

# **BMIS UK Case-study: HM Government Response to Information Security & Creation of Security Policy Framework (SPF)**

**Vernon Poole**  
**Head of Business Consultancy,**  
**Sapphire, UK**



## Speaker Credentials – Vernon Poole

- Recognised global trainer in Information Security Management for over 15 years
- Member of UK & International 27000 User Groups
- Member of ISACA's COBIT5 Taskforce
- UK & European CISM trainer
- Head of Business Consultancy at Sapphire – totally independent Information Security Services Company
- One of the first persons to be awarded the CGEIT qualification

# Agenda

1. Background - UK Poynter Report & emergence of BMIS
2. Global IS Environment
3. SPF – 7 Information Security Policy Areas (linked to BMIS)
4. Latest SPF Guidance

# 1. Poynter Report - Background

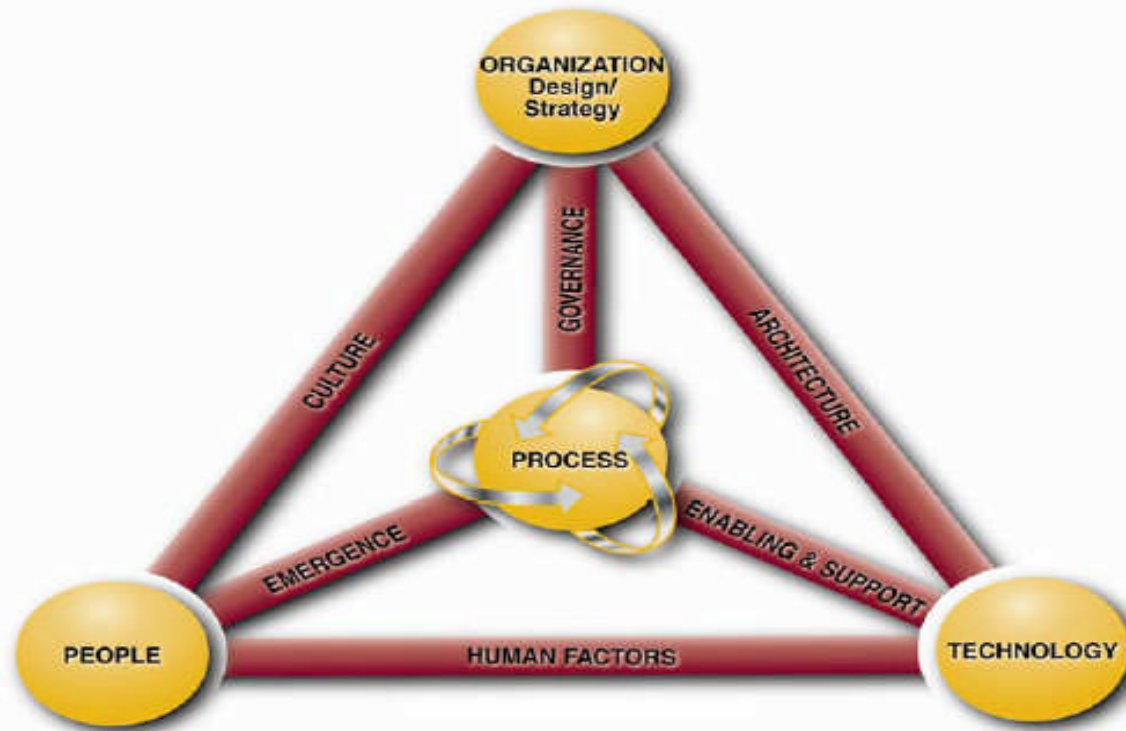
- UK's HM Revenue & Customs lost discs containing 25million people
- Discs were placed in an internal envelope for couriers to take to External Audit (NAO – National Audit Office)
- Discs never turned up – major embarrassment for HMRC & the Government – led to the Poynter inquiry
- Poynter Report made 45 recommendations – to date 39 have been addressed at a cost of £155million
- Recommendations deployed the Business Model as outlined above

