Cyber skills

Defining the Skills-base for the Future

Professor Bill Buchanan

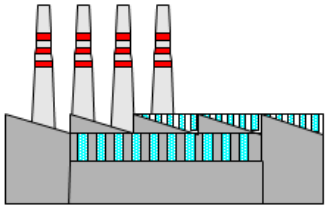
Author: Prof Bill Buchanan

Industrial Age

Postal system
Paper voting
Telephone
Physical shopping

Information Age

Email
E-voting
Voice-over-IP
E-shopping



Fundamentals:
Security
Assurance
Authentication

Authentication
(Device, User, Servers, Connections, etc)

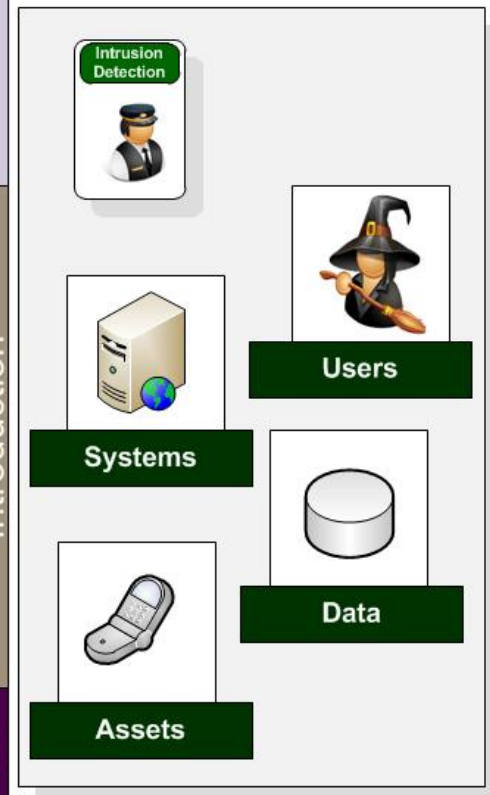
Confidentiality
(Encryption)

Assurance
(Integrity)

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-sevice)

Firewall/ Gateway (cannot deal with internal threats)

Personal abuse

Worms/viruses

Fraud

Terrorism/ extortion

Network/ Organisational perimeter

Author: Prof Bill Buchanan

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.

Cyber infrastructur

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.

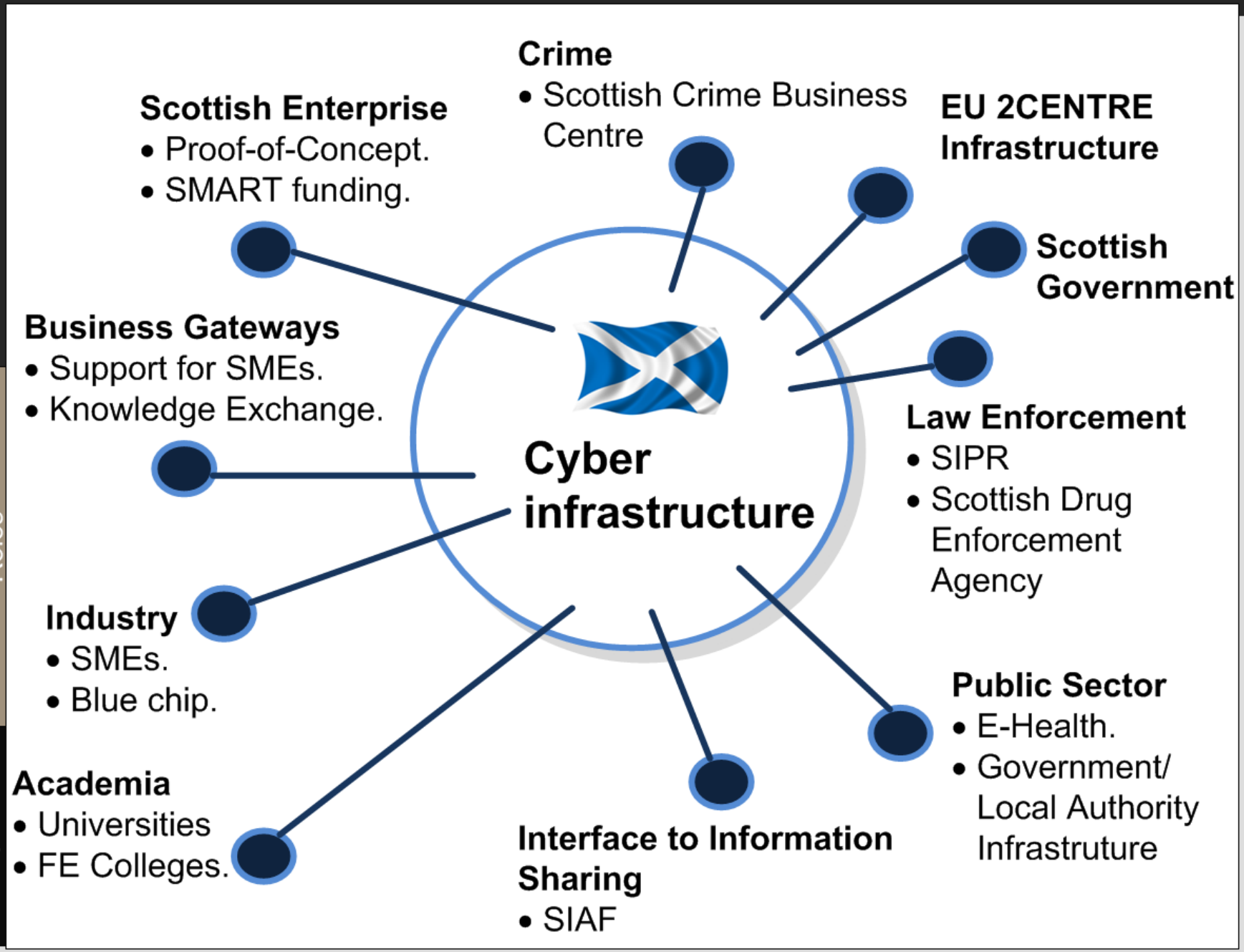
Better Society

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

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.


