



SAPPHIRE

ISACA's Business Model for Information Security & Developments in Security Metrics

8 June 2009

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



SAPPHIRE

Speaker Credentials – Vernon Poole

- Recognised global trainer in Information Security Management for over 15 years – inc. CISM
- Member of UK & International 27000 User Groups
- Member of ISACA's Security Management Committee – focussed on advancing best practice (.inc ISO Group rep)
- UK leader on ISACA's Business Model as part of COBIT5 Taskforce
- Head of Business Consultancy at Sapphire – totally independent Information Security Services Company
- CGEIT qualified – representing ISACA globally





SAPPHIRE

Presentation – Aim & Objective

Aim

Challenge conventional thinking to enable you to re-evaluate your IS investment creatively. The Business Model is a life cycle engineering approach to IS...it allows us to unlock ideas

Objective

People talk of 'recession, credit crunch and economic downturn'; I see it as 'challenge and opportunity' with the Business Model as the 'catalyst for change' –to move IS from the periphery of the Board's vision to making it as a 'driver for growth'.



SAPPHIRE

Agenda

1. Impact of the Global IS Environment 2009
2. ISACA's new Business Model – with UK examples
3. Developments in Security Metrics



SAPPHIRE

1. Global Environment : Threats

- Malicious Insiders (Rising) – always the biggest threat
- Malware authors (Steady) – esp websites that host malware
- Exploited Vulnerabilities (Reducing) – perennial hackers
- Social Engineering (Rising) – a range of methods being deployed
- Careless Employees (Rising) – mistakes
- Reduced Budgets (Rising) – recessionary impact
- Remote & Mobile Workers (Steady/Rising) - increasing
- Unstable Third Party Providers (Rising) – recessionary impact
- Downloaded Software (Steady) – open source/freeware

2009 is proving to be a very challenging year!!!



SAPPHIRE

1. Global Environment : 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

The recessionary situation is exacerbating these vulnerabilities



SAPPHIRE

1. Global 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

Well controlled organisations will prosper in 2009!!



SAPPHIRE

1. Global Environment 2009 : 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

As the recession bites, criminal groups will go out to exploit these risks – e.g. false car website scam exposed yesterday



SAPPHIRE

1. Global Environment 2009 : Controls

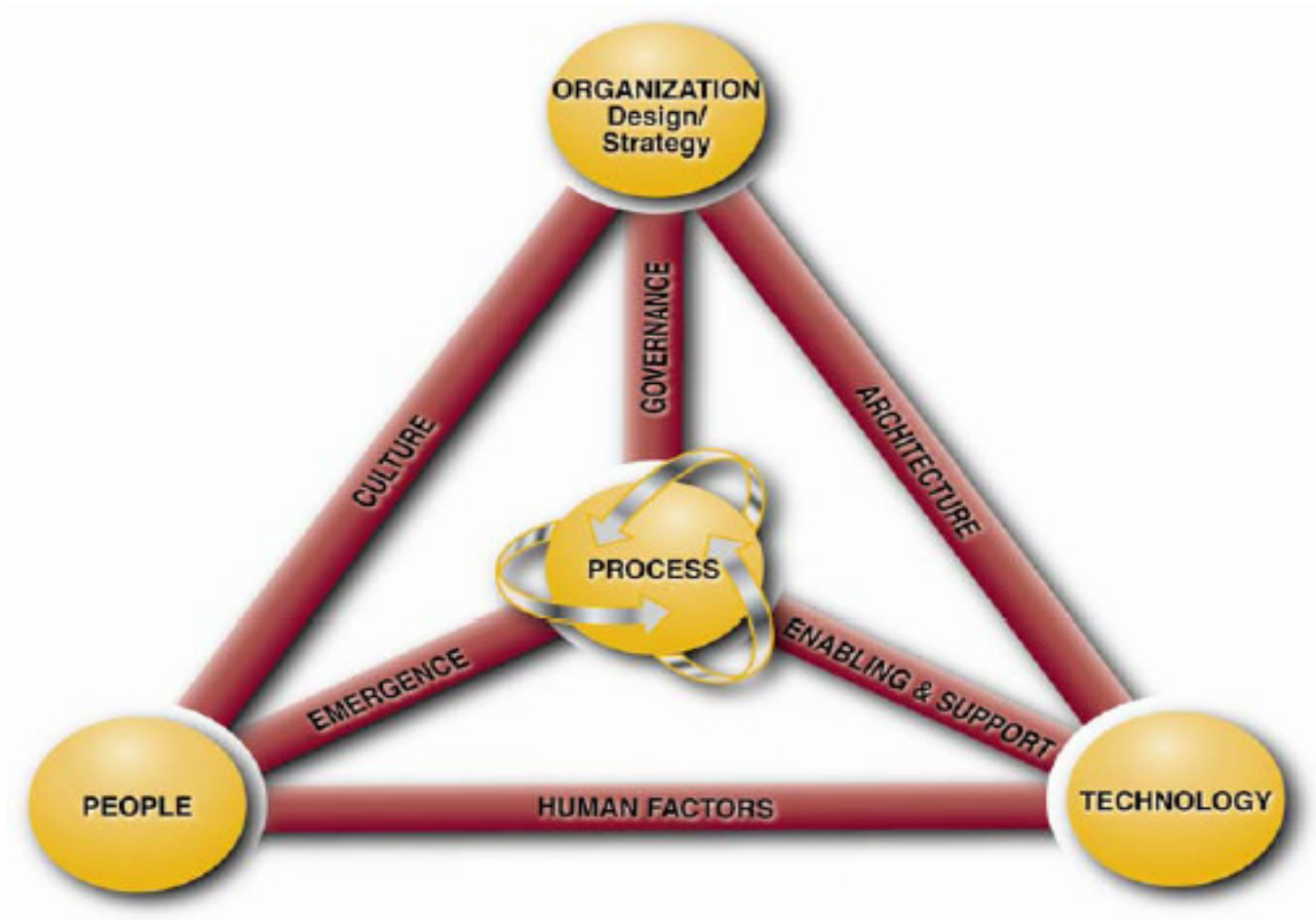
- Investment on a comprehensive ISMS
- Data Confidentiality Controls
- Data Integrity Controls
- System Integrity Controls
- Proactive technical vulnerability management
- Anti – everything software (malware; spam; spyware)
- Proactive IT audit, monitoring & reporting
- Enforcement of rights & compliance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

