Designing Security
Top Down Approach

Richard Skaife

Security Failures Cost

Lives

The Environment

Business Failures

Financial Loss

Brand Image

COSTS ARE TAXPAYERS' OR INVESTORS' MONEY – I.E. OURS

Security Failures Cost

Lives

The Environment

Business Failures

Financial Loss

Brand Image

COST OF SECURITY BREACH EXCEEDS THE COST OF SECURITY

Attitudes To Risk Management

Piecemeal Approach

Conflicts (Security vs Privacy)

Lack of Timeliness

Infrequency

Limited Accuracy

Incomplete

(Anne Robins Gartner)

SECURITY IS TOO IMPORTANT TO BE LEFT TO SPECIALISTS

Why Top Down

"I want CCTV here, access control here, RFID here……."

Going straight to technology may provide security but do you have confidence it is adequate?

Motivation of equipment vendors may not align with your requirements.

DON'T LEAVE IT TO CHANCE
STRUCTURED APPROACH

What Are We Trying To Do?

Protect:

- People
- Environment
- Business Continuity
- Business Reputation
- Information

BE CLEAR ABOUT SECURITY OBJECTIVES

Security Management Principles

Security is not 100% Guaranteed

Need to analyse threats, vulnerabilities

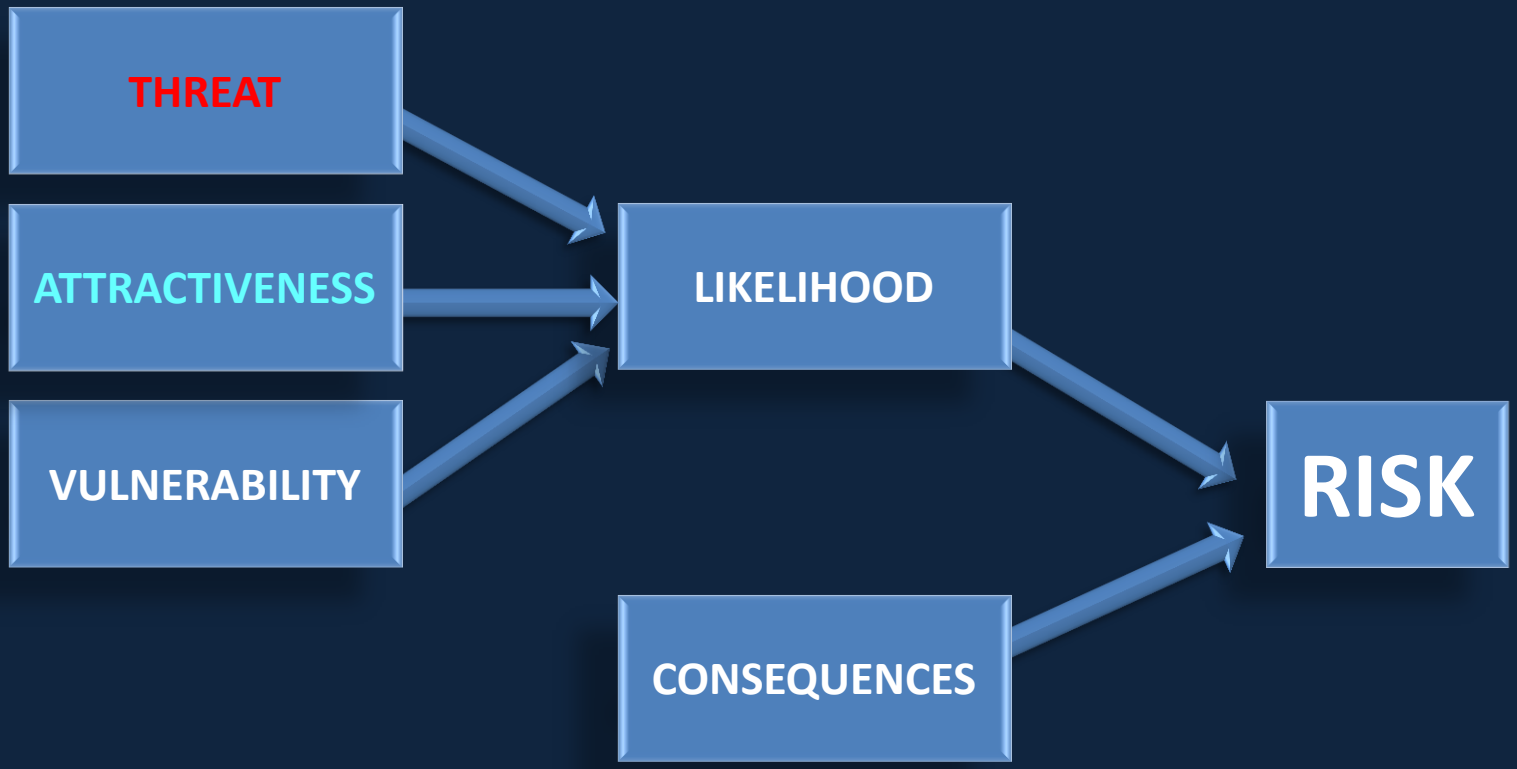
Evaluate Countermeasures

Security strategy based on:

- Deter
- Detect
- Delay/Deny
- Respond

SECURITY IS ABOUT MANAGING RISK

What is RISK?



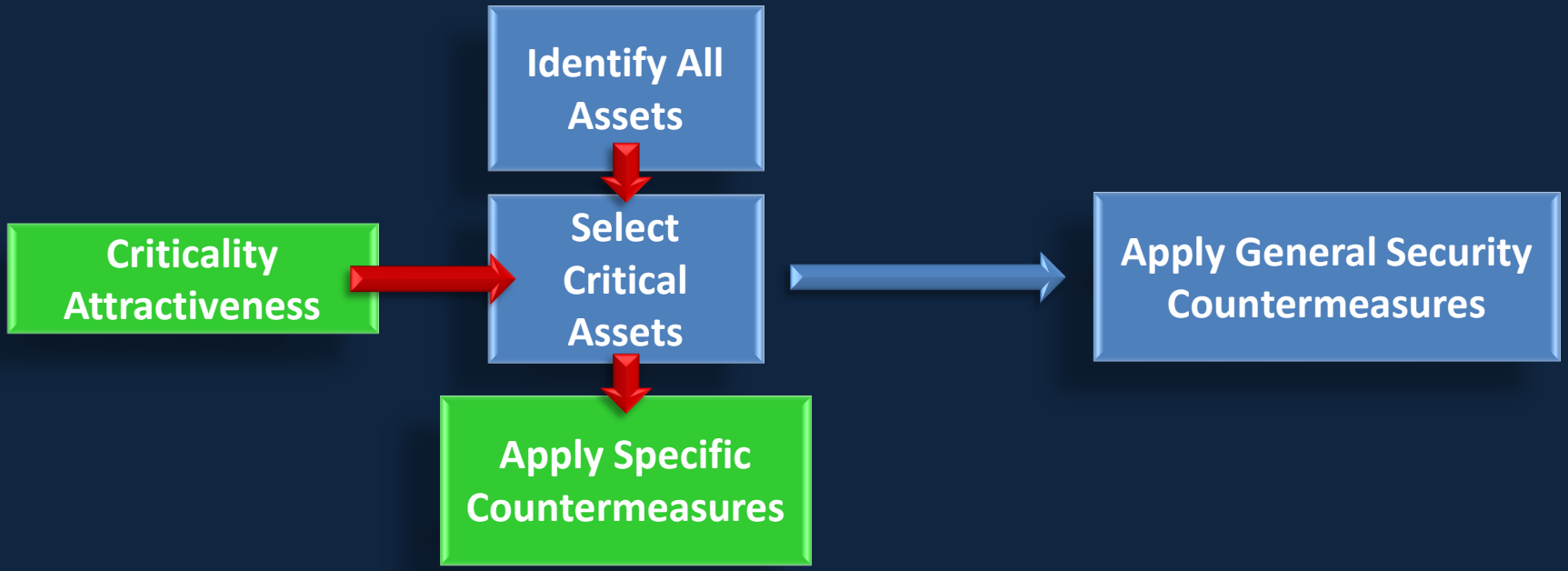
RISK IS A COMBINATION OF LIKELIHOOD AND CONSEQUENCE

A Security and Vulnerability Assessment Process

Five Step Process:

1. Select Your Critical Assets
2. Assess The Threat to These Assets
3. How Vulnerable Are They
4. How Exposed Are They - RISK
5. What is the Best Way to Mitigate That Risk

General Asset Screening



SVA Stage 1 – Asset Characterisation

Assets | Threat | Vulnerability | Risk | Countermeasures

What Are The Critical Functions These Assets Carry Out

What Critical Infrastructure do These Assets Depend On

What Existing Protection Is There

What Is The Impact Of An Attack

Medium to High Impact – Add Asset to Critical Asset List.