Crime
• Scottish Crime Business Centre
Scottish Enterprise
• Proof-of-Concept.
• SMART funding.
EU 2CENTRE Infrastructure
Scottish Government
Business Gateways
• Support for SMEs.
• Knowledge Exchange.
Cyber infrastructure
Law Enforcement
• SIPR
• Scottish Drug Enforcement Agency
Industry
• SMEs.
• Blue chip.
Public Sector
• E-Health.
• Government/ Local Authority Infrastruture
Academia
• Universities
• FE Colleges.
Interface to Information Sharing
• SIAF
Roles
Cyber
Roles

Cyber skills

Defining the Skills-base for the Future

Focusing on Risks, Threats and Vulnerabilities ...

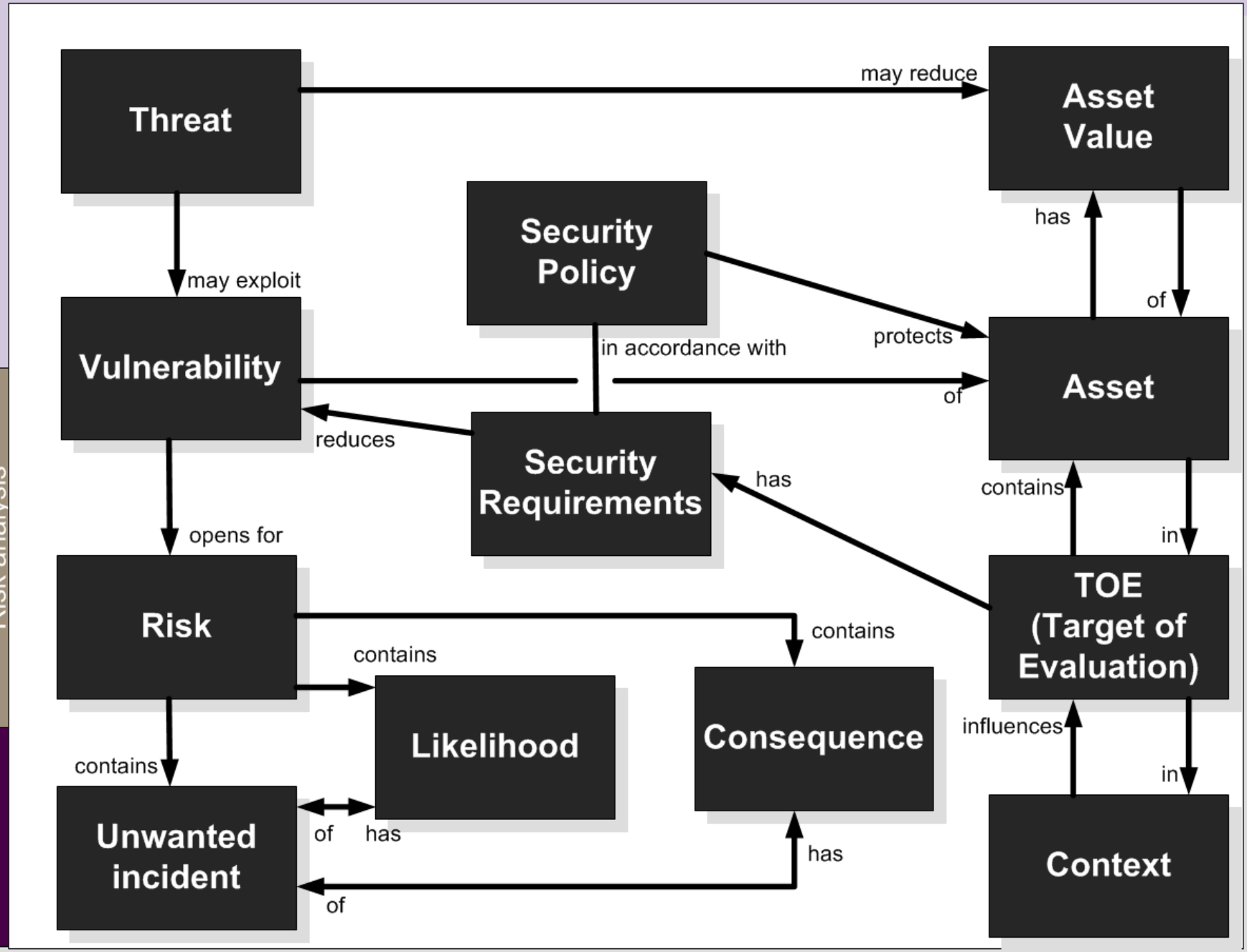
Author: Prof Bill Buchanan

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)

