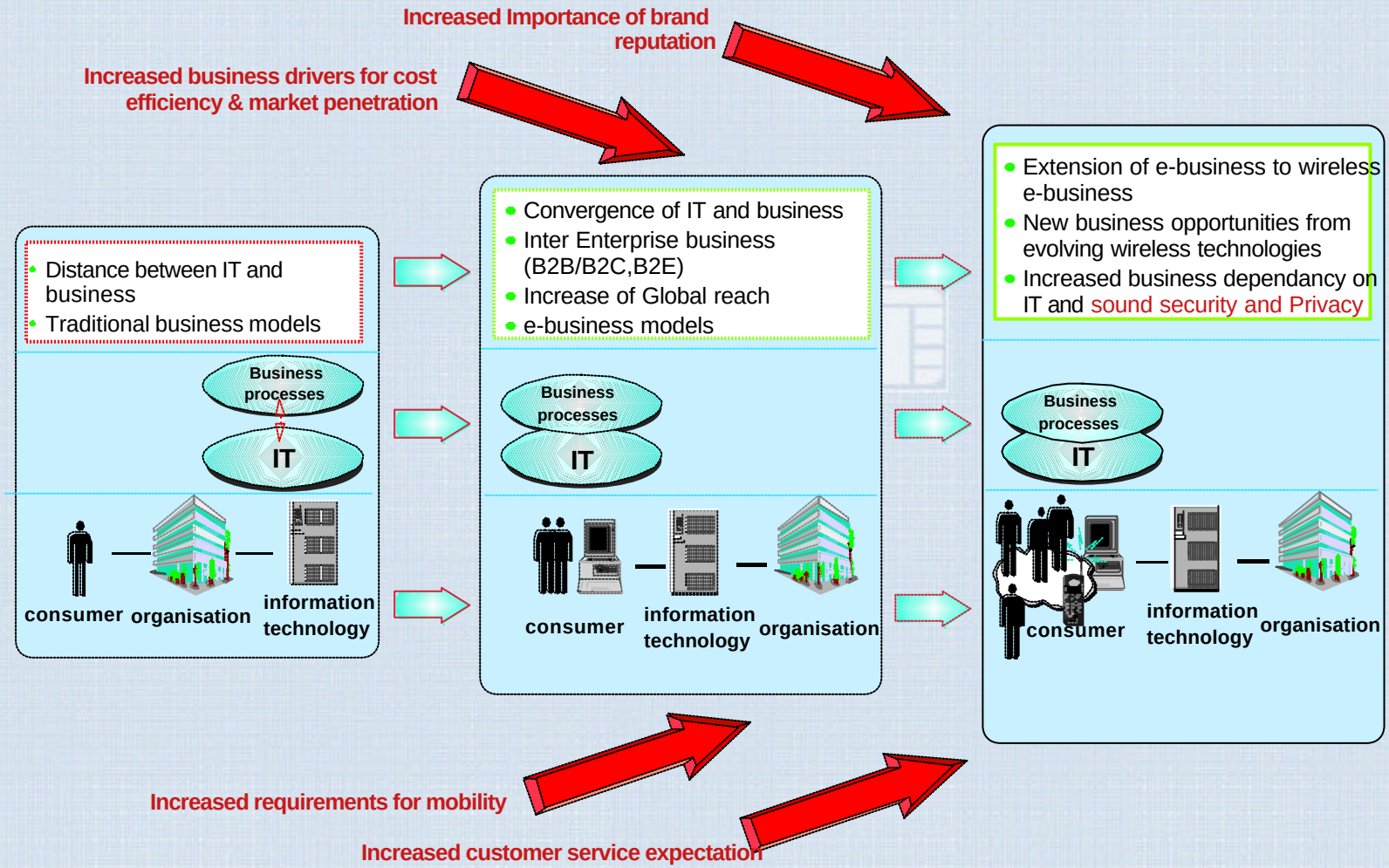
Wireless e-business Security

Lothar Vigelandzoon

E-business evolution



End to End Security Service Offerings

Assessment

- Health Check
- Assessments:
  - Site
  - Process
  - System
  - Network
  - Internet
  - Application
  - Privacy
  - Wireless
- Ethical Hacking
- e-risk

