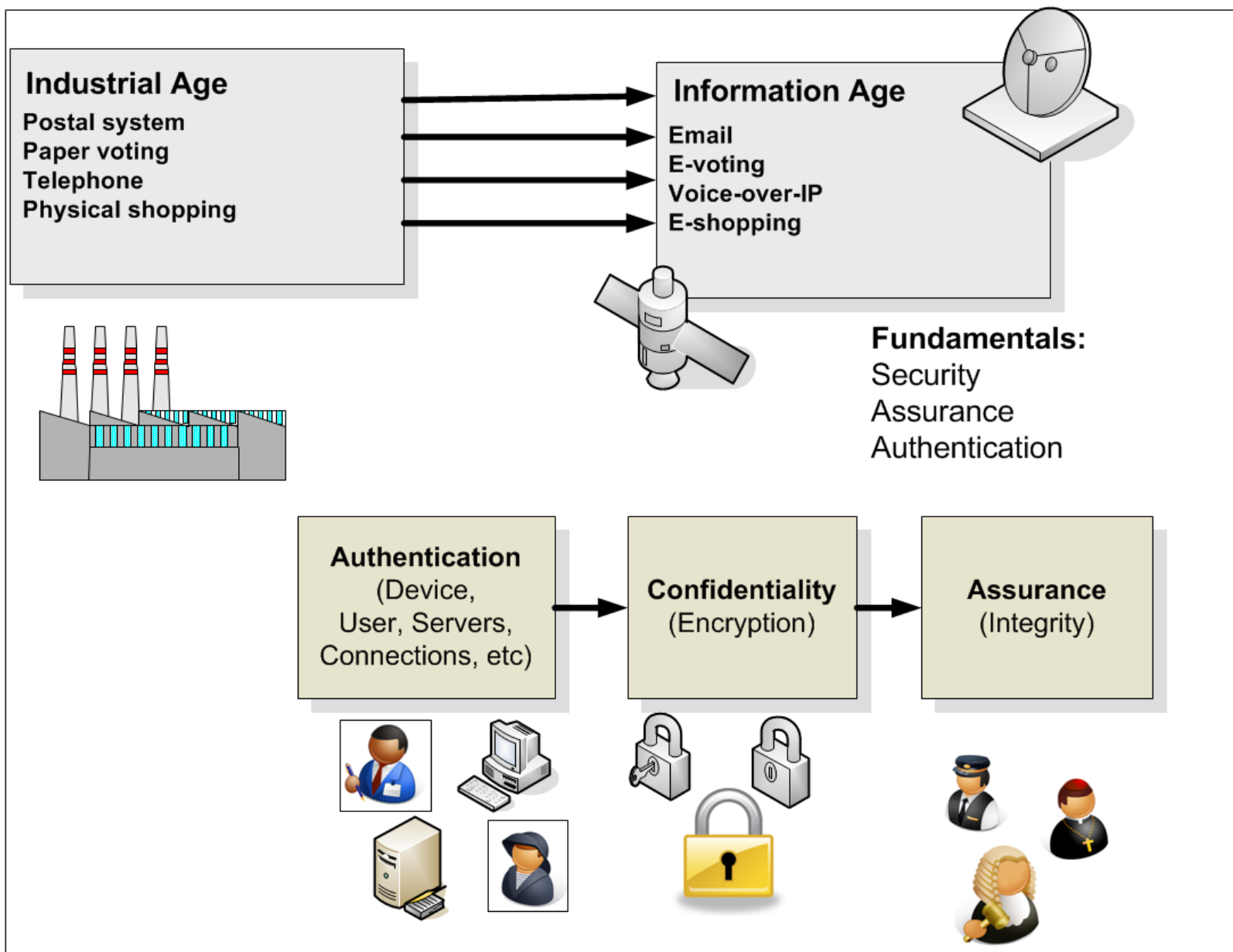


Cyber skills



Defining the Skills-base for the Future

Professor Bill Buchanan



Author: Prof Bill Buchanan

CSI (Computer Security Institute) found:

- 70% of organisation had breaches
- 60% of all breaches came from inside their own systems

Corporate access

Data stealing

External hack

DoS (Denial-of-service)

Personal abuse

Worms/viruses

Fraud

Terrorism/extortion

**Firewall/
Gateway**
(cannot deal with
internal threats)

**Network/
Organisational
perimeter**



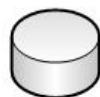
**Intrusion
Detection**



Users



Systems



Data



Assets

Introduction

Fundamentals

Author: Prof Bill Buchanan

Outside and inside threats

- Aging population.
- Climate Change.
- Transport and mobility issues.
- Failure to Innovate.
- Old methods of governance.
- Lack of integration of Government, Industry, Academia and the Public Sector.

Better Society

Funding will be focussed on the following challenges:

- Health, demographic change and wellbeing;
- Food security, sustainable agriculture, marine and maritime research, and the bio-economy;
- Secure, clean and efficient energy;
- Smart, green and integrated transport;
- Inclusive, innovative and secure societies;
- Climate action, resource efficiency and raw materials



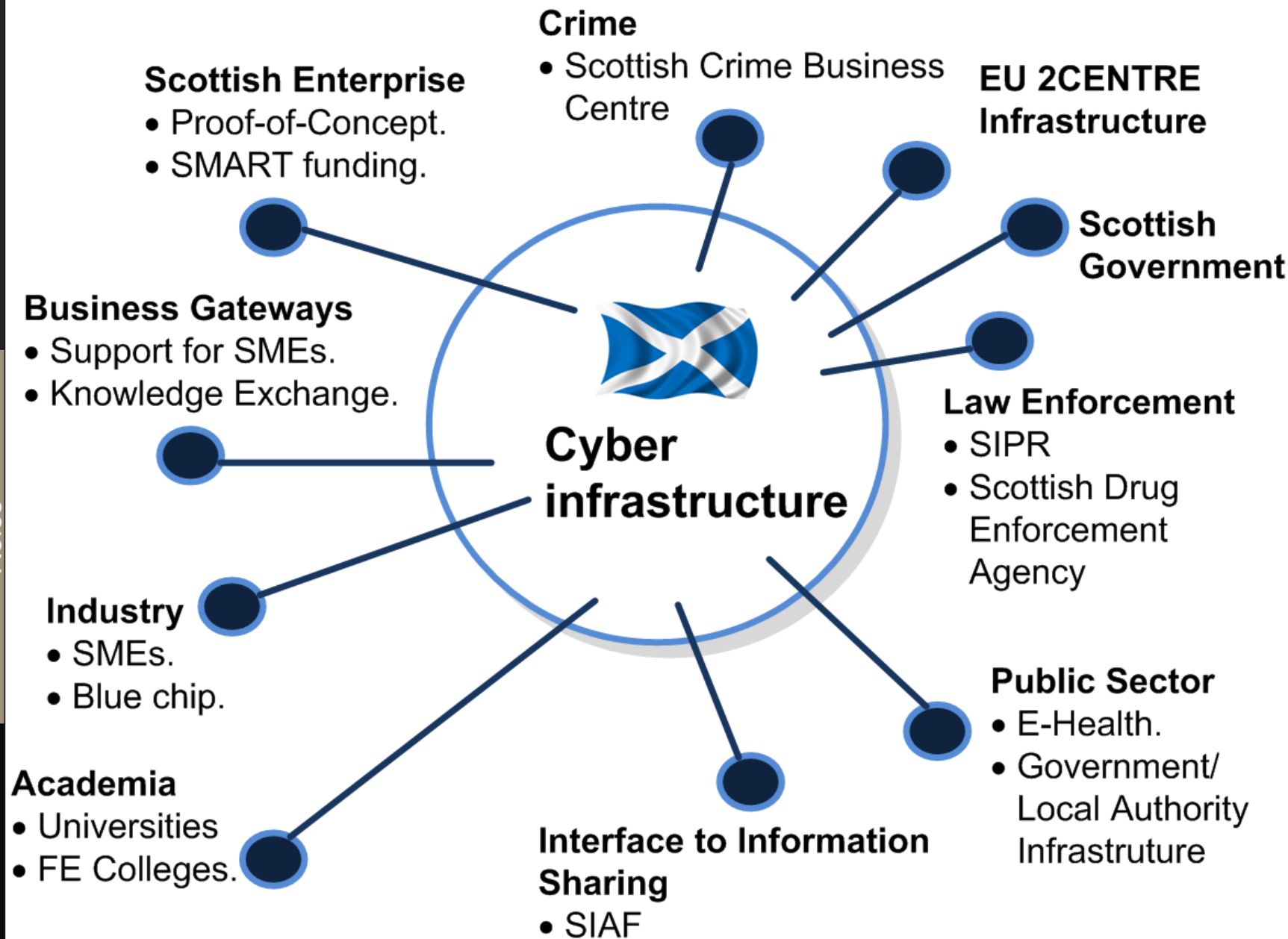
Cyber infrastructure

Excellent science

... Europe a more attractive location to invest in research and innovation, by promoting activities where businesses set the agenda ... help innovative SMEs to grow into world-leading companies.