Author: Prof Bill Buchanan



CORAS ontology

Cyber skills

Defining the Skills-base for the Future

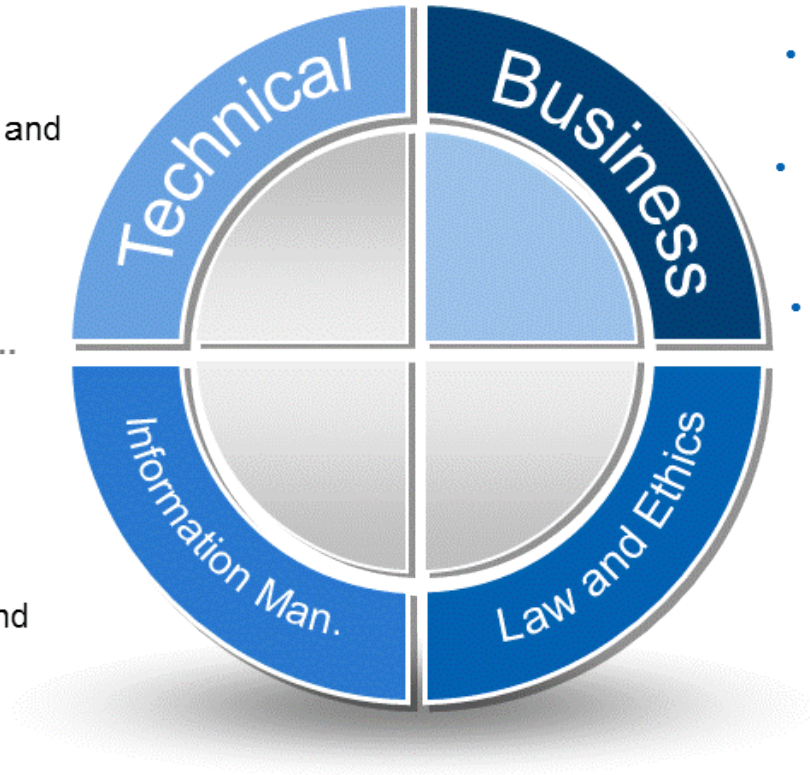
The Skills Road Map

Author: Prof Bill Buchanan

- 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 Envrionment Security
- Human Resource Security
- Incident Management.
- Security Policy Definition.

.....

- Ethical responsiblitiy.
- Legal infrastructure.
- Compliance.

Insiders

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

Intruders

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

Author: Prof Bill Buchanan

Roles

Cyber

Dissemination events

Challenges

International Prizes

Roles

MPhil/PhD

MSc level Security/Digital Forensics Dissertation (1x60 credits)

CISSP

EnCase

CEH

Cisco

Microsoft

MSc level Security/ Digital Forensics (6x20 credits)

Four Year Undergraduate Degree

Work-based Learning

60 credits

Part-time/Full-time mode

Distance/Blended Learners

Defining standards:

- Academia.
- Scottish Police.
- SMEs.
- Large industry.
- Professional Bodies.
- Public sector.
- Etc.

Roles

Cyber

Roles

Cyber skills

Defining the Skills-base for the Future

Virtualised Training in the Cloud

Author: Prof Bill Buchanan

Terminals

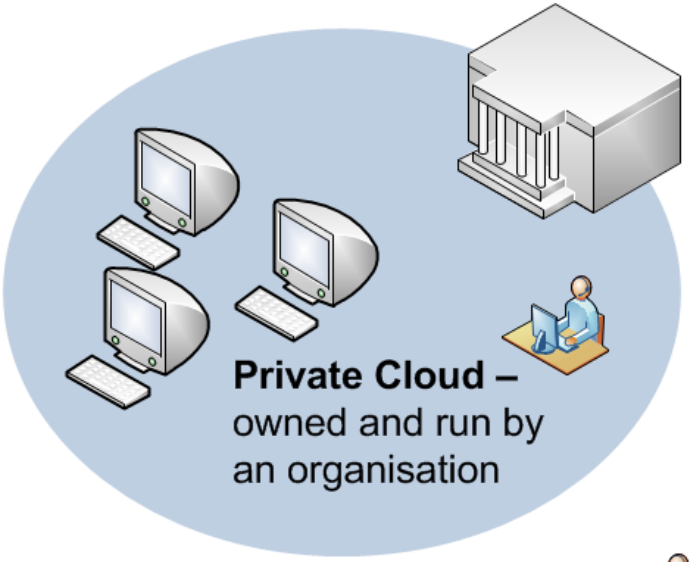
Mainframe

Stand-alone computers

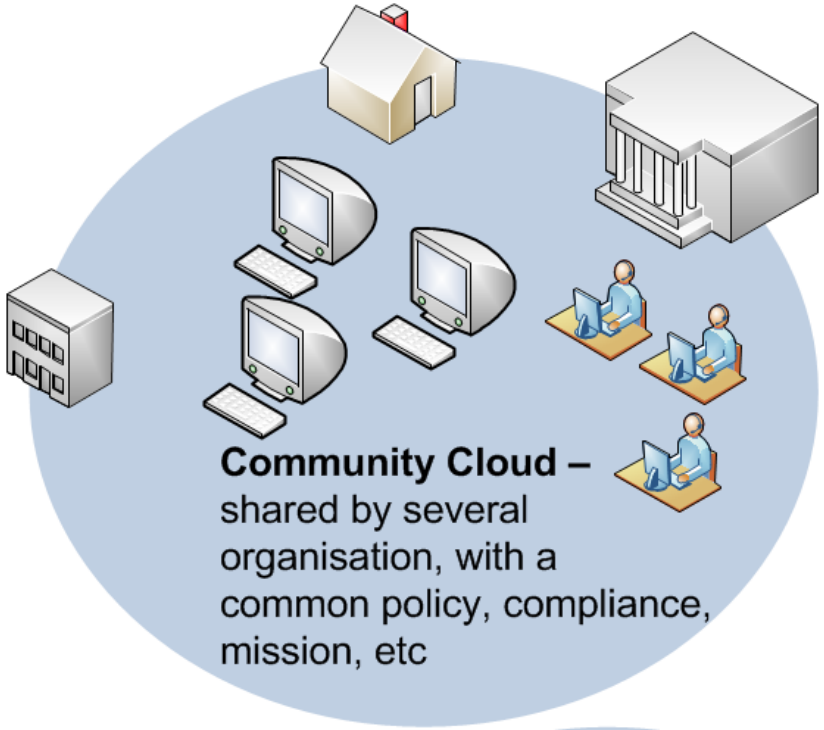
Computers connect to services (SoA)

