State of the Art in Electronic Security

Ir. Luc De Clercq

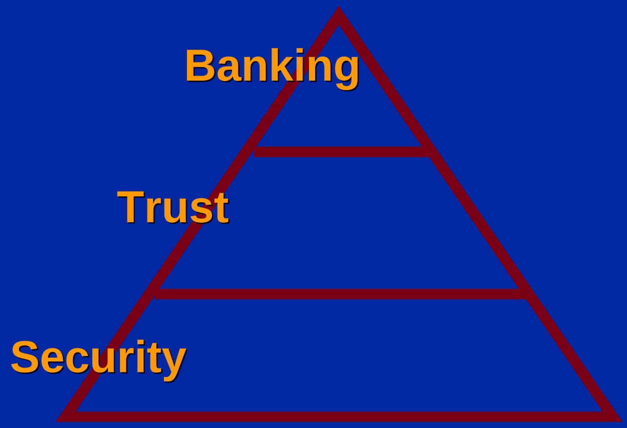
Senior manager,

Global Information Security

Agenda

1. Current Threats & Vulnerabilities
2. Emerging Security Technology
3. State-of-the-Art Security Regime
4. S.W.I.F.T.'s Security Strategy - Security Benchmarking Tool
5. The Way Ahead

Security


Banking

Trust

Security

Banking is based on trust

Trust is based on security

Availability

Reliability

Accountability

Integrity

Confidentiality

Risks

1. More hackers ↑

   Programmers are positive, hackers are not.

Hostile Environment

2. Readily available sophisticated hacking tools ↑

3. Increased dependence of banks on IT ↑

4. Open (insecure) technologies
   - Internet - hostile environment
   - UNIX - comes with 8000 open doors
   - TCP/IP - can easily be manipulated