Competitive Industries

... Europe a more attractive location to invest in research and innovation, by promoting activities where businesses set the agenda ... help innovative SMEs to grow into world-leading companies.



Cyber skills



Defining the Skills-base for the Future

Focusing on Risks, Threats and Vulnerabilities ...

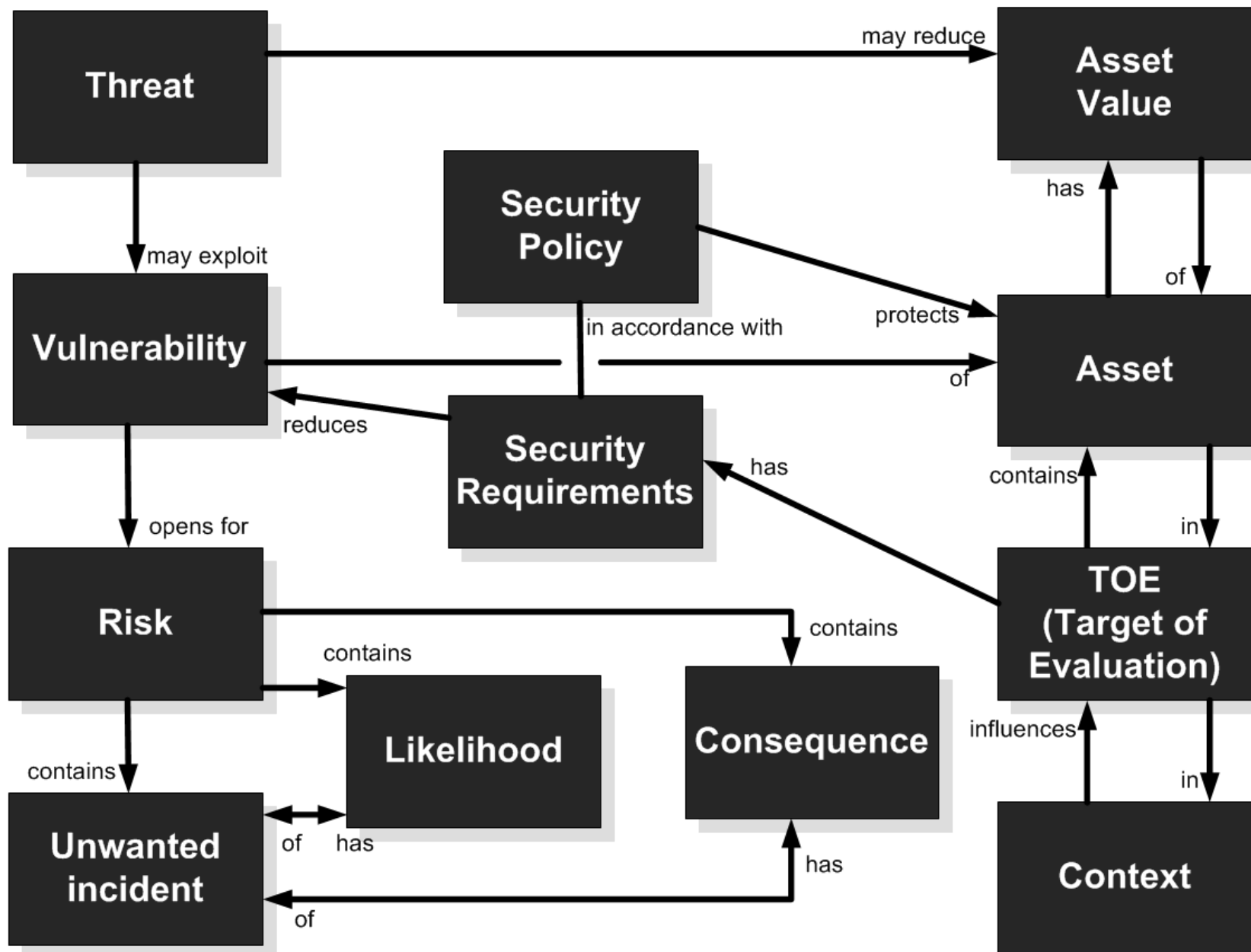
Business context



Technical context



“Get two risk management experts in a room, one financial and the other IT, and they will NOT be able to discuss risk. Each puts risk into a different context ... different vocabularies, definitions, metrics, processes and standards ... “
Woloch (2006)



Cyber skills

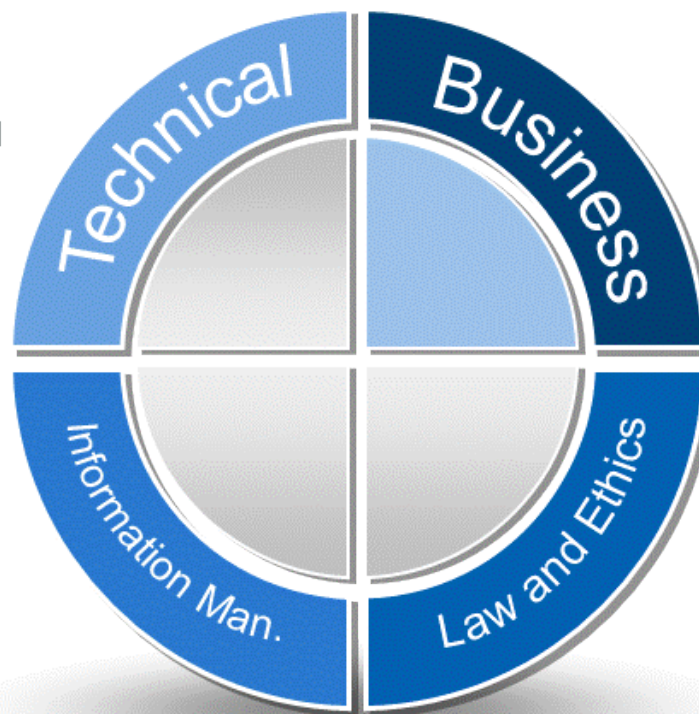


Defining the Skills-base for the Future

The Skills Road Map

- Computer/Network Security.
- Intrusion Detection.
- Access Control.
- System Development and Maintance.
- Security Policy Implentation.

-
- Access Control.
 - Data Leakage.
 - Auditing.
 - Asset Classification and Control.
 - Data Infrastructure.



- Risk Management.
- Business Continuity.
- Physical and Envrioment Security
- Human Resource Security
 - Incident Management.
- Security Policy Definition.

-
- Ethical responsiblitiy.
 - Legal infrastructure.
 - Compliance.



Insiders



Intruders



Digital Investigator

- Disk Forensics.
- Phone forensics.
- Network forensics.
- Criminal Analysis.
- Social Networks.

Real-time Defence/ Critical Response

- Response Units

Proactive Defence

- Firewalls
- Intrusion Detection.
- Server/Network infrastructure

Homeland Defence

- Terrorism.
- Society threats

Security Maintenance

Security Evaluation

Business Crime Investigator

- Accounting Forensics.
- Fraud analysis.



Audit/Compliance

- ISO 27001.
- PCI.
- HIPPA.