Computers connected to servers

Servers

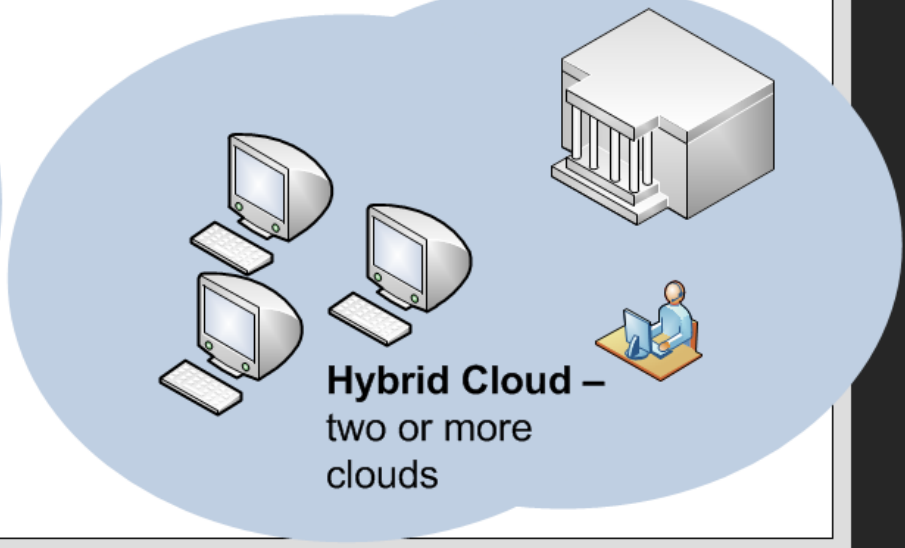


Private Cloud – owned and run by an organisation

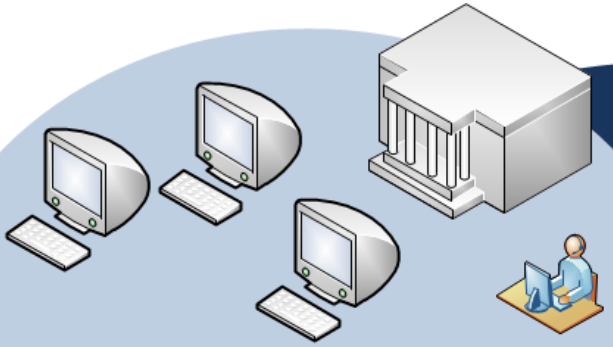


Community Cloud – shared by several organisation, with a common policy, compliance, mission, etc

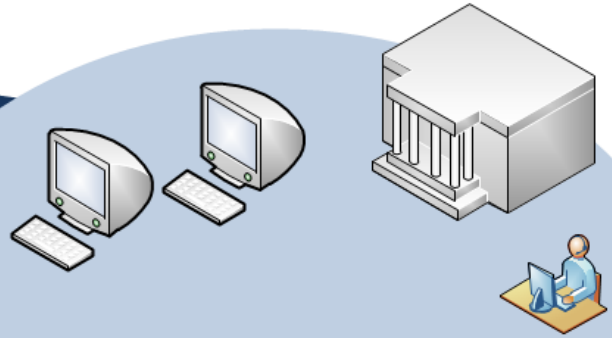
Public Cloud – owned by an organisation selling a cloud infrastructure



Hybrid Cloud – two or more clouds

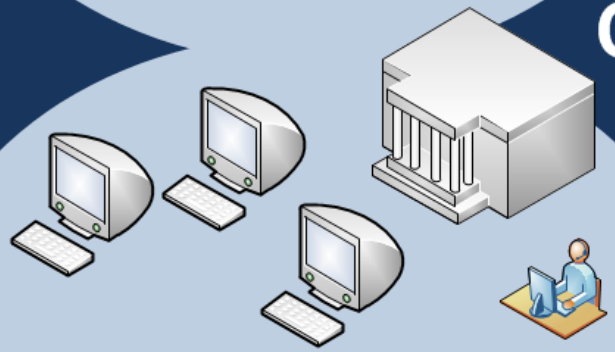


On-demand self-service. Consumers get server CPU, memory, bandwidth and storage resources whenever required.

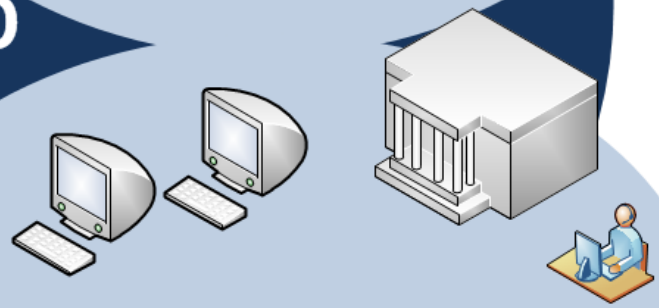


Location independent resource pooling. Multiple customers use shared resources within the provider, without actually knowing where the exact location of these are.

