“Real-Time” ARMENIA!...

...Securing Government & Financial Enterprise Operations

Dr David E Probert
VAZA International

Armenian ICT Leaders Conference
Yerevan, Armenia : 21st to 22nd Feb 2009

Download Conference Presentation On-Line @ www.valentina.net/vaza/eARMENIA.pdf

Dual Themes: *Security & Growth*

- eSecurity: ICT Security is critical to Armenia’s future economy
  - “Real-Time” Armenia requires distributed e-defence network
  - Current networks are quite fragile, insecure & open to cyber attack
- eGrowth: Armenia needs to boost economic & eBusiness growth
  - Extend eGovernment Services & Leverage the global Armenian Diaspora
  - Propose ambitious 3-Phase Armenian eProgramme over next 3 to 5 Years

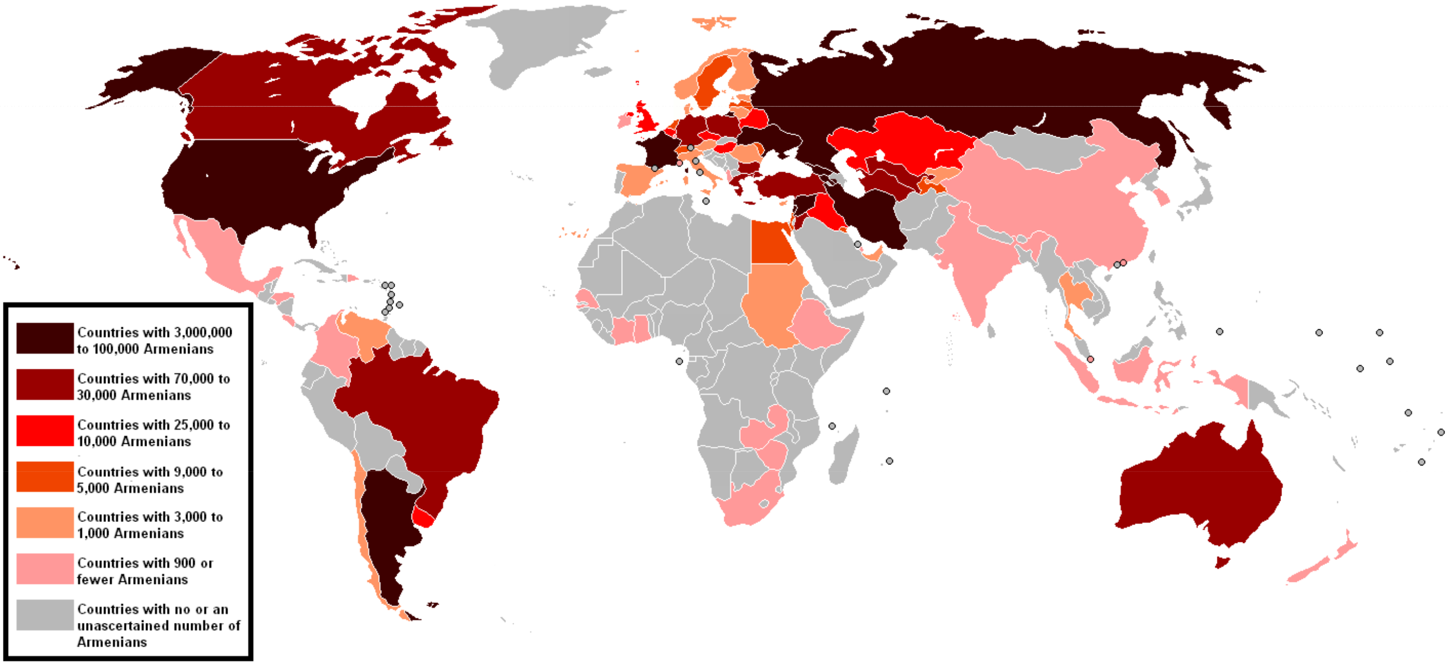
...“Economic Growth through Security”...

“Security” - *Dual Summits of Mt Ararat* - “Growth”

Current Security Situation

- Too many single points of network & system failure
- Inadequate data back-up & info storage procedures
- Often there is no real communicated security policy
- Networks open to Cyber Attacks and Cyber Crime
- Small skill base of specialist IT security professionals
- Security is not a "quick patch" but requires a multi-year programme based upon recognized ISO 2700x Standards

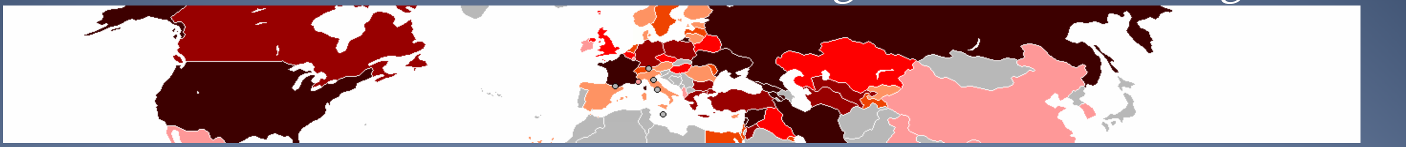
Worldwide Armenian Diaspora


Countries with 3,000,000 to 100,000 Armenians
Countries with 70,000 to 30,000 Armenians
Countries with 25,000 to 10,000 Armenians
Countries with 9,000 to 5,000 Armenians
Countries with 3,000 to 1,000 Armenians
Countries with 900 or fewer Armenians
Countries with no or an unascertained number of Armenians

Propose "secure" global electronic trading network – "eDiasporaNet"

"Electronic DiasporaNet"-eDN

- Leverage the business potential of global Armenian Diaspora
- Engineer International Electronic Business Trading Network
- Applications may include: Banking Loans, Credits, On-Line Support for complex deals, logistics, delivery, tax and customs
- Establish Yerevan as the Global Banking & Financial Trading Hub

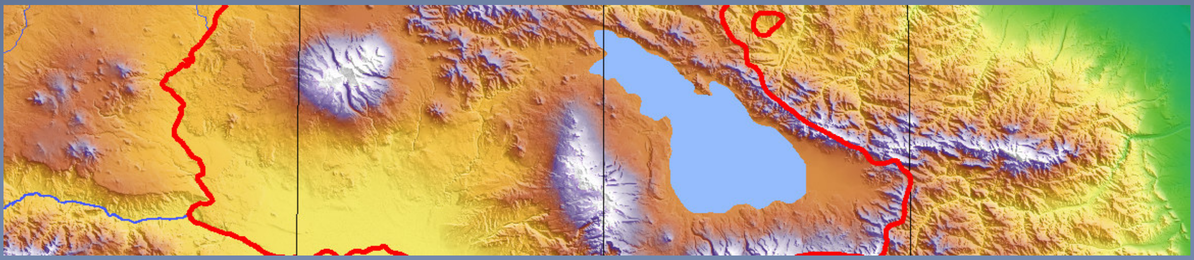


- Spreads financial risk over 25+ countries & several continents
- Extend eDN Membership to 3rd Parties through Annual Fees
- Implement in 3 Phases – eGovernment (Taxation, Customs), Real-Time Armenia (National eTradeNet), then eDiasporaNet (Global).....

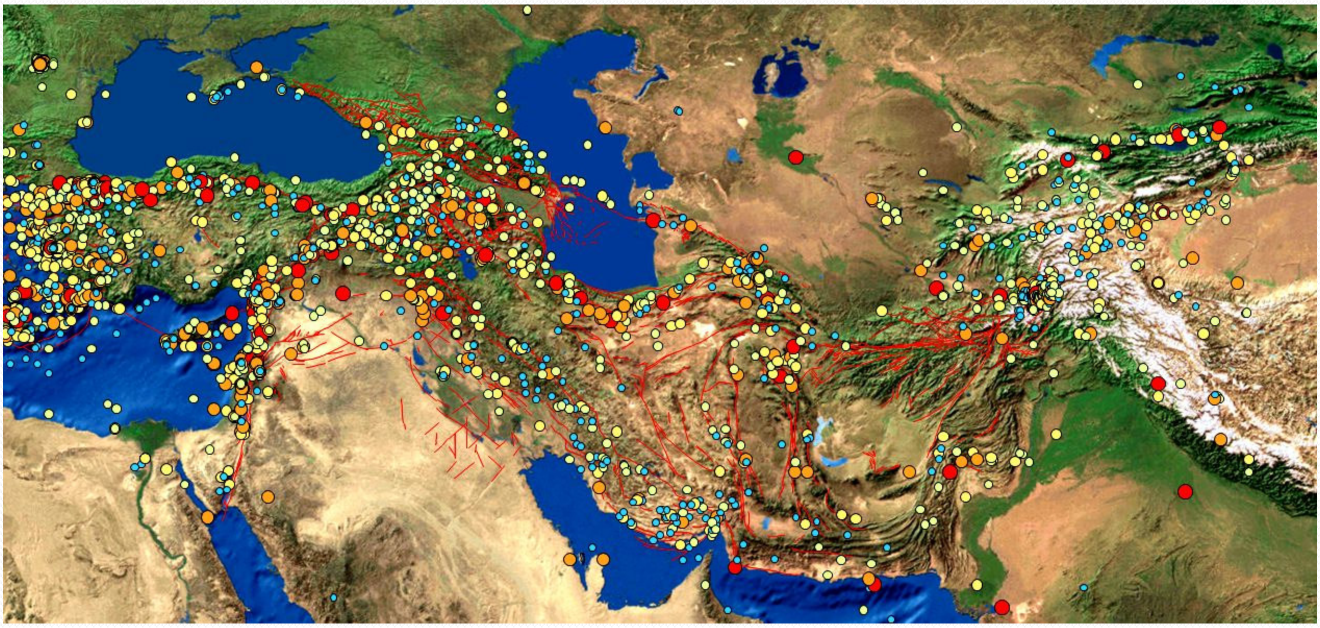
...Proposed eDN Project combines "Security" with "Growth"

Major 21stC Security Threats

- Distributed Denial of Service (DDOS) through "Botnets"
- Targeted Trojan Horses (including dormant sleepers)
- Destructive Viruses (often by email & exe files & scripts)
- Theft of Information, Passwords, ID & Keys
- Fake Web Sites and IP Addresses
- Physical Destruction through fires, floods, earthquakes....
- Planned Cyber Attacks and Cyber Crime
- Remote Agent interception & control of "secure" networks