Risk Analysis/Brand Awareness/ Data Leakage

Governance/Judicial Infrastructure

Roles

Cyber

Roles

Cyber skills



Defining the Skills-base for the Future

Engaging Students

Dissemination events

Symposium on Security Risk, Cybercrime and Critical Infrastructure

Context

The main focus for the Symposium is to engage a wide range of domains to collaborate effectively, to understand current and future threats to our citizens and society. The event is free, and is intended to increase the collaboration of organizations around Scotland.

The Symposium is organised and delivered with the support of Scottish Enterprise, Finmeccanica Cy Napier University.

- [\[Current programme for the Symposium\]](#)
- [\[Book for the Symposium\]](#)
- [\[Book for the Meet-the-Buyer Event\]](#)
- [\[Scottish Cipher Excellence 2011 Award\]](#)
- [\[Raytheon Global Security Challenge\]](#)

Aim and Scope of Symposium

This symposium aims to bring together knowledge from many different domains in order to create collaborative infrastructures, which address the key risks that Scotland faces. The focus on this symposium is cybercrime and the protection of critical infrastructure, with a key focus on:

- Collaborative networks within Scotland and links to the EU and the UK.
- Knowledge networks related to computer security, cybercrime and in risk analysis.
- Security and Cybercrime risks of the Cloud.
- Training requirements for Scotland related to Computer Security and Cybercrime.
- Emergency response infrastructures, and risk within critical infrastructure.
- Criminal risks and new attack vectors.
- Risks to privacy and identity theft.
- Intelligence-led activities.

International Prizes

Symposium on Security Risk, Cybercrime and Critical Infrastructure

Outline

The **Raytheon Global Security Challenge** prize is one of the most advanced to be run on a Global basis. The prizes will be awarded at the Symposium on Security Risk, Cybercrime and Critical Infrastructure on Tuesday 6 December 2011. There are 25 questions to answer, each getting more difficult (from simple to complex), and there will be a number of prizes on offer.

These prizes will be based on the number of points that are gained on the day of the challenge.

- [\[Symposium Web Site\]](#)
- [\[Book for the Symposium\]](#)
- [\[Book for the Meet-the-Buyer Event\]](#)
- [\[Scottish Cipher Excellence 2011 Award\]](#)
- [\[Raytheon Global Security Challenge\]](#)

Details

The challenge will be held on **Monday 5 December 2011**, and you can join the challenge at any time during the day, and leave and come back. There will be 25 challenges, and you will work your way through them, and can use any internet-based tools or sources that you want.

You can either join as an **individual** or as a **team**. Register [\[here\]](#).

If you need more details, contact any of the following:

- w.buchanan@napier.ac.uk or R.MacFarlane@napier.ac.uk or r.ludwinski@napier.ac.uk
- Mike.Just@jcu.ac.uk
- George.Weir@ios.strath.ac.uk
- l.ferguson@abertay.ac.uk
- l.georgieva@hw.ac.uk
- ishbel@cs.st-and.ac.uk

Specialist team

Challenges

Symposium on Security Risk, Cybercrime and Critical Infrastructure

Outline

The Flexiant Cipher Challenge prize - Scottish Cipher Excellence 2011 Award - will be awarded at the Symposium on Security Risk, Cybercrime and Critical Infrastructure on Tuesday 6 December 2011. It involves a number of ever more difficult cipher challenges which students must solve in order to get to the next round. Some of these challenges will be timed, where others are open to be completed within certain deadlines. First prize will be a **Fujitsu notebook**.

Round 1

The Round 1 Flexiant Cipher Challenge is [\[here\]](#):



Round 2

The Round 2 Flexiant Cipher Challenge is [\[Here\]](#):

Round 3

The Round 3 Flexiant Cipher Challenge is [\[here\]](#):



```

MjU0MzZDNkNCEJCMjQzMUNwQjQzRDY3OTNEMENQzENCjYyQ0MwQjRFQkIwQjU3Q
jQwMzZDNkNCEJCMjQzMUNwQjQzRDY3OTNEMENQzENCjYyQ0MwQjRFQkIwQjU3Q

```

If you can crack this, email your answer to w.buchanan@napier.ac.uk or Mike.Just@jcu.ac.uk or George.Weir@ios.strath.ac.uk or l.ferguson@abertay.ac.uk or l.georgieva@hw.ac.uk or ishbel@cs.st-and.ac.uk.

Round 4

The Round 4 challenge is timed, and relates to a current news item. It is [\[here\]](#).

Final Round

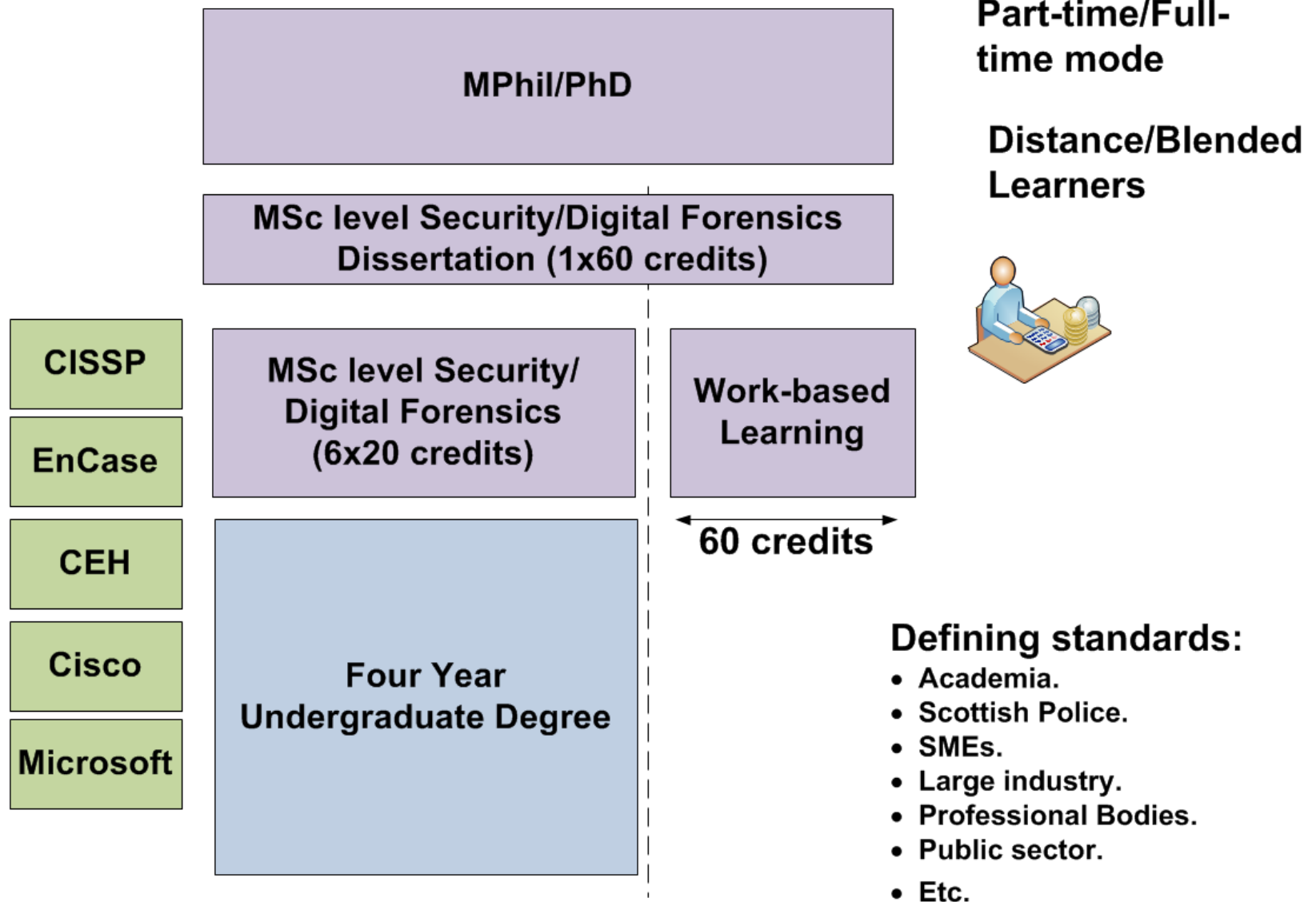
There are four challenges. Once you have each of the codes, email the answer immediately to w.buchanan@napier.ac.uk.



