

# Business Oriented Security Strategy



## IT-business-security alignment

[daniel.dresner@ncc.co.uk](mailto:daniel.dresner@ncc.co.uk)  
[andy.hopkirk@ncc.co.uk](mailto:andy.hopkirk@ncc.co.uk)



1

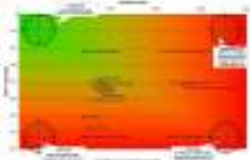
# Business Oriented Security Strategy



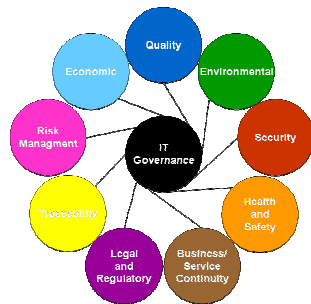
- The National Computing Centre



- IT-Business-Security alignment



- Doing it... IT governance



- We're only human...

- Standards and Good Practice

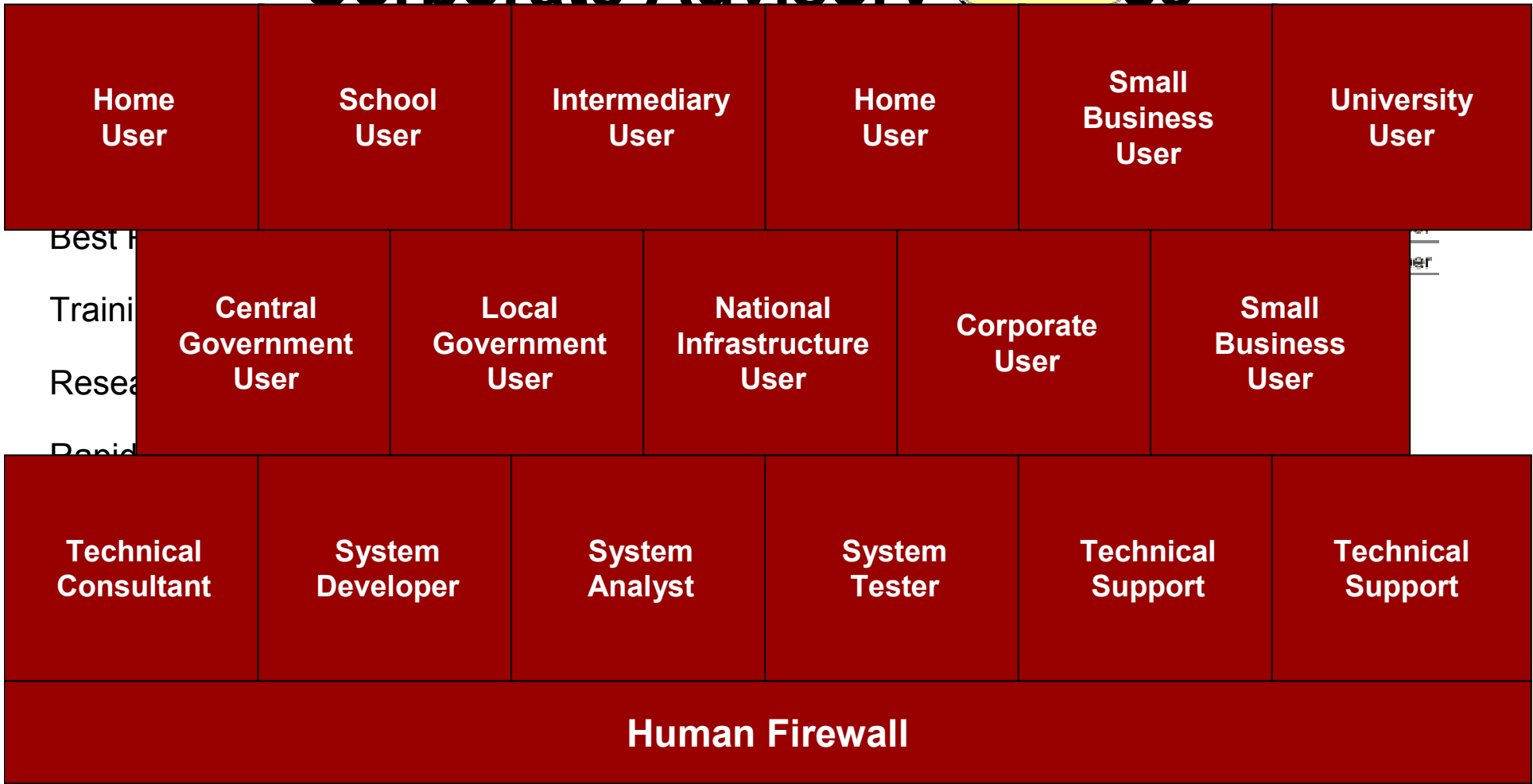
Responsibility	Strategy	Acquisition
Performance	Conformance	Human Behaviour



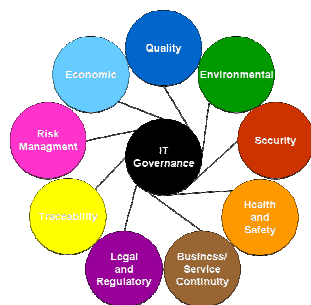
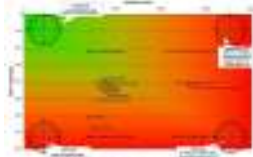
ITadviser  
Benchmarks