Armenia: Major Earthquake Zone



Increased National Security Risk from Natural Disasters such as Earthquakes

Metsamor Nuclear Power Plant

Security Risk of Nuclear Accident from "End-of-Life" VVER Type Power Plant

Cyber Attack using Global Botnets

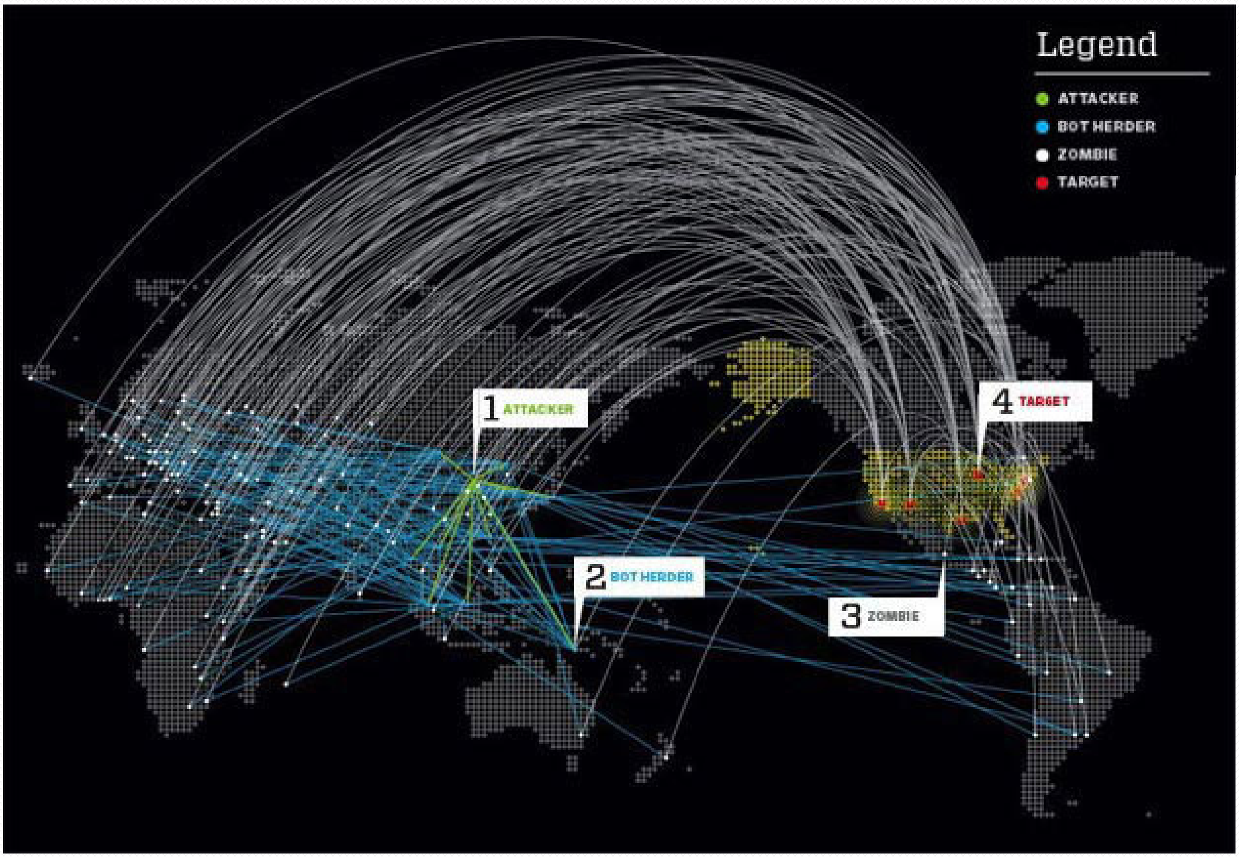


Diagram from Wired Magazine

The CyberCrime Business Model

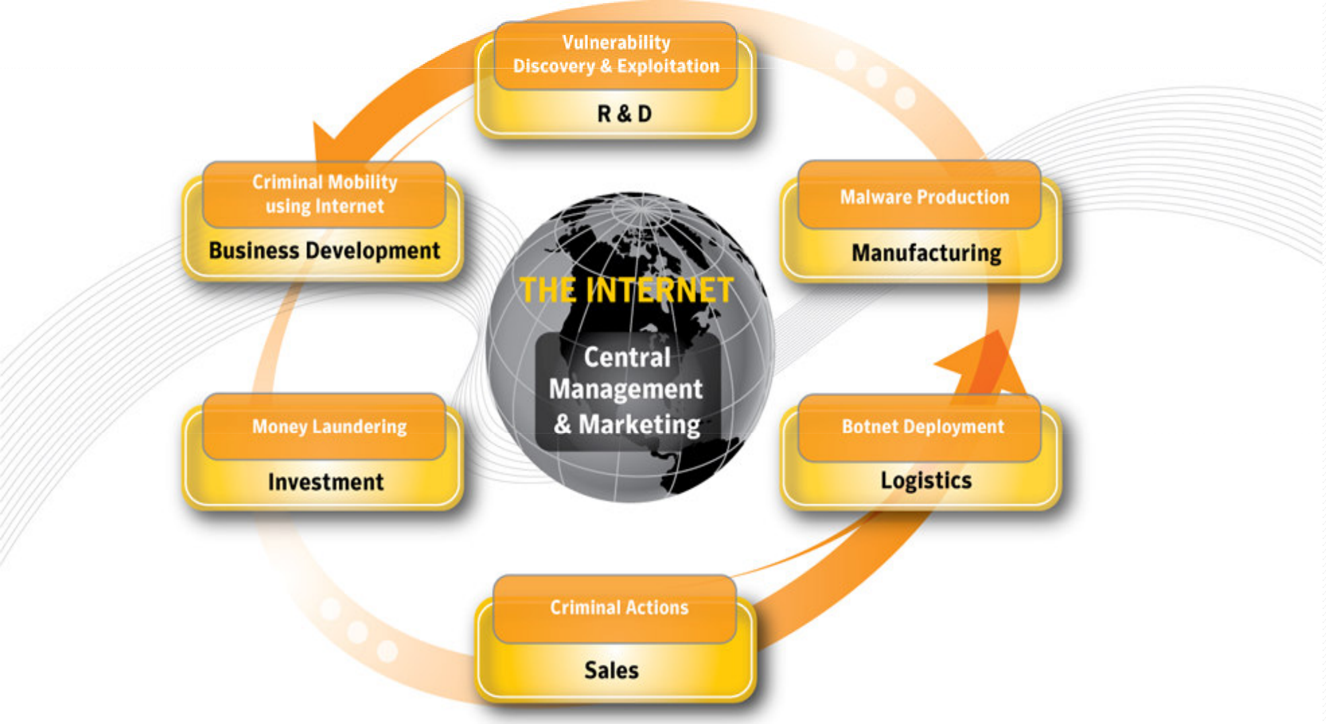


Diagram Courtesy of Symantec - UK

Technological Solutions

- ❖ Intrusion Detection & Protection Systems (IDS/IPS)
- ❖ Threat and Vulnerability Management (TVM)
- ❖ Real-Time Deep-Packet Inspection to detect DDOS Attack
- ❖ Web-Site & IP Address Assessment
- ❖ End-User Log-On Authentication & Certificates– IEEE802.1X
- ❖ Encryption both for secure networks as well as storage
- ❖ Digital Signatures to secure Data & Document Integrity
- ❖ Biometric access both for IT Devices as well as access security

Operational Solutions

- ❖Business Continuity Programme (BCP)
- ❖Disaster Recovery Planning & Training (DR)
- ❖Electronic Asset Management (RFID Tagging)
- ❖Physical Building Security (Networked IP CCTV)
- ❖CERT (Computer Emergency Response Team)
- ❖Professional Security Training to ISO Standards
- ❖Communication of comprehensive security policy

➢*…….Integrated Tech & Op Solution = Cyber Defence Centre*

Integrated Security in the Wild!

The Sociable Weaver Bird

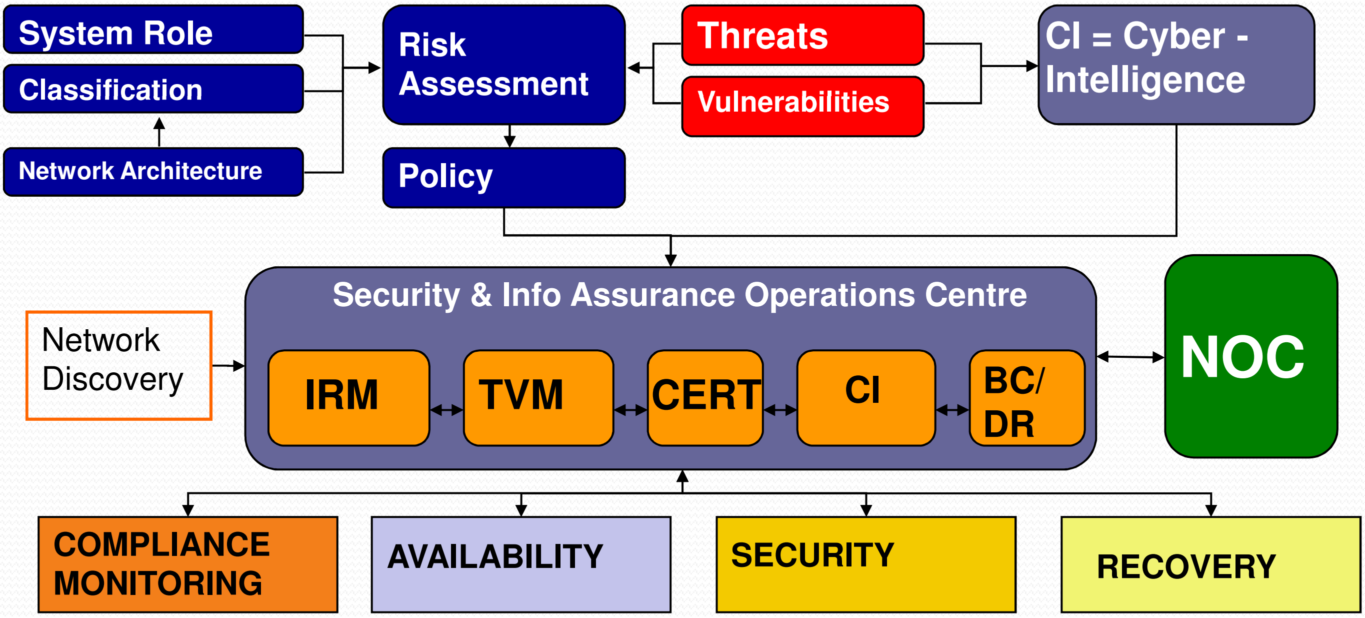
"World's largest Bird Nests"

*** Southern Africa ***

- Secure Living Community
- Self-Organising Architecture
- Fully scalable for long term growth
- Supports 250+ Weaver Birds
- Real-Time Disaster Alert System
- Sustainable in Semi-Desert Steppe
- Robust against "Enemy Risks" such as Eagles, Vultures & Snakes

...all the features of a 21stC-"Cyber Defence Centre"–including Disaster Recovery & Business Continuity!