Sophisticated Attack Tools

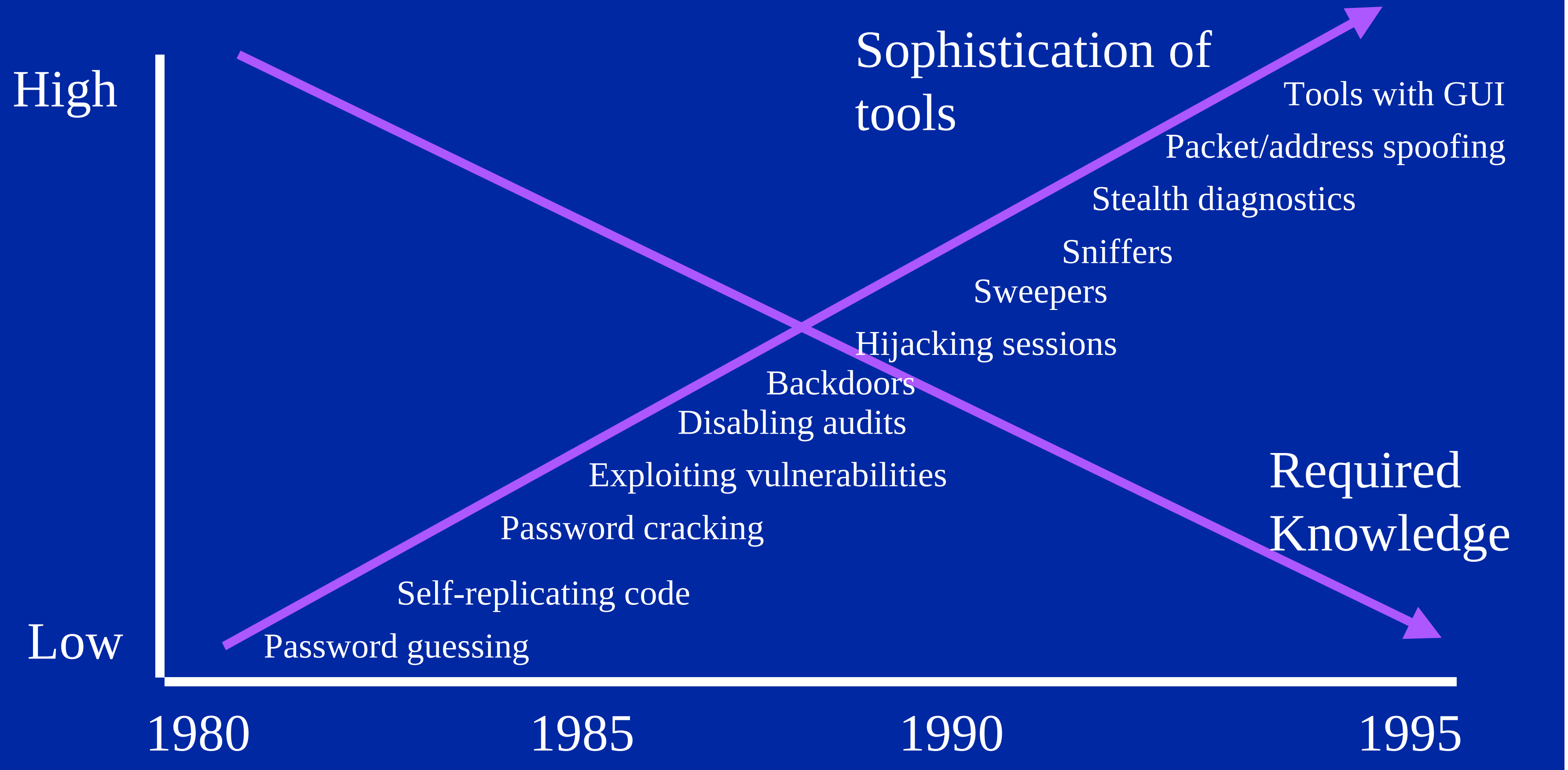
Low-security Technology

Viruses

5. Increased electronic access by customers ↑

6. E-cash, E-commerce, E-mail E-TC!

System Attacks



Sophistication of tools

Tools with GUI

Packet/address spoofing

Stealth diagnostics

Sniffers

Sweepers

Hijacking sessions

Backdoors

Disabling audits

Exploiting vulnerabilities

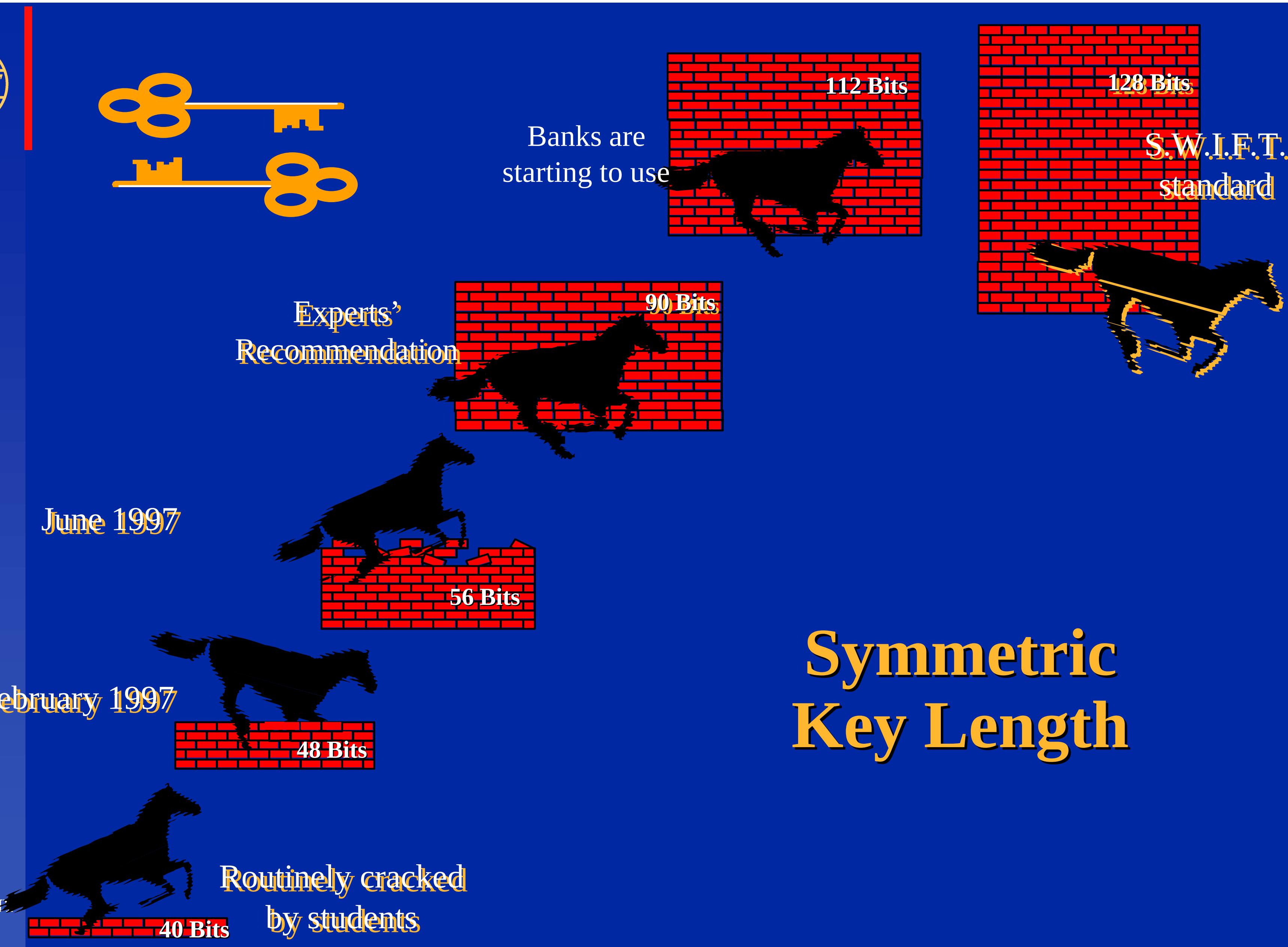
Password cracking

Self-replicating code

Password guessing

Required Knowledge

Symmetric Key Length



40 Bits

Routinely cracked
by students

48 Bits

February 1997

56 Bits

June 1997

90 Bits

Experts'
Recommendation

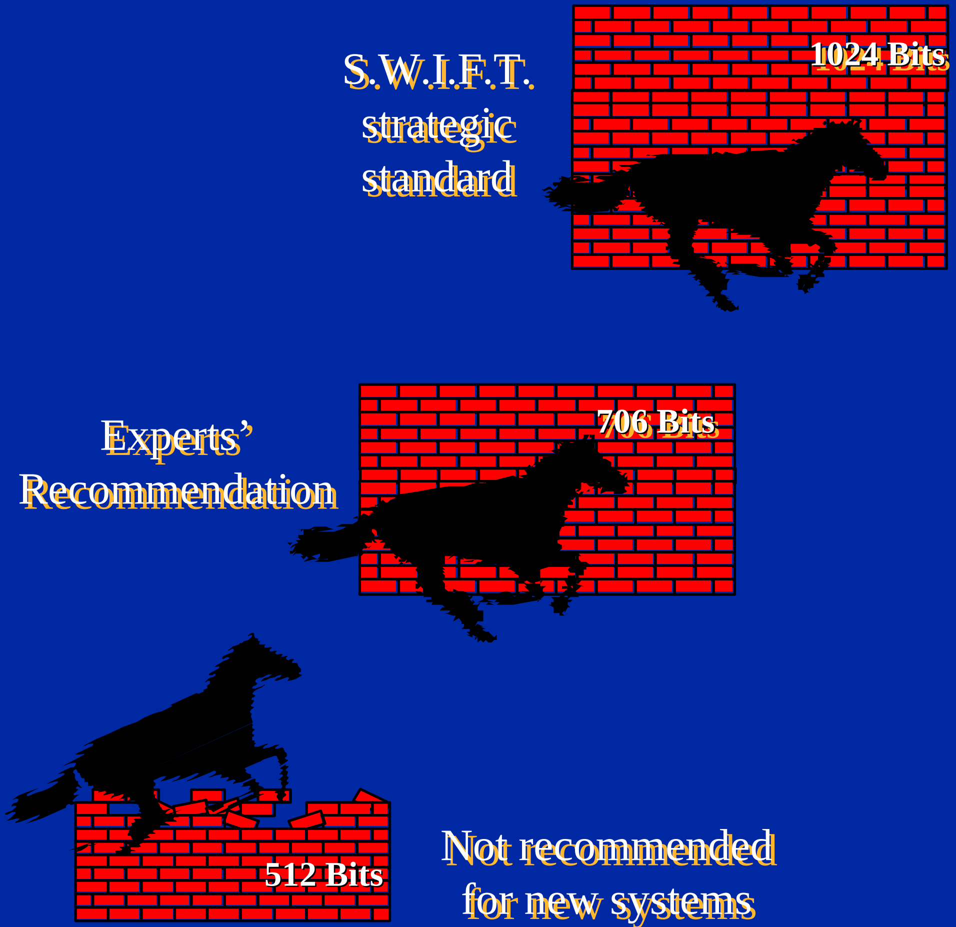
112 Bits

Banks are
starting to use

128 Bits

S.W.I.F.T.
standard

Asymmetric Key Length (RSA)



S.W.I.F.T.
strategic
standard

1024 Bits

Experts'
Recommendation

706 Bits

512 Bits

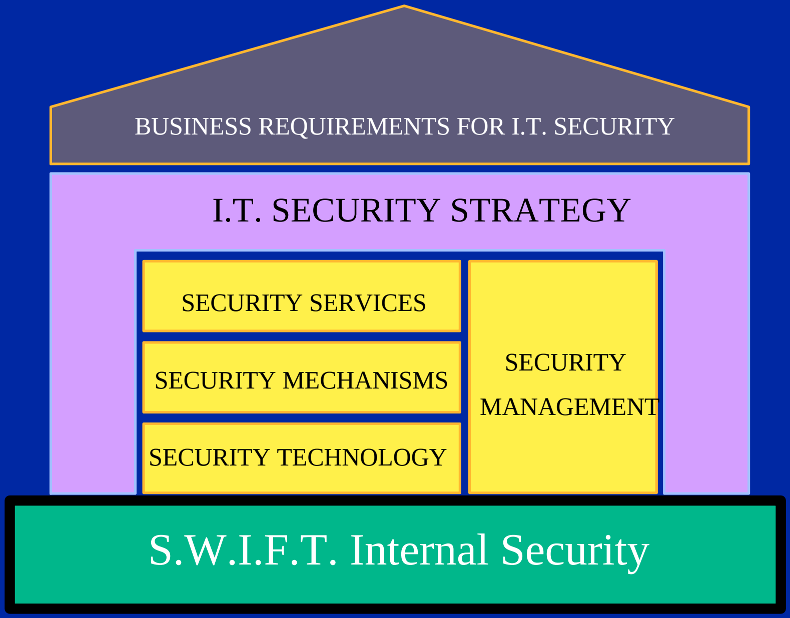
Not recommended
for new systems

Agenda

1. Current Threats & Vulnerabilities
2. Emerging Security Technology
3. State-of-the-Art Security Regime
4. S.W.I.F.T.'s Security Strategy - Security Benchmarking Tool
5. The Way Ahead