Blue Team



Red Team

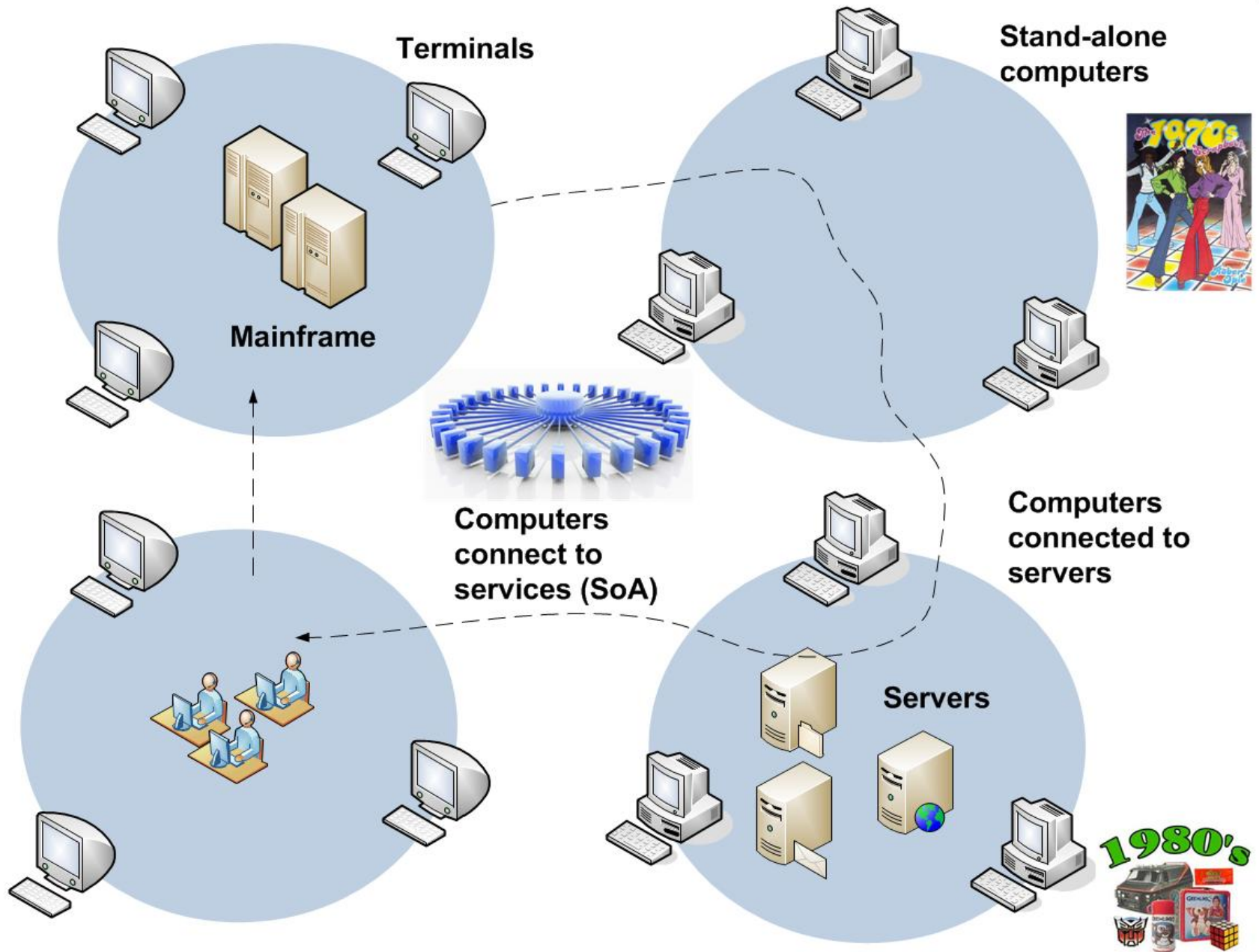


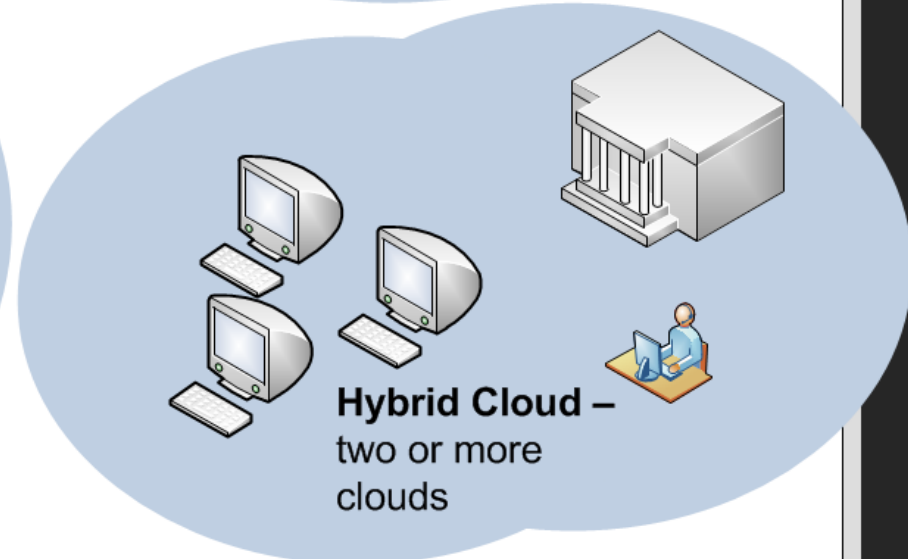
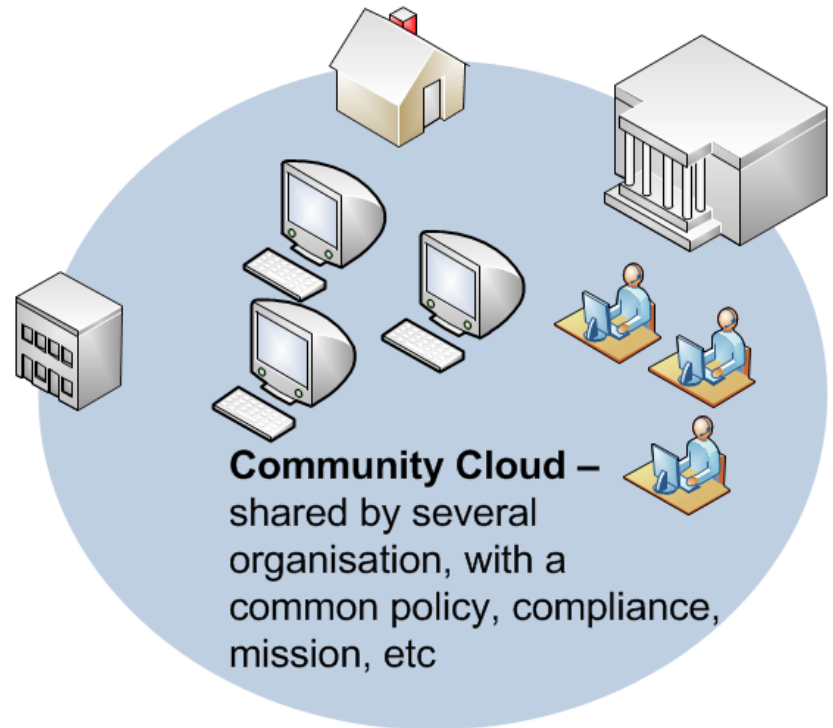
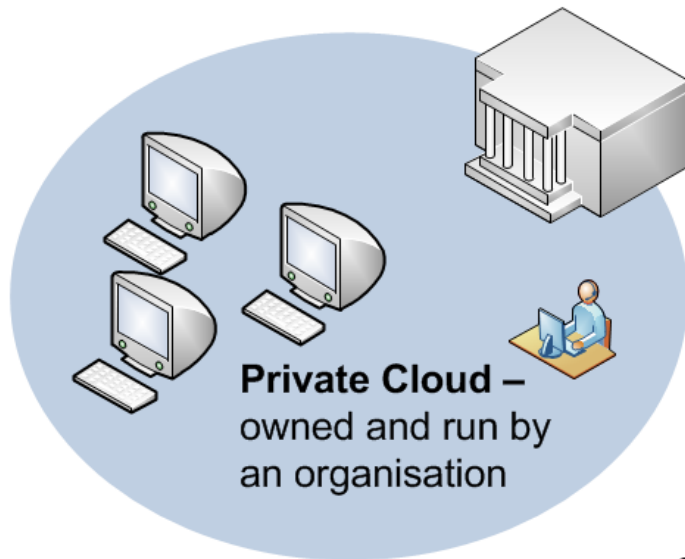
Cyber skills