Integrated Cyber Defence Centre

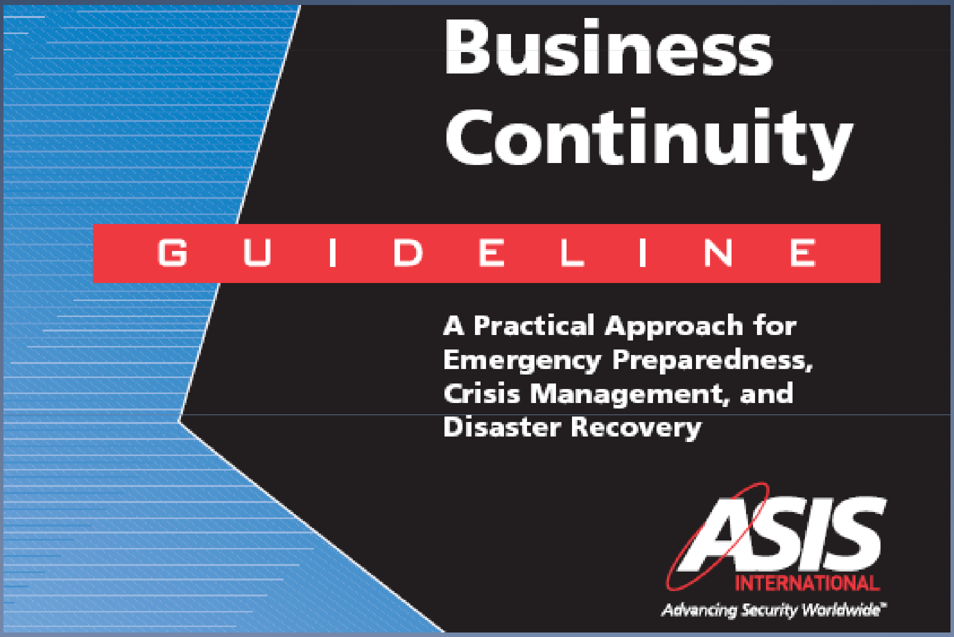


COMPLIANCE MONITORING	AVAILABILITY	SECURITY	RECOVERY
•Compliance tools	•Anti Spam	•IDS/IPS	•Back Up Services
•Network Discovery	•Anti Virus	•Firewalls	•Business Continuity
•Full Reporting	•Clustering/RAID	•Correlation Engines	•Disaster Recovery

Diagram Courtesy of Symantec - UK

Business Continuity Guidelines

- ASIS International Commission on Business Continuity & Disaster Recovery Guidelines- 2005



Business Continuity

GUIDELINE

A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery

ASIS INTERNATIONAL

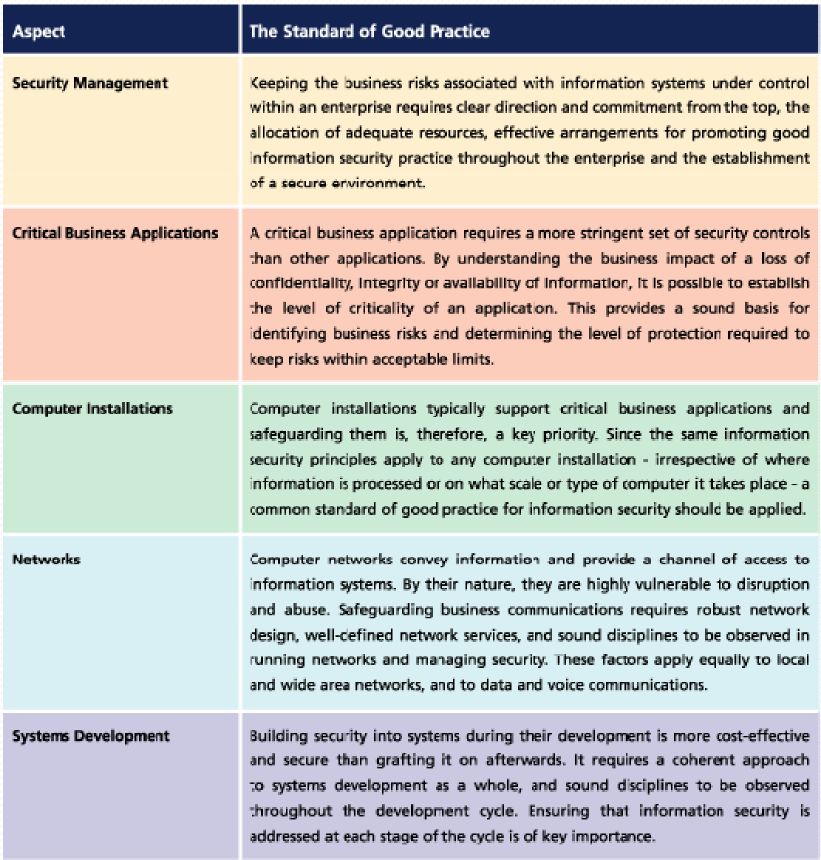
Advancing Security Worldwide

- ASIS Guidelines also include an excellent complete checklist for Business Continuity Planning

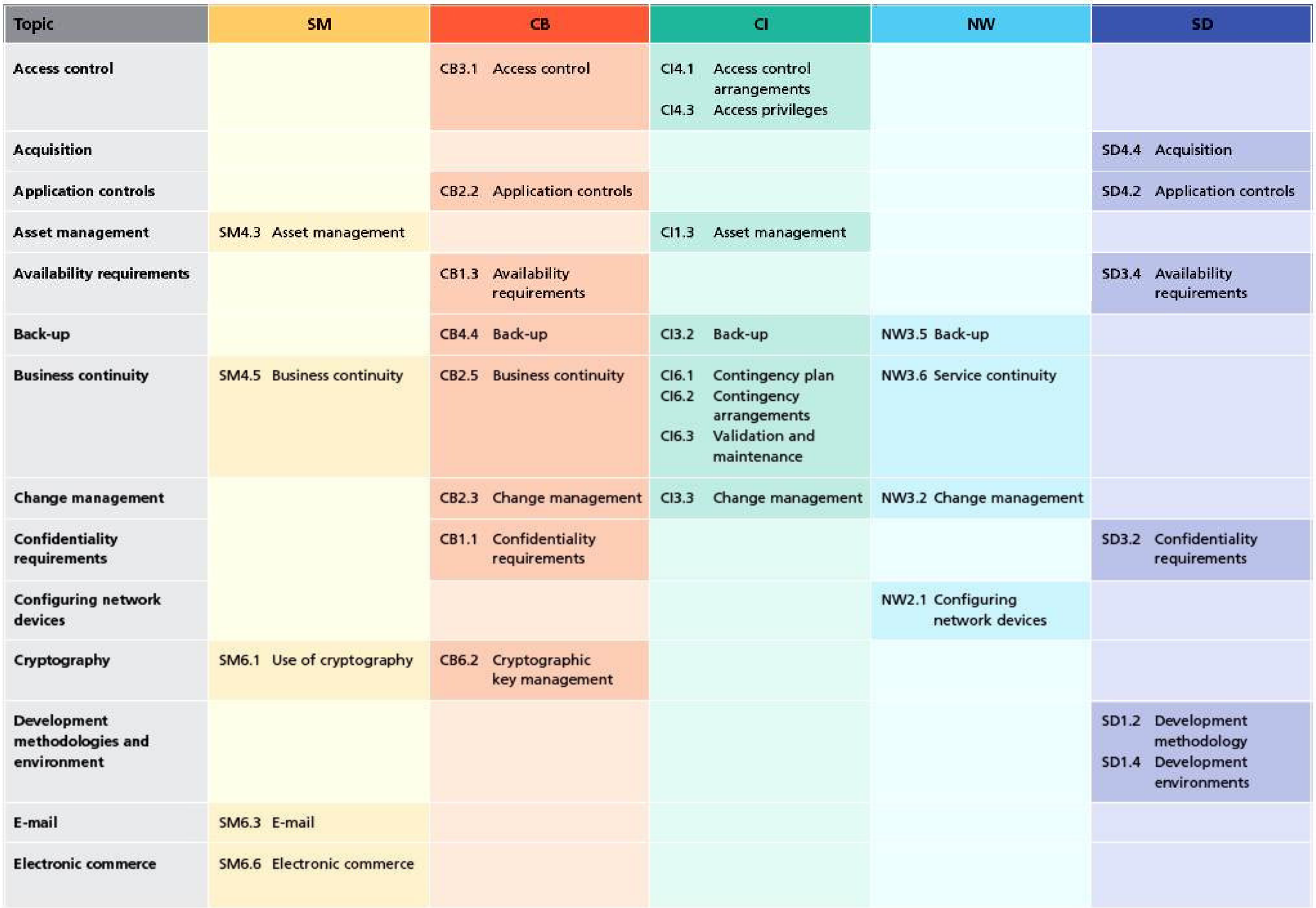
Security Standards - Matrix

- Framework for comprehensive security policy from Information Security Forum : ISF
- Security Standards includes the ISO/IEC – 27000 Series – 27001 and 27002 & 2700x
- European Countries such as UK and Germany have full-time security teams
- Armenian Government requires full-time Security Team to implement & monitor Policy

Information Security Forum (ISF) : “Top Themes”



