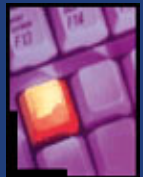
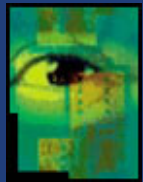


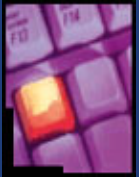
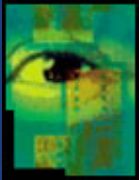
Standards Observatory: The Landscape of Business Continuity

Daniel Dresner (NCC)





Enabling
Effective
IT



The National Computing Centre

UK's foremost membership organization for IT Users

Mission to promote the effective use of IT

1000 member organisations in the UK

Representing £billions in turnover

Members drive the agenda (by board and survey)

Size, public and private sector representation

Voice of the IT user

1966-1996-1999-2003

DTI, OeE, EPSRC, SAINT, SANS, ISACA, IAAC

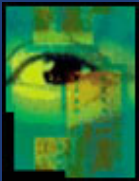


Identifying, creating, disseminating best practice in IT

Not for profit/limited by guarantee

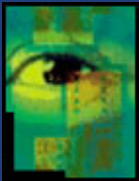
ISO 9001:2000/TickIT

BS 7799:2002 Part 2



www.ncc.co.uk

- Publications
- myITadviser (10,000)
- Advice line
- Guidelines
- Best Practice Guides
- Viewpoints
- Knowledge Networks
- Events
- Surveys (Security from '94)
- On-line resources
- Software
- Collaborative research
- Technology Evaluations
- Managed Projects
- Standards
- Secure web hosting
- Vulnerability tool
- CIO Connect
- Certus
- IITT
- Current themes
 - Risk and security
 - e-Business
 - Knowledge Management
 - Open Source
 - Standards
 - Skills
 - Legal
- Developing
 - Vertical groups
 - Regeneration
 - Leadership

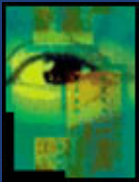


What to put into a 'BCP'

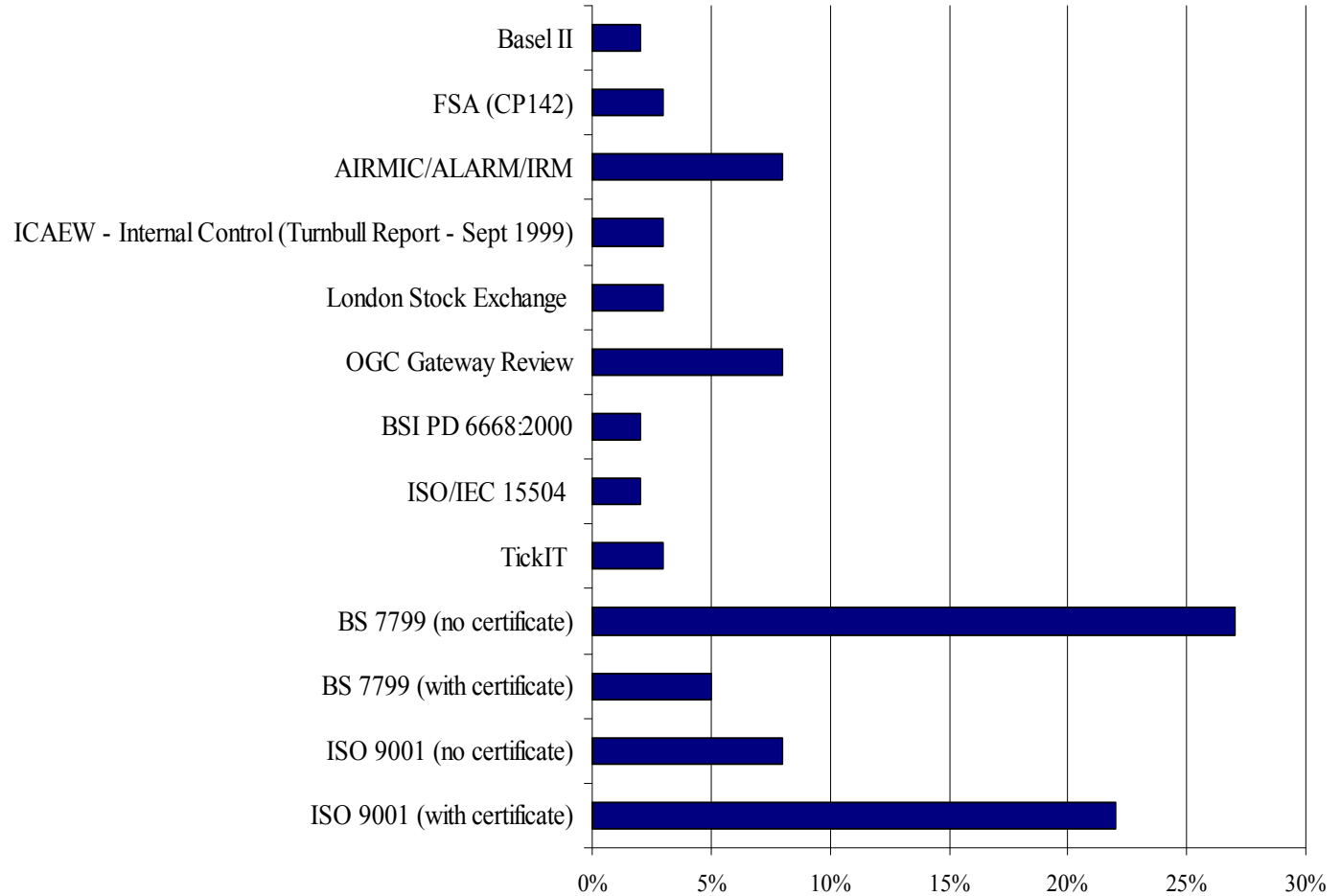
- Technical Aspects
 - Modification
 - Contents
 - Introduction
- Document Management
 - Document control
 - Storage
 - Off-site-storage of this
 - Updates
 - Distribution
- Audits
 - Rehearsals
 - Tests of the
- Prioritisation
 - How is the disaster?
 - Key assets
 - Category Outage Damage
 - Key services
 - Continuity priorities
- Incident Management
 - Responsibilities
 - Process in event of incident
 - Incident/Action Log
 - Process at end of incident
- Contacts
 - Scenario action team contacts
 - Service contractors, suppliers, and maintenance companies
- Disaster Recovery Plan
 - Related Documents
 - Alternative strategies
 - Action when off-line
 - Solutions for Minor incidents
 - Solutions for Major incidents
 - Systems Organisation
 - Emergency premises