Planning

- Workshops
  - Security
  - Privacy
  - PKI
  - Wireless
- Info Asset Profile
- Privacy Strategy and Implementation
- PKI Planning and Design
- Wireless Planning and Design
- Privacy Planning and Design

Design

- Policy Definition
- Standards Definition
- Process Dev't
- Enterprise Arch
- Internet Arch
- Secure Solution
- Design
- VPNs
- Wireless
- Metadirectories

Build

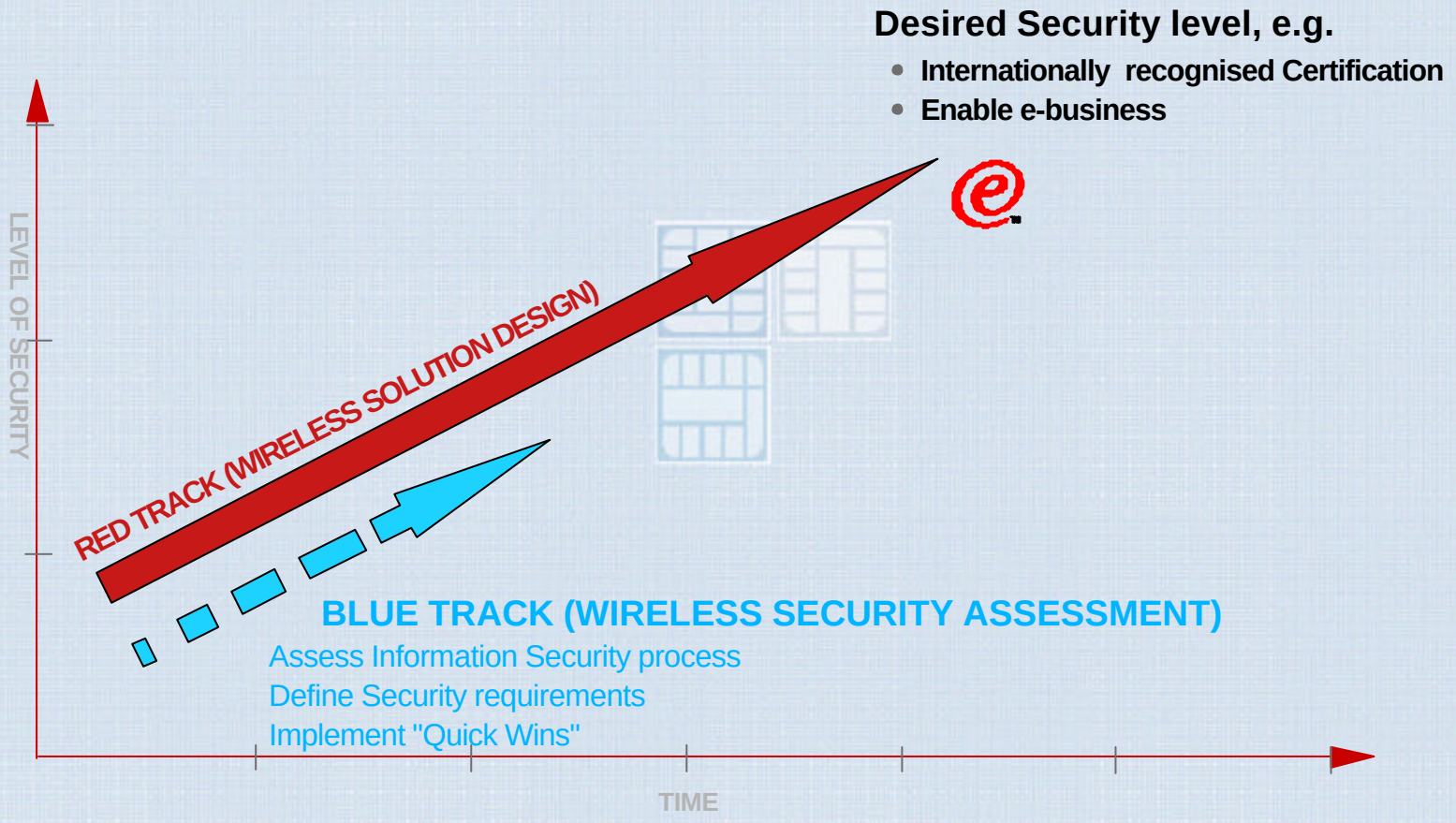
- Product Selection
- Product Implem.
  - Firewalls
  - Tivoli PKI
  - Policy Director
  - Entrust
  - Baltimore
- *Other Product Implementation*
- Single Signon
- Risk Manager
- Identrus Reference Implementation Quick Start and testing