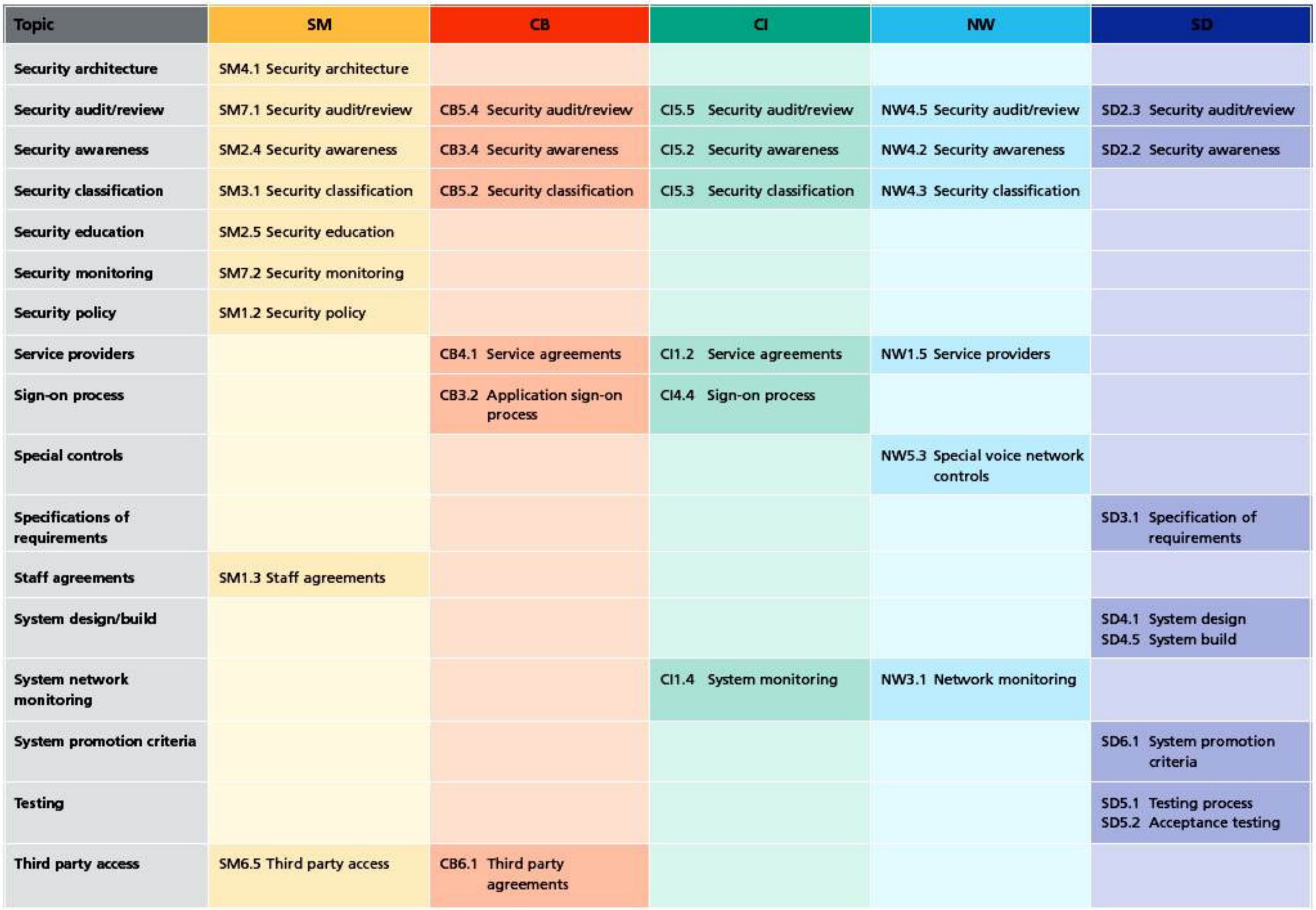
Aspect	The Standard of Good Practice
Security Management	Keeping the business risks associated with information systems under control within an enterprise requires clear direction and commitment from the top, the allocation of adequate resources, effective arrangements for promoting good information security practice throughout the enterprise and the establishment of a secure environment.
Critical Business Applications	A critical business application requires a more stringent set of security controls than other applications. By understanding the business impact of a loss of confidentiality, integrity or availability of information, it is possible to establish the level of criticality of an application. This provides a sound basis for identifying business risks and determining the level of protection required to keep risks within acceptable limits.
Computer Installations	Computer installations typically support critical business applications and safeguarding them is, therefore, a key priority. Since the same information security principles apply to any computer installation - irrespective of where information is processed or on what scale or type of computer it takes place - a common standard of good practice for information security should be applied.
Networks	Computer networks convey information and provide a channel of access to information systems. By their nature, they are highly vulnerable to disruption and abuse. Safeguarding business communications requires robust network design, well-defined network services, and sound disciplines to be observed in running networks and managing security. These factors apply equally to local and wide area networks, and to data and voice communications.
Systems Development	Building security into systems during their development is more cost-effective and secure than grafting it on afterwards. It requires a coherent approach to systems development as a whole, and sound disciplines to be observed throughout the development cycle. Ensuring that information security is addressed at each stage of the cycle is of key importance.



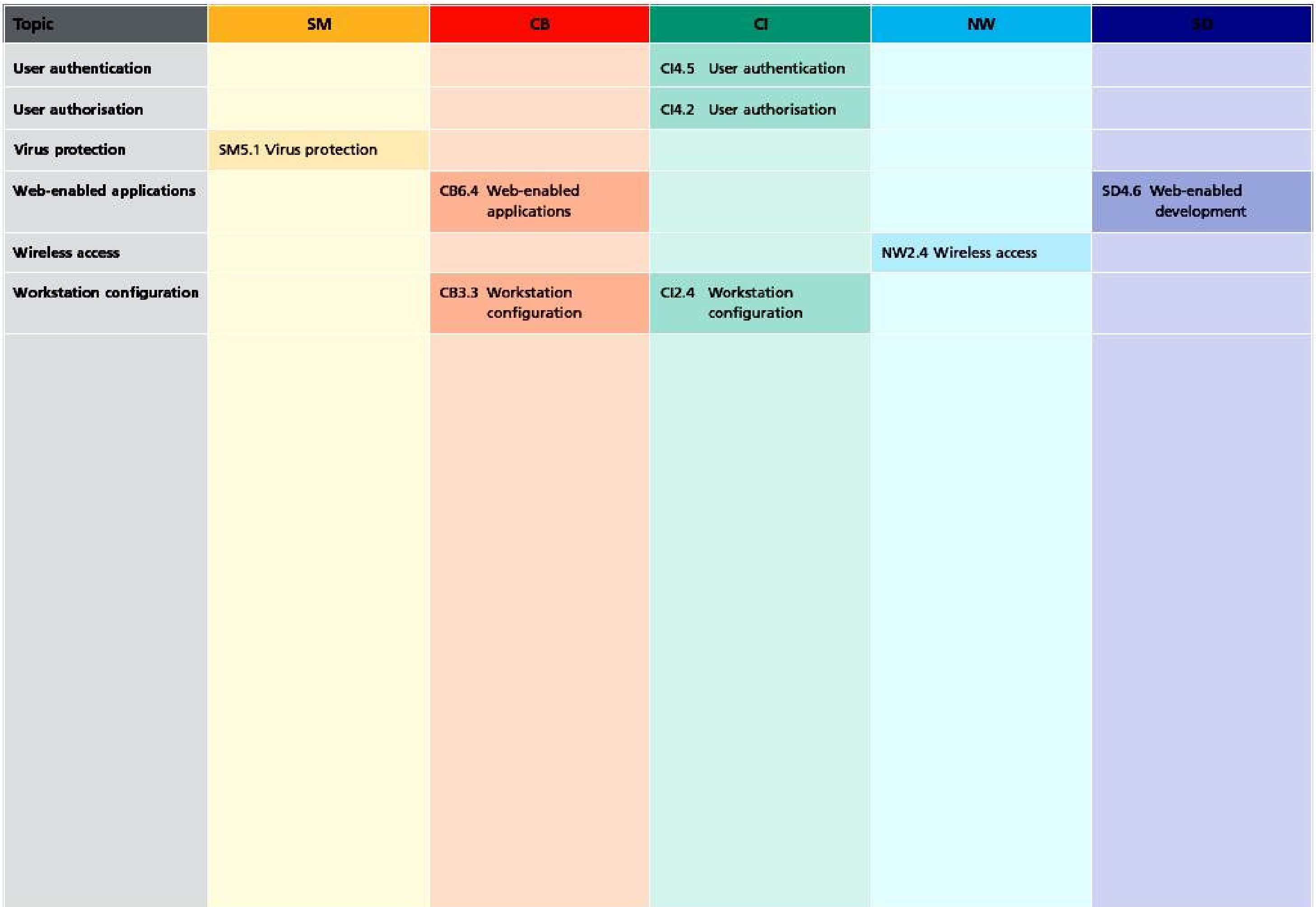
Topic	SM	CB	CI	NW	SD
Access control		CB3.1 Access control	CI4.1 Access control arrangements CI4.3 Access privileges		
Acquisition					SD4.4 Acquisition
Application controls		CB2.2 Application controls			SD4.2 Application controls
Asset management	SM4.3 Asset management		CI1.3 Asset management		
Availability requirements		CB1.3 Availability requirements			SD3.4 Availability requirements
Back-up		CB4.4 Back-up	CI3.2 Back-up	NW3.5 Back-up	
Business continuity	SM4.5 Business continuity	CB2.5 Business continuity	CI6.1 Contingency plan CI6.2 Contingency arrangements CI6.3 Validation and maintenance	NW3.6 Service continuity	
Change management		CB2.3 Change management	CI3.3 Change management	NW3.2 Change management	
Confidentiality requirements		CB1.1 Confidentiality requirements			SD3.2 Confidentiality requirements
Configuring network devices				NW2.1 Configuring network devices	
Cryptography	SM6.1 Use of cryptography	CB6.2 Cryptographic key management			
Development methodologies and environment					SD1.2 Development methodology SD1.4 Development environments
E-mail	SM6.3 E-mail				
Electronic commerce	SM6.6 Electronic commerce				