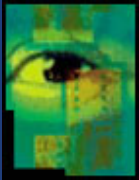
X

Not today!



Current use of standards





Binyon's Philosophy

- Nothing is easy
- If it's easy . . . you're not doing it right.
- Everything is more urgent¹ than everything else.
- It's never the right time to do anything.
- Nothing is what it seems

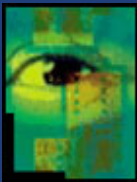
¹ I know it's urgent but is it important?





National Computing Centre

Enabling Effective IT



ISO 9000

Consumer

Corporate Social Responsibility

BS 7799

Business continuity

CoBIT Towards Software Excellence

TickIT

Viruses, worms
Basel A

Spam e-mails
Copyright and patents

ISO 15288

Data Protection

**Recognising Responsibility
Managing Risk
Business Continuity**

CMM Electronic communications
Programme
ISO 15400

Freedom of information
Identity theft

Telecommunications

Regulation of investigatory powers

Metadata

e-GIF

Digital Obligations

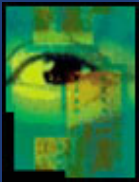
Fraud

Companies

ISO 14598

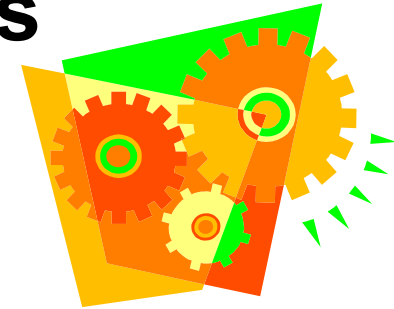
EFQM

Jurisdiction



Finding the order . . .

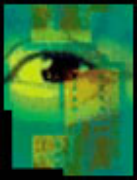
- The business operations
- The operational risks
- Mitigating the risks
- Business continuity