Information Security - Architecture

Security enables, protects and supports the financial business



BUSINESS REQUIREMENTS FOR I.T. SECURITY

I.T. SECURITY STRATEGY

SECURITY SERVICES

SECURITY MECHANISMS

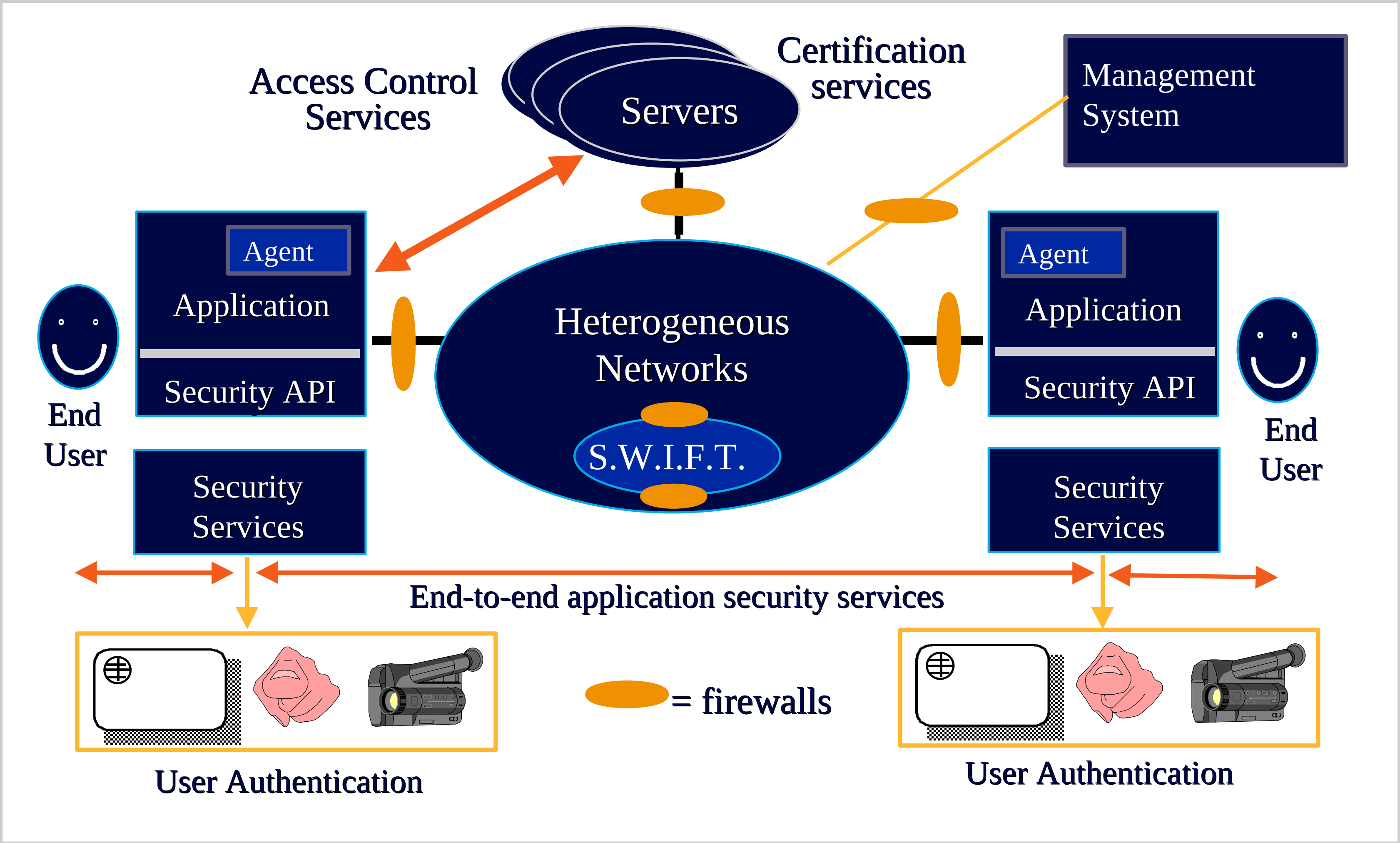
SECURITY TECHNOLOGY

SECURITY MANAGEMENT

S.W.I.F.T. Internal Security

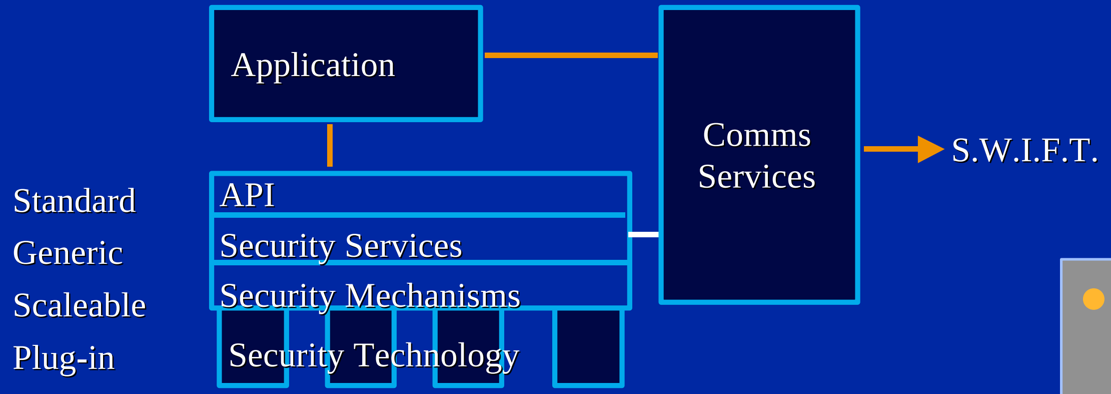
- User-friendly security
- Strong internal security foundation built on internal security acting on process & culture
- Standardised security services
- Truely end-to-end & multi-tiered
- Modular & scaleable mechanisms
- State-of-the-art technology
- Protection from hostile environment
- Security management services
- Certified with risks underwritten

Security Technology Infrastructure

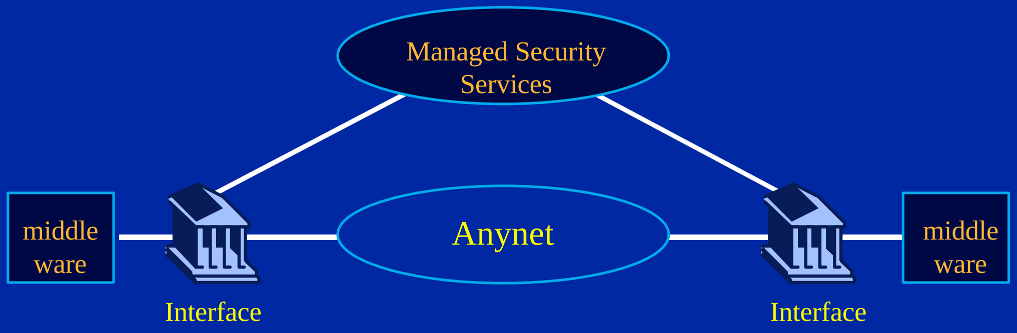


Application Security - Cryptography

PKI - "middle ware"



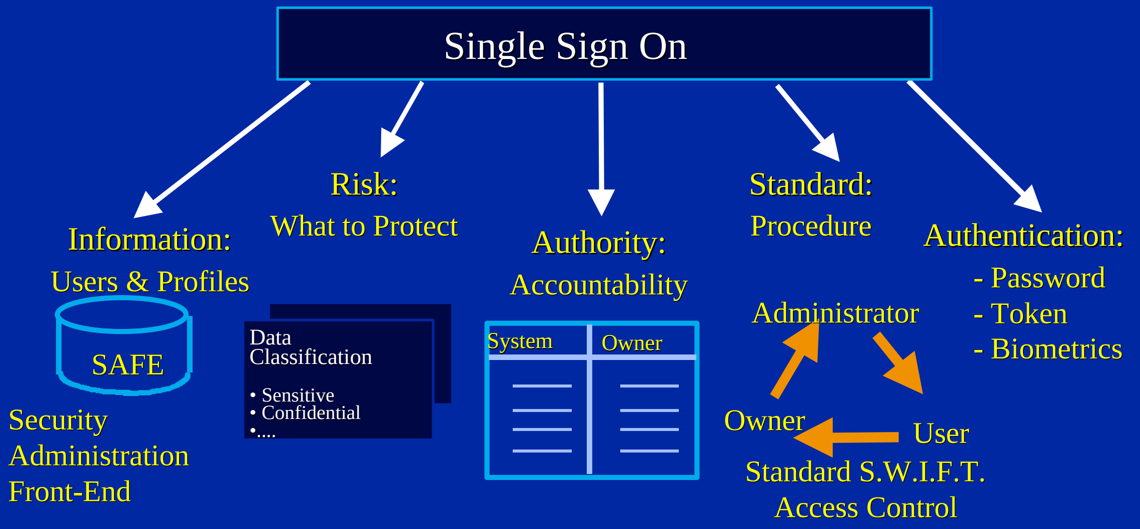
PKI - Secure services



- End-to-end message encryption
- End-to-end message authenticity and non-repudiation
- System integrity

System Access Control

- Strong human-being authentication
- Client to server session authentication
- Integrated access control: SECURE single sign-on



Single Sign On

Information:
Users & Profiles

SAFE

Security
Administration
Front-End

Risk:
What to Protect

Data
Classification

- Sensitive
- Confidential
- ....