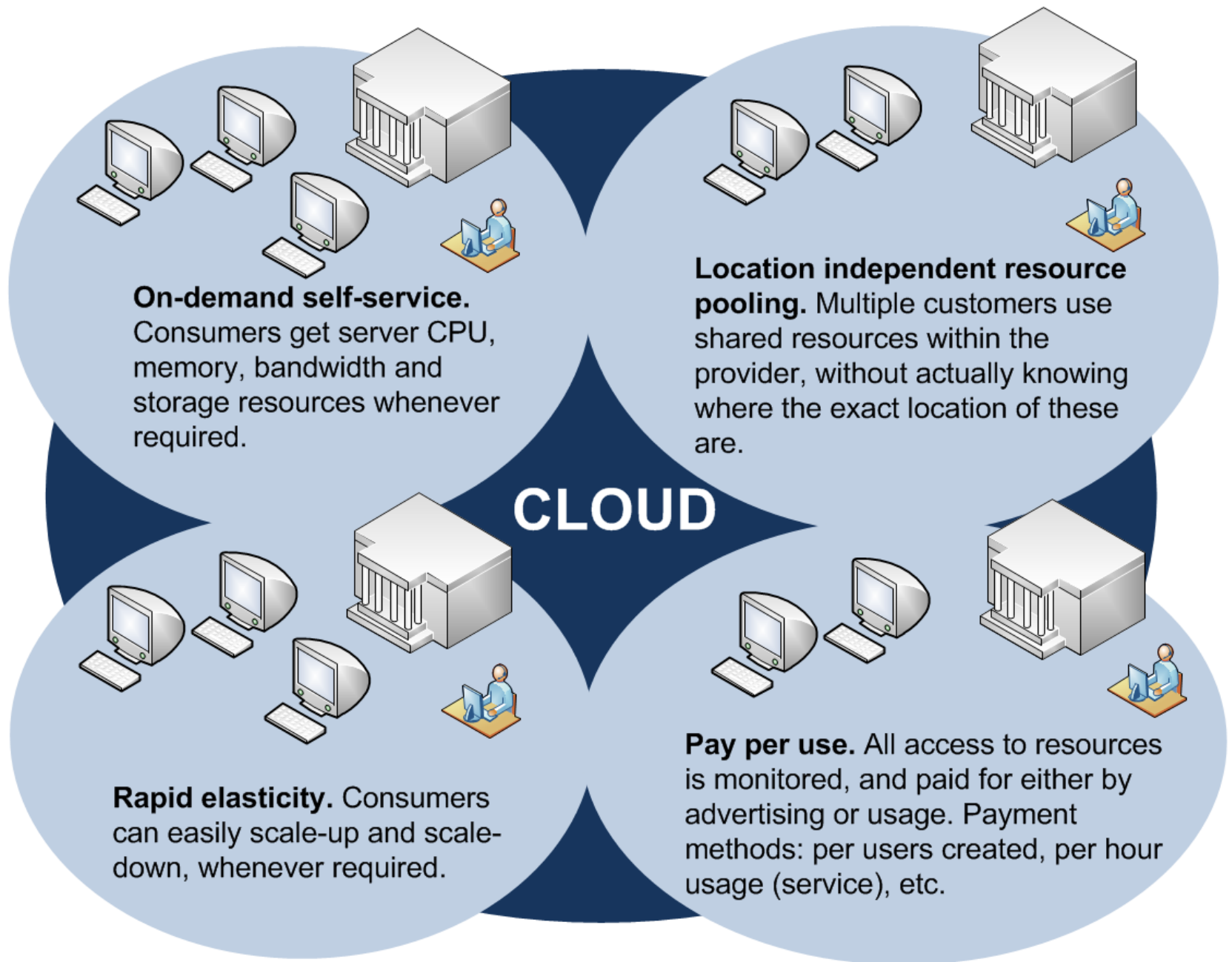


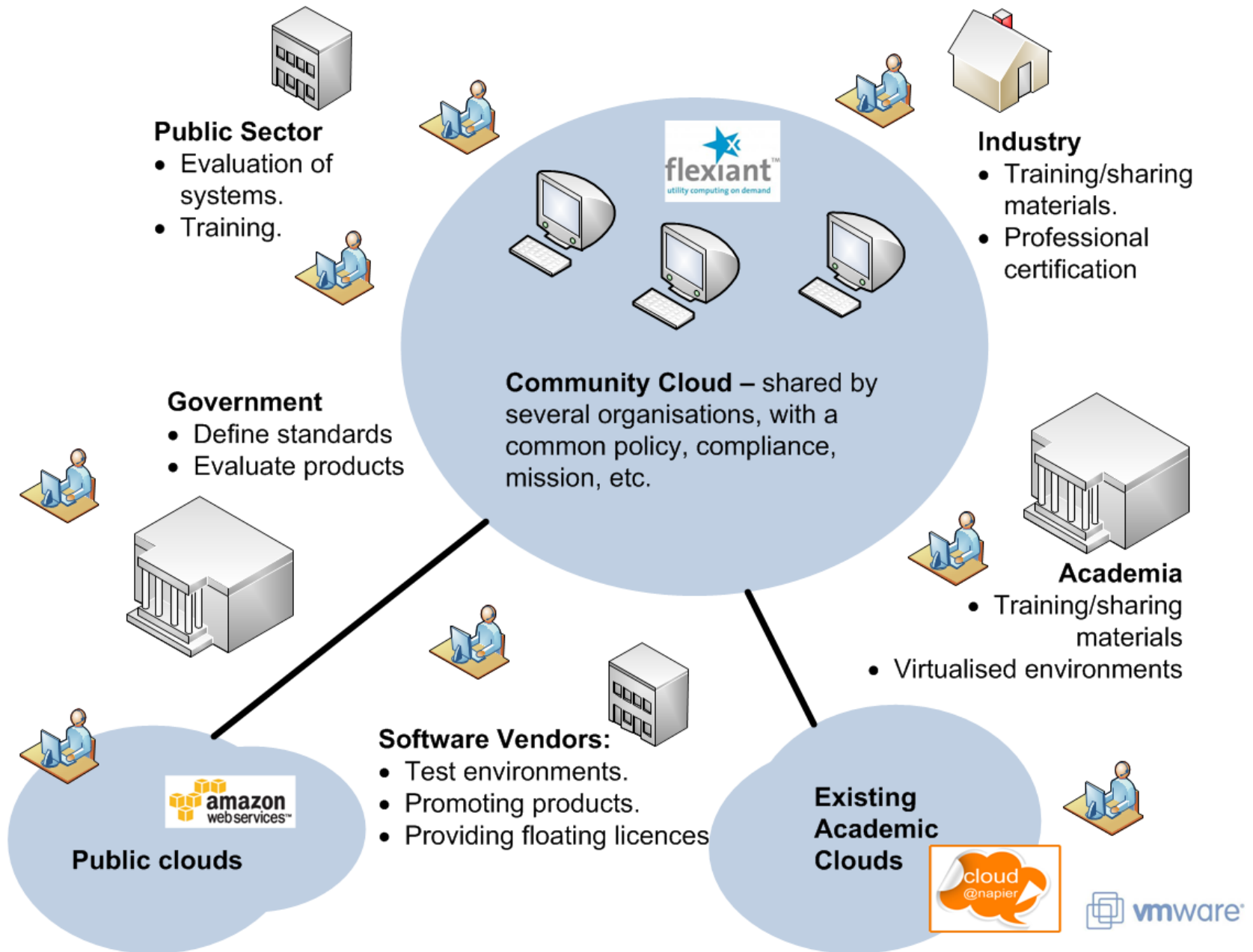
Defining the Skills-base for the Future

Virtualised Training in the Cloud









**Distance learners**

- Exact environments as face-to-face students.
- Blended learners have greater choice and flexibility.