Go to **THREAT** Assessment

SVA Stage 2 – Threat Assessment

Assets | **Threat** | Vulnerability | Risk | Countermeasures

What Are The THREATS I am Likely To Face?

What is their overall HISTORY?

Any SITE SPECIFIC HISTORY

Potential ACTIONS (Threat Vectors)

Adversary MOTIVATION/INTENT

Threat Ranking HIGH – Add Adversary to THREAT LIST

SVA Stage 2 – Threat Assessment

Assets | **Threat** | Vulnerability | Risk | Countermeasures

THREAT RANKING

Credible Threat exists against this specific asset Adversary demonstrates the capability and intent to launch an attack.	5 – VERY HIGH
Credible Threat exists against the asset based on knowledge of adversary capability and intent to attack similar assets.	4 - HIGH
There is a possible threat based on adversary's desire to attack similar premises.	3 - MEDIUM
Low threat against the asset and there are few known adversaries that might pose a threat.	2 - LOW
No credible evidence of capability or intent and no history of planned or actual attacks against similar assets.	1 – VERY LOW

SVA Stage 1 – Attractiveness

Assets | **Threat** | Vulnerability | Risk | Countermeasures

Assess Attractiveness of Asset to the High Risk Adversaries.

- **Identify Critical Functionality**
- **Identify Attractiveness to Threat category**
- **Rank ATTRACTIVENESS**
- **Ranking MEDIUM to HIGH – Add Asset/Adversary to VULNERABILITY Analysis**

SVA Stage 1 – Attractiveness

Assets | **Threat** | Vulnerability | Risk | Countermeasures

TARGET ATTRACTIVENESS

Adversity would have a very high level of interest in this asset	5 – VERY HIGH
Adversity would have a high degree of interest in this asset	4 - HIGH
Adversity would have a moderate level of interest in this asset	3 - MEDIUM
Adversity would have some level of interest in this asset	2 - LOW
Adversity would have no level of interest in this asset	1 – VERY LOW

SVA Stage 3 – Vulnerability Analysis

Assets | Threat | **Vulnerability** | Risk | Countermeasures

For each critical ASSET and THREAT

What is the security **EVENT TYPE**

What are the Existing **COUNTERMEASURES**?

What are the **VULNERABILITIES** that are exploited?

SVA Stage 3 – Event Type

Assets | Threat | **Vulnerability** | Risk | Countermeasures

Generic Statement of Security Event e.g.

- Injury/Death
- Loss of Facility
- Environmental Damage
- Business Disruption

SVA Stage 3 – Vulnerability and Ranking

Assets | Threat | **Vulnerability** | Risk | Countermeasures

Describe EXISTING COUNTERMEASURES

Assess VULNERABILITY

Rank VULNERABILITY

SVA Stage 3 – Vulnerability and Ranking

Assets | Threat | **Vulnerability** | Risk | Countermeasures

VULNERABILITY and Ranking

No effective protective measures in place.	5 – VERY HIGH
Some protective measures, it would be relativey easy for adversary to attack the asset.	4 - HIGH
Although there are some effective measures in place, they are incomplete and there is a likelihood that asset can be compromised.	3 - MEDIUM
Effective countermeasures in place but at least one weakness exists that could be exploited by an adversary.	2 - LOW
Multiple layers of countermeasures exist and the likelihood of exploitation is very low.	1 – VERY LOW