# The National Computing Centre Corporate Advisory Service

Standards and good practice

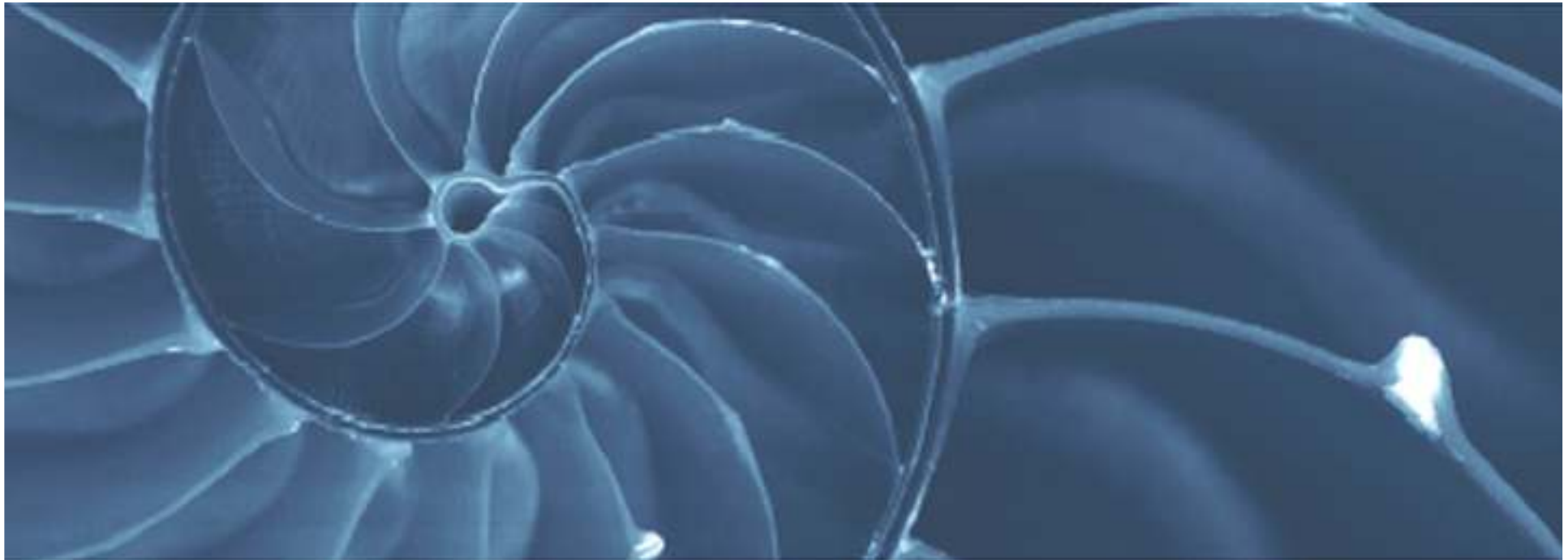


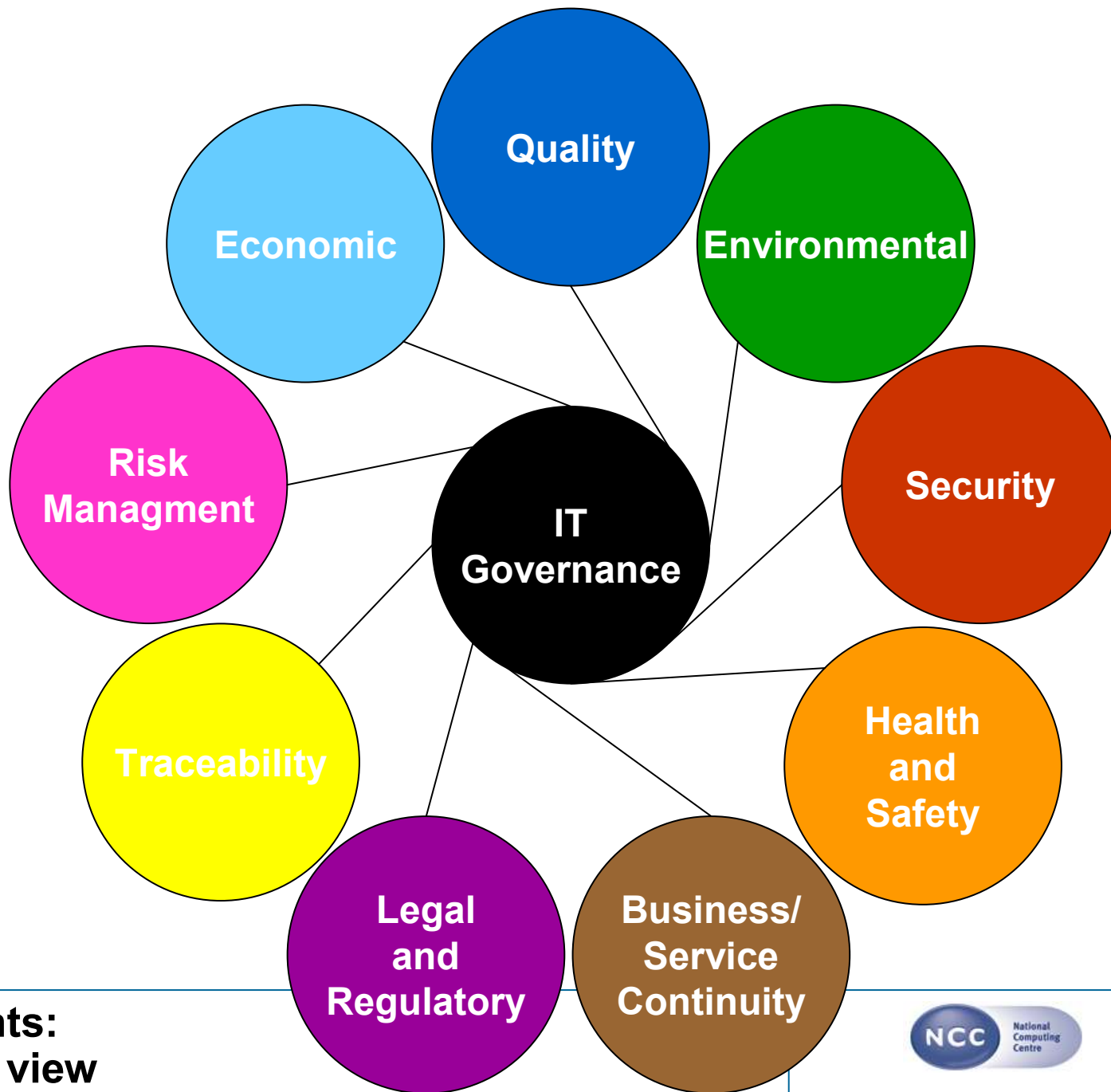
# Aligning what people do and what the business needs them to do!