# 1. Poynter Report - Highlights

- ‘Information Security was not a Management priority’  
Arrangements were ‘woefully inadequate’
- The report outlined 3 areas of concerns:-
  - A weakness in specific IS policies
  - Inadequate communications; training & awareness programmes
  - A lack of clarity around the governance & accountability for data guardianship
- The report recommended the use of ISO 27002 & the associated CMM – aiming for a minimum level of 3 (Defined) & progressing to level 4 (Managed & Monitored)

# 1. Poynter Report - Basis of Recommendations

- Recommendations were outlined over 4 areas, namely:
  - Strategy; People; Process & Technology
- These areas represent the emerging 'Business Model for IS'(BMIS):



# 1. Recommendations : Strategy

## 14 recommendations:-

1. IS to be a corporate objective – formalised in business strategy
2. Business objectives for IS support corporate objectives
3. Business/IT Strategies be updated in line with IS objectives
4. Review specific policies or legislation
5. Formalise IS strategy ( to support business/IT strategies)
- 6/7. Identify ‘quick wins’ /medium term objectives for IS framework

# 1. Recommendations : Strategy (contd)

8. Aim for better balance between strategic & tactical investment

9/10. IS Programme should coordinate activities with m. Support

11/12. Appoint a Corporate Risk Officer & CISO

13. Establish a formal; Risk Management function

14. Board & senior management hold periodic ISF meetings

# 1. Recommendations : People

## 7 recommendations:-

1. Need for effective staff communications on IS
2. Align HR, communications & training activities to ensure IS are integrated
3. Ensure staff understand their responsibilities/accountabilities
4. Personal IS policies are integrated into employee's lifecycle
5. Develop awareness programmes
6. Build appropriate levels of capabilities for IS management
7. Consider compliance tools to drive changes in IS behaviour

# 1. Recommendations : Process

## 14 recommendations:-

- 1/2. IS guidance should be simple, short, accessible & locally tailored
3. Enhance ISM capabilities on incident management
4. Adopt a structured approach on performance monitoring
- 5/6. Business units should identify both RM/IS sponsors
7. Manage interdependencies effectively

# 1. Recommendations : Process (contd)

8. Information owners should inc. explicit authorisation responsibilities
9. Clear accountability for media handling
10. Need for consistency in access control across all systems/estate
11. Conduct capacity reviews on data storage
12. Sufficiently detailed data-flows to enable effective risk management
13. Service level agreements should be agreed to meet operational needs
14. Initiate a programme of third party assurance