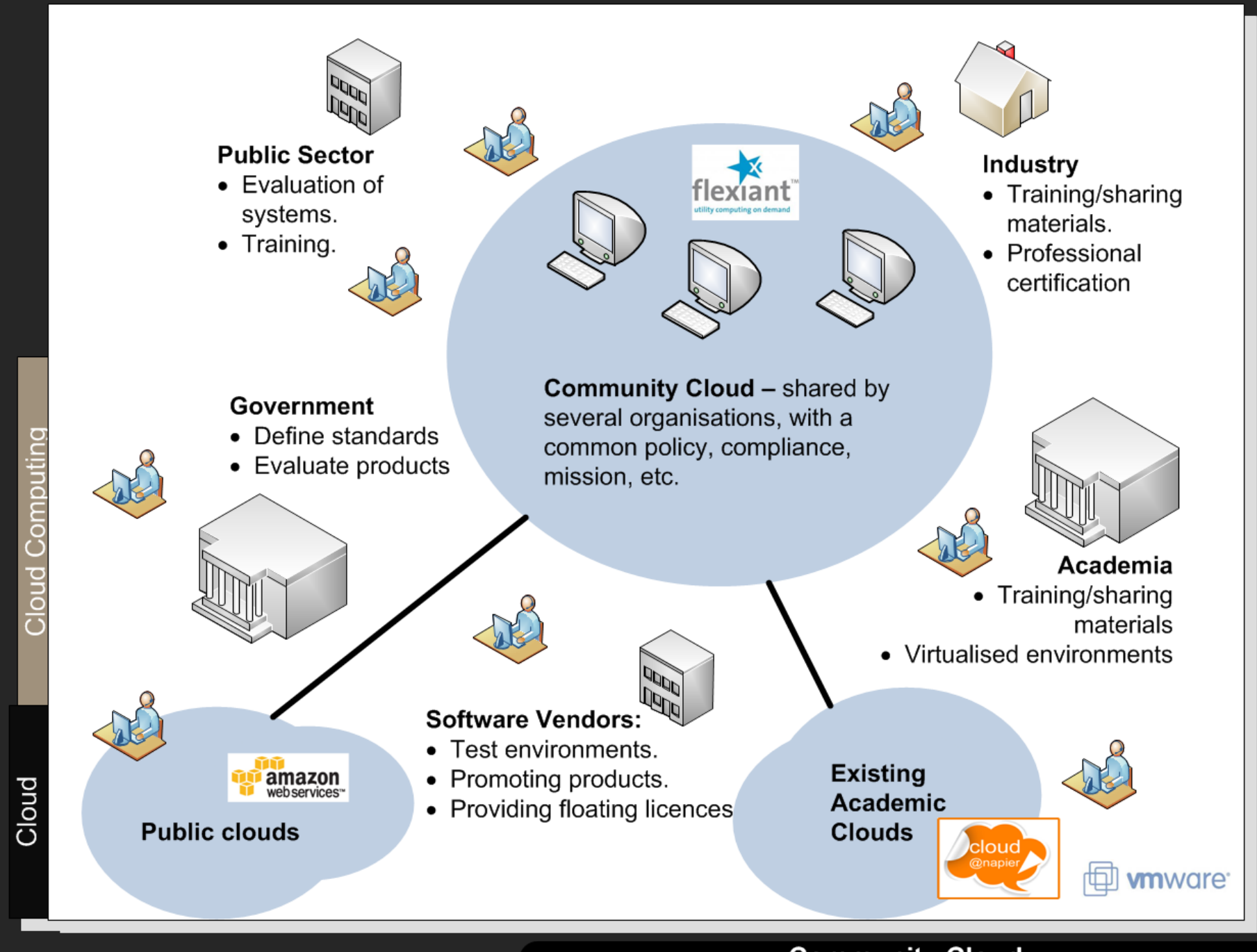
CLOUD



Rapid elasticity. Consumers can easily scale-up and scale-down, whenever required.



Pay per use. All access to resources is monitored, and paid for either by advertising or usage. Payment methods: per users created, per hour usage (service), etc.


Cloud Computing
Cloud
Public Sector
• Evaluation of systems.
• Training.
Industry
• Training/sharing materials.
• Professional certification
flexiant
utility computing on demand
Community Cloud – shared by several organisations, with a common policy, compliance, mission, etc.
Government
• Define standards
• Evaluate products
Academia
• Training/sharing materials
• Virtualised environments
Software Vendors:
• Test environments.
• Promoting products.
• Providing floating licences
amazon web services
Public clouds
Existing Academic Clouds
cloud @napier
vmware
Community 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 enviroments 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

Community Cloud – shared by several organisations, with a common policy, compliance, mission, etc

Continuation of work
- Students can carry their infrastructures throughout modules/ years.

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 amoungst them.

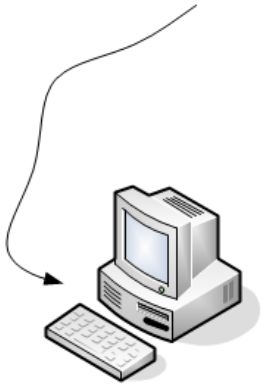
White Hat

Good...