Authority:
Accountability

System | Owner

Standard:
Procedure

Administrator

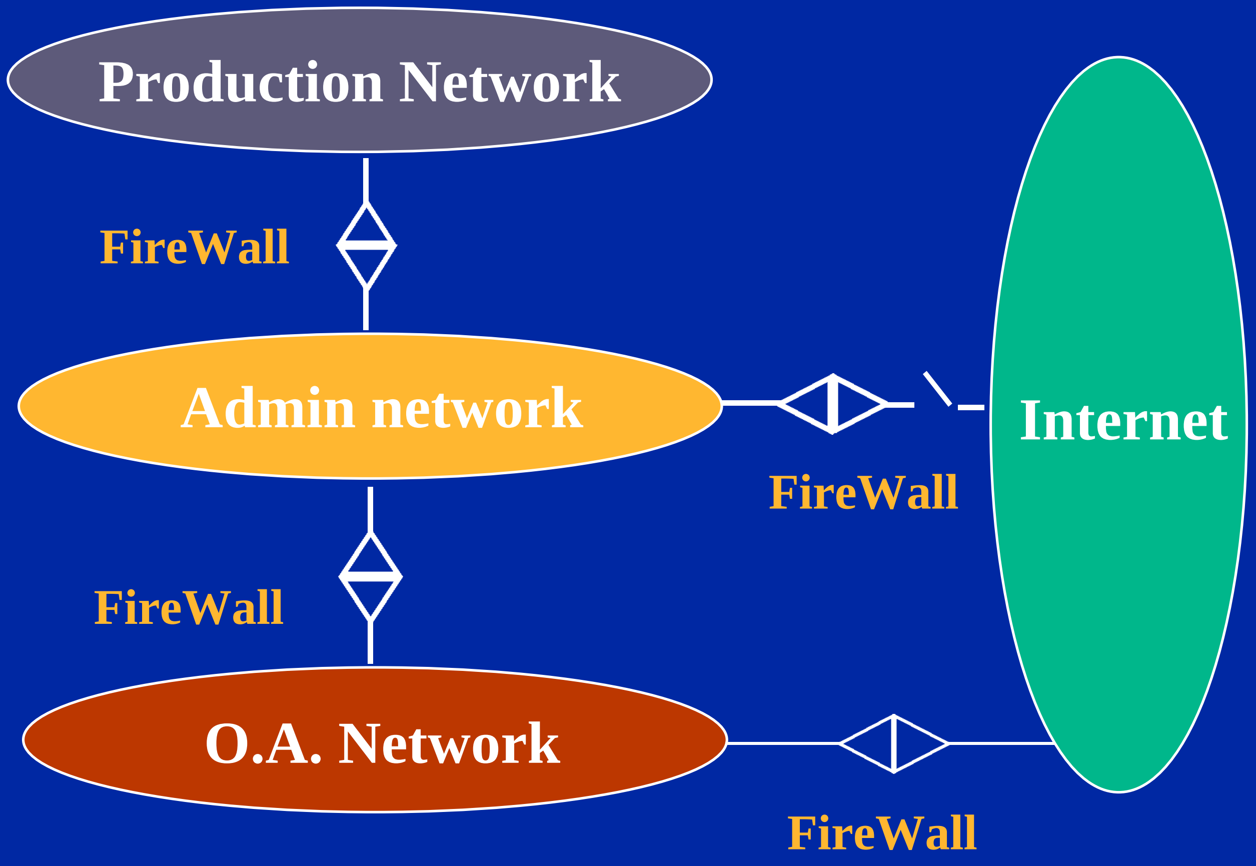
Owner

User

Standard S.W.I.F.T.
Access Control

Authentication:
- Password
- Token
- Biometrics

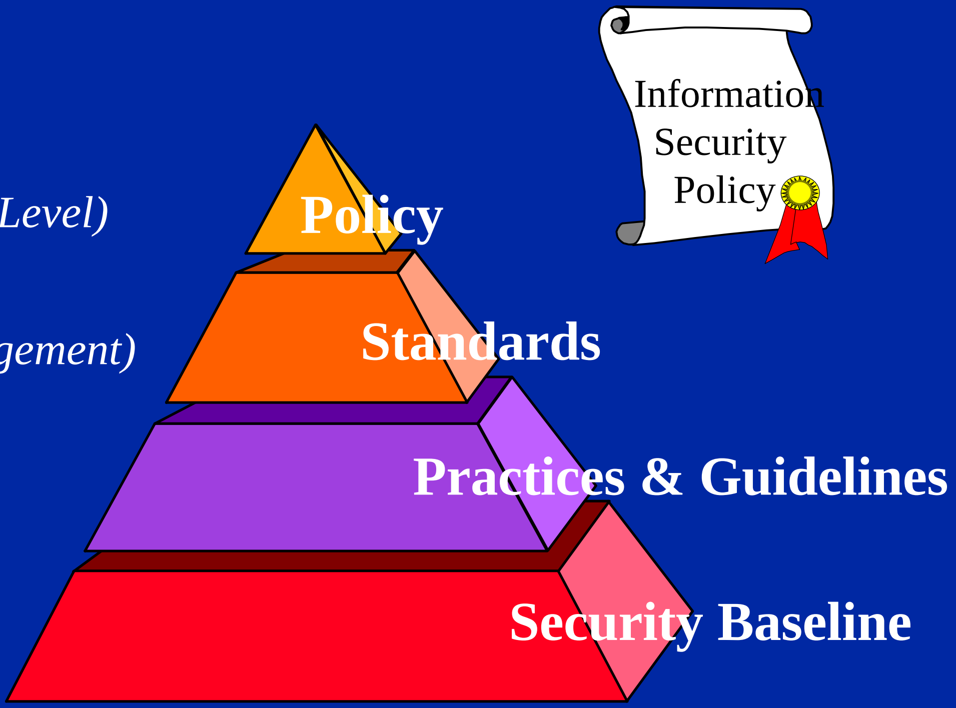
Network Segregation



Agenda

1. Current Threats & Vulnerabilities
2. Emerging Security Technology
3. State-of-the-Art Security Regime
4. S.W.I.F.T.'s Security Strategy - Security Benchmarking Tool
5. The Way Ahead