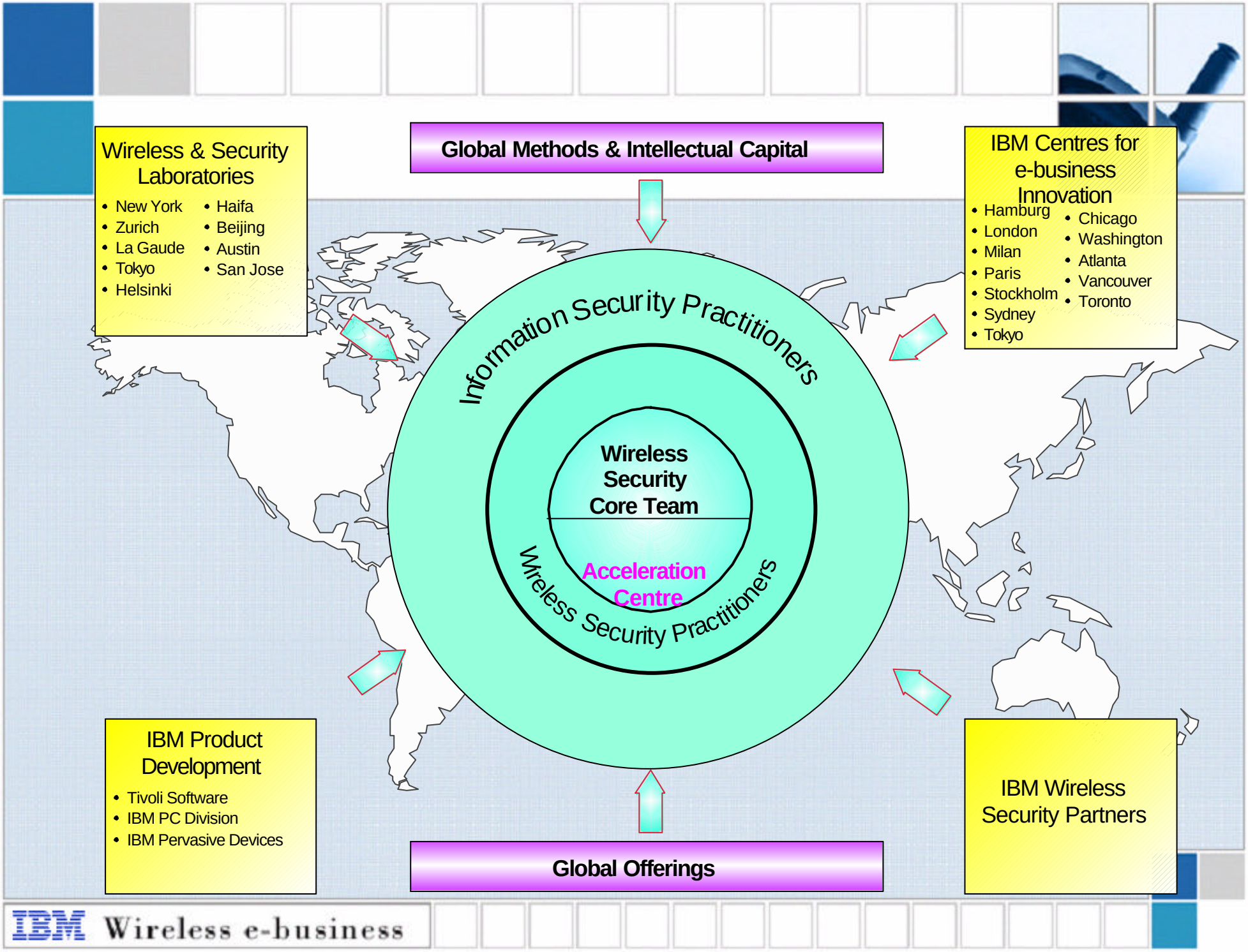
Management

Managed Security Services

- Intrusion Detection
- Vulnerability Scanning
- Firewall Management
- Incident Management
- Security Management Standards/Controls
- Physical & Logical Security
- Compliance Checking
- Security Integrity and Advisories
- Virus Services
- Network Security
- Risk/Issue Mgmt
- Security Education

In order to expedite implementation, security can be approached using tactical and strategic solutions.
IBM's services are aligned to this approach



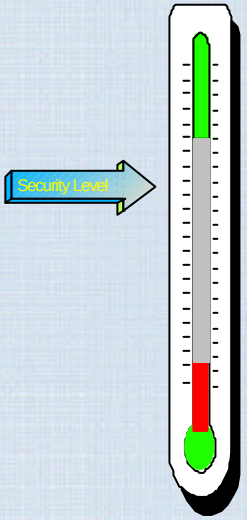

Wireless & Security Laboratories
• New York
• Zurich
• La Gaude
• Tokyo
• Helsinki
• Haifa
• Beijing
• Austin
• San Jose
Global Methods & Intellectual Capital
IBM Centres for e-business Innovation
• Hamburg
• London
• Milan
• Paris
• Stockholm
• Sydney
• Tokyo
• Chicago
• Washington
• Atlanta
• Vancouver
• Toronto
Information Security Practitioners
Wireless Security Practitioners
Wireless Security Core Team
Acceleration Centre
IBM Product Development
• Tivoli Software
• IBM PC Division
• IBM Pervasive Devices
IBM Wireless Security Partners
Global Offerings

What does security mean to me?

... Security is to a business, what oxygen is to a human being...

Too little oxygen
Too much oxygen

