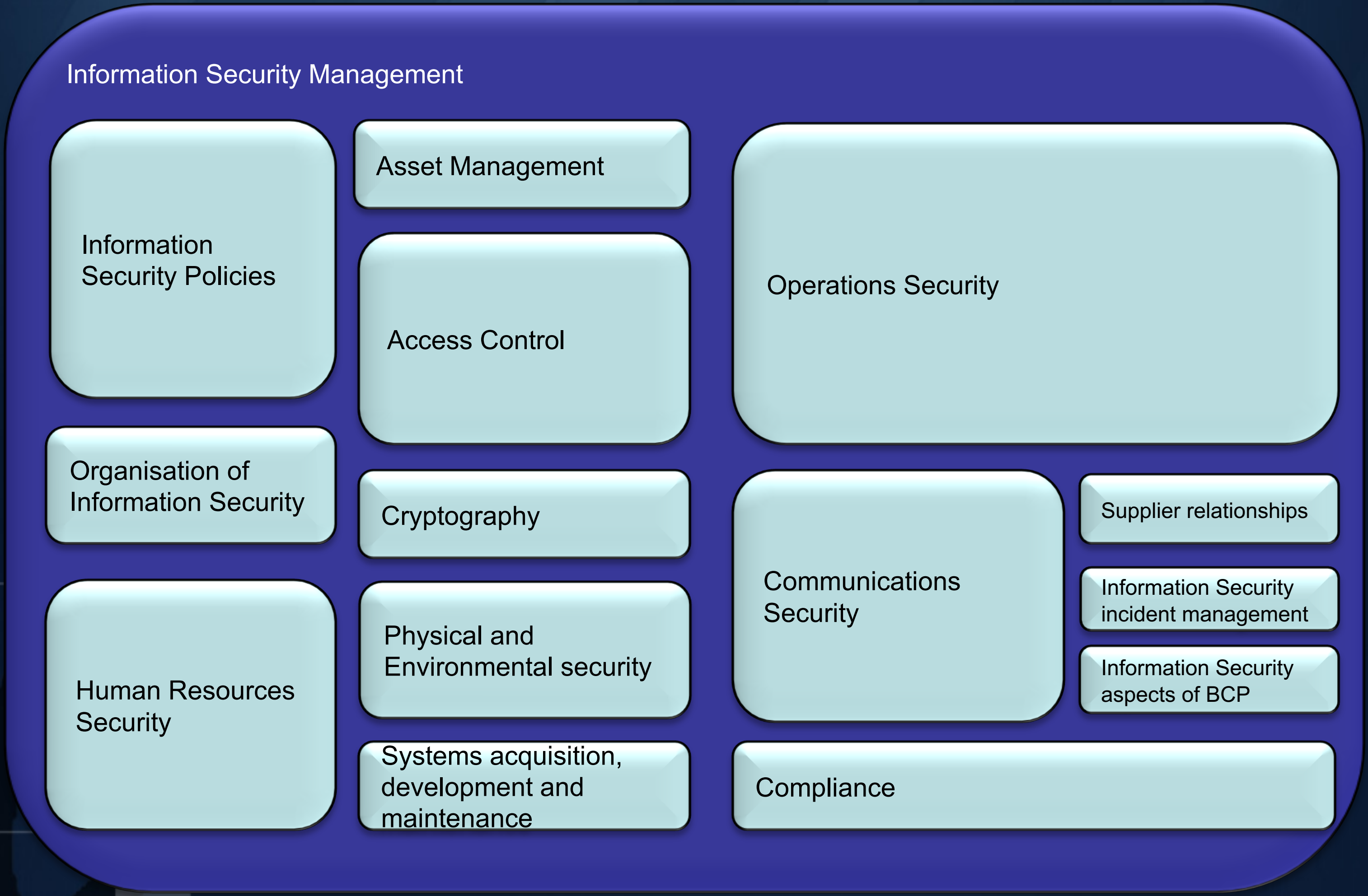
Perform Compliance Audit

Management Review

Act

Improve IT's Capabilities and Maturity in Information Security

# Where the work happens



Information Security Management

Information Security Policies

Asset Management

Access Control

Operations Security

Organisation of Information Security

Cryptography

Communications Security

Supplier relationships

Information Security incident management

Information Security aspects of BCP

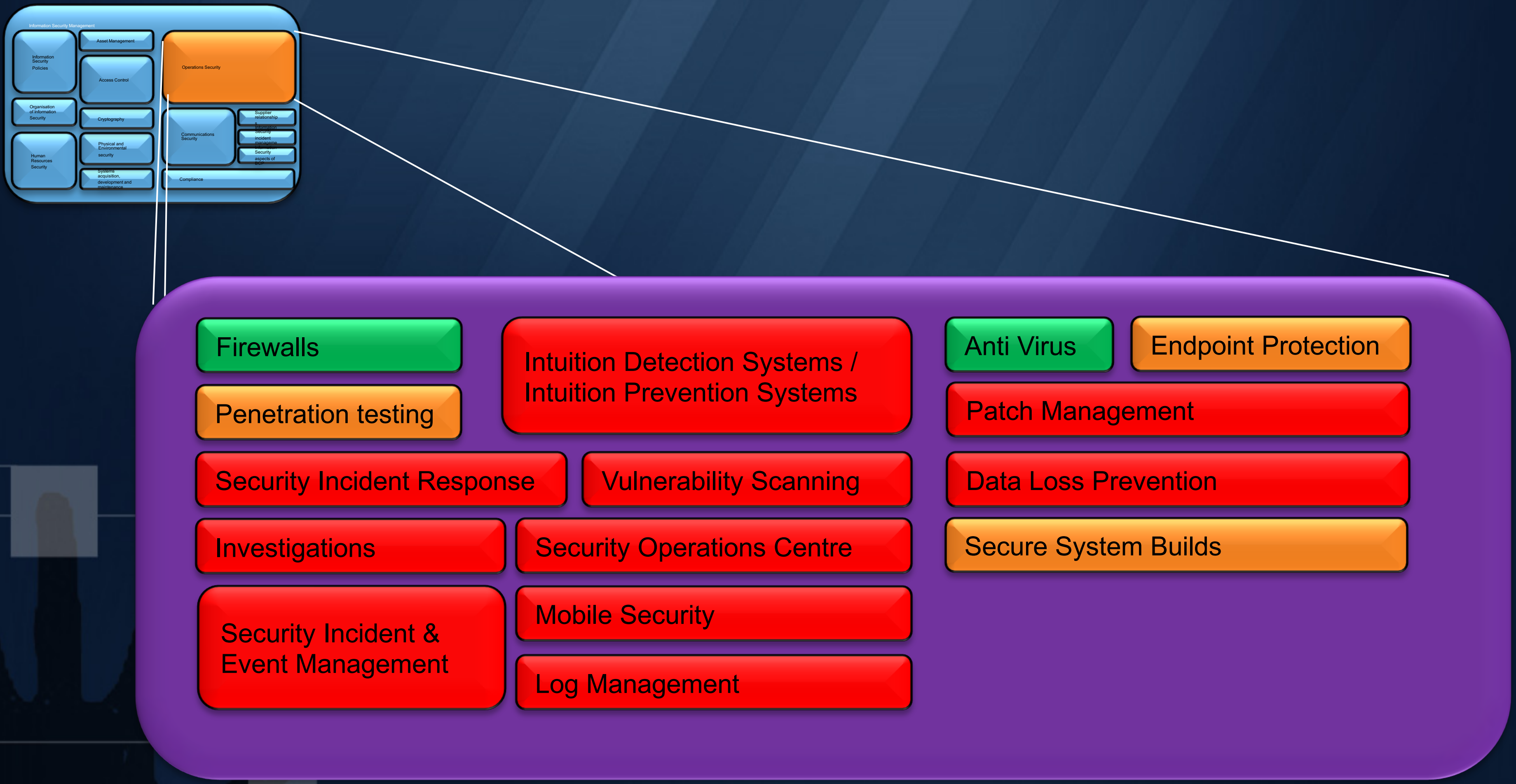
Human Resources Security

Physical and Environmental security

Systems acquisition, development and maintenance

Compliance

# Where the work happens



Information Security Management
Information Security Policies
Asset Management
Access Control
Operations Security
Organisation of Information Security
Cryptography
Communications Security
Supplier relationships
Information Security incident manageme
Information Security aspects of BCP
Human Resources Security
Physical and Environmental security
Systems acquisition, development and maintenance
Compliance