1. Security Policy



Information Security Policy

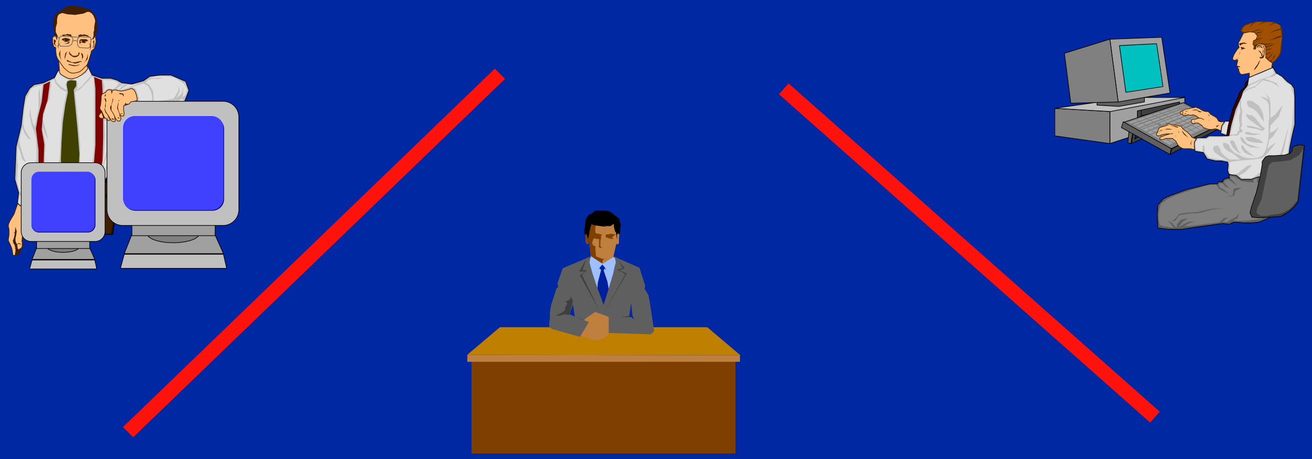
(Executive Level) Policy

(Middle Management) Standards

(Staff) Practices & Guidelines

(Products) Security Baseline

2. Allocation of responsibilities



Organisational security

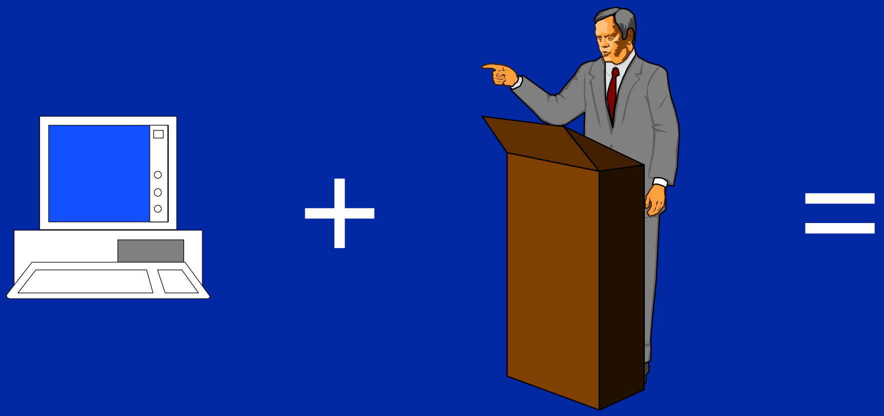
- Separation of Duties
- Dual control

3. Assets classification

- Assign owner
- Business Risk Analysis
- Asset Classification
  - Confidentiality
  - Integrity
  - Availability
- Minimum Security requirement and controls

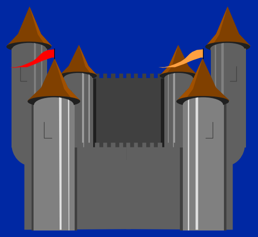
4. Personnel Security

- A battle for the hearts and minds of employees
- Technology versus education
- Measuring Security orientation
- Certifying Security awareness
- Awareness campaign
- Hiring - background and credit checks

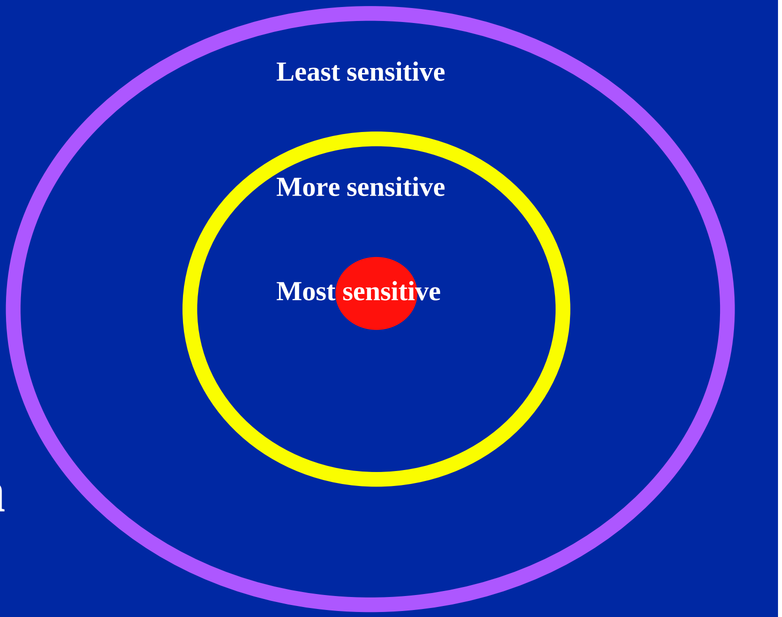


Effective Security

5. Physical Security



- Concentric security perimeters
- Locks, guard-desks, & identification
- Power supply
- Alarm systems
- Fire control
- Access for cleaning and maintenance

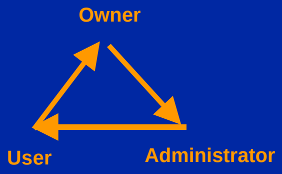


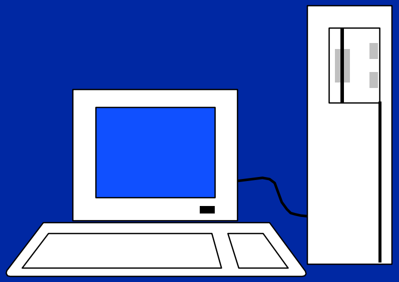
Concentric Security Perimeters

6. I.T. Security

System Access Control

- User Identification
- User Authentication
- User Authorisation

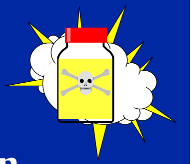




Secure Transmissions

- Message encryption
- Message authentication
- Message signature
- Non-repudiation
- Proof-of-origin
- Proof-of-delivery

System Integrity

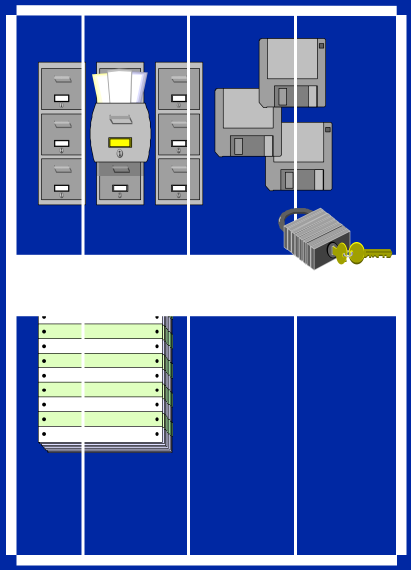


- Integrity at delivery
  - Quality assurance
  - ITSEC
- Integrity at production
  - Virus controls
  - DB integrity : R/W access
  - Secure Operating system
    - Orange book
    - UNIX & NT Security

8. Legal requirement

Safeguards on company records

- Legal constraints in the financial industry
- Off-site archival
- regular archives reload & testing

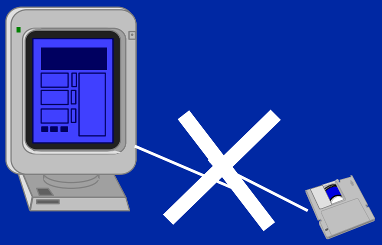


Residual risks underwritten

- Transfer risks via insurance
- Retain risks via self-insurance
- Assign risks to cheapest cost avoider

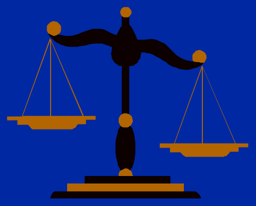
8. Legal requirement

Safeguards against illegal software copying



- licenced software
- Beware of Business Software Association (B.S.A.)