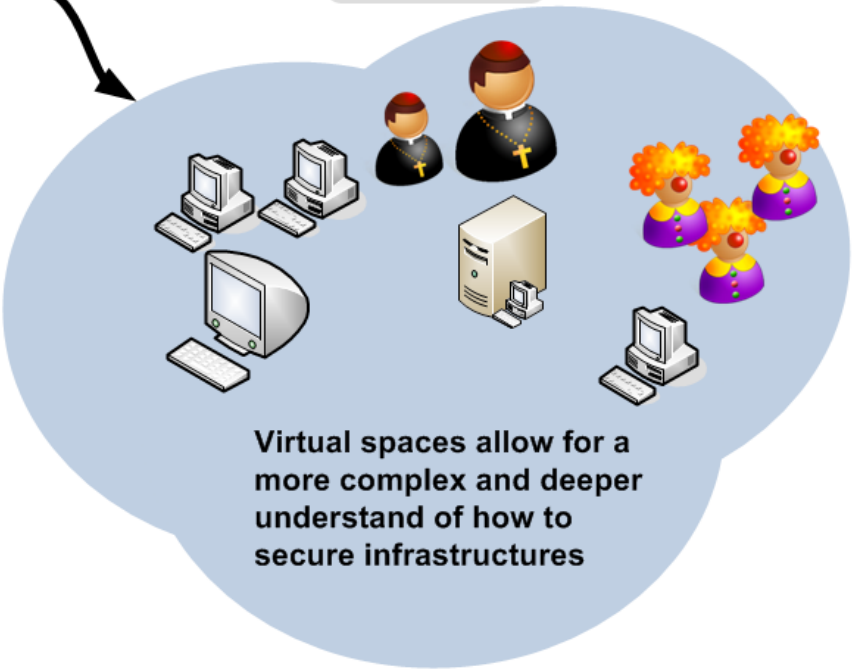
... Bad

Black Hat

Grey Hat



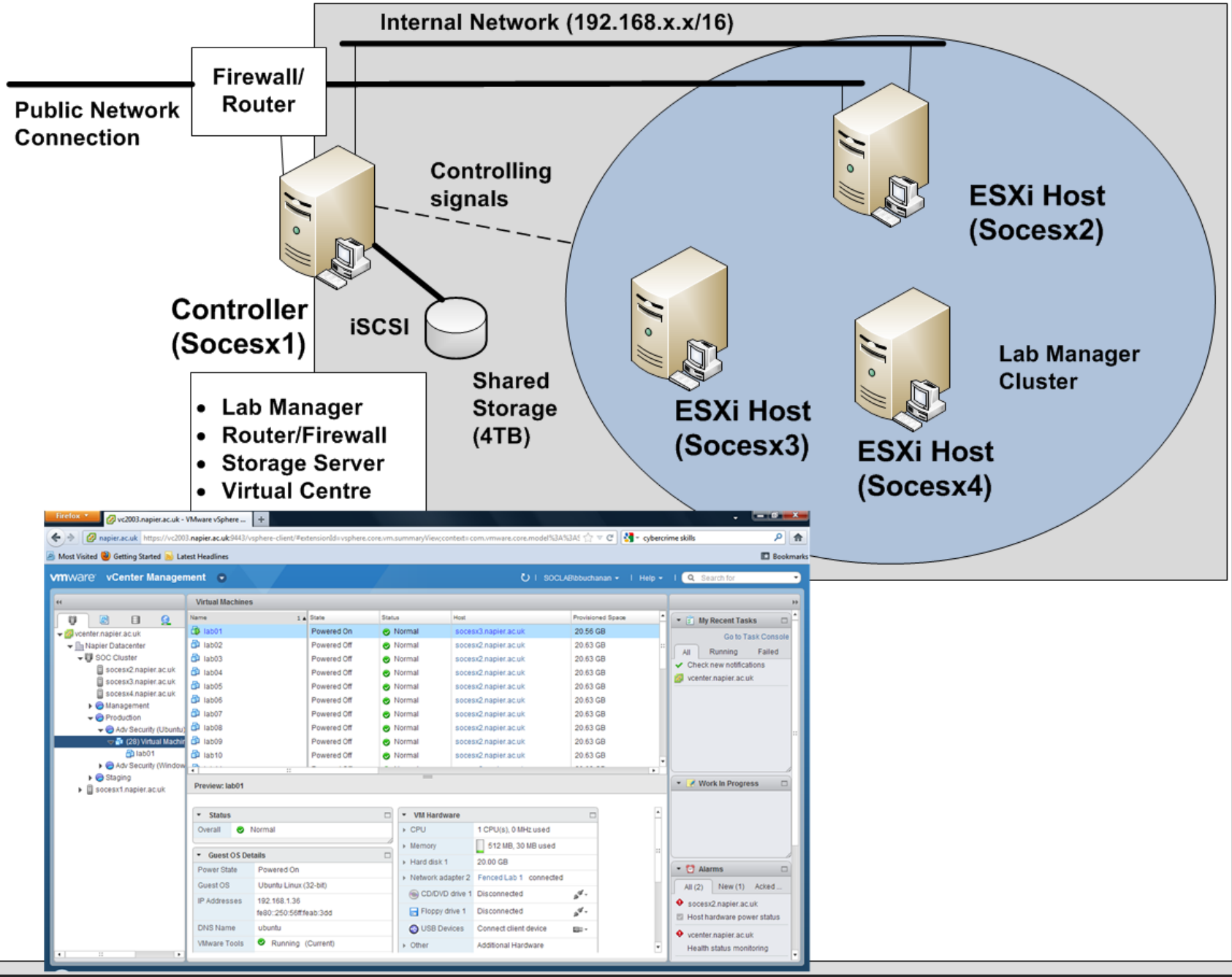
Difficult to use many of the techniques within a real-life space