SVA Stage 4 – Consequences

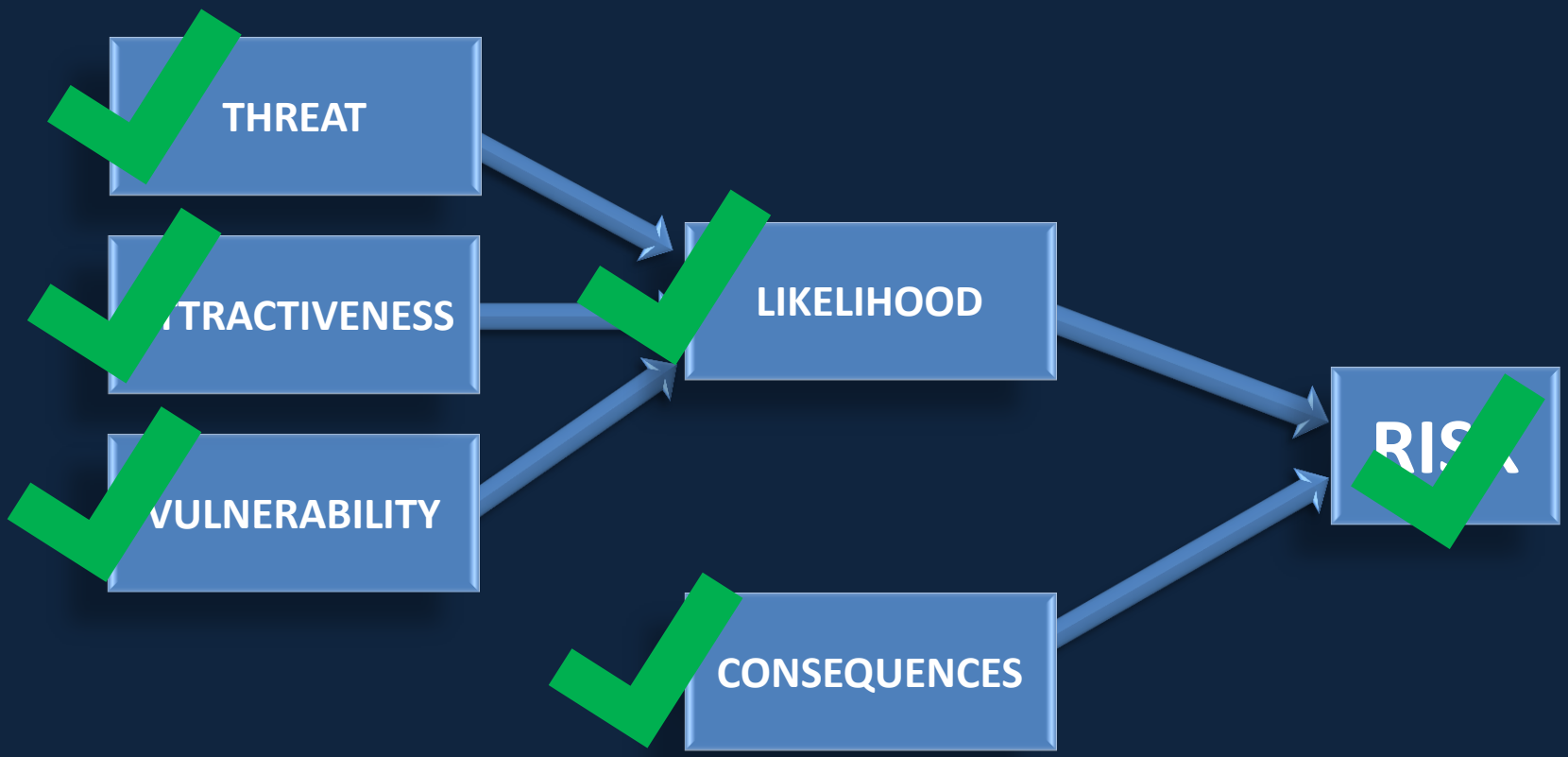
Assets | Threat | Vulnerability | **Risk** | Countermeasures

CONSEQUENCES and Ranking

Major Onsite and Public Fatalities Major Environmental Damage Very Long Term Business Disruption	5 - VERY HIGH
Possible onsite and offsite fatalaties Large Environmental Damage Long term (months – years) business Disruption	4 - HIGH
No offsite fatalities or injuries, possible onsite fatalities and injuries. Onsite environmental impact, little or no offsite environmental impact Medium term (months) business disruption	3 - MEDIUM
Limited onsite injuries in the vicinity of the incident location Minor environmental damage to site of incident Short term business interruption	2 - LOW
Possible minor injury No environmental damage Limited business disruption (weeks)	1 – VERY LOW

SVA Stage 4 – Risk Assessment

Assets | Threat | Vulnerability | **Risk** | Countermeasures



SVA Stage 5 – Countermeasures

Identify options to further reduce vulnerabilities:

- To Reduce Probability of Successful Attack
- How Effective is the Option?
- What is the Implementation Cost?
- Is the Proposal Feasible?
- Not Just Technical – Include Operational, Organisational and Procedural Measures