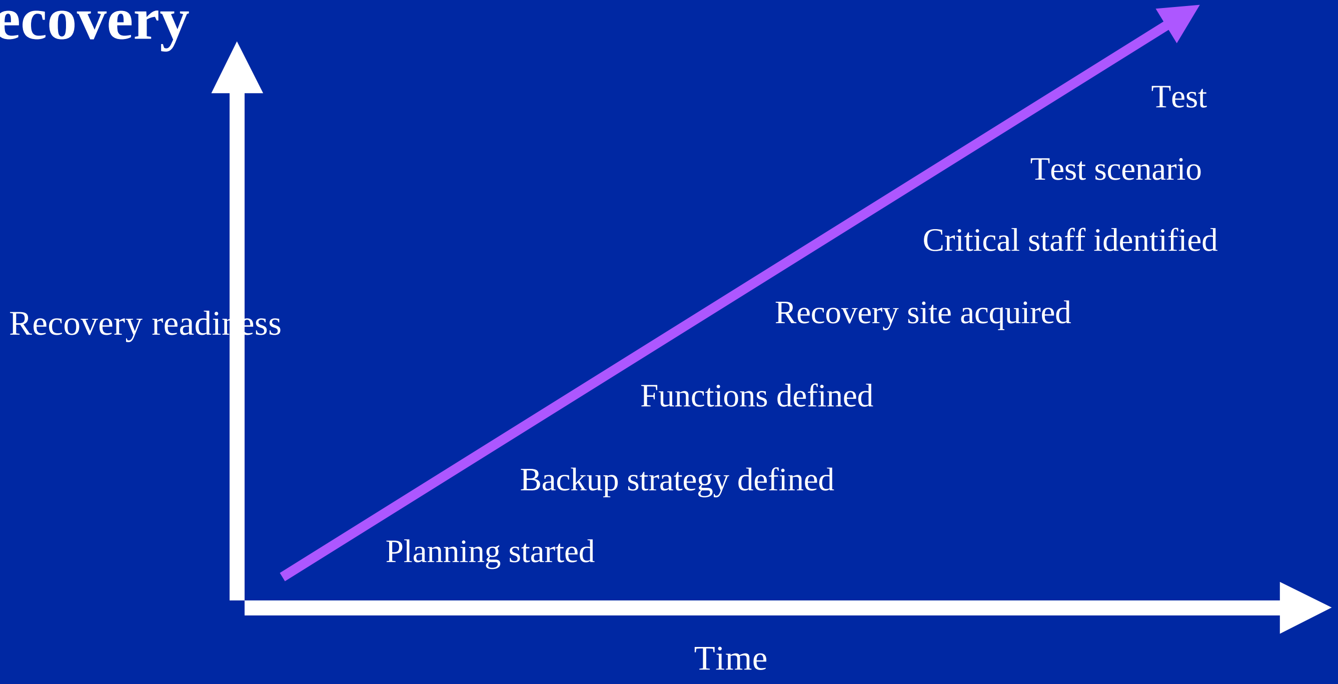
Private Data Protection



- Legal constraint
- Data may only be used for the purpose it was collected for.

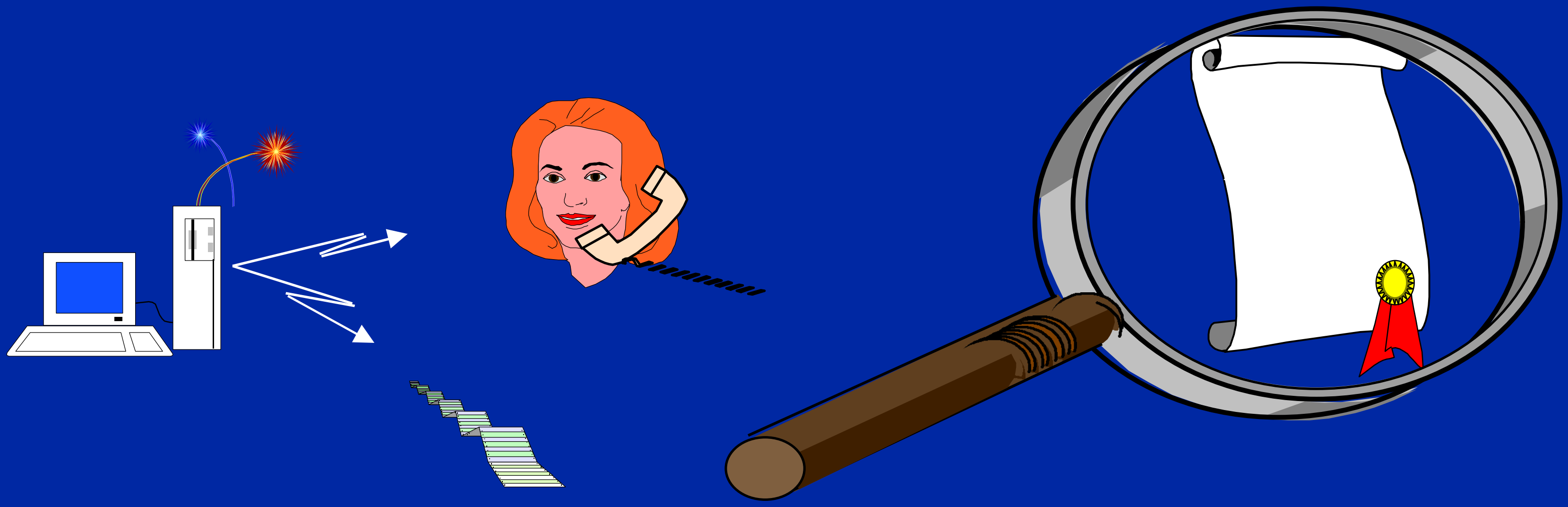
9. Business Continuity Planning

- General principles
- Backup and recovery
- Local versus offsite storage
- Recovery contracts
- Testing recovery



10. Compliance with security policy

- Monitor compliance
- Reporting Security incidents and analysing correlation
- Independant auditing

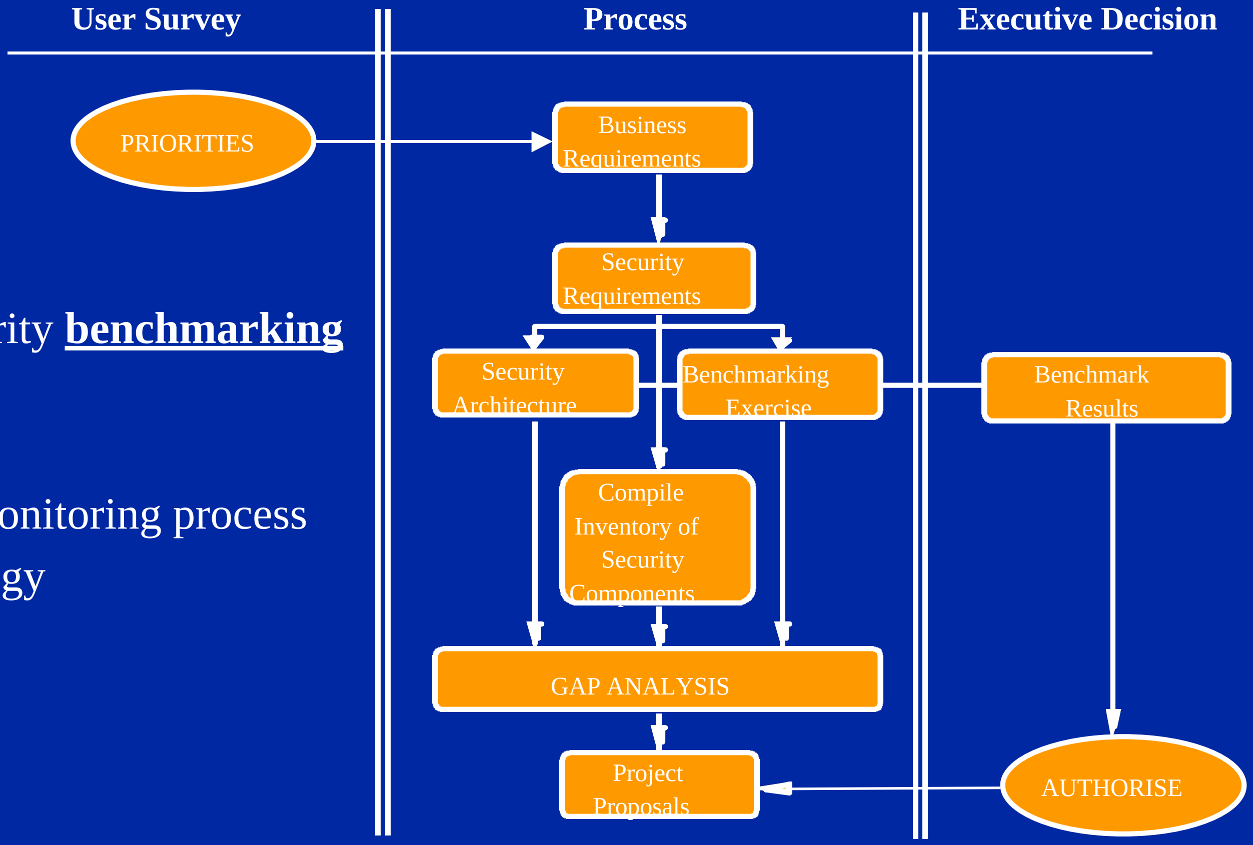


Agenda

1. Current Threats & Vulnerabilities
2. Emerging Security Technology
3. State-of-the-Art Security Regime
4. S.W.I.F.T.'s Security Strategy - Security Benchmarking Tool
5. The Way Ahead