**Industry**

- Adding evaluation infrastructures.
- Post project work/interesting areas of work.
- Ability to review materials presented to students.
- Ability to study within the workplace.

**Enhancing skills**

- Supports a wide range of pre-built environments within a sandboxed infrastructure

Working across institutions

- Cloud environments allow for working across traditional boundaries.

**Project work**

- Students can start from existing well-tested environments.

**Engaging students**

- State-of-the-art infrastructures

**Group working**

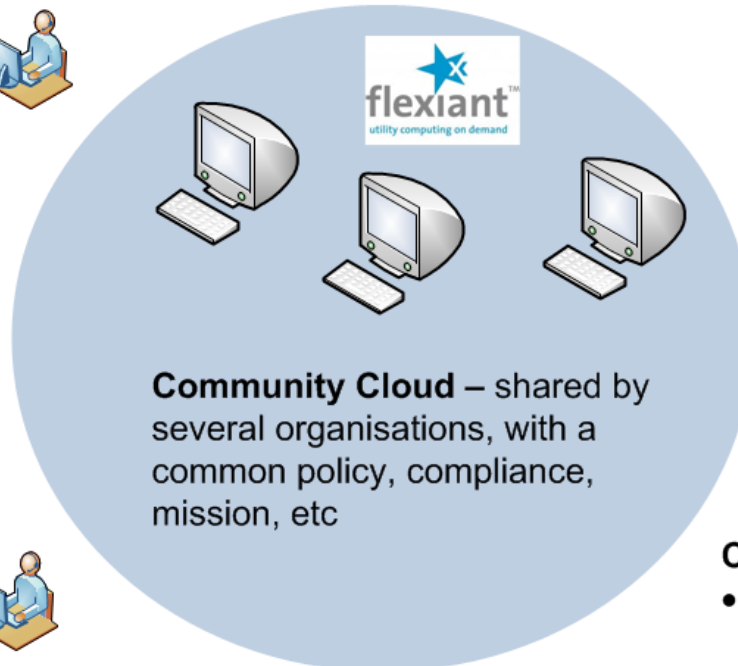
- Students can integrate their systems in an isolated environment.