Topic	SM	CB	CI	NW	SD
Emergency fixes			CI3.5 Emergency fixes		
Event logging			CI2.2 Event logging		
External access/ connections		CB4.3 External connections		NW2.3 External access	
Firewalls				NW2.2 Firewalls	
Forensic investigations	SM5.5 Forensic investigations				
General security controls					SD4.3 General security controls
Handling information		CB2.6 Sensitive information	CI3.1 Handling computer media		
Hazard protection			CI2.6 Hazard protection		
Host system configuration			CI2.3 Host system configuration		
Incident management	SM5.4 Emergency response	CB2.4 Incident management	CI3.4 Incident management	NW3.3 Incident management	
Information privacy	SM4.2 Information privacy				
Information security function	SM2.2 Information security function				
Installation and network design			CI2.1 Installation design	NW1.2 Network design	
Instant Messaging	SM 6.8 Instant Messaging				
Installation process					SD6.2 Installation process
Integrity requirements		CB1.2 Integrity requirements			SD3.3 Integrity requirements
Intrusion detection	SM5.3 Intrusion detection				

Topic	SM	CB	CI	NW	SD
Local security co-ordination	SM2.3 Local security co-ordination	CB5.1 Local security co-ordination	CI5.1 Local security co-ordination	NW4.1 Local security co-ordination	SD2.1 Local security co-ordination
Management commitment	SM1.1 Management commitment SM2.1 High-level control				
Malicious mobile code protection	SM5.2 Malicious mobile code protection				
Network documentation				NW1.4 Network documentation NW5.1 Voice network documentation	
Outsourcing	SM6.7 Outsourcing				
Patch Management	SM 5.6 Patch management		CI3.6 Patch management		
Physical protection	SM4.4 Physical protection		CI2.8 Physical access	NW3.4 Physical security	
Post-implementation review					SD6.3 Post-implementation review
Power supplies			CI2.7 Power supplies		
Public key infrastructure	SM6.2 Public key infrastructure	CB6.3 Public key infrastructure			
Quality assurance					SD1.3 Quality assurance
Remote maintenance				NW3.7 Remote maintenance	
Remote working	SM6.4 Remote working				
Resilience		CB4.2 Resilience	CI2.5 Resilience	NW1.3 Network resilience NW5.2 Resilience of voice networks	
Risk analysis/assessment	SM3.3 Information risk analysis	CB5.3 Information risk analysis	CI5.4 Information risk analysis	NW4.4 Information risk analysis	SD3.5 Information risk assessment
Roles and responsibilities	SM3.2 Ownership	CB2.1 Roles and responsibilities	CI1.1 Roles and responsibilities	NW1.1 Roles and responsibilities	SD1.1 Roles and responsibilities

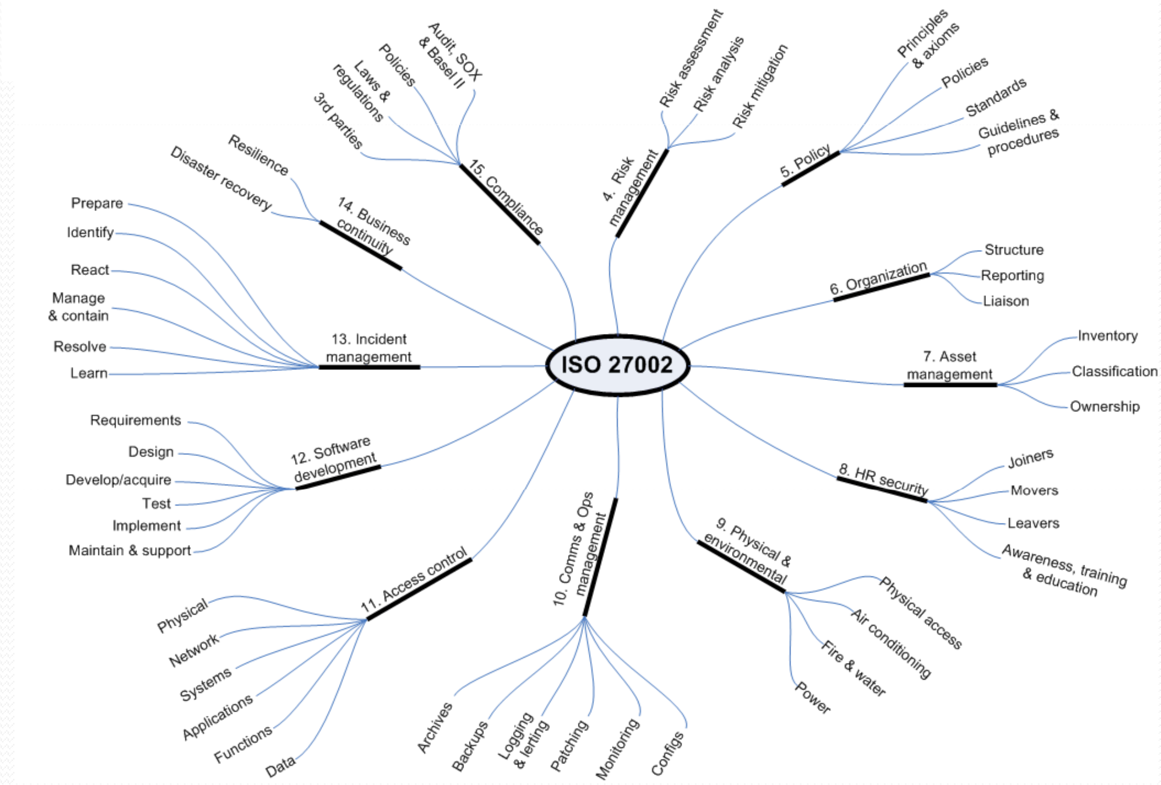


Topic	SM	CB	CI	NW	SD
Security architecture	SM4.1 Security architecture				
Security audit/review	SM7.1 Security audit/review	CB5.4 Security audit/review	CI5.5 Security audit/review	NW4.5 Security audit/review	SD2.3 Security audit/review
Security awareness	SM2.4 Security awareness	CB3.4 Security awareness	CI5.2 Security awareness	NW4.2 Security awareness	SD2.2 Security awareness
Security classification	SM3.1 Security classification	CB5.2 Security classification	CI5.3 Security classification	NW4.3 Security classification	
Security education	SM2.5 Security education				
Security monitoring	SM7.2 Security monitoring				
Security policy	SM1.2 Security policy				
Service providers		CB4.1 Service agreements	CI1.2 Service agreements	NW1.5 Service providers	
Sign-on process		CB3.2 Application sign-on process	CI4.4 Sign-on process		
Special controls				NW5.3 Special voice network controls	
Specifications of requirements					SD3.1 Specification of requirements
Staff agreements	SM1.3 Staff agreements				
System design/build					SD4.1 System design SD4.5 System build
System network monitoring			CI1.4 System monitoring	NW3.1 Network monitoring	
System promotion criteria					SD6.1 System promotion criteria
Testing					SD5.1 Testing process SD5.2 Acceptance testing
Third party access	SM6.5 Third party access	CB6.1 Third party agreements			



Topic	SM	CB	CI	NW	SD
User authentication			CI4.5 User authentication		
User authorisation			CI4.2 User authorisation		
Virus protection	SM5.1 Virus protection				
Web-enabled applications		CB6.4 Web-enabled applications			SD4.6 Web-enabled development
Wireless access				NW2.4 Wireless access	
Workstation configuration		CB3.3 Workstation configuration	CI2.4 Workstation configuration		

ISO27002: Security Standard - Scope



ISO 27002

- 4. Risk management
  - Risk assessment
  - Risk analysis
  - Risk mitigation
- 5. Policy
  - Principles & axioms
  - Policies
  - Standards
  - Guidelines & procedures
- 6. Organization
  - Structure
  - Reporting
  - Liaison
- 7. Asset management
  - Inventory
  - Classification
  - Ownership
- 8. HR security
  - Joiners
  - Movers
  - Leavers
  - Awareness, training & education
- 9. Physical & environmental
  - Physical access
  - Air conditioning
  - Fire & water
  - Power
- 10. Comms & Ops management
  - Archives
  - Backups
  - Logging & lerting
  - Patching
  - Monitoring
  - Configs
- 11. Access control
  - Physical
  - Network
  - Systems
  - Applications
  - Functions
  - Data
- 12. Software development
  - Requirements
  - Design
  - Develop/acquire
  - Test
  - Implement
  - Maintain & support
- 13. Incident management
  - Prepare
  - Identify
  - React
  - Manage & contain
  - Resolve
  - Learn
- 14. Business continuity
  - Resilience
  - Disaster recovery
- 15. Compliance
  - Audit, SOX & Basel II
  - Policies
  - Laws & regulations
  - 3rd parties

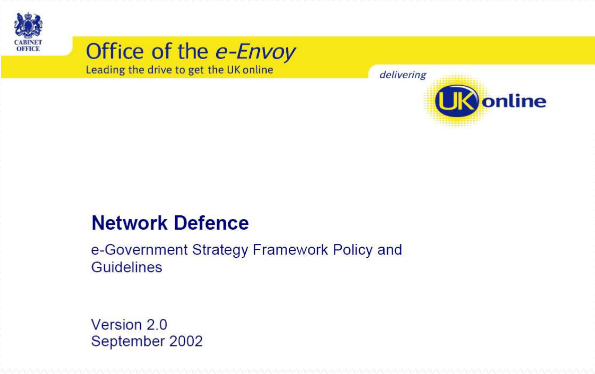
EU Country Model Review

❖UK Developed e-Government Security Architecture, Data Interchange Format as well as framework for disaster recovery and management – 2002

❖German Government published detailed IT Security Guidelines – 2004

❖Also worthwhile researching other EU National Government Security Frameworks as input for Republic of Armenia – Government Security Policy