- Sample of 5 assets to protect:
  - Realise the corporate business plan – needs to be realised 
  - Individual objectives – need to set 
  - Compliance with regulations – needs to go on 
  - Compliance' with good practice (that means 'lessons learnt – is optional but why risk avoidable mistakes 
  - Organisational brand – the golden goose that may be all we have 
- Events that could expose us:
  - Corporate business plan: Not carried thru' to day-to-day
  - Individual objectives – Mismatch between what is done and what you say you do
  - Compliance with regulations – Compliance is only apparent after the work is done.
  - Compliance' with good practice –so many standards . . . how can we choose them
  - Organisational brand – you can't build a reputation on what you're going to do . . .

# How you do it . . . IT governance

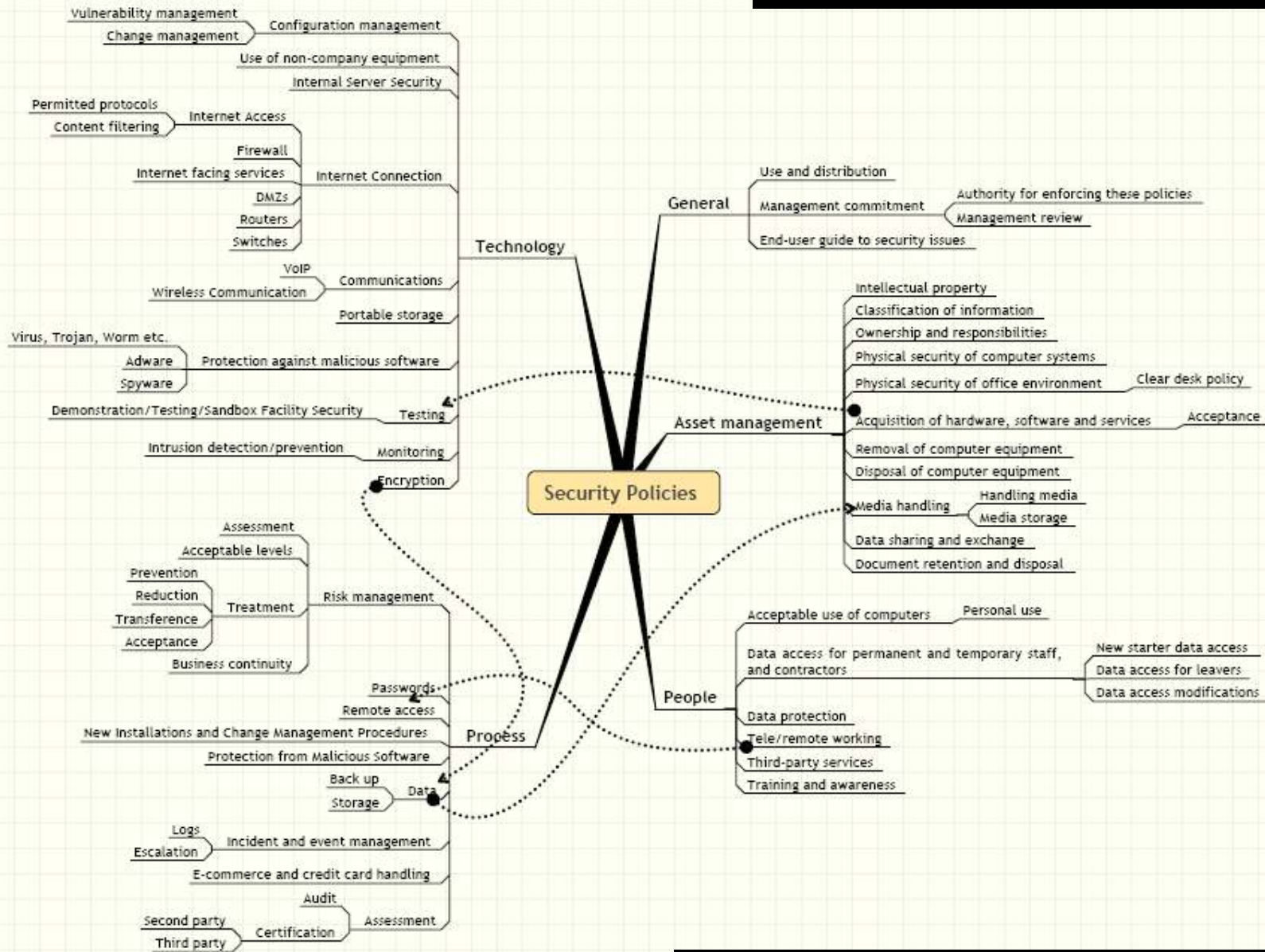




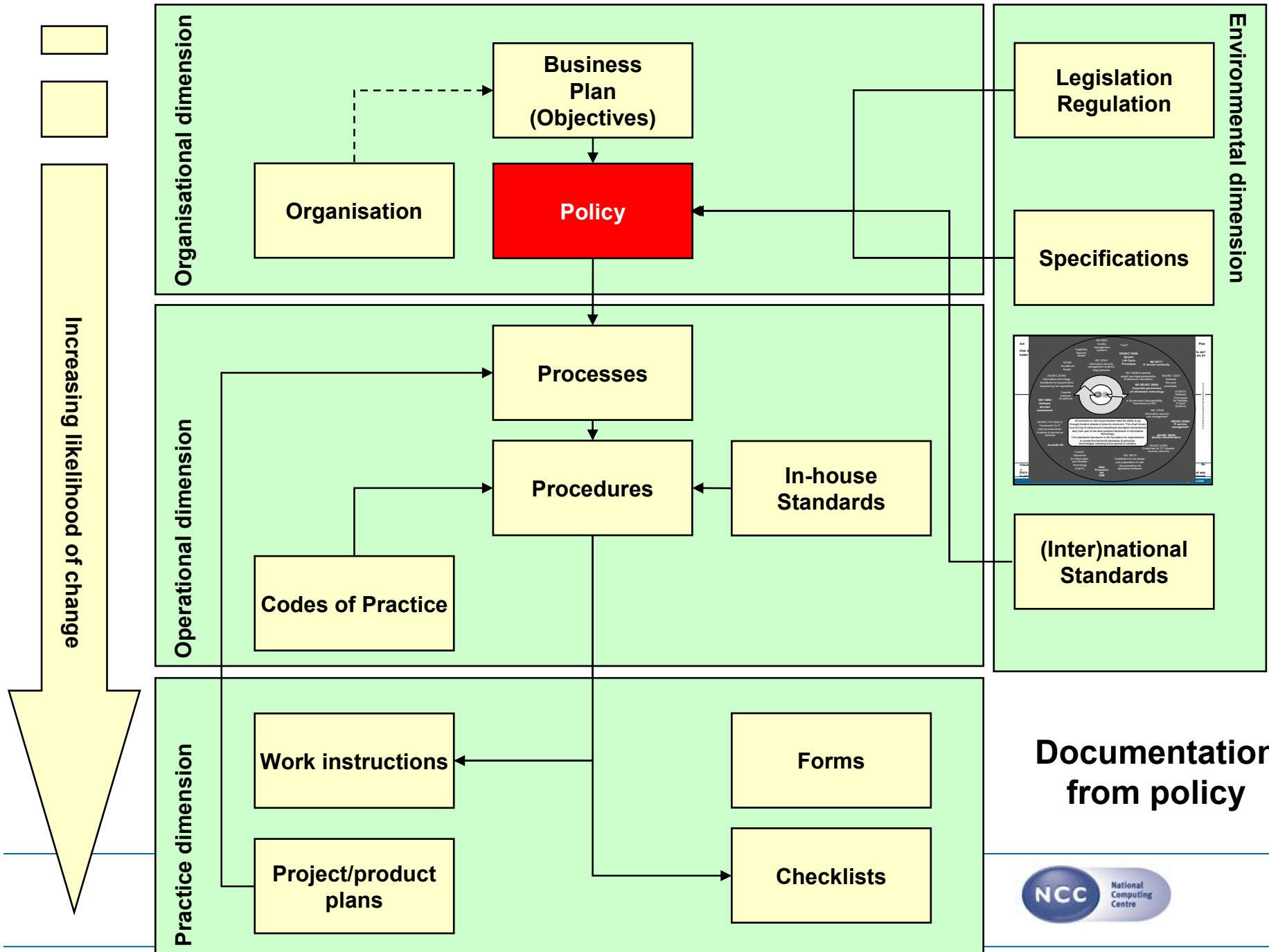
**Components:  
a practical view**



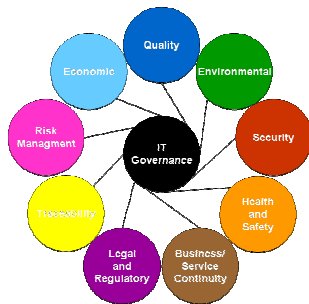
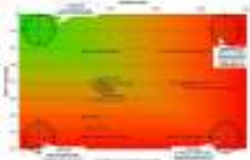
# Recommended minimum set