Security Plan

CONCEPT OF OPERATIONS

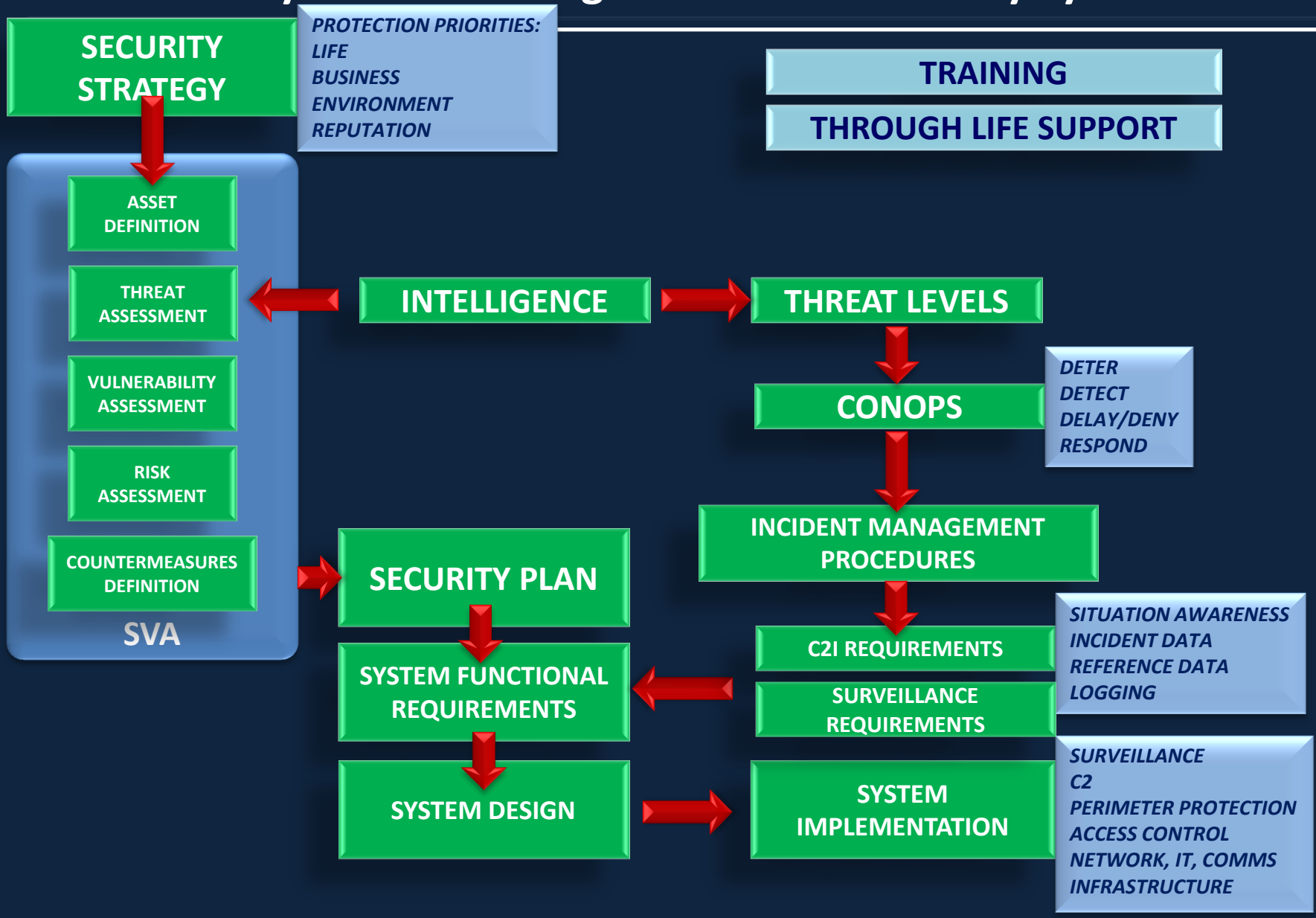
SECURITY PLAN

- ADMINISTRATION AND TRAINING
- STAFF TRAINING
- DRILLS AND EXERCISES
- RECORDS AND DOCUMENTATION
- RESPONSE TO CHANGES IN ALERT STATES
- COMMAND, CONTROL AND COMMUNICATIONS
- SECURITY SYSTEMS AND MAINTENANCE
- ACCESS CONTROL POLICIES
- POLICIES FOR RESTRICTED AREAS
- INCIDENT MANAGEMENT PRODCEDURES
- SECURITY AUDITS AND REVIEWS
- SVA REPORT

CONOPS IS WHAT YOU WANT TO DO

SECURITY PLAN IS HOW YOU INTEND TO DO IT

Summary – Overall Design Process for Security Systems



References

American Petroleum Institute

Security Guidelines for the Petroleum Industry Third Edition April 2005

Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries Second Edition Jan 2004

UK Home Office

Safer Places – A Counter Terrorism Supplement Consultation Document April 2009 ISBN 978-1-84726-838-9

RIBA Manchester Police

Design for Security RIBA Plan of Work 2013