Governments & regulators are looking closely at what ‘checks & balances’ you have in place – this is now a major reputation issue.



SAPPHIRE

2. Need for a Business Model is Vital!





SAPPHIRE

Business 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 will address this gap and show the role of each element in relation with the dynamic interconnections (softer/nebulous issues that have not been discussed enough)



SAPPHIRE

2. Business Model 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
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)



SAPPHIRE

Model 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.



SAPPHIRE

Model 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



SAPPHIRE

Model 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



SAPPHIRE

Model 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).



SAPPHIRE

Model 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.



SAPPHIRE

Model 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’



SAPPHIRE

Model 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



SAPPHIRE

Model 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



SAPPHIRE

Model 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)



SAPPHIRE

Model 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



SAPPHIRE

UK Example – Poynter Report on HMRC (HM Revenue & Customs Department)

- ‘Information Security was not a Management priority’
Arrangements were ‘woefully inadequate’
- 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
- Report recommended the use of ISO 27002 & the associated CMM – aiming for a minimum level of 3 (Defined) & progressing to level 4 (Managed & Monitored)
- 45 recommendations made using Business Model elements



SAPPHIRE

Recommendations Detail : Strategy

14 recommendations covering:-

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
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



SAPPHIRE

Recommendations Detail : People

7 recommendations covering:-

1. Need for effective staff communications on IS
2. Align HR, comms & 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



SAPPHIRE

Recommendations Detail : Process

14 recommendations covering:-

- 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
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



SAPPHIRE

Recommendations Detail : Technology

10 recommendations covering:-

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
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



SAPPHIRE

UK : HMG Security Management Framework

- ‘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 SPF replaces MPS & Counter-Terrorist PS manual – sets out mandatory stds, with guidance on RM & new compliance/assurance 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. 5 core security principles
 3. 7 key policy documents – 70 min. mandatory requirements (MR)
 4. Detailed tools for practitioners (tec stds; policy/guidance; websites)



SAPPHIRE

Levels 1 & 2 : Statement & Principles

Level 1: Overarching Security Statement

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: Core Security Principles

1. Ultimate responsibility rests with PM/Cabinet O.
Depts/agencies (via PSec/CEO) 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



SAPPHIRE

Level 3: Seven Security Policies (Mandatory Requirements in brackets)