Firewalls

Intuition Detection Systems / Intuition Prevention Systems

Anti Virus

Endpoint Protection

Penetration testing

Patch Management

Security Incident Response

Vulnerability Scanning

Data Loss Prevention

Investigations

Security Operations Centre

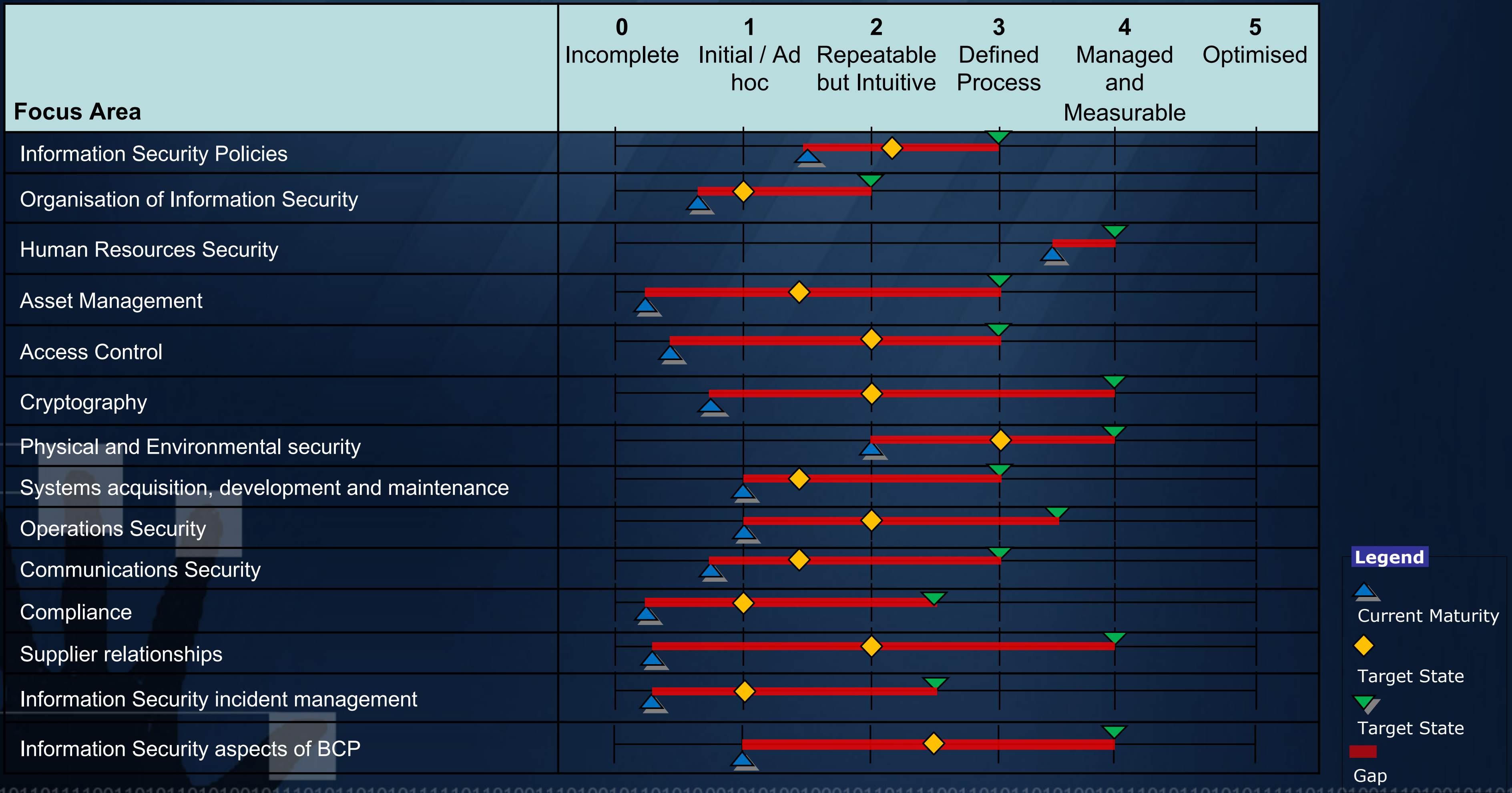
Secure System Builds

Security Incident & Event Management

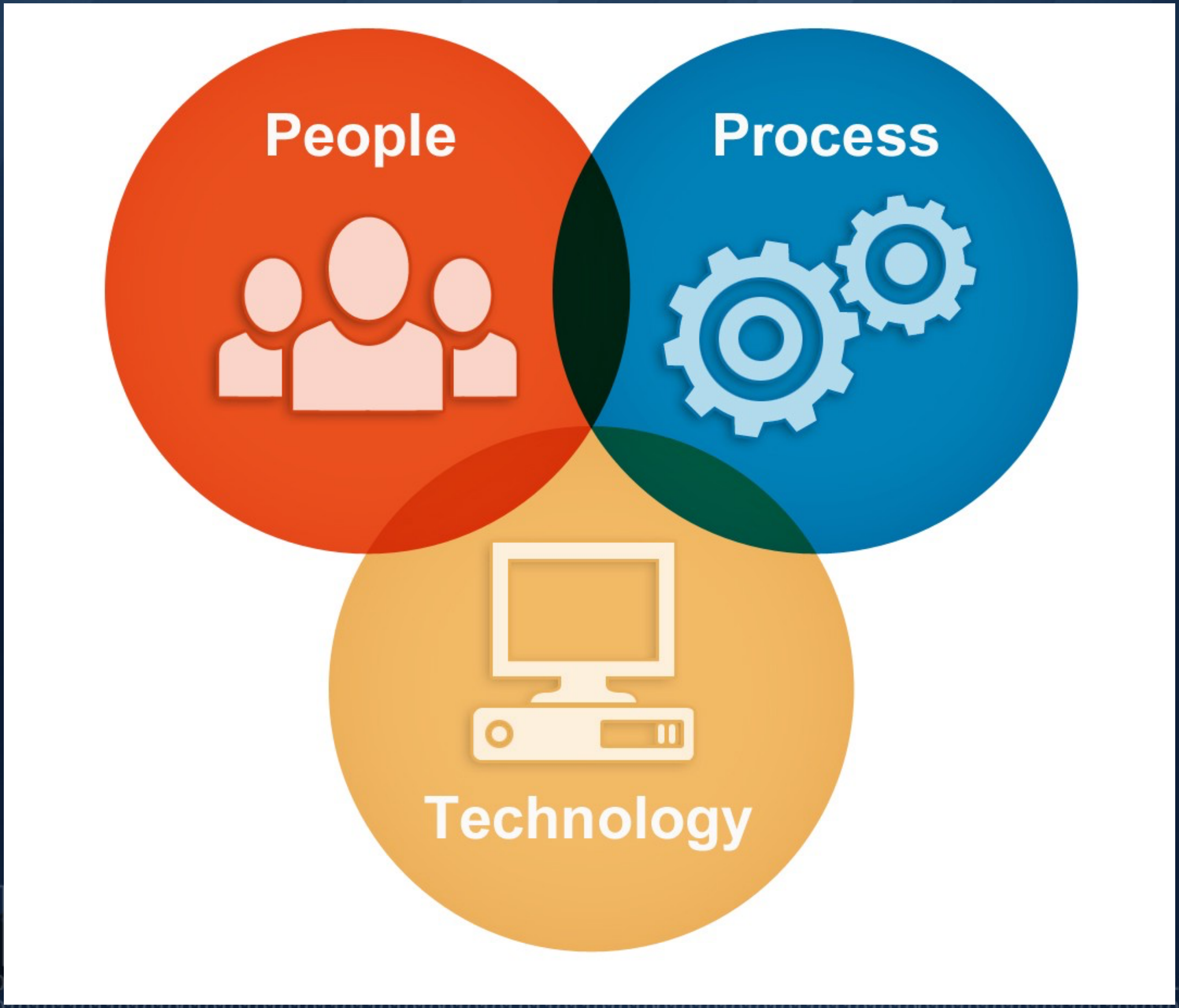
Mobile Security

Log Management

# Security Maturity as a measurement for success



# Doing the Basics Right



# People

1. Make sure that all staff read the Acceptable Use Policy;
2. Create a culture of security in your business;
3. Enable Security Awareness Campaigns for all staff;
4. Give specific security awareness training to business Executive’s, their P.A’s;
5. Focused training for IT and specifically Developers;
6. Consider a Red team exercise;

# Processes

- Security Governance
- Policy Management
- Awareness and Education
- Identity and Access Management
- Vulnerability Management
- Incident Response
- Change Management
- Business Continuity Management and Disaster Recovery Management
- Project Life Cycle Management
- Vendor Management

# Technology

1. Automate successful processes. If you cannot do it manually you cannot automate it.
2. Build the defense as a defense in depth model;
3. Right tool for the right job;
4. Do the basics right
    1. Change default passwords;
    2. Disable the guest account;
    3. Rename the Admin account;
    4. Remove interactive logon rights from service accounts;
    5. Make sure staff and apps work under the “User” context and not “Local Admin”
    6. Ensure that the OS and APPS are updated regularly;
    7. Disable services that are not needed / used
    8. Enable hard disk encryption
    9. Do regular vulnerability scans (MS Baseline Security Analyzer is free)

Questions?