# 1. Recommendations : Technology

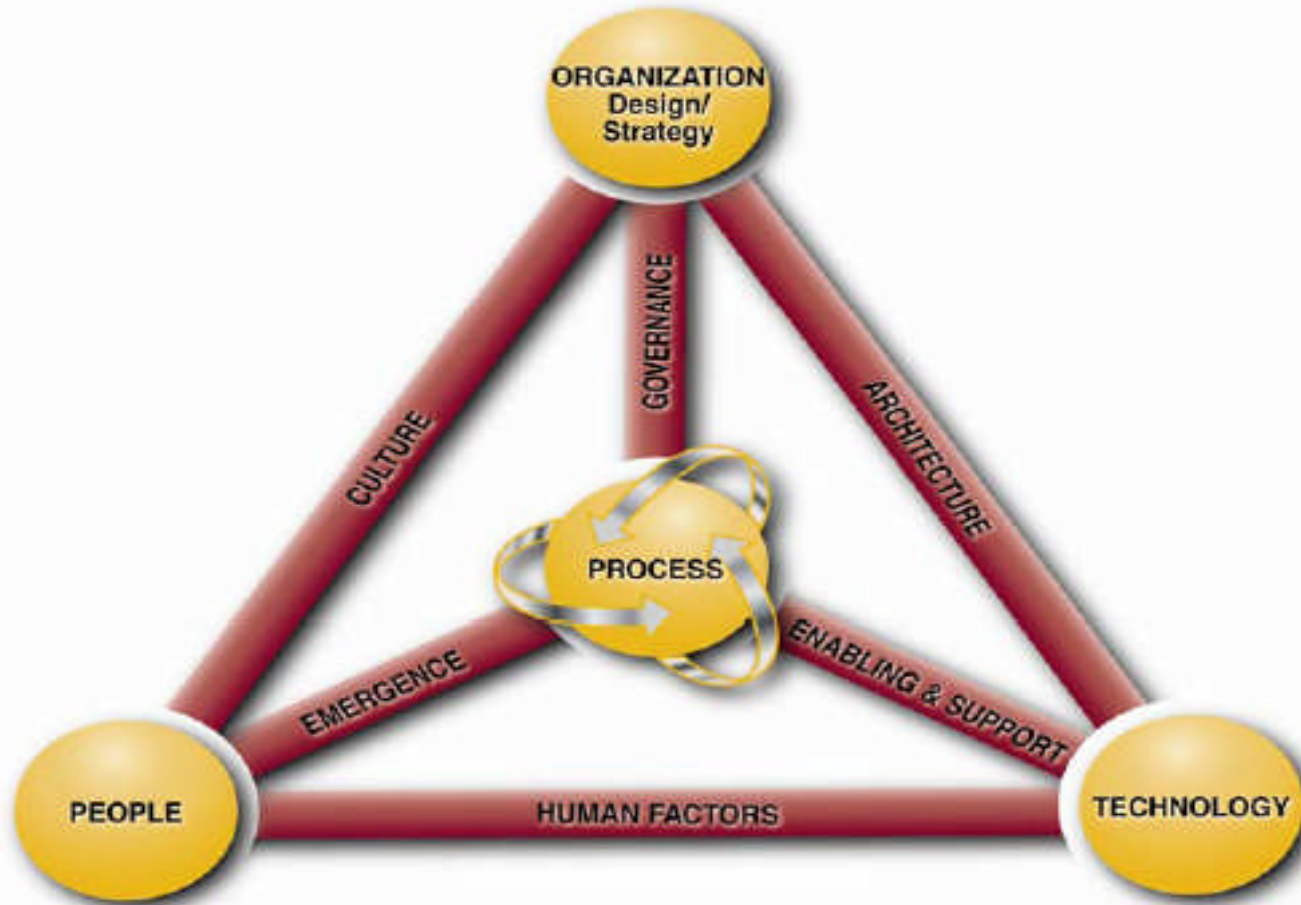
## 10 recommendations:-

1. New system approvals should ensure IS risks are accepted
2. Contract reviews should include adequate IS
3. IT Strategy reviews should include IS as a business factor
4. IT Investment models should emphasise risk quantification
5. Strengthen system specs in respect of IS coverage

# 1. Recommendations : Technology (contd)

6. Enhance BCM in terms of business resilience
7. Move from local to corporate prioritisation of IT projects
8. Build realistic business cases on IS levels of investments/timescales
9. Engage professional help in building effective IS frameworks
10. Enhance staff capabilities to implement IS framework appropriately

# 1. Need for IS Governance– a Business Model



# 1. Model Relationships

- Organisations are familiar with the people, process & technology elements; but, in essence, the focus was mainly on process & technology – but this approach is purely operational & at best, tactical. This method addresses the ‘people element in depth
- What is missing is the crucial ‘strategic’ Business (Organisation) element
- It is imperative that the business (service) value of security is respected and driven by senior management
- This new model hopes to address this gap and to question the role of each element in relation with the dynamic interconnections (softer/nebulous issues that have not been discussed enough)

# 1. BMIS Components

## 4 main elements:-

1. Organisation (Strategy) – embraces risk/governance/IS at board level;
2. People – addressing human behaviour & leveraging human intelligence
3. Process – need for an appropriate IS framework
4. Technology – embrace the most appropriate technical solutions available