Security Strategy

Aligned with industry needs, measurable



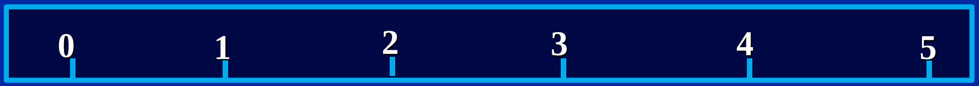
- Comprehensive IT security **benchmarking**
- Gap analysis
- Generic architecture
- Executive decision & monitoring process
- 5 Year IT security strategy

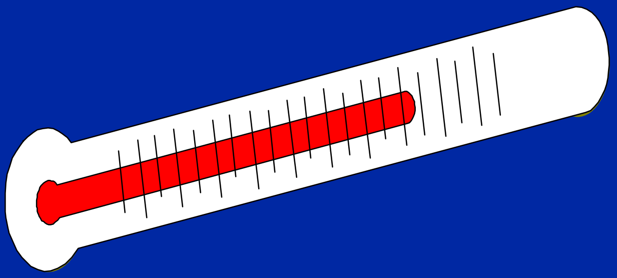
Measuring Security

- Industry standards
- Benchmarks
- Descriptions of each measure
- Easy to plan improvements

“Where do I go from here” asked Alice.
“Depends on where you want to get to”
said the White Rabbit.

Scales of Measurement





The Scale:

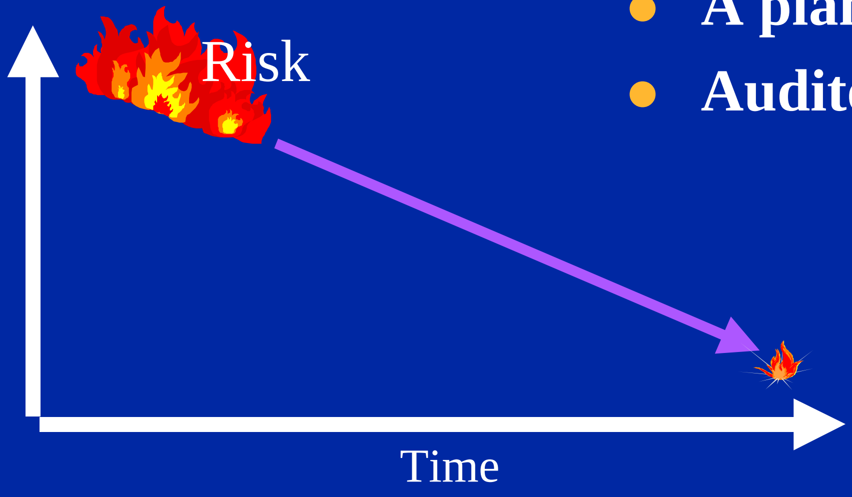
5 Excellent:	Best possible, highly integrated
4 Very Good:	Advanced level of practice
3 Good:	Moderately good level of practice
2 Fair:	Some effort made to address issues
1 Poor:	Recognise the issues
0 Very poor:	Complete lack of good practice

Agenda

1. Current Threats & Vulnerabilities
2. Emerging Security Technology
3. State-of-the-Art Security Regime
4. S.W.I.F.T.'s Security Strategy - Security Benchmarking Tool
5. The Way Ahead

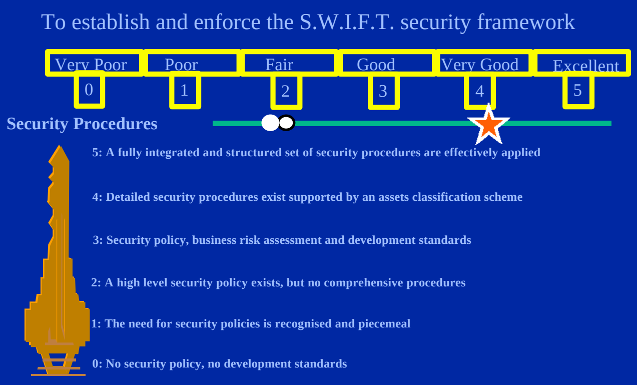
Risk Reduction

- Not aiming to solve ‘today’
- Risk reduction over time
- A planned approach
- Auditors’ role



A Planned Approach

Security Strategy Process



To establish and enforce the S.W.I.F.T. security framework

Very Poor 0 | Poor 1 | Fair 2 | Good 3 | Very Good 4 | Excellent 5

Security Procedures

5: A fully integrated and structured set of security procedures are effectively applied

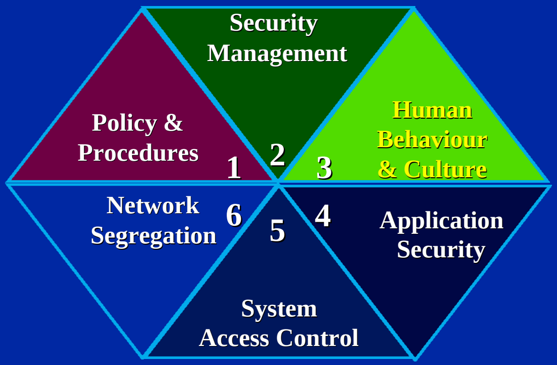
4: Detailed security procedures exist supported by an assets classification scheme