1. Governance, RM & Compliance (10)
2. Protective Marking & Asset Control (11)
3. Personnel Security (9)
4. IS & Assurance (19)
5. Physical Security (14)
6. Counter – Terrorism (6)
7. Business Continuity (1)



SAPPHIRE **Business Model – Deliverables 2009 onwards**

- Introductory Guide – Q1 2009: A brief guide that outlines the key elements of the Model to emphasis the importance of creating that appropriate IS culture.
- Executive Brochure – to educate & influence key stakeholders (especially Boards & Senior Management) on the importance of this new Business Model – Q2/3 2009
- Practitioners Guide – a detailed guide on how to implement an effective Model. This Guide will take time to complete. No dates set at present

As the global business environment comes under great strains in 2009, the value of this Model will be very significant.



SAPPHIRE

3. Security Metrics - ISO 27000 series

27000 Fundamentals & Vocabulary

27005
Risk
Management

27001:ISMS

27002 Code of Practice for ISM

27003 Implementation Guidance

27004 Metrics & Measurement

27006 Guidelines on ISMS accreditation

27007 Guidelines for ISMS Auditing



SAPPHIRE

3. ISO 27004 : Programme Objectives



Objectives:

- Evaluate the effectiveness of security controls & control objectives;
- Evaluate the effectiveness of the ISMS inc. continual improvement;
- Provide security indicators to assist management review
- Facilitate improvement of information security
- Provide input for security audits;
- Communicate the effectiveness of ISM to the organization;
- Serve as an input into the risk management process
- Provide output for internal comparison & benchmarking of effectiveness



3. Security Metrics - ISO 27004

Subject	Potential Metrics
1. Security Policy	
IS policy	Policy coverage (i.e. % of sections of ISO 27001/2 for which policies plus assoc. stds, procedures & guidelines have been specified, written, approved & issued). Extent of policy deployment & adoption across the organization (measured by audit or control self assessment).



SAPPHIRE

3. Security Metrics - ISO 27004

Subject	Potential Metrics
2. Organising Information Security	
Internal Organisation	% of functions/business units for which a comprehensive strategy has been implemented to maintain IS risks within accepted thresholds. % of employees who have (a) been assigned, & (b) formally accepted, IS security roles & responsibilities.
External Parties	% of 3rd-party connections that have been identified, risk-assessed & deemed secure.



SAPPHIRE

3. Security Metrics - ISO 27004

Subject	Potential Metrics
3. Asset Management	
Responsibility for Information Assets	% of assets at each stage of classification process (identified; inventoried; owner nominated; risk assessed; secured). % of key assets for which a comprehensive strategy has been implemented to mitigate IS risks and to maintain within acceptable thresholds
Information Classification	% of assets in each classification category (including not-yet-classified).



SAPPHIRE

3. Security Metrics - ISO 27004

Subject	Potential Metrics
4. Human Resources Security	
Prior to Deployment	% of new employees plus contractors, consultants, temps etc that have been fully screened & approved in line with IS policies prior to starting.
During Employment	Response to IS awareness activities measured by, say, no. of emails & calls relating to individual awareness initiatives.
Termination or Change of Employment	% of user IDs belonging to people who have left - separated into active (pending deactivation) & inactive (pending archival & deletion) categories.



SAPPHIRE

3. Security Metrics - ISO 27004

Subject	Potential Metrics
5. Physical Environmental Security	
Secure Areas	Reports from periodic site surveys, inc. regular status updates on corrective items identified in previous surveys & still outstanding.
Equipment Security	No. of stop- or stock-checks performed in the previous month, & % of checks that revealed unauthorized movement of IT equipment, media etc . or other security issues.



SAPPHIRE

3. Security Metrics - ISO 27004

Subject	Potential Metrics
6. Communications & Operations Management	
Ops Procedures & Responsibilities	Maturity metrics e.g. “half-life” for applying IS patches (time to update 50% of pop of vulnerable systems)
3rd Party Service Delivery Management	Cost of downtime due to non-fulfillment of SLAs. Performance evaluation to inc. quality of service, delivery, cost etc.
System Planning & Acceptance	% of emergency, H, M & L risk changes. No./trends of reversed changes, rejected vs. successful changes. % of systems that (a) comply with baseline security & (b) have been tested.
Protection Against Malicious/Mobile Code	No. of viruses, worms, trojans,spams detected & stopped. No/costs of malware incidents.
Backup	% successful. (inc test restores). Time to retrieve media from off-site storage. % sensitive data encrypted.