## 6 dynamic interconnections

1. Architecture – IS design in the overall infrastructure (h/w; s/w)
2. Culture – build an *intentional* culture (set of expectations & desires)
3. Emergence – be flexible to change (benchmarking; use of best practice)
4. Enabling & Support – aligned relationship between process & technology
5. Governing (Governance) – business alignment; trust & communication
6. Human Factors – usability factor (ease of use & understanding)

# 1. BMIS Elements : 1. Organisation

- Develop a strategy for ‘continuous monitoring’ alongside a strategy for ‘constant vigilance’.
- Create a clearly articulated purpose & sustainability (preservation) statement - corporate policy guidance.
- Boards recognise the ‘business value of security’ and lead on it
- Inform & educate all staff about the value of IS
- In strategic planning terms, each individual and business unit must demonstrate alignment with agreed IS/IS Management standards.

## 1. BMIS Elements : 2. People

Defines the aspects that impact on human resources:

- Job Descriptions – do they include IS responsibilities
- Recruitment & Selection – are necessary screening/vetting checks
- Placement & Rotation – impact on logical access controls
- Skills, Training & Development – do they include IS awareness
- Rewards System & HR Policies – do Personal IS Policies exist
- Performance standards – do they include IS
- Placement – remote/flexible working

# 1. BMIS Elements : 3. Process

- Agree ISMS Framework required e.g. ISO27002 guiding principles:-
  1. IS Policy
  2. Organising IS
  3. Asset Management
  4. Human Resources
  5. Physical/Environmental Security
  6. Communications & Operations
  7. Logical Access Controls
  8. Systems Acquisition, Development & Maintenance
  9. Incident Management & Reporting
  10. Business Continuity Management
  11. Compliance

# 1. BMIS Elements : 4. Technology

- In addition to the broader technology infrastructure - IS technology falls into several broad categories:
  1. Security Design & Configuration (controls, change management)
  2. I&A: Identification & Authorization (Identity Management)
  3. Enclave internal (Desktop protection e.g. anti-virus s/w)
  4. Enclave boundary (Firewalls, IDS/IPS)
  5. Physical & Environmental (control devices , biometric devices etc).

# 1. BMIS Interconnections : 1. Architecture

- SANS enterprise architecture framework consists of 5 phases:
  1. IS assessments to determine IS requirements
  2. IS architecture design based on recommendations (in 1. above).
  3. Development of IS policies & procedures
  4. Implementation of target IS architecture (technology) designs.
  5. Integration of IS practices by change management & project management methodology to introduce IS as a process.

# 1. BMIS Interconnections : 2. Culture

- Typical aspects of culture are :-
  1. Rules & Norms – assumptions = repetitive attitudes/behaviour
  2. Tolerance for Ambiguity - flexibility, resilience, & adaptability
  3. Power Distance - perceived authority & how levels are delineated
  4. Politeness Norm – cultural etiquette or diplomacy
  5. Context - shared values
  6. Collectivist v. Individualist (we v. me)

It is important to build an 'intentional culture'

# 1. BMIS Interconnections : 3. Emergence

1. Create an organizational design that has rigor, feedback loops, & critical thinking - 'challenging' concept (with associated risks & opportunities)
2. Use rigorous processes & innovative practices in assessing liabilities and risks.
3. Ensure the quality of the "process" element (positive culture; balanced processes; improvement processes)
4. Ensure alignment with the "people" element (cultural norms on hiring, training & review; be innovative – enlightenment; focussed process improvement programs inc. best practice IS tools.
5. Develop a research team focused on future sources/means of IS harm
6. Ensure that behaviours are demonstrated consistently by senior management & the board
7. Build the above into all decisions, projects, etc.
8. Expect & embrace radical emergence, not just incremental emergence of continuous improvement.
9. Establish IS Governance policies that support & reinforce the above