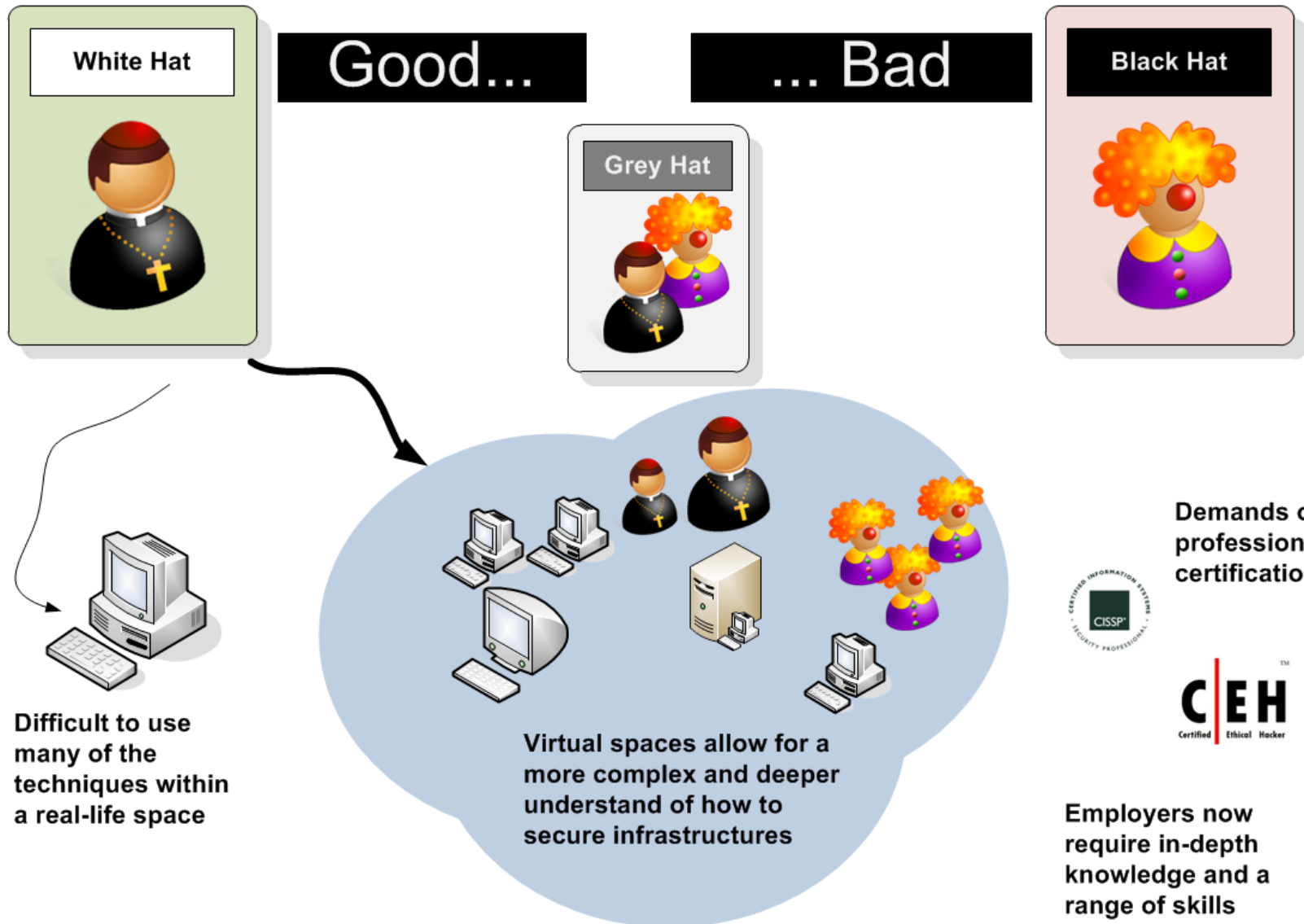
**Robust infrastructures**

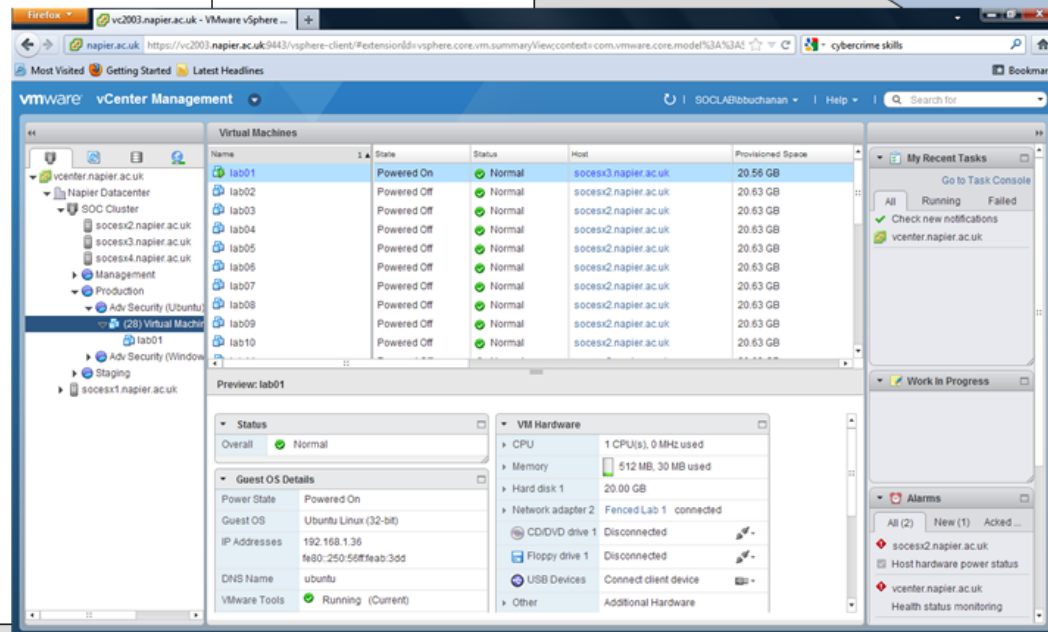
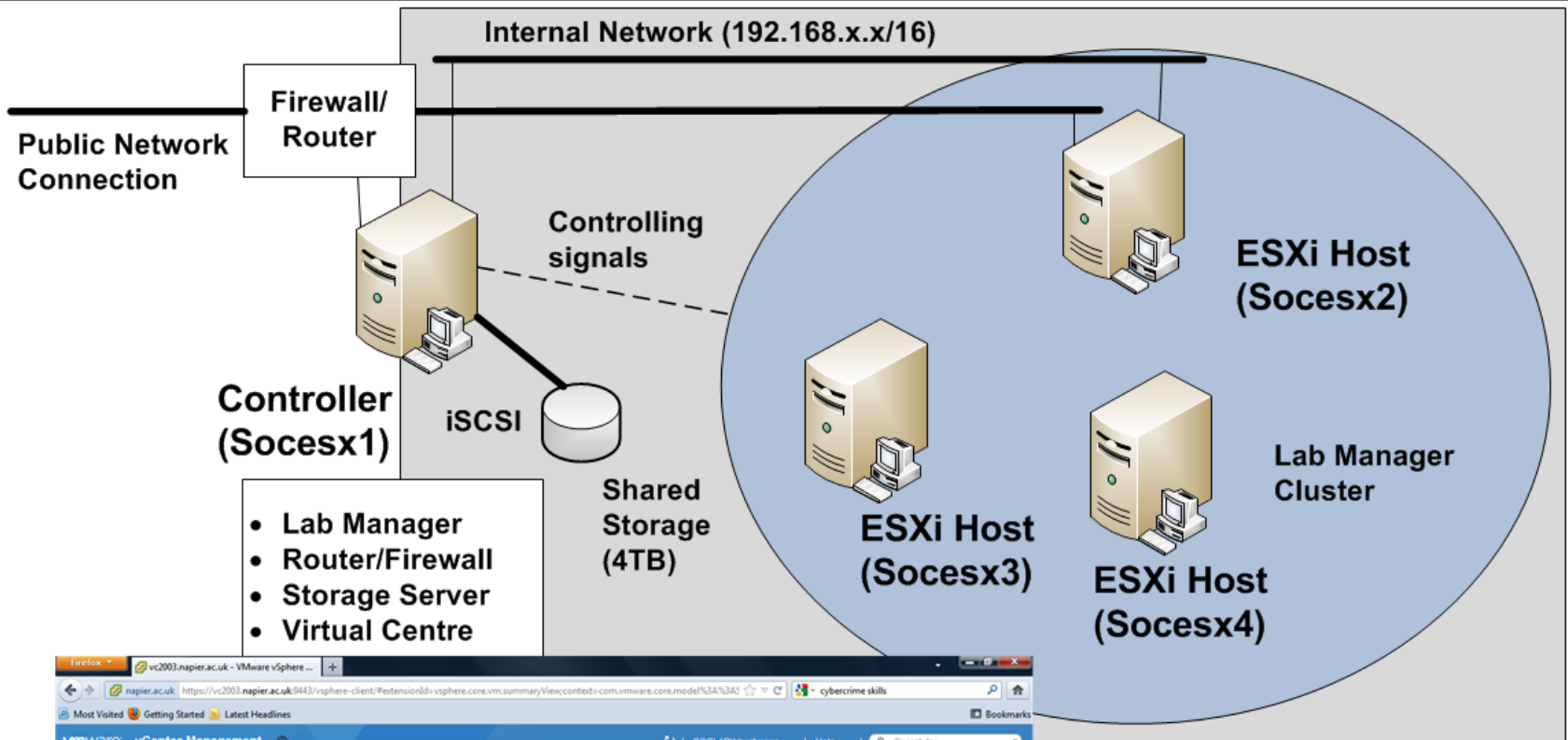
- No more 9-5pm, Mon-Friday environments.

**Snap-shots of work**

- Student can create snap-shots, and move back and forward amongst them.









The image is a collage of screenshots from a VMware vCenter Lab Manager interface, illustrating a virtual machine configuration and management workflow.

Top Left: Configuration: bill
 This window shows the main configuration page for a virtual machine named 'bill'. It includes a sidebar with navigation options like 'Organization', 'Build and Deploy', 'Monitor', and 'Manage'. The main area displays a table of virtual machines:

Console	VM Name	Status	NIC	Network	IP Address	External IP	Template	Host	Conn
	CONSOLE	Deployed	1*	Student Network	DHCP	-	Ubuntu	socess2.napier.ac.uk	
	UBUNTU	Deployed	1*	Student Network	DHCP	-	Ubuntu	socess2.napier.ac.uk	
	WINDOWS2003	Deployed	1*	Student Network	DHCP	-	Windows 2003	socess2.napier.ac.uk	
	Back	Deployed	1*	Student Network	DHCP	-	BackTrack	socess2.napier.ac.uk	

Top Right: cloud @napier
 An orange speech bubble logo with the text 'cloud @napier'.

Bottom Left: Ubuntu VM Terminal
 This window shows the terminal output for the Ubuntu VM. The user has run the command 'ifconfig' and the output shows the network configuration for the 'eth5' interface:

```

File Edit View Terminal Help
Ping Scan Timing: About 50.00% done; ETC: 12:48 (0:00:01 remaining)
Note: Host seems down. If it is really up, but blocking our ping probe...
Nmap done: 1 IP address (0 hosts up)
napier@ubuntu:~$ ifconfig
eth5
Link encap:Ethernet HWaddr 12:34:56:78:9A:BC
inet addr:192.168.242.24 Bcast:192.168.242.255 Mask:255.255.255
inet6 addr: fe80::250:56ff:fe78:9abc:1234:5678 Scope:link
UP BROADCAST RUNNING MULTICAST
RX packets:1000001 errors:0 dropped:0 overruns:0 on interface
TX packets:4919 errors:0 dropped:0 overruns:0 on interface
collisions:0 txqueuelen:1000
RX bytes:76528956 (76.5 MB)
Interrupt:19 Base address: 0x00000000

to
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.255.255
inet6 addr: ::1 Scope:host
UP LOOPBACK RUNNING MTU:65536
RX packets:11 errors:0 dropped:0 overruns:0 on interface
TX packets:11 errors:0 dropped:0 overruns:0 on interface
collisions:0 txqueuelen:0
RX bytes:744 (744.0 B) TX bytes:0
napier@ubuntu:~$
  
```

Bottom Middle: Windows 2003 VM Desktop
 This window shows the desktop environment of a Windows 2003 VM. The Start menu is open, displaying a list of applications including 'Backtrack', 'Internet', 'Services', 'Graphics', 'Multimedia', 'System', 'Utilities', 'KSnapshot', 'Settings', 'System Menu', 'Run Command...', 'Lock Session', and 'Log Out...'. The desktop background features a blue and white abstract design with the text 'BackTrack 4'.