- Knowledge management
- Predictability

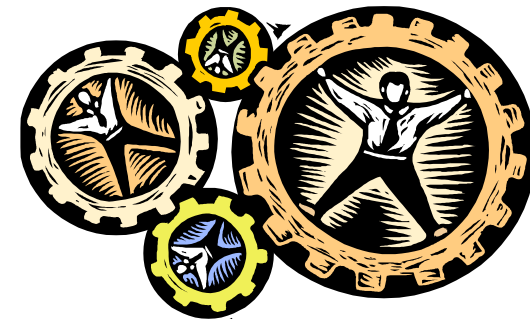


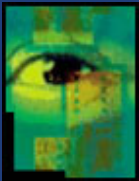
- **Standards Standards Standards**



For example

- Poorly specified **requirements**
 - ISO 9126 Quality Characteristics
 - STARTS
- **Security** breaches
 - ISO 17799 ISMS
- Software source code **availability**
 - CWA 13620 Escrow
- e-Business **interoperability**
 - e-GIF/e-BIF
- Inadequate **outsourcing** arrangements
 - BS 15000

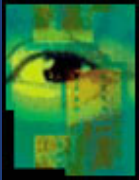




Lessons to be learned



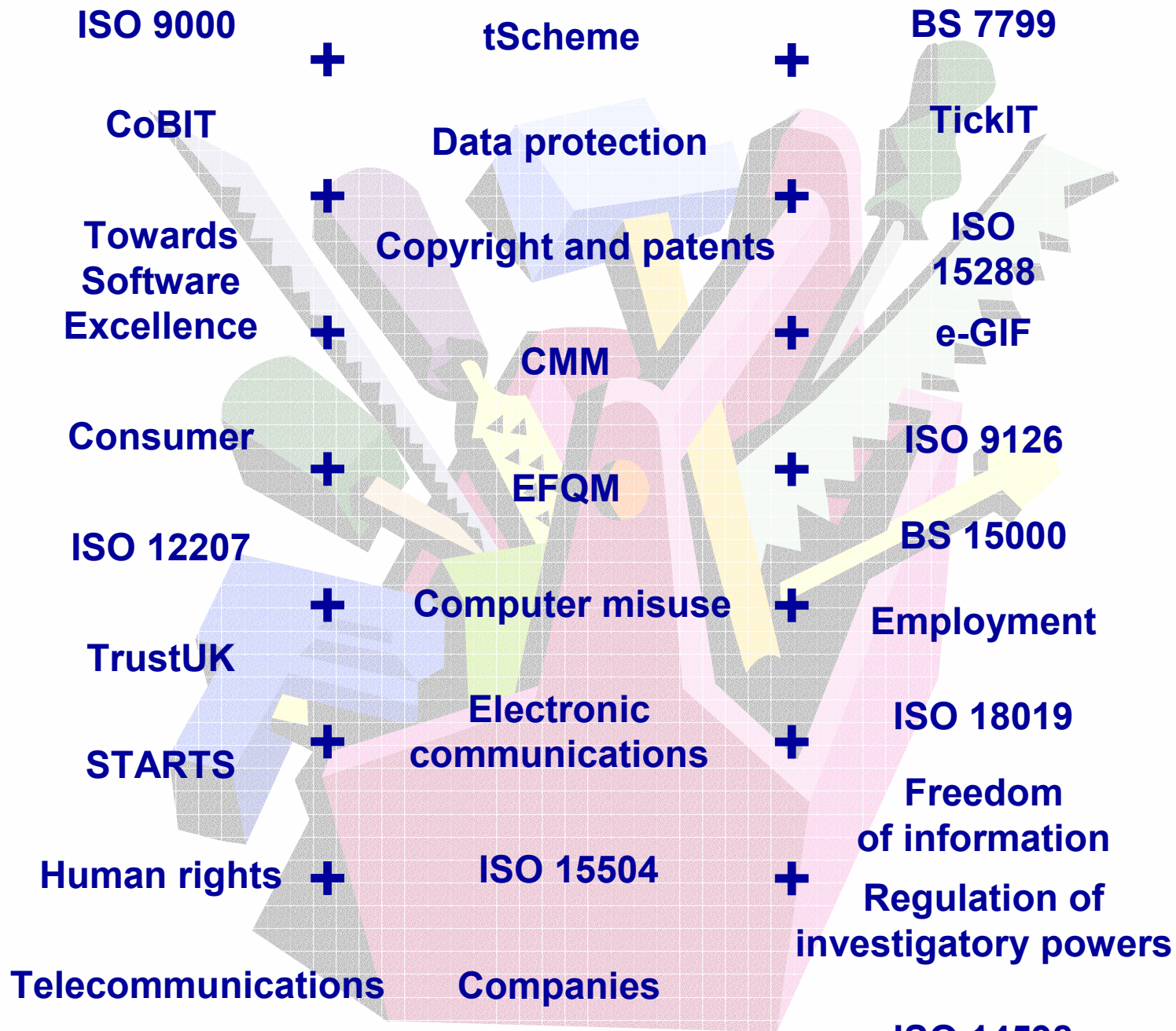
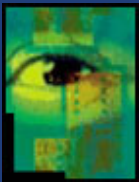
- ISO 9001 for Quality
- BS 7799 for Information Security
- TickIT for Software Quality
- ISO/IEC 15504 for Process Assessment
- tScheme for digital signatures
- Firm Risk Assessment Framework
- CCTA Risk Analysis and Management Method
- Risk Management Standards (AIRMIC/ALARM/IRM) - 2002
- BSI PD 6668.2000 – Managing Risks for Corporate Governance
- OGC (Office of Government Commerce)
 - Gateway Review - Management of Risk – Guidance for practitioners 2002
- PAC (Public Accounts Committee) – Improving the Delivery of Government IT Projects, 2000
- ISO 9004: 2000 Guidelines for Performance Improvement
- London Stock Exchange
 - The Combined Code: Principles of Good Governance & Code of Best Practice (May 2000)
- ICAEW
 - Internal Control: Guidance for Directors on Combined Code
 - (Turnbull Report – Sept 1999)
- FSA (CP142 – Operational Risk Systems and Controls) – July 2002
- Basel II (consultative papers CP2 & CP3 including Operational (& IT) Risk Management)
- Review of the role and effectiveness of non-executive directors (Higgs Report)