# 1. BMIS Interconnections : 4. Enabling/Support

- Typical aspects cover :-
  1. Restructure & reconfigure the process - to enhance customization & to streamline processes, care must be taken not to dilute IS requirements.
  2. Change information flows around the process. This can increase the amount of information that exists, creating vulnerability to cyber security attacks, but also providing the possibility for improved IS systems
  3. Change knowledge management around the process. Knowledge generated can also be used to provide input to IS processes & their interactions

# 1. BMIS Interconnections : 5. Governing

- Align individual actions towards corporate mutual benefit
- Means by which each individual can trust others towards mutual benefit
- Means by which information can quickly flow between stakeholders to ensure that changing needs and desires are accounted for
- Directors & managers act in the interests of the organisation its shareholders, & its staff
- Managers accountable to investors & employees for the use of assets

Governing demands this articulation (strategy) into the organisation's processes with two way communication (monitoring & compliance)

# 1. BMIS Interconnections : 6. Human Factors

Steps must be taken to close the gap between technology and people to create a synergistic environment – typical concerns are:

1. Sharing the corporate jewels
2. Granting unauthorized access
3. Failure to follow IS Policies & Procedures
4. Physical intrusion

It is well accepted that ‘normal accidents and human error’ - account for most breaches

## 2. Global IS Environment :Threats

- Organised crime using identity theft
- Cyber-criminals
- Malware authors
- Phishers
- Spammers
- Negligent technical staff or disgruntled staff
- Fraudsters
- Hackers
- Unethical competitors & saboteurs
- Unauthorised access or modification

Compounded by increasing legal/regulatory demands & natural disasters

## 2. Global IS Environment 2008 : Vulnerabilities

- Software bugs/design flaws
- IT complexities – new & legacy systems
- Inadequate investment in IS controls
- Insufficient attention to human factors in design/implementation
- Ignorance & negligence by users
- Poor governance of information assets
- Frequent business changes – impacting on IS responsibilities
- Inadequate contingencies & BCM
- Legacy system weaknesses

## 2. Global IS Environment : Business Impacts

- Disruption to business processes – trading interruptions, loss of income
- Financial losses through information theft & fraud
- Decrease in shareholder value because of decline in public confidence
- Loss of privacy especially as identity theft increases
- Reputational damage caused by brand devaluation, loss of customers
- Loss of confidence in IT
- Fines, suspension of licences
- Replacement costs/expenses from IS incidents
- Loss of competitive advantage
- Reduced profitability - impairing growth
- Injury or loss of life

## 2. Global IS Environment : Risks

- Theft of personal data or loss of mobile devices
- Information leakage, extraction or loss of information
- Social engineering or targeted phishing/malware attacks
- Environmental disasters
- Inadequate IS risks/controls & associated staffing
- Deception – frauds; repudiation & false allegations
- Endangerment of information – either accidental or deliberate
- Unauthorised exploitation of intellectual property

## 2. Global IS Environment : Controls

- Investment on a comprehensive ISMS
- Data Confidentiality Controls
- Data Integrity Controls
- System Integrity Controls
- Proactive technical vulnerability management
- Anti – everything software (malware; spam; spyware)
- Proactive IT audit, monitoring & reporting
- Enforcement of rights & compliance obligations
- Resilience engineering in business processes
- Contingency arrangements
- IS awareness, training & education

## 3. HMG Security Policy Framework (SPF)

- ‘Effective security is central to how we handle many of the challenges facing Government. It is vital for public confidence & the effective/safe conduct of public business’.
- The new Framework – sets out mandatory standards, with guidance on Risk Management & new Compliance arrangements
- Focus – IS policies & processes in line with new & changing threats based on four levels:
  1. Security not only supports business goals but to be viewed as a business enabler
  2. Five core security principles
  3. Seven key policy documents – 70 mandatory requirements
  4. Detailed tools for practitioners (technical standards; policy/guidance; websites)