SAPPHIRE

3. Security Metrics - ISO 27004

Subject	Potential Metrics
6. Communications & Operations Management (contd)	
Network Security Management	No. of incidents per month, (minor/significant/serious) with trends analysis & details of serious events.
Handling	% of physical backup/archive media that are encrypted.
Exchange of Information	% of 3rd-party links for which IS requirements have been satisfactorily (a) defined & (b) implemented.
Electronic Commerce Services	"eSecurity status" i.e . management confidence , based on analysis of pen tests, incidents, vulns, changes etc.
Monitoring	% of systems whose IS logs are (a) approp.configured, (b) captured to a centralised management facility & (c) routinely monitored/reviewed/assessed. Trends in no.of security log entries that have been (a) captured; (b) analyzed; & (c) led to follow-up activities.



3. Security Metrics - ISO 27004

Subject	Potential Metrics
7. Access Control	
Business Requirement for Access Control	% of corp application systems with "owners" (a) identified, (b) accepted responsibilities, (c) risk-based IS & access reviews, & (d) defined role-based rules.
User Access Management	Av. delay between change requests raised/actioned, & no. of change requests actioned per month (with trends analysis on any peaks/troughs).
User Responsibilities	% of job descriptions inc (a) documented & (b) accepted.
Network Access Control	Firewall stats e.g.% of outbound packets blocked (e.g. attempted access to blacklisted websites; no. of potential attacks repelled, (trivial/concern/critical).
Operating System Access Control	System/network vuln stats e.g. no. of vulns closed, open & new; av.speed of patching vulns (by vendor or in-house priorities/categories).



SAPPHIRE

3. Security Metrics - ISO 27004

Subject	Potential Metrics
7. Access Control (continued)	
Application & Information Access Control	% of platforms fully compliant with baseline stds (by independent testing), with notes on non-compliant systems
Mobile Computing & Teleworking	'security status' i.e. commentary on mobile IT (laptops, PDAs, cellphones etc.) & teleworkers (home working, mobile workforce etc.), with notes on incidents, vulns & projections of increasing risks, coverage of configs, antivirus, personal firewalls etc.



SAPPHIRE

3. Security Metrics - ISO 27004

Subject	Potential Metrics
8. Information Systems Acquisition, Development and Maintenance	
Security Requirements of Information Systems	See 11.1
Correct Processing in Applications	% of systems where data validation controls adequately (a) defined; & (b) implemented & effective by testing.
Cryptographic Controls	% of systems with sensitive data where controls fully implemented (3/12monthly reporting).
Security of System Files	% of systems independently assessed as compliant with baseline stds; not been assessed, or not compliant, or no approved baseline .
Security in Development and Support Processes	'security status' commentary on status of development processes, with notes on incidents, vulns; risks etc.
Tec Vuln Management	Patch latency i.e. deploy half-life.



SAPPHIRE

3. Security Metrics - ISO 27004

Subject	Potential Metrics
9. Information Security Incident Management	
Reporting IS events & weaknesses	Service Desk stats with analysis of no./types of calls relating to IS (e.g. pswd changes; queries on IS risks & controls as a % of total). Then create & publish a league table of departments on IS-consciousness
Management of IS incidents & reports	No. & gravity of breaches, e.g costs to analyze, stop & repair & any tangible/intangible losses incurred. % of IS incidents that caused costs above acceptable management thresholds.



SAPPHIRE

3. Security Metrics - ISO 27004

Subject	Potential Metrics
10. Business Continuity Management	
IS Aspects of BCM	<p>% of BCPs at each stage of the lifecycle (needed / specified / documented / proven).</p> <p>% of business units with BCPs that have been adequately (a) documented & (b) proven by suitable testing within the past 12 months.</p>



SAPPHIRE

3. Security Metrics - ISO 27004

Subject	Potential Metrics
11. Compliance	
Compliance & legal requirements	No. of legal compliance recommendations analyzed by status (closed, open, new, overdue) & significance or risk level (H, M or L). % of key external requirements n deemed by objective audit to be compliant.
Compliance with IS Policies & Standards & Technical Compliance	No. of internal policy/compliance recommendations analyzed by status (closed, open, new, overdue) & significance or risk level (H, M or L). % of IS compliance reviews with no major violations noted.
Information Systems & Audit Considerations	No.of audit recommendations analyzed by status (closed, open, new, overdue) & significance or risk level (H, M or L). % of IS-related audit findings resolved & closed vs. opened.. Resolution/closure time for recommendations .