Policies: ready decided treatments

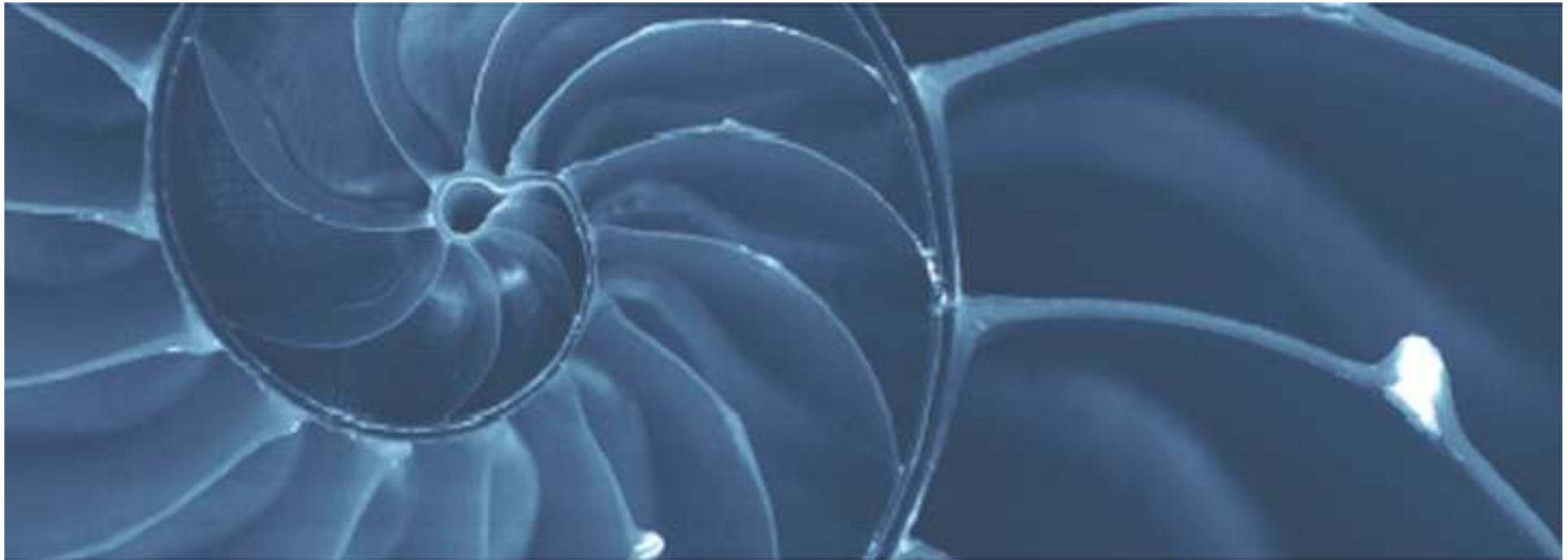


# Write words for good policies



- Purpose
  - Why do we need it and what's the risk of not having it
- Scope
  - What it applies to, and what – if anything – is excluded
- What the policy is
  - Clear, pithy, and imperative
- How it's monitored
  - If it's worth having, it's worth checking
- What happens if the policy is breached
  - Because Murphy was right
- What to do to enforce it
  - Technology, awareness, or a mix of both
- Controls
  - Processes, procedures and other related documents (the 'how to's')

# Policies and procedures: the human side



Change

Asset management

Information systems

Assess impact

Impact levels

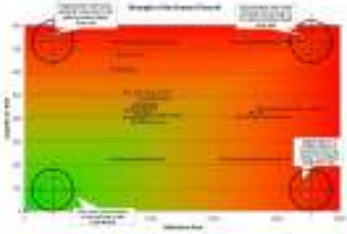
Risk assessment

Risk treatment plan

Policy setting (controls)

Applicability

Implementing procedures



What needs to be governed?

How important are the information assets to the achievement of corporate objectives?

Balancing the risk appetite of the community with the risk attitude of the individual.