### 3. SPF – Who it applies to?

- SPF outlines mandatory security policy requirements that :
  - all Departments and Agencies must meet.
  - it should also be extended, to any organisations working on behalf of, or handling HMG assets.
  - in areas where statutory security requirements apply
  - Senior managers will need to determine where & what level of compliance is required of their delivery partners, & where equivalent security policies are acceptable.
- Website link -  
[http://www.cabinetoffice.gov.uk/sites/default/files/resources/hmg-security-policy\\_0.pdf](http://www.cabinetoffice.gov.uk/sites/default/files/resources/hmg-security-policy_0.pdf)

# Levels 1 & 2 : Statement & Principles

## Level 1

Protective security (inc. physical, personnel & information security), is an essential enabler to making government work better. Security risks must be managed effectively, collectively & proportionately, to achieve a secure & confident working environment

## Level 2

1. Ultimate responsibility rests with Governance leaders who must manage their security risks.
2. Employees (& contractors) to ensure assets are proportionately protected
3. Need to share info confidently (reliable, accessible, protected)
4. Need to employ staff (inc contractors) in whom they have confidence & whose identities are assured
5. HMG business to be resilient to disruptive events with plans to minimise damage & rapidly recover capabilities



## Level 3: Seven Security Policies

1. Governance, RM & Compliance (10) – **Strategy: Governing & Culture**
2. Protective Marking & Asset Control (11) – **Process & Technology: Enabling & Support**
3. Personnel Security (9) – **People: Culture, Emergence and Human Factors**
4. IS & Assurance (19) – **Process & Technology: Emergence, Enabling & Support, and Human Factors**
5. Physical Security (14) – **Process & Technology: Emergence, Enabling & Support, and Human Factors**
6. Counter – Terrorism (6) – **Strategy, Process, Technology & People**
7. Business Continuity (1) – **Strategy, Process, Technology & People**

# Governance, RM & Compliance

## Governance – partnership approach

- 1: Ensure staff understand relevant requirements & responsibilities by SPF & meet MRs (where statutory requirements takes precedence; regulators to conform to SPF)
- 2: Ensure their agencies/delivery partners are compliant with SPF & extent to which 'others' comply

## Leadership & roles/responsibilities

- 3: Board level responsibility for security (inc. inter-relationships)
- 4: Appoint a designated officer with daily responsibility for IS

## Risk Management

- 5: Adopt a risk management approach (inc. risk register)

# Protective Marking & Asset Control

PMS – Government administrative system for IS

11: Apply PMS & necessary controls & technical measures

Legal requirements

12: Provide guidance on statutes with guidance on specific roles

13: Official Secrets Act

14: Data Protection Act

15: Freedom of Information Act

Need to know principle – protecting sensitive information

16: Access to protectively marked assets is based on this principle

International security standard adherence – ISO27001

International security agreements

17: Adhere to obligations in respect to international markings



## Protective Marking & Asset Control (contd)

### Material originating outside UK

18: non-HMG material indicating sensitivity be offered PROTECT

### Gov PMS – top secret, secret, confidential, restricted and protect

19 : access only granted on need to know; assets to be clearly marked; only owner can protectively mark; assets sent overseas to be marked in accordance with international agreement; no records can be destroyed without formal review; file to carry highest marked asset

### Special handling – e.g. for your eyes only

20: Meet special handling arrangements & ensure staff understand.

### Breaches – consequences could be disciplinary

21: Have a breach system with guidance on deliberate/accidental compromise

# Personnel Security

Purpose – level of assurance on trustworthiness, integrity & reliability

RM – in personnel dealings

22: Apply personnel security controls against specific posts & access to sensitive assets

## PSC – Baseline Policies

23: Apply to all staff

24: National Security Vetting where necessary

25: Follow set procedures

26: Only departments or police can take security clearance decisions

27: Establish aftercare arrangements

28: Establish appeals process

29: Inform managers where an individual initiates a challenge

30: Record no. of vetting clearances annually

## IS Policy

31: Have an IS Policy setting out compliance

## Managing information risk

32: Conduct an annual risk assessment.