E-Government – UK Security Model



Office of the *e-Envoy*

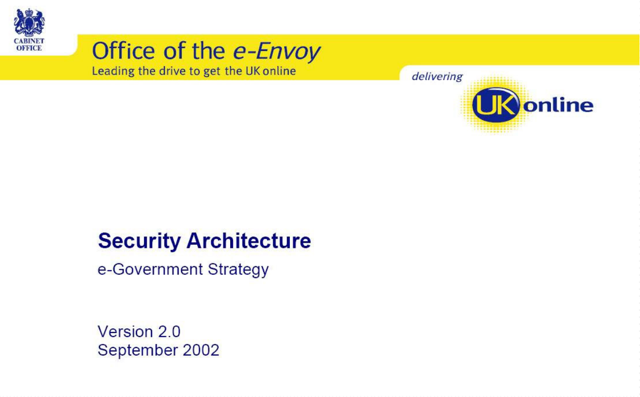
Leading the drive to get the UK online

delivering UK online

Network Defence

e-Government Strategy Framework Policy and Guidelines

Version 2.0
September 2002



Office of the *e-Envoy*

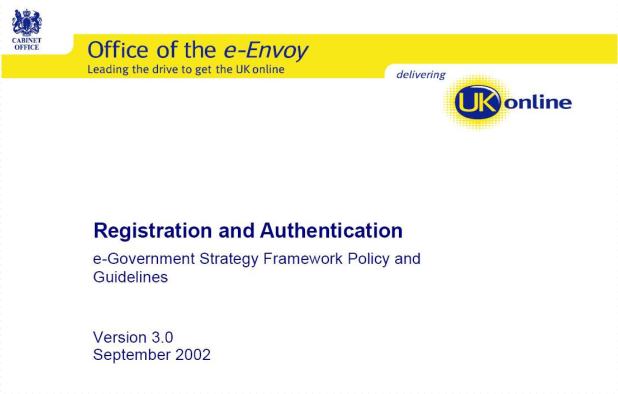
Leading the drive to get the UK online

delivering UK online

Security Architecture

e-Government Strategy

Version 2.0
September 2002



Office of the *e-Envoy*

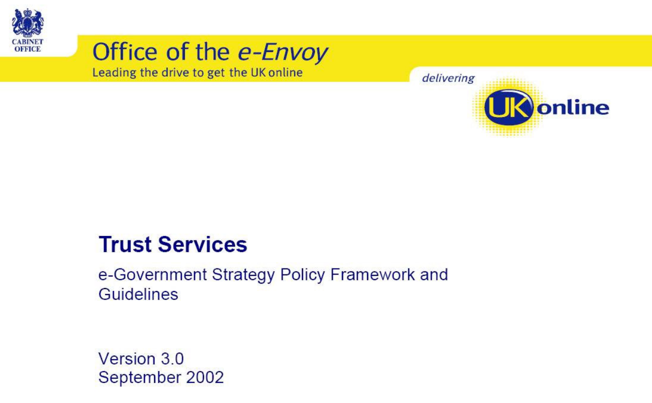
Leading the drive to get the UK online

delivering UK online

Registration and Authentication

e-Government Strategy Framework Policy and Guidelines

Version 3.0
September 2002



Office of the *e-Envoy*

Leading the drive to get the UK online

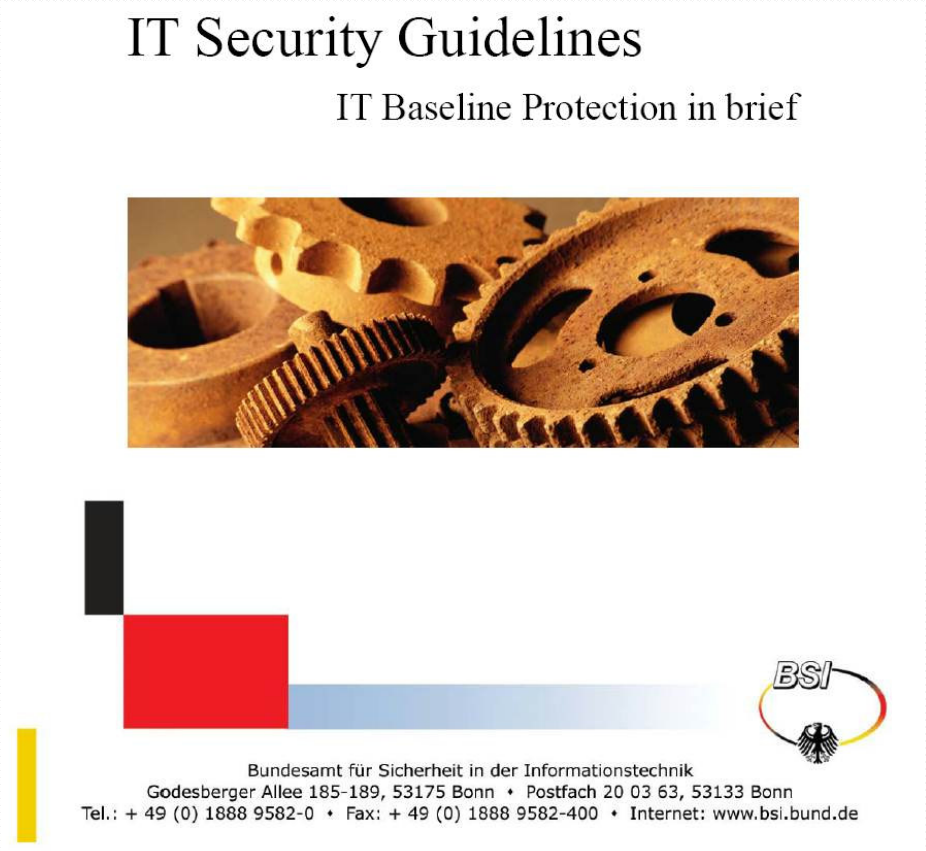
delivering UK online

Trust Services

e-Government Strategy Policy Framework and Guidelines

Version 3.0
September 2002

German Government Guidelines



IT Security Guidelines

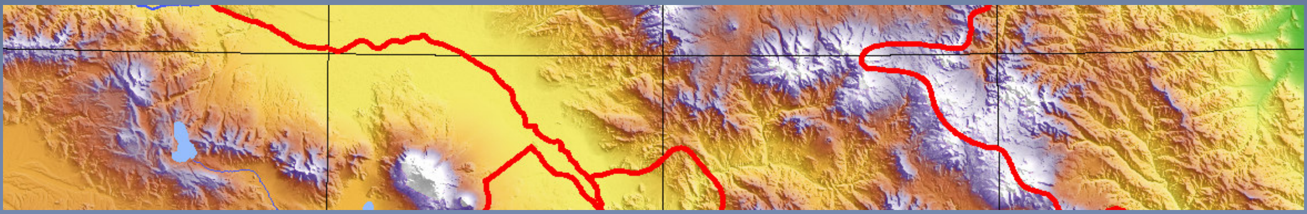
IT Baseline Protection in brief

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

Short Term Programme…

…Next 12 Months – Up to 2010 - eGovernment

- Establish Armenian eGovernment On-Line Services Team
- Review & Audit Government Applications & Net Security
- Recommend & Prioritise Top Applications for eGovernment
- Upgrade Security Software & Systems to ISO Standards
- Appoint PPP Team to Plan & Specify "Real-Time Armenia"
- Consider Proposal to Engineer the "Electronic DiasporaNet"

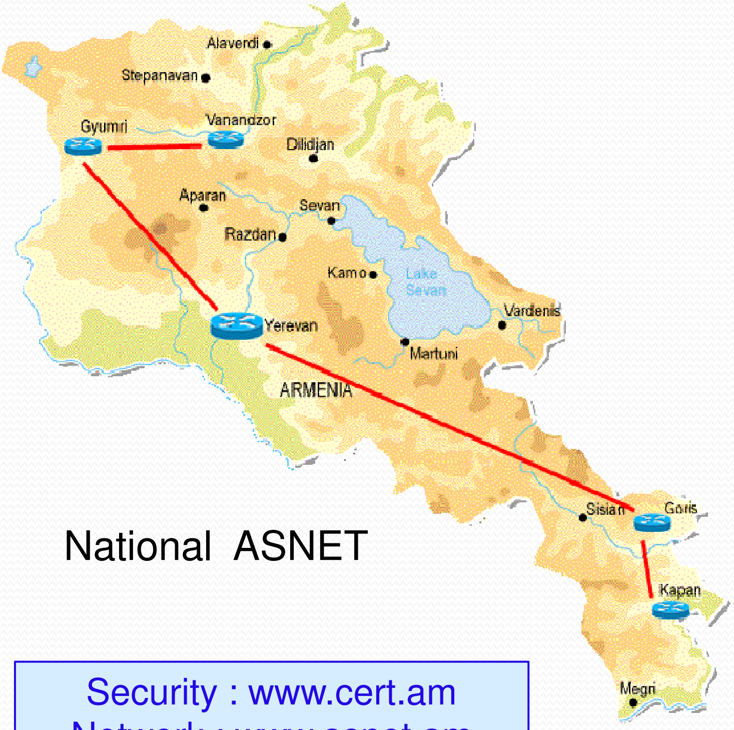


Medium Term Programme…

…3 Years – Up to 2012 – "Real-Time Armenia"

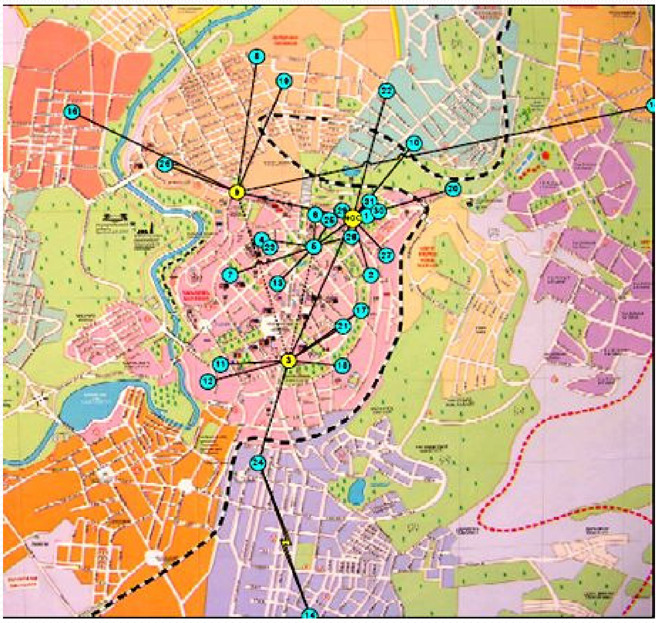
- Data Centre Storage, Virtualisation & Remote Back-Up
- Security for the Regional and Local Government Offices
- Professional Security Training with Government Certification
- Develop in-depth BCP and Disaster Recovery Programmes
- Implement Deep-Packet Inspection as early alert for DDOS
- Launch fully secure e-Business Ventures in target sectors
- Consider ASNET.am – Armenian Research & Academic Network
    - An excellent reference point & foundation for eArmenia & eDiasporaNet
    - Already includes a Computer Emergency Response Team - CERT.am