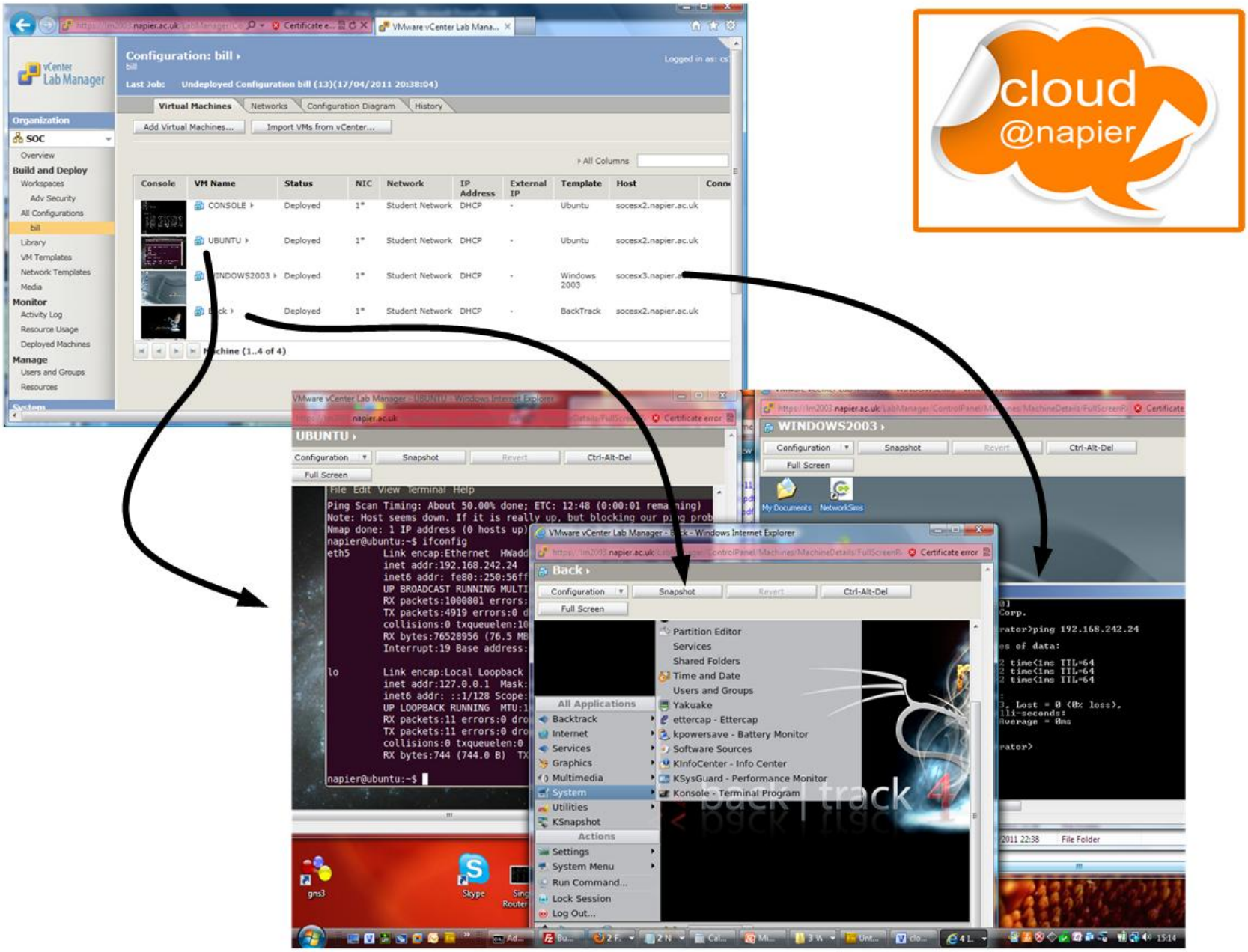
Virtual spaces allow for a more complex and deeper understand of how to secure infrastructures