Bottom Right: Windows 2003 VM Console
 This window shows the console output for the Windows 2003 VM. The user has run the command 'ping 192.168.242.24' and the output shows the results of the ping command:

```

C:\>ping 192.168.242.24
Pinging 192.168.242.24 with 32 bytes of data:
2 time=1ms TTL=64
2 time=1ms TTL=64
2 time=1ms TTL=64
Ping statistics for 192.168.242.24:
    3. Last = 0 (0% loss),
    111 seconds = 0ms,
    Average = 0ms
  
```

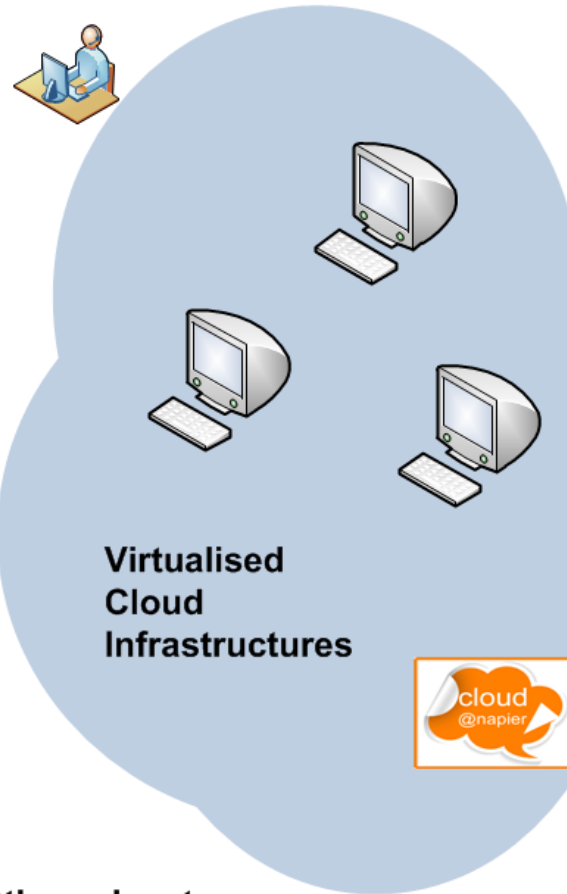
Arrows indicate the flow of the workflow: from the VM list in the top left, to the specific VM details in the bottom left, and then to the terminal output in the bottom right.

Tool validation:

- Supports a wide range of tool validation.
- Ever changing environment for a range of testing.

Skills:

- Allows students to remotely complete labs.
- Students training on state-of-the-art infrastructures.
- Different labs can be created for different situations (DF Tools/OSs/etc).
- Supports remote/distance learning.
- Infrastructure can be ring-fenced.
- Supports group work in an isolated environment.
- In-depth analysis of infrastructures.
- Students can build systems from scratch.
- Students can update their own infrastructure/tools, as required.
- Seems to engage the students, and show them a wide potential.
- Encourages students to continue work after the lab/tutorial.
- Time windows of labs/tutorials can be carefully controlled.
- Extensive and complex infrastructures assessed within a sandboxed environments.

**Drawbacks:**

- Requires an investment in time in creating and maintaining the virtual image.
- Students can avoid the lab situation.
- Possibly requires a backup strategy for labs (if using network-based virtualisation – but has advantages that a standalone version does not need a network connection).
- Goes against the stand-alone machine philosophy.

Other advantages:

- Easy for teaching team to update.
- Helps with franchised colleges.
- Easy setup for classroom demonstrations.
- Infrastructure can be ring-fenced.
- Produces repeatable labs.
- Not dependent on Napier/network infrastructure.
- Time windows of labs/tutorials can be carefully controlled.

HORIZON 2020

THE FRAMEWORK PROGRAMME FOR RESEARCH AND INNOVATION

- Aging population.
- Climate Change.
- Transport and mobility issues.
- Failure to Innovate.
- Old methods of governance.
- Lack of integration of Government, Industry, Academia and the Public Sector.

Better Society

Funding will be focussed on the following challenges:

- Health, demographic change and wellbeing;
- Food security, sustainable agriculture, marine and maritime research, and the bio-economy;
- Secure, clean and efficient energy;
- Smart, green and integrated transport;
- Inclusive, innovative and secure societies;
- Climate action, resource efficiency and raw materials



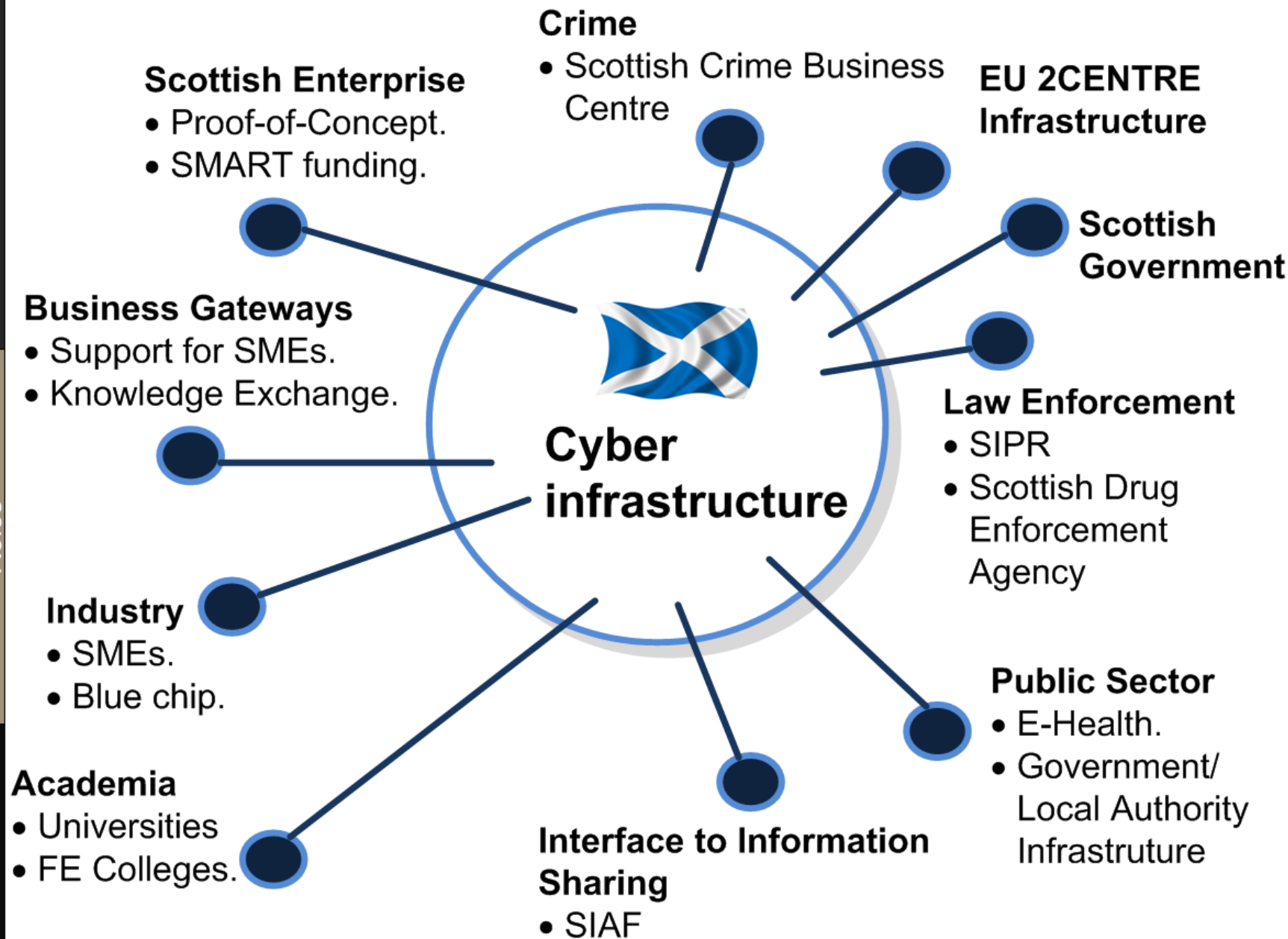
Cyber infrastructure

Excellent science

... Europe a more attractive location to invest in research and innovation, by promoting activities where businesses set the agenda ... help innovative SMEs to grow into world-leading companies.

Competitive Industries

... Europe a more attractive location to invest in research and innovation, by promoting activities where businesses set the agenda ... help innovative SMEs to grow into world-leading companies.



Cyber skills



Defining the Skills-base for the Future

Professor Bill Buchanan