SAPPHIRE

Presentation - Conclusion

I hope you can see that my aim was to bring delegates together in a 'strong call of action' – consider using TSD – Think, Solve & Do.

The Business Model enables 'strategic/tactical systemic thinking'

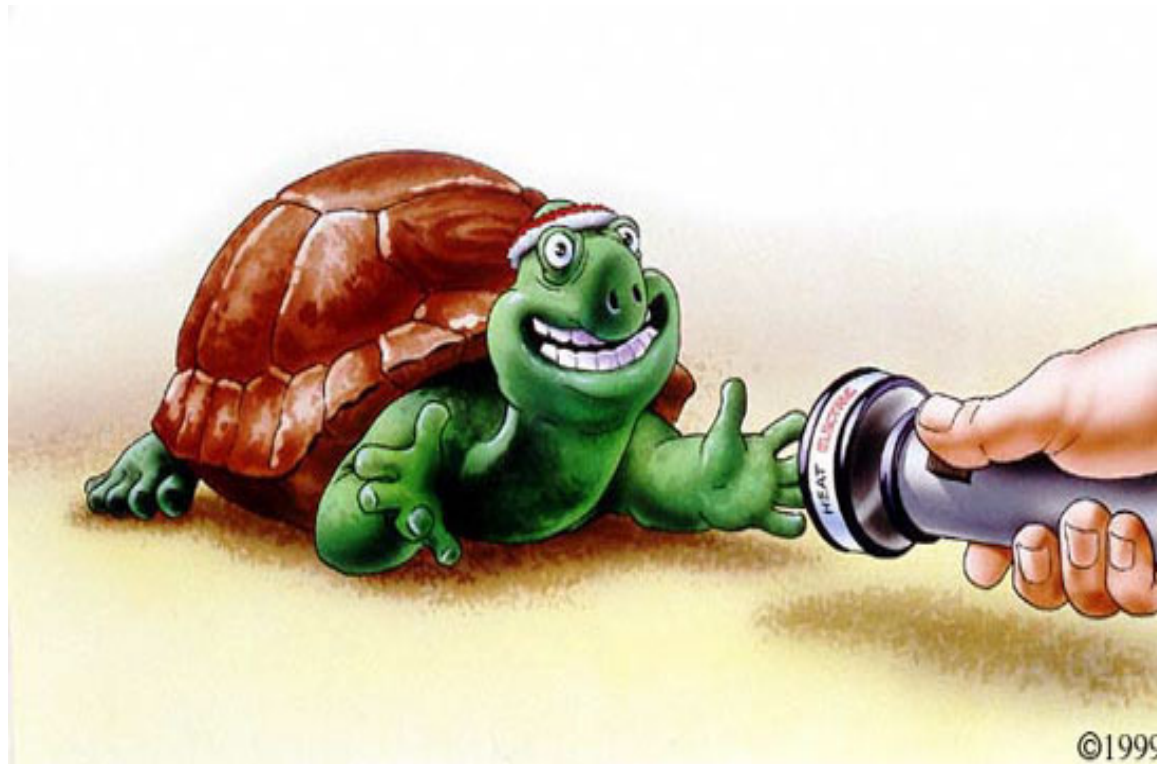
The benefits of the Model are that you will be able to:-

- Define your strengths
- Maximise reputation/brand
- Increase awareness of IS culture
- Provide effective risk communication across the enterprise on IS
- Provide a 'return on investment'
- Reduce your IS exposure



SAPPHIRE

Any Questions





SAPPHIRE

Sapphire

FORENSICS

- Computer Forensics
- Data Recovery
- Forensic Email Archiving
- Forensic Training

BUSINESS CONSULTANCY

- ISO27000 series
- Information Governance
- CLAS
- Business Resilience

Thank you

Vernon Poole – vernon.poole@sapphire.net

TECHNICAL CONSULTANCY

- Content Security
- Policy Compliance
- Application Firewalls
- End Point Security
- High Availability
- Remote Access SSL VPN
- Strong Authentication

BUSINESS ASSURANCE

- Penetration Testing
- Vulnerability Assessments
- Strategic Support Agreements
- Security Audits