Demands on professional certification

Employers now require in-depth knowledge and a range of skills



Napier vCenter infrastructure



Cloud Computing

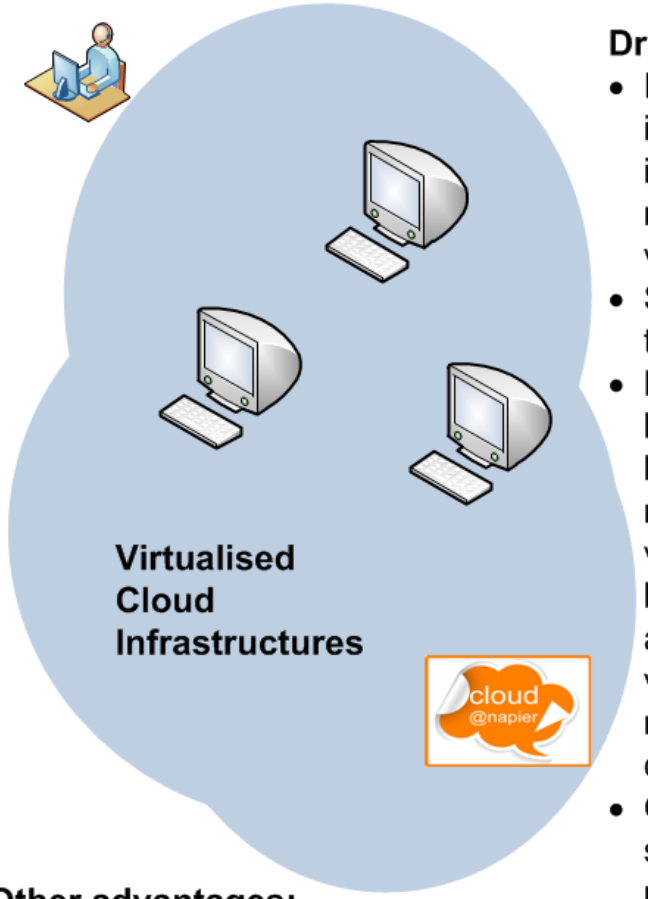
Cloud

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.

Cyber infrastructur

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.

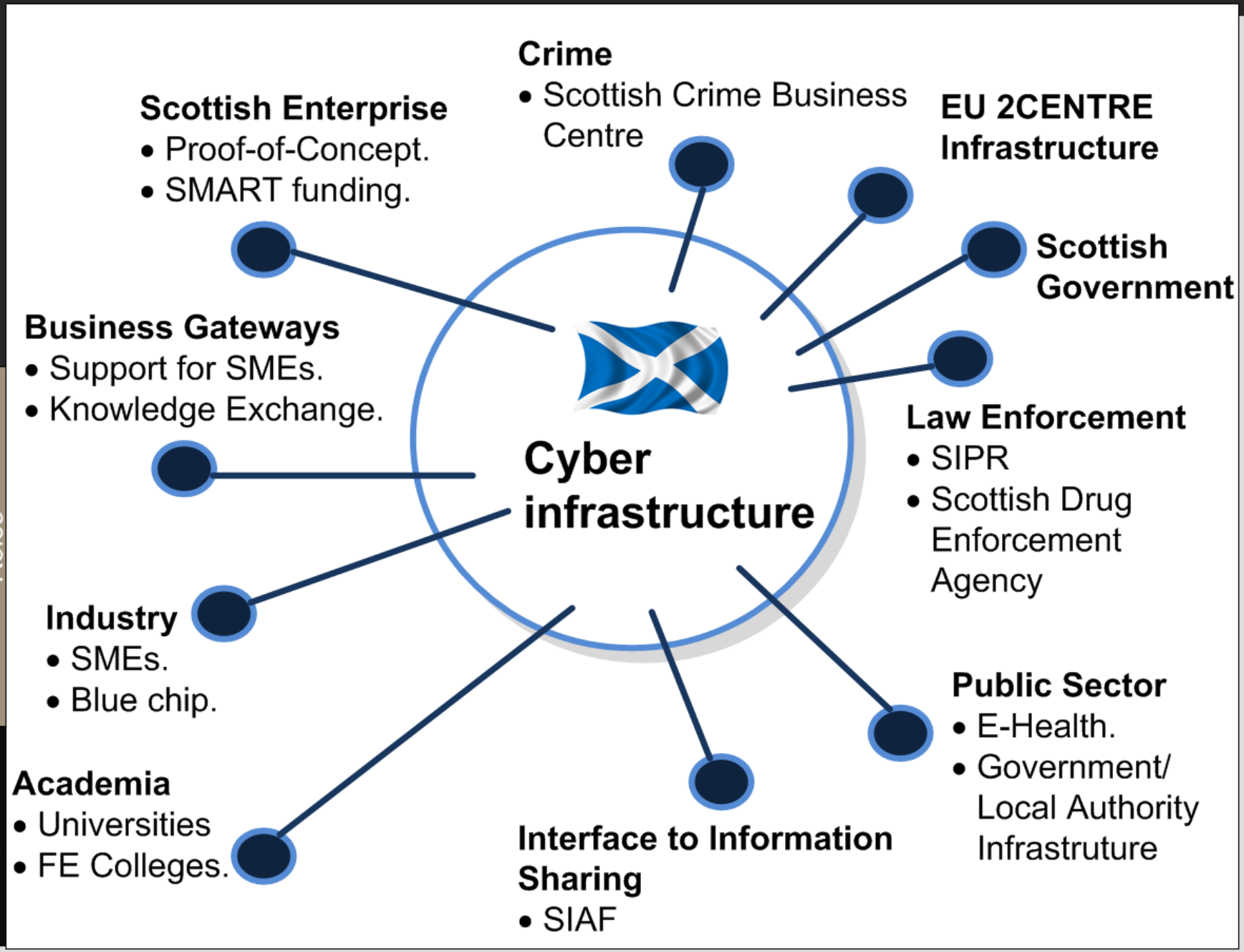
Better Society

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

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.


Crime
• Scottish Crime Business Centre
Scottish Enterprise
• Proof-of-Concept.
• SMART funding.
EU 2CENTRE Infrastructure
Scottish Government
Business Gateways
• Support for SMEs.
• Knowledge Exchange.
Cyber infrastructure
Law Enforcement
• SIPR
• Scottish Drug Enforcement Agency
Industry
• SMEs.
• Blue chip.
Public Sector
• E-Health.
• Government/ Local Authority Infrastruture
Academia
• Universities
• FE Colleges.
Interface to Information Sharing
• SIAF
Roles
Cyber
Roles

Cyber skills

Defining the Skills-base for the Future

Professor Bill Buchanan

Author: Prof Bill Buchanan