Right level of oxygen



Wireless e-business Security

Challenges and enablers

Daniel Keely

Wireless e-business is much more than the addition of wireless transport networks and introduces new security requirements

Wireless Applications

- Wireless transactions
- Wireless lifestyle factilitors
- Wireless messaging

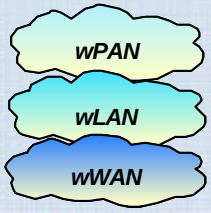
Pervasive Devices

Wireless Protocols

WAP, WTLS, SMS

Channels to wired e-business solutions and Intranets

Wireless Networks



New Wireless Technology = New Vulnerabilities = New Risks

It is difficult for an organisation to gain assurance of the confidentiality and integrity of its data as it passes over wireless data networks

wWAN/LAN/PAN

- Wireless Wide Area Networks
  - GSM/GPRS encryption weaknesses
  - RF jamming
  - Loss of data routing control
  - Pre-paid services are anonymous
- Wireless LANs and PANs
  - limited "out of the box" protection
  - weak 802.11 encryption
  - Will be implemented in public areas e.g. airports
  - Bluetooth users may not be aware of their devices being active and accessible
- WAP "gap" vulnerability

Wireless connected mobile devices are the new interfaces to e-business applications. However, their security capabilities are severely restricted