## Business Impact

33: Use agreed levels to assess/identify impacts through loss of CIA of data

## Personal data –Roles/Responsibilities

34: Information risks addressed in Statement on Internal Control

35 : appoint nominated officers & asset owners

## Accreditation/audit

36: data to be accredited & status reviewed annually

37: Regularly audit information assets (compliance checks; forensics readiness policy)

38: Suitable identification & authentication controls to manage against unauthorised access

## IS & Assurance (contd)

### Codes of connection & technical controls

39: Adopt agreements & shared services – to cover patching; malicious software; boundary devices (firewalls); content checking/blocking; lockdown policy.

### Cryptography

40: Comply with standards in respect of encryption; use of approved solutions; staff clearances

### Eavesdropping & electro-magnetic countermeasures

41: Follow agreed procedures in these cases

### Remote working/mobile media

42: Establish policy covers these areas

### Procurement

43: Security requirements specified in contracts

# IS & Assurance (contd)

## Reporting Incidents

44: Clear policy on incident management\_– reporting to appropriate bodies

## Secure Disposal

45: All media is disposed of or sanitised

## Personnel & physical security

46: Privileged users to be subject to security clearances

47: Locations have appropriate levels of physical security

## Education, training & awareness

48: users be familiar with procedures; receive appropriate training & aware of reporting incidents; with staff securing ICT infrastructure & data handling

## BC & DR Planning

49: All locations have appropriate plans

# Physical Security

Purpose - range of security arrangements

Defence in depth – layered approach based on threats/vulnerability; value.

50: Adopt layered approach to prevent, detect & respond to incidents

Storage of sensitive assets

51: use assessment questions/ baseline controls matrix to identify measures

Secure containers

52: Protectively marked material is secured in appropriate security containers

Secure rooms

53: Ensure all entry controls meet appropriate security standards

Office areas

54 : Adopt clear desk policy

Building security

55: Security risks to their estate are fully integrated into facility design

# Physical Security (contd)

## Physical access control

56: Control access using safeguards to prevent unauthorised access

57: Procedures to intercept unauthorised persons – inc systematic search

58: Access control policies for all staff ( & briefed on their responsibilities)

## Incoming mail & deliveries

59: Appropriate procedures for screening mail/deliveries for suspicious items

## Manned guards

60: Consider use of guard forces

## Perimeter Security

61: Establish a secure perimeter (barriers/entry controls)

62: Produce a detailed operational requirement in respect of CCTV; lighting

## CCTV

63: deployment of CCTV must be in accordance with law

# Counter - Terrorism

Introduction need to consider terrorist groups

Gov strategy published

RM – to establish baseline CT measures

Categorisation of Estate (H,M,L)

64: Categorisation in accordance with likelihood or close proximity to a target

Threat levels – low, moderate, substantial, severe or critical

Threat info/briefings

Response level system – normal, heightened & exceptional

65: Ensure baseline physical & incremental security measures

## Counter – Terrorism (contd)

### Protective security policy/plans

66: Policy (advice, roles, management controls, communicate/test/liaise)

67: Plan (measures; threats, evacuation, BCP, communicate/test/liaise)

### Protective security measures – physical, personnel & information

### Assurance

68: Annual security report to management must explicitly provide a statement of assurance inc. compliance to response levels

### Testing arrangements – well versed procedure

69: Part of BCM, must test arrangements regularly (high risk – annual; medium risk – once every 2 yrs; low risk – discretion) with tests inc. annual reporting

# Business Continuity

What is BCM – holistic approach (BS25999) to continue critical processes  
70: must have a robust, up-to-date, fit for purpose & flexible arrangements  
- regularly tested/reviewed & supported by competent staff to maintain & resume provision of key products & services in the event of disruption

What should a BCM system look like

- Strategy endorsed/supported by Board
- Program appropriate to size/complexity of department
- Plans adequate to manage impact of events & recover
- Arrangements exercised & reviewed
- Effective communication to responsible staff

What are the outcomes

Critical assets protected; effective incident response; holistic approach; staff trained; stakeholder requirements met; effective communication/support; supply chain secured; reputation is protected

## Any Questions