Academic Science Networks of ARMENIA



National ASNET

Security : www.cert.am
Network : www.asnet.am

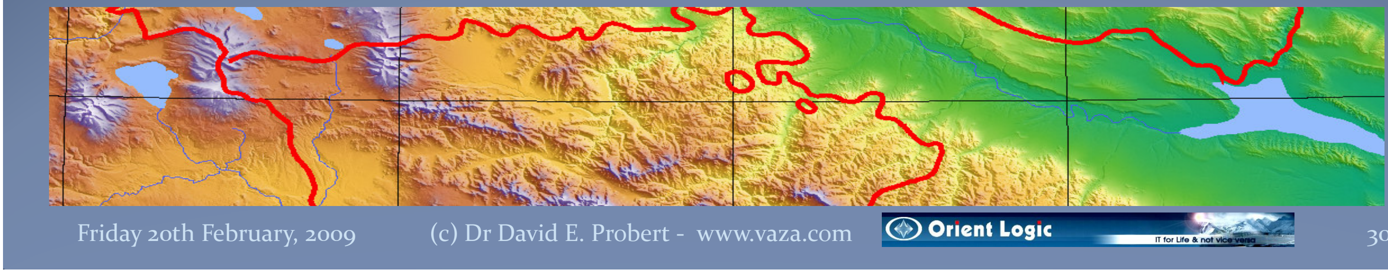


Yerevan University Network

Longer Term Programme…

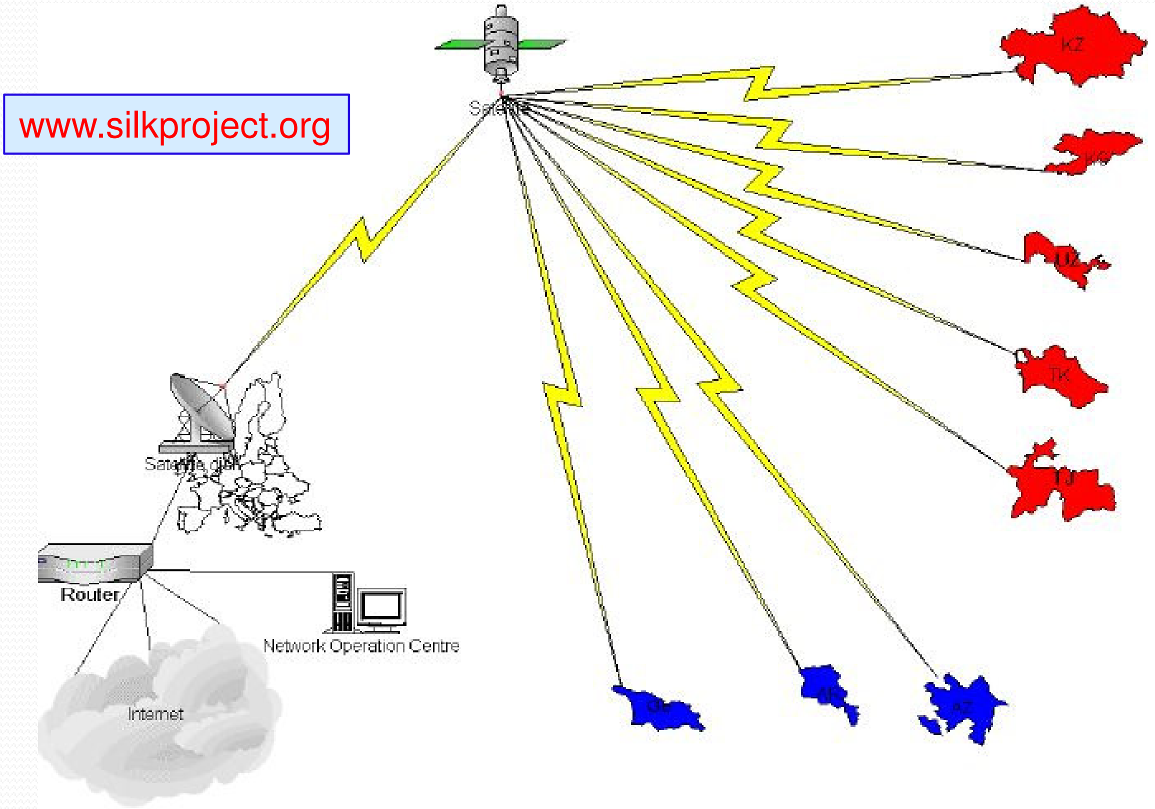
…5 Years – Up to 2014 – "Electronic DiasporaNet"

- ❖ Real-Time 24/7 Global Armenian eTrading Network – "eDN"
- ❖Networked CCTV and Electronic IP Security Integration
- ❖Biometric ID Resource Access and RFID Asset Management
- ❖ Security of End-User Devices and New Software Applications
- ❖ Integration of "eDN" with Trans-Euro eGovernment Framework-EIF
- ❖"Real-Time Armenia" as fully secure International e-Trading Hub
- ❖ The NATO sponsored satellite based Virtual Silk Highway Project is an excellent regional reference project – SilkProject.org

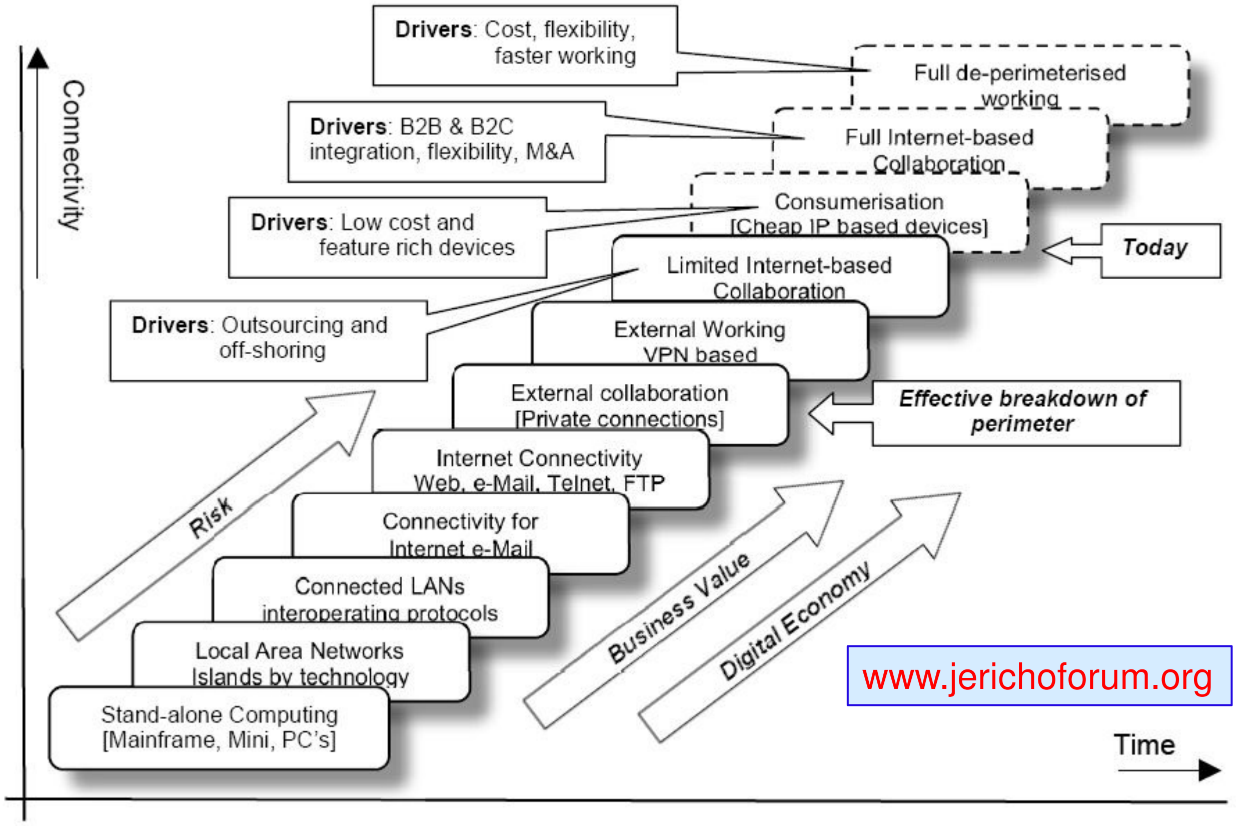


NATO : Virtual Silk Highway Project

www.silkproject.org



New Security for 21stC Networks


Connectivity

Drivers: Cost, flexibility, faster working

Full de-perimeterised working

Drivers: B2B & B2C integration, flexibility, M&A

Full Internet-based Collaboration

Drivers: Low cost and feature rich devices

Consumerisation [Cheap IP based devices]

Today

Limited Internet-based Collaboration

Drivers: Outsourcing and off-shoring

External Working VPN based

External collaboration [Private connections]

Effective breakdown of perimeter

Internet Connectivity Web, e-Mail, Telnet, FTP

Connectivity for Internet e-Mail

Connected LANs interoperating protocols

Local Area Networks Islands by technology

Stand-alone Computing [Mainframe, Mini, PC's]

Risk

Business Value

Digital Economy

www.jerichoforum.org

Time

Biometric Security Solutions

- Latest Biometric Technologies include : Finger Print, Palm Print, Vein ID, Iris Scan, 3D Facial Recognition
- Personal ID Documents – Passports, Driving Licences
- Applications for Border Protection, Offices, Hospitals, Prisons, Transportation, Banks, IT Mobile Devices
- Easily integrated using the ISO BioAPI Specification, and IP networked as total physical security solution
- Extremely portable and robust security solution in difficult environmental locations – quickly installed

Next Practical Steps…

…6 Months - Jan 2009 to June 2009

- Appoint a full-time joint team of Government & Enterprise ICT Professionals – Experts in eSecurity and On-Line Info Services
- Undertake an survey of current Government & Financial Services, and in-depth audit of the current levels of on-line ICT Security
- Define priority for eGovernment – Taxation, Licences, Customs…
- Develop detailed engineering plans & specifications for:
  - Phase 1 - eGovernment – Now! - Secure On-Line Interactive Info Services
  - Phase 2 - Real-Time Armenia – 3 Year Plan – National eCommerce/eTrade
  - Phase 3 - Electronic DiasporaNet – 5 Year Plan - Worldwide eTrading Net

…Engineering Economic Growth through Secure On-Line Trading!