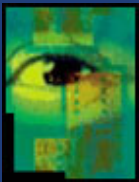


Desert Island Standards

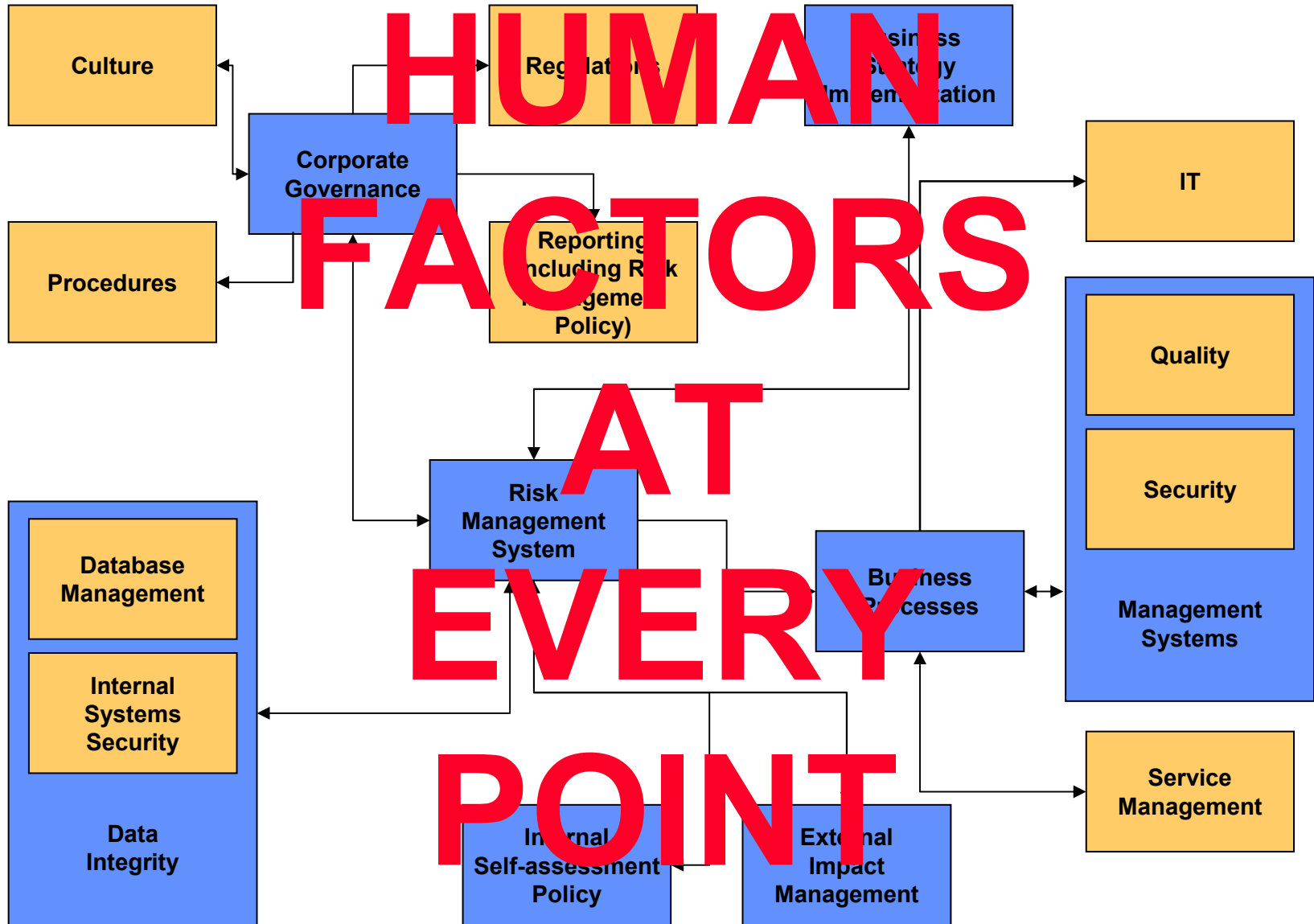
- **ISO 15288: Information Technology - Life Cycle Management - System Life Cycle Processes**
- **ISO 9126 Software engineering - Product quality**
- **BS 15000 IT service management**
- **ISO 15504 Information technology - Software process assessment**
- **The Data Protection Act 1998**
- **STARTS Software Techniques for Reliable, Trusted Systems**
- **e-GIF (the e-Government Interoperability Framework)**
- **ISO 18019 Guidelines for the design and preparation of user documentation for application software**