3: Security policy, business risk assessment and development standards

2: A high level security policy exists, but no comprehensive procedures

1: The need for security policies is recognised and piecemeal

0: No security policy, no development standards



Security Management

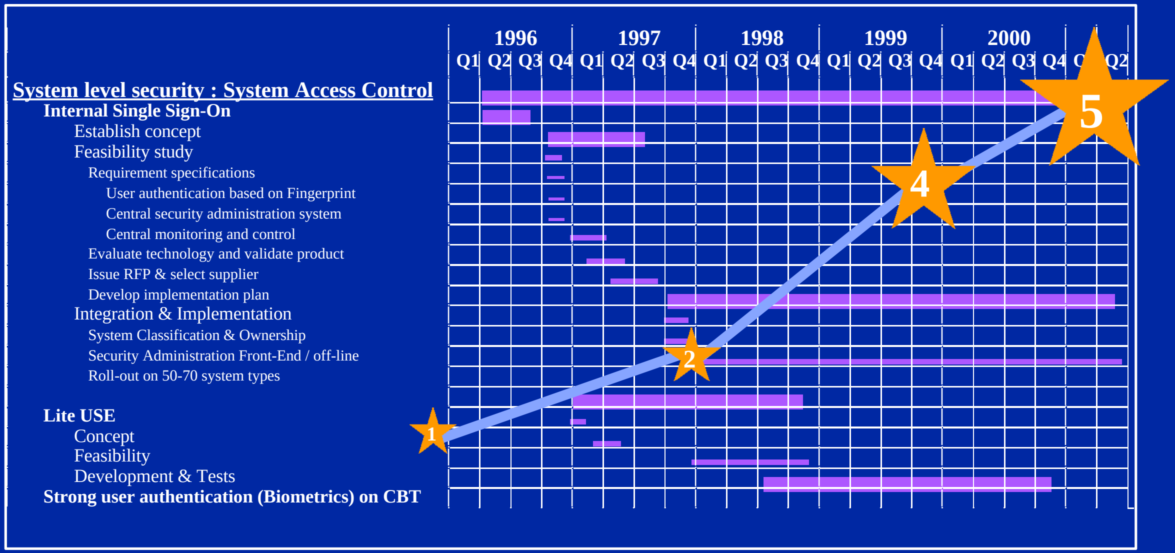
Policy & Procedures

Human Behaviour & Culture

Network Segregation

Application Security

System Access Control



System level security : System Access Control

Internal Single Sign-On

Establish concept

Feasibility study

Requirement specifications

User authentication based on Fingerprint

Central security administration system

Central monitoring and control

Evaluate technology and validate product

Issue RFP & select supplier

Develop implementation plan

Integration & Implementation

System Classification & Ownership

Security Administration Front-End / off-line

Roll-out on 50-70 system types

Lite USE

Concept

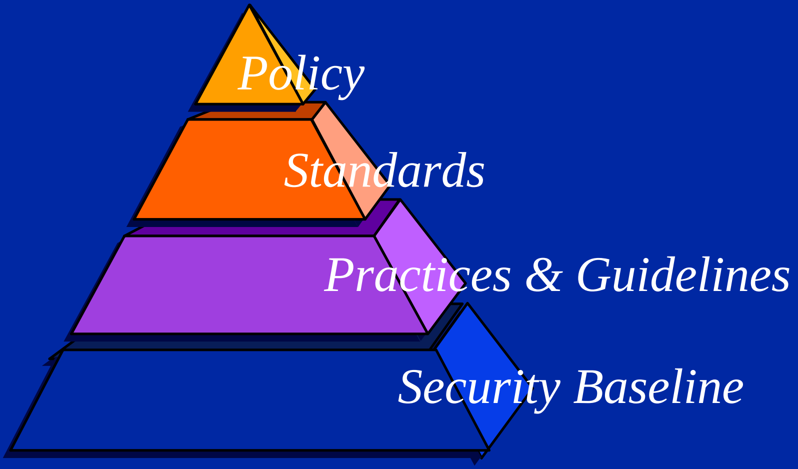
Feasibility

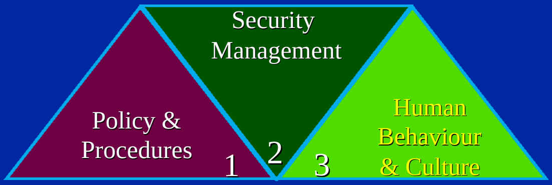
Development & Tests

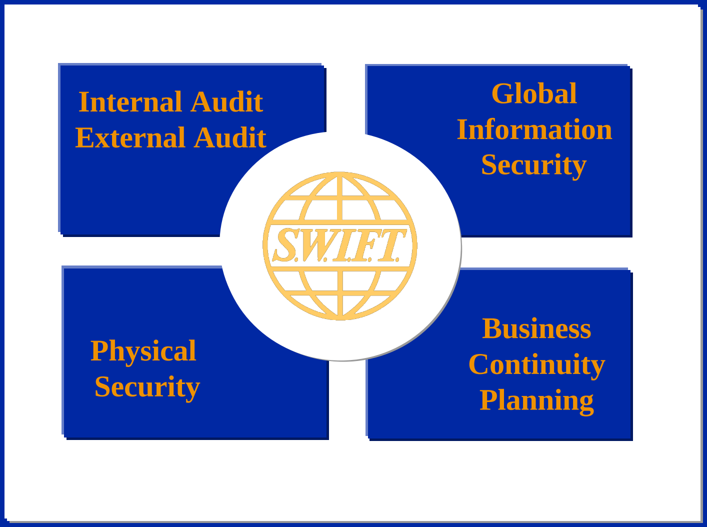
Strong user authentication (Biometrics) on CBT

For each of the domains there is a detailed benchmark and gap analysis, translated into clear project plans, monitored by Management, Auditors and the Board.

Security Management Infrastructure



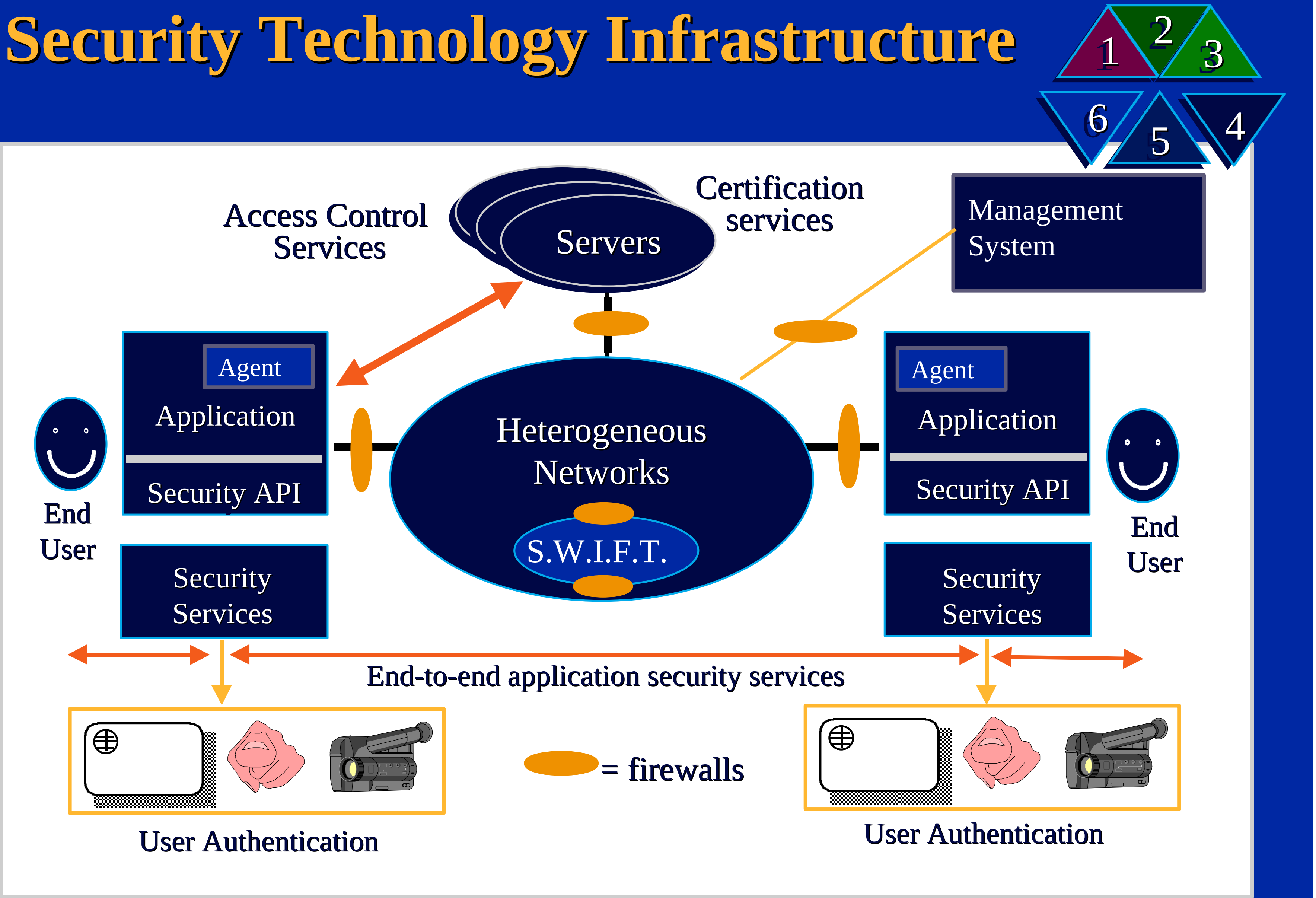



Internal Audit External Audit
Global Information Security
SWIFT
Physical Security
Business Continuity Planning

Human Behaviour & Culture

- Security awareness campaign
- Role definition & appraisal
- Security certification
- Image & visibility for leadership role

Security Technology Infrastructure



S = Strategy

O = Organisational

T = Technology

P = Procedural