Mobile Devices

- Initial user access (PIN/Password) can be deactivated by the user
- Devices are easily lost or stolen (with data)
- Limited OTA backup and restore facilities
- Weak synchronisation access controls
- Targets for viruses
- Vulnerable to "bugs"
- Remote access configuration capabilities/undocumented APIs
- Vulnerable to denial of service attacks
- "Always-on" connectivity increases window of opportunity for hackers
- Lack of content filtering

Wireless e-business delivers new applications that introduce privacy concerns. In addition, Standards are not developing fast enough

Apps and Standards

- Immature standards
- Privacy concerns with location based services
- Increased user base and requirements for mobile access
- Usability issues

How will the security challenges evolve?

- Drivers
  - increased business dependancy on technology
  - business partnerships, alliances; M&As
  - increasing user base
  - rapidly developing technologies & complexity
- Security issues
  - recreational hacker -> hactivist -> organised crime -> industrial espionage
  - greater proliferation of viruses
  - increased tooling to exploit vulnerabilities
  - internal vs external threats
  - malicious intent vs accidental
  - skills shortages

The challenges can be addressed using security solutions. These solutions help enable Wireless e-business

Technology

Session cryptography/VPNs
File encryption
Content and virus filtering
Personal firewalls
User and device authentication
User authorisation
Wireless PKI
Intrusion detection
Security management

Architecture

Structured design method
Functional architecture
Operational architecture
End-to-end security design

Secure and resilient industry solutions

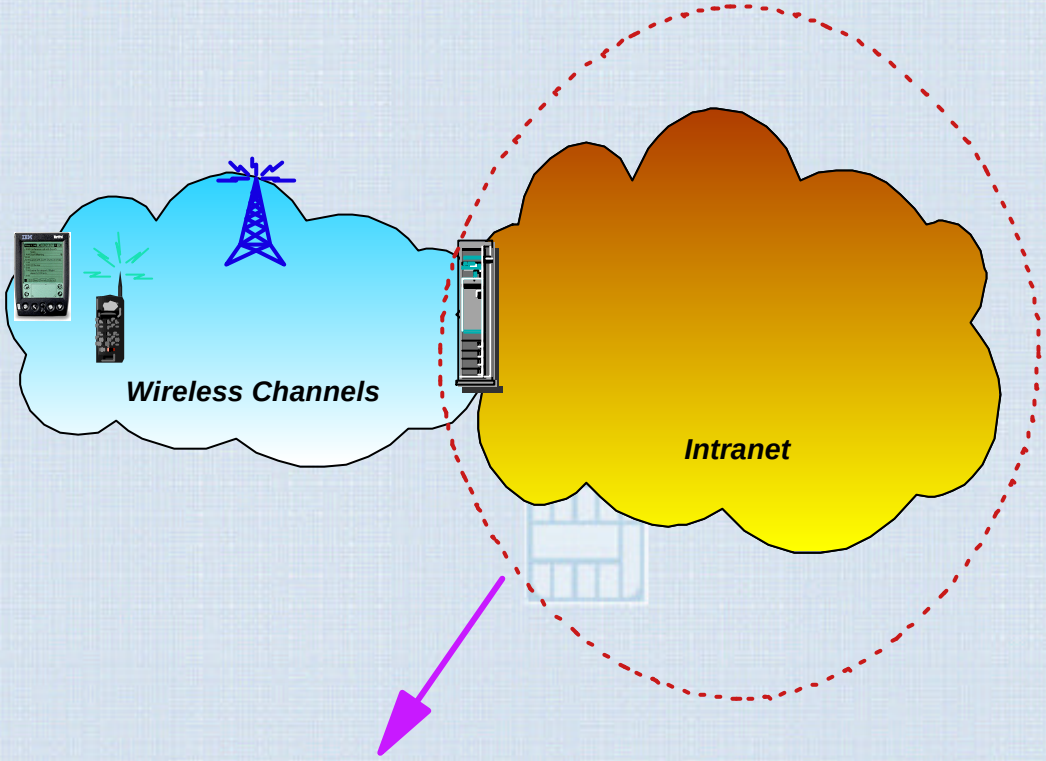
Processes

Risk management process
Incident management process
Change management process
Audit process
Security awareness program