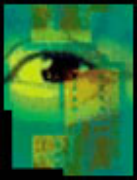




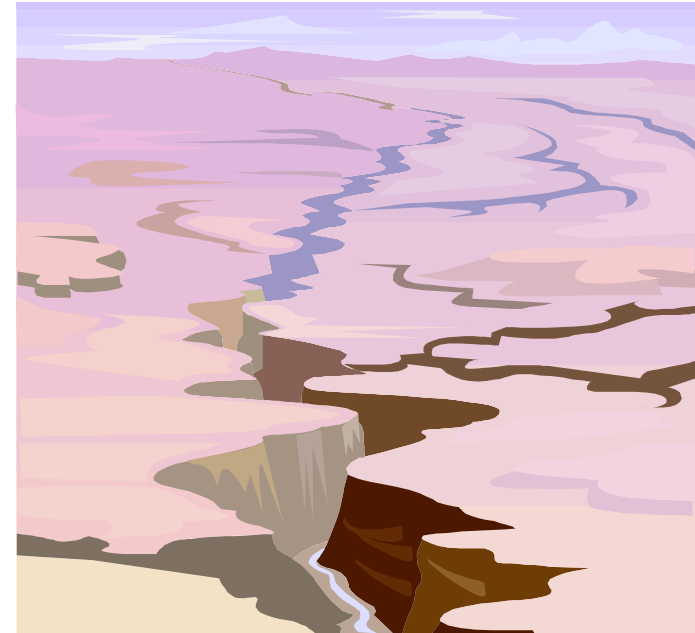
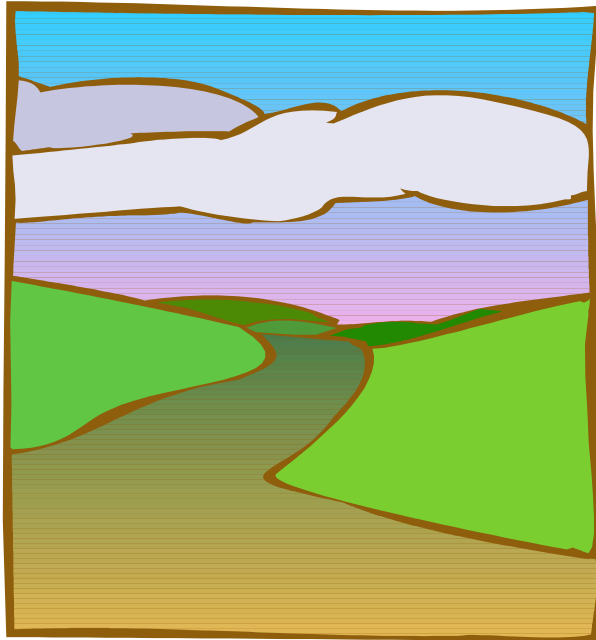


Interconnectedness

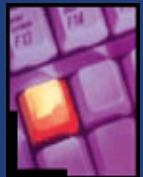
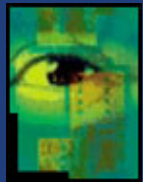




Doing it right



With standards . . . or without?



Questions?

daniel.dresner@ncc.co.uk