Commensurate deployment

Market forces

Innovation

Business plan

Resourcing

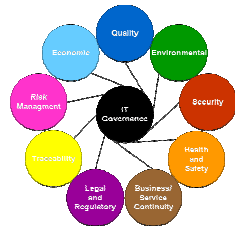
Corporate objectives

Risk literacy

Individual objectives

Appraisals

Audits/monitoring



Alignment

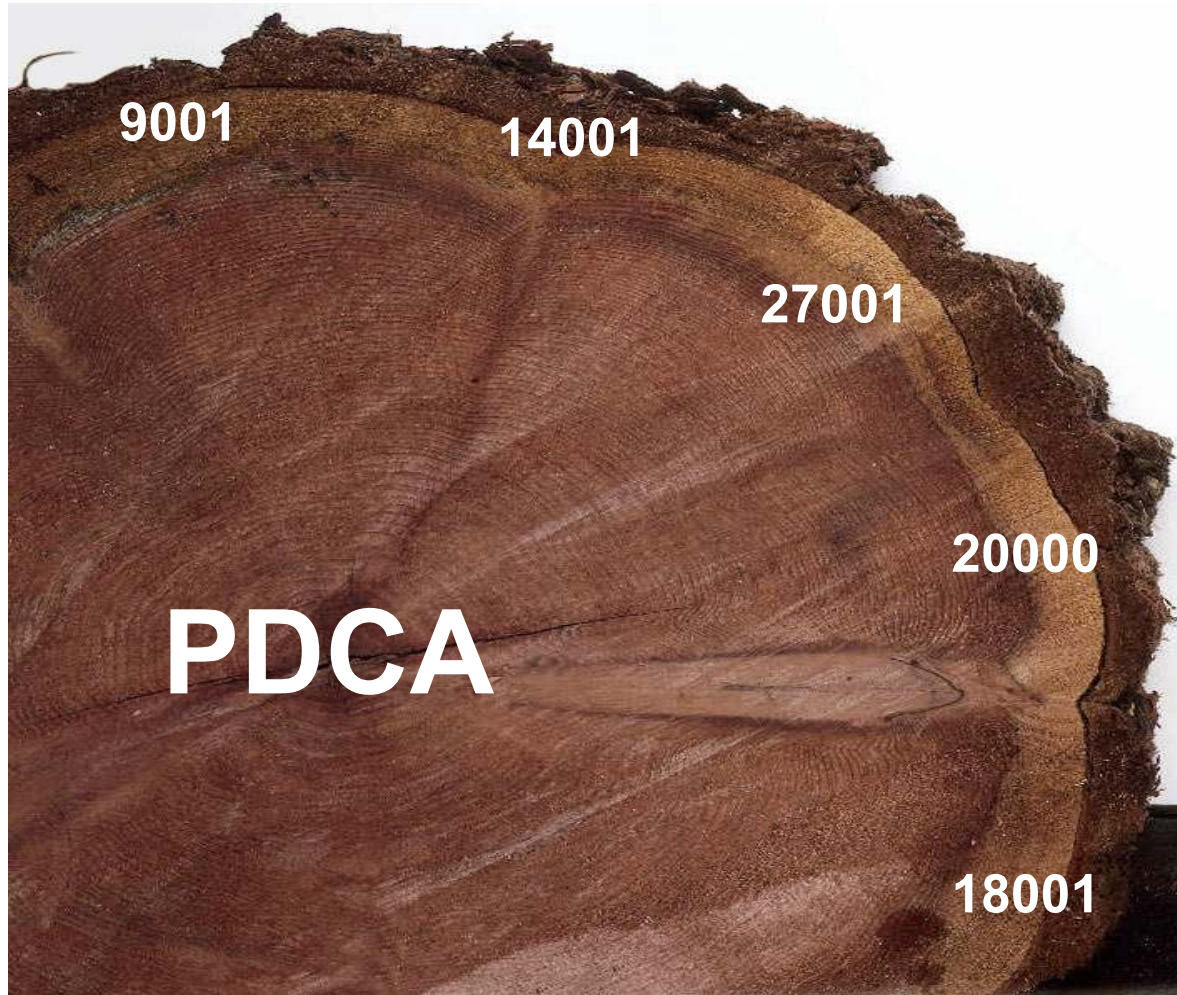


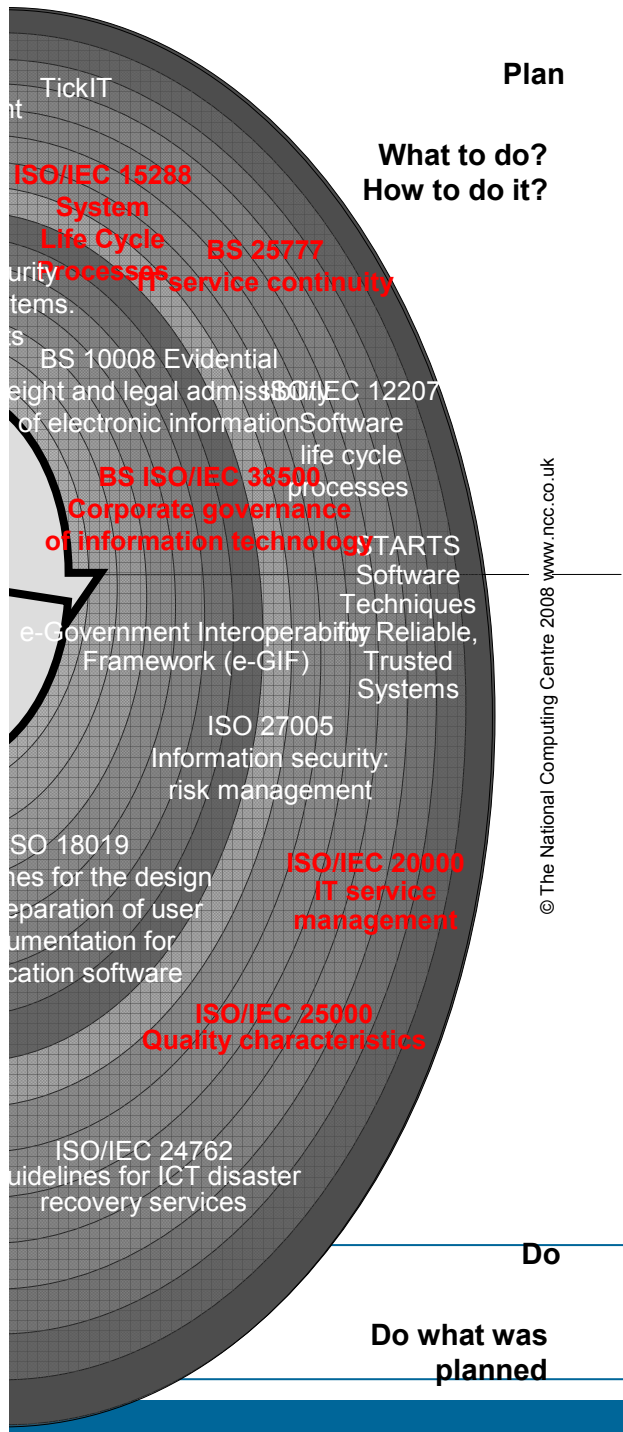
# Standards and good practice

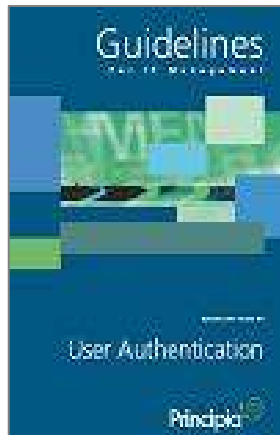
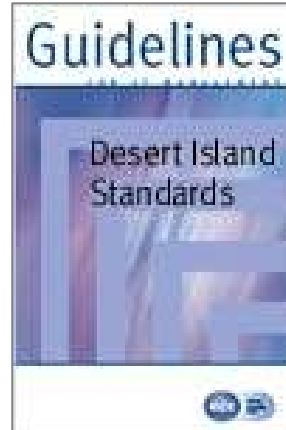
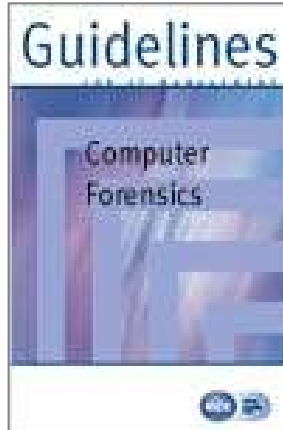
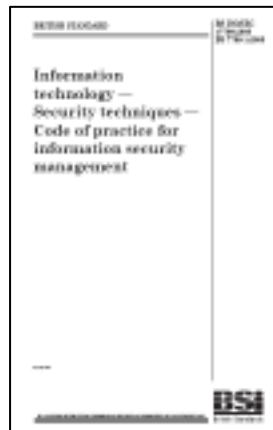


## The business toolbox

# PDCA: one rule to ring them all







**TOWARDS SOFTWARE EXCELLENCE**

### Customer-Supplier

The Customer-Supplier process category consists of processes that directly impact the customer, support development and transition of the software to the customer, and provide for the correct operation and use of the software product and/or service.

#### Buying in Software and Related Services (Acquisition, 2)

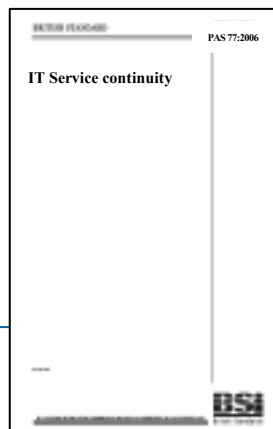
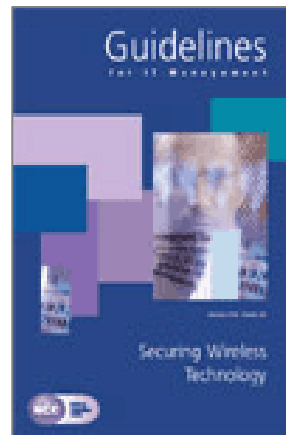
Preparing to buy-in products and services (Acquisition preparation, 3)

**About this activity**

For any organisation, buying a software application or information system is rarely straightforward. For a small company, the consequence of getting it wrong can be substantial. To ensure your business goals are achieved, you users' needs are met and you get maximum benefit from your investment, you must prepare thoroughly **before** any suppliers are involved. (Just because you are a small company, doesn't mean that you don't need to prepare for acquisition seriously - it can be even **more** important because of the potentially greater impact of getting it wrong.)

At the end of this preparation step you should know the following:

- The expected result of the acquisition (for example, a new system, a updated application, a new way of working) - in other words what you will have been achieved when the acquisition has been completed
- A set of requirements that can later be used as a basis for evaluating and accepting the system or application
- The strategy or approach you expect to apply in making the acquisition
- How you will evaluate the delivered system and decide whether it is acceptable or if more work is required



### Practical advice for business

#### IT risk assessment tool

It is vital to recognise the risks associated with the use of IT in business environments, those unaddressed dangers that can be considered a real and substantial operational risk. Investigate further, to identify from these risks, you may wish to identify control measures your business needs, there are even events in which a total ITD overhaul is required if you don't take these harmful and vital to your business practices and systems.

This tool will help you understand the main dangers to your systems and networks (such as hardware, software, engineering, and what to do to recover from when an ITD business) - it should have about five minutes to complete.

The information that this tool gives you should never be used as a substitute for legal or professional advice.

Go straight to the back section.