eARMENIA & eDiasporaNet

- Mission Critical Programme for the 21stC Armenian Economy
- In-Depth Real-Time Armenian Security Project required to protect eGovernment and eEnterprises against future Cyber Attacks
- From the *"Physical Eagle - 20thC"* to *"Electronic Lion - 21stC"*
- Initiate *"Electronic DiasporaNet"* to grow global Armenian Trade!

eGovernment

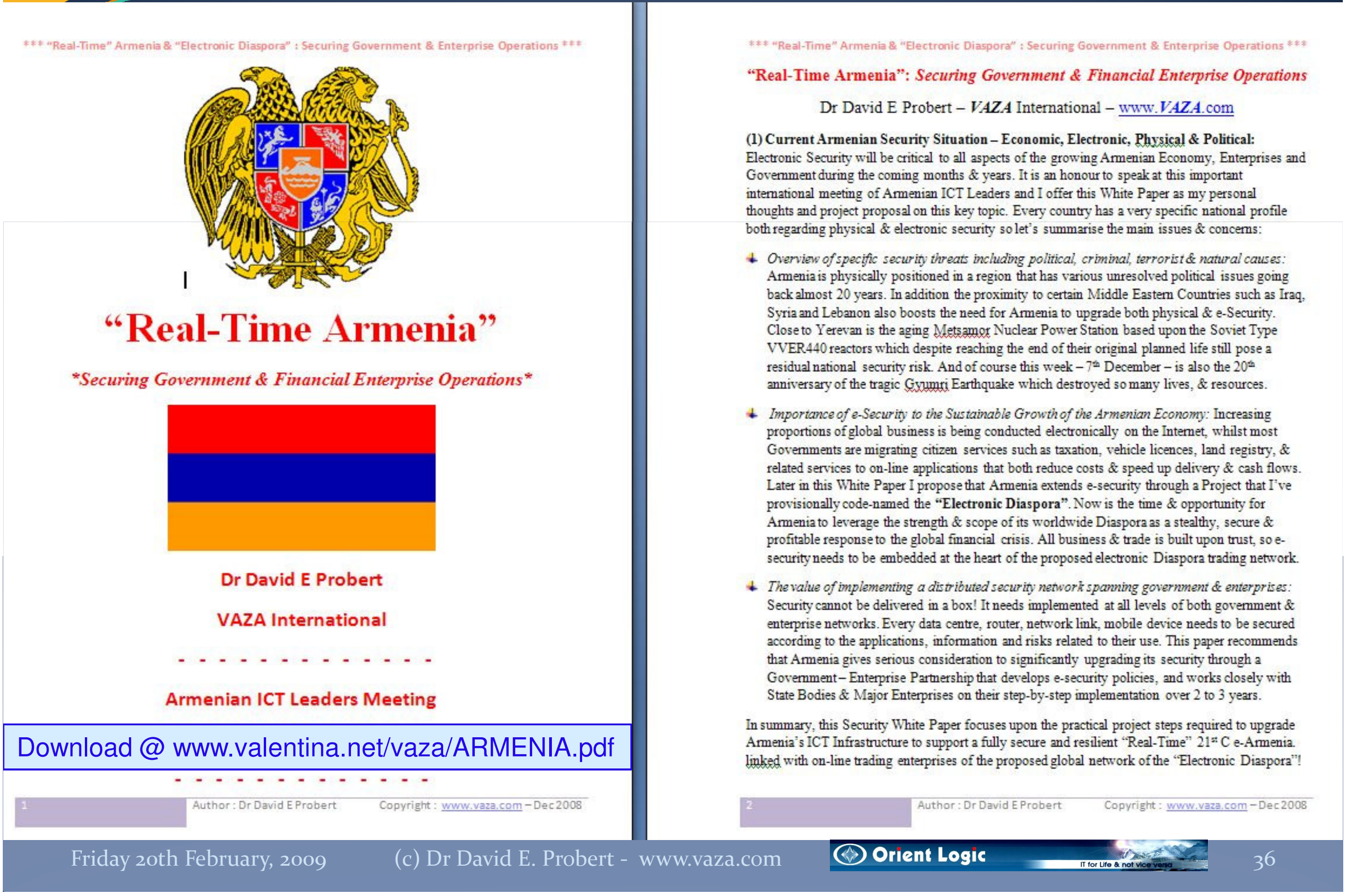
eArmenia

eDiasporaNet

21stC

Download "White Paper" – "Real-Time ARMENIA" @ www.valentina.net/vaza/ARMENIA.pdf

Real-Time Armenia : "White Paper"



*** "Real-Time" Armenia & "Electronic Diaspora" : Securing Government & Enterprise Operations ***

"Real-Time Armenia"

Securing Government & Financial Enterprise Operations

Dr David E Probert

VAZA International

- - - - - - - - - - - - - -

Armenian ICT Leaders Meeting

Download @ www.valentina.net/vaza/ARMENIA.pdf

- - - - - - - - - - - - - -

1 Author : Dr David E Probert Copyright : www.vaza.com – Dec 2008

*** "Real-Time" Armenia & "Electronic Diaspora" : Securing Government & Enterprise Operations ***

"Real-Time Armenia": *Securing Government & Financial Enterprise Operations*

Dr David E Probert – ***VAZA*** International – www.*VAZA*.com

(1) Current Armenian Security Situation – Economic, Electronic, Physical & Political:
Electronic Security will be critical to all aspects of the growing Armenian Economy, Enterprises and Government during the coming months & years. It is an honour to speak at this important international meeting of Armenian ICT Leaders and I offer this White Paper as my personal thoughts and project proposal on this key topic. Every country has a very specific national profile both regarding physical & electronic security so let's summarise the main issues & concerns:

- *Overview of specific security threats including political, criminal, terrorist & natural causes:* Armenia is physically positioned in a region that has various unresolved political issues going back almost 20 years. In addition the proximity to certain Middle Eastern Countries such as Iraq, Syria and Lebanon also boosts the need for Armenia to upgrade both physical & e-Security. Close to Yerevan is the aging Metsamor Nuclear Power Station based upon the Soviet Type VVER440 reactors which despite reaching the end of their original planned life still pose a residual national security risk. And of course this week – 7th December – is also the 20th anniversary of the tragic Gyumri Earthquake which destroyed so many lives, & resources.
- *Importance of e-Security to the Sustainable Growth of the Armenian Economy:* Increasing proportions of global business is being conducted electronically on the Internet, whilst most Governments are migrating citizen services such as taxation, vehicle licences, land registry, & related services to on-line applications that both reduce costs & speed up delivery & cash flows. Later in this White Paper I propose that Armenia extends e-security through a Project that I've provisionally code-named the **"Electronic Diaspora"**. Now is the time & opportunity for Armenia to leverage the strength & scope of its worldwide Diaspora as a stealthy, secure & profitable response to the global financial crisis. All business & trade is built upon trust, so e-security needs to be embedded at the heart of the proposed electronic Diaspora trading network.
- *The value of implementing a distributed security network spanning government & enterprises:* Security cannot be delivered in a box! It needs implemented at all levels of both government & enterprise networks. Every data centre, router, network link, mobile device needs to be secured according to the applications, information and risks related to their use. This paper recommends that Armenia gives serious consideration to significantly upgrading its security through a Government – Enterprise Partnership that develops e-security policies, and works closely with State Bodies & Major Enterprises on their step-by-step implementation over 2 to 3 years.

In summary, this Security White Paper focuses upon the practical project steps required to upgrade Armenia's ICT Infrastructure to support a fully secure and resilient "Real-Time" 21st C e-Armenia linked with on-line trading enterprises of the proposed global network of the "Electronic Diaspora"!

2 Author : Dr David E Probert Copyright : www.vaza.com – Dec 2008

Security References

- ISO/IEC – 27001/27002 Guidelines www.iso.org - 2005
- ISF - Information Security Forum: Security Guidelines – 2007
- OECD Security Guidelines for Information Systems & Networks
- US Congress – Security in the Information Age - 2002
- UK Government – Security Architecture - Version4.0
- German Government – IT Security Guidelines - 2004
- EIF – European Interoperability Framework – 2004
- ASIS International Guidelines for BCP/DPR - 2005

Profile – Dr David E Probert

- ***Computer Integrated Telephony (CIT)*** – Established and led British Telecom's £25M EIGER Project during the mid-1980s' to integrate computers with telephone switches (PABX's). This resulted in the successful development and launch of CIT software applications for telesales & telemarketing operations in a worldwide marketplace.

- ***Blueprint for Business Communities*** – Visionary Programme for Digital Equipment Corporation during late-1980's that included the creation of the "knowledge lens" and "community networks". The Blueprint provided the strategic framework for Digital's Value-Added Networks Business that secured significant contracts for enterprise networks.

- ***European Internet Business Group (EIBG)*** – Established and led Digital Equipment Corporation's European Internet Group for 5 years, from 1994 to 1999. Projects included support for the national Internet infrastructure for countries across EMEA as well as major enterprise, government & educational Intranet deployments. Dr David Probert was a sponsoring member of the European Board for Academic & Research Networking (EARN/TERENA) for 7 years (1991 ➔1998)

- ***Supersonic Car (ThrustSSC)*** – Worked with Richard Noble OBE, and the Mach One Club to set up and manage the 1st Multi-Media and e-Commerce Web-Site for the World's 1st Supersonic Car – ThrustSSC – for the World Speed Record.

- ***Secure Wireless Networking*** – Business Director & VP for Madge Networks to establish a portfolio of innovative fully secure wireless Wi-Fi IEEE802.11 networking products with technology partners from both UK and Taiwan.

- ***Networked Enterprise Security*** - Appointed as the New Products Director (CTO) to the Management Team of the Blick Group plc with overall responsibility for 55 professional engineers & a diverse portfolio of hi-tech security products.

- ***Republic of Georgia*** – Senior Security Adviser – Appointed by the European Union to investigate and then to make recommendations on *all* aspects of IT security, physical security and BCP/DR relating to the Georgian Parliament.

- *Dr David E. Probert is a Fellow of the Royal Statistical Society. He has a 1st Class Honours Degree in Mathematics (Bristol University) & PhD from Cambridge University in Self-Organising Systems (Evolution of Stochastic Automata) , and his full professional biography is featured in the Marquis International Directory of Who's Who in the World – 2007 / 2009 Editions.*