This tool developed with:

# Knowledge Transfer

***“Excellent, relevant and refreshingly represented”***

***“Lots of ideas and good starting points”***

***“Very informative and constructive”***

***“Impressed with the content”***

***“Plenty of useful examples”***

***“Good being involved”***

***“In-depth knowledge”***

***“Good programme”***

***“Valuable”***

**The National Computing Centre  
Corporate Advisory Service . . .**

[daniel.dresner@ncc.co.uk](mailto:daniel.dresner@ncc.co.uk)

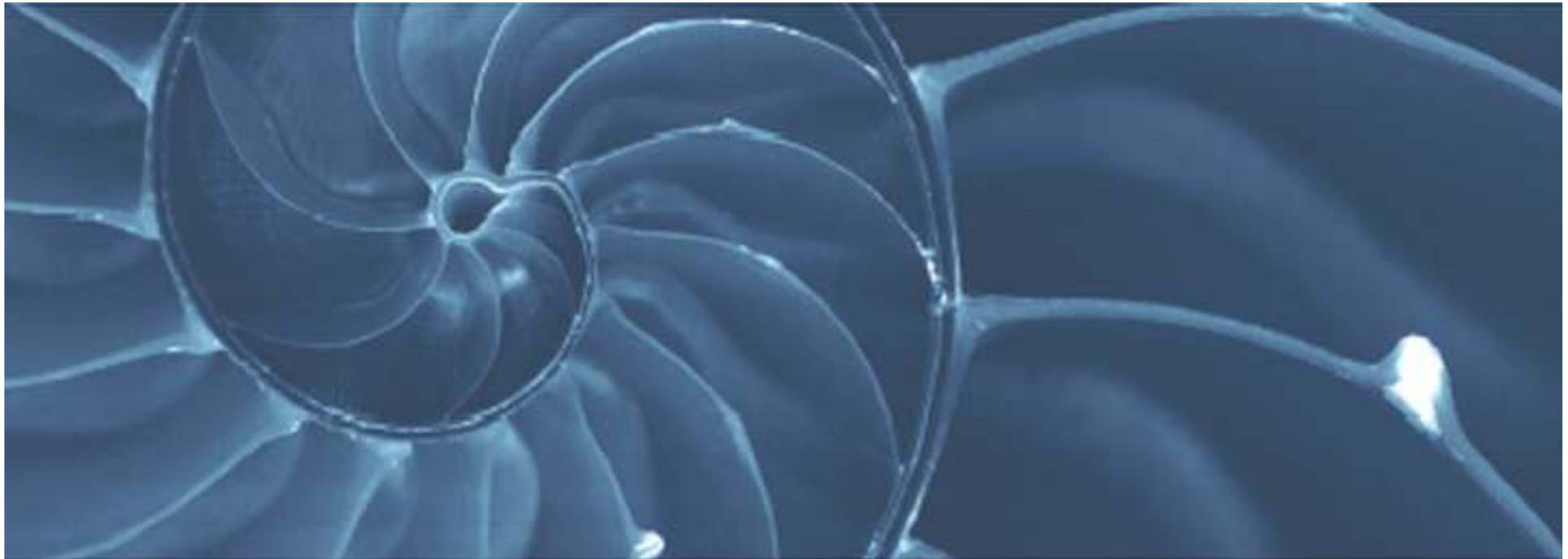
07703 501 167

[andy.hopkirk@ncc.co.uk](mailto:andy.hopkirk@ncc.co.uk)

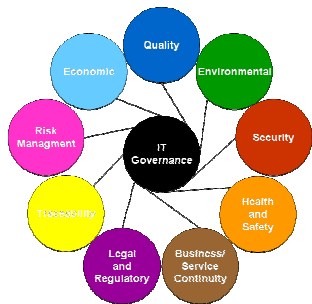
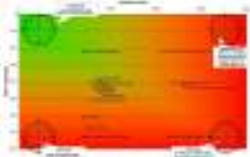
07880 788 871






The collage features several screenshots of the National Computing Centre (NCC) website. The top screenshot shows the 'Security - From risk to treatment' event page, dated 26 Feb 2009. Below it is a screenshot for 'IT Governance' events, listing dates from June 2009 to February 2010. A central screenshot titled 'Information security: the people element' includes a bar chart with red bars of varying heights. To the right, a woman with long brown hair is pointing her finger at the bar chart. The bottom right corner of the collage shows the NCC logo and the text 'National Computing Centre'.

Conclusion: business centric; risk aware



# Aligning what people do and what the business needs them to do!



- |  |  |   |
|--|--|---|
| <ul style="list-style-type: none"> <li>• Events that could expose us:             <ul style="list-style-type: none"> <li>– Corporate business plan: Not carried thru' to day-to-day</li> <li>– Individual objectives – Mismatch between what is done and what you say you do</li> <li>– Compliance with regulations – Compliance is only apparent after the work is done.</li> <li>– Compliance' with good practice –so many standards . . . how can we choose them</li> <li>– Organisational brand – you can't build a reputation on what you're going to do . . .</li> </ul> </li> </ul> | <br><br><br><br><br><br><br><br> | <ul style="list-style-type: none"> <li>• What happens to our 5 risks?             <ul style="list-style-type: none"> <li>– Corporate business plan – policies translated it to actions</li> <li>– Individual objectives – translate plan and consistent policies into actions for individuals</li> <li>– Compliance with regulations – Design policies and processes with regulations in mind</li> <li>– Compliance' with good practice –key standards that make framework for others</li> <li>– Organisational brand – strengthen it by securing your place in the greater firewall</li> </ul> </li> </ul> |
|--|--|---|

**Business-centric security – policy is policy**