Skills

Risk management expertise
IT security expertise
Architecture and design expertise
Industry knowledge

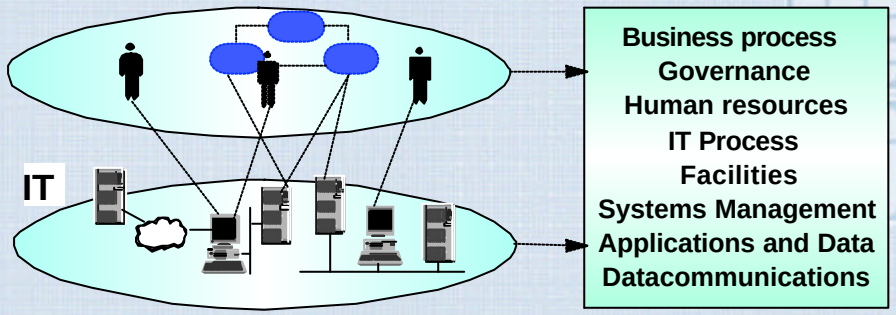
Existing "wired" security controls will be pushed to their limits and become increasingly important



- Policy management
- Intrusion detection
- Hardened platforms
- Security verification
- Secure device management
- Incident management
- Firewalls
- Content/E-mail filtering
- Anti-virus
- Identification & authentication
- Authorisation
- Security organisation

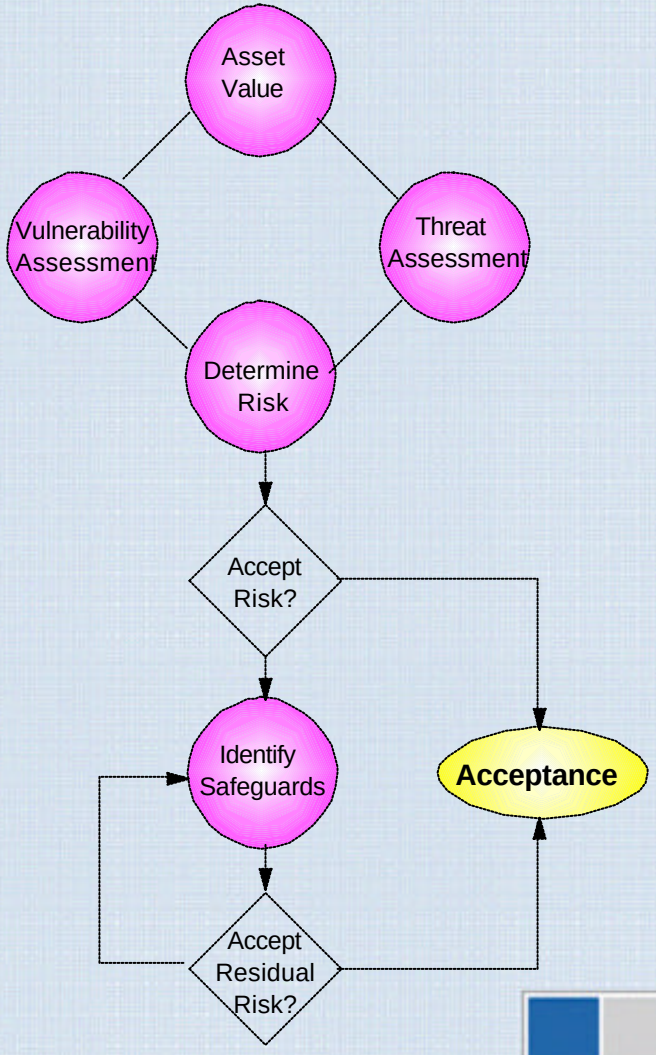
What is information risk management?

"Risk Management must be part of a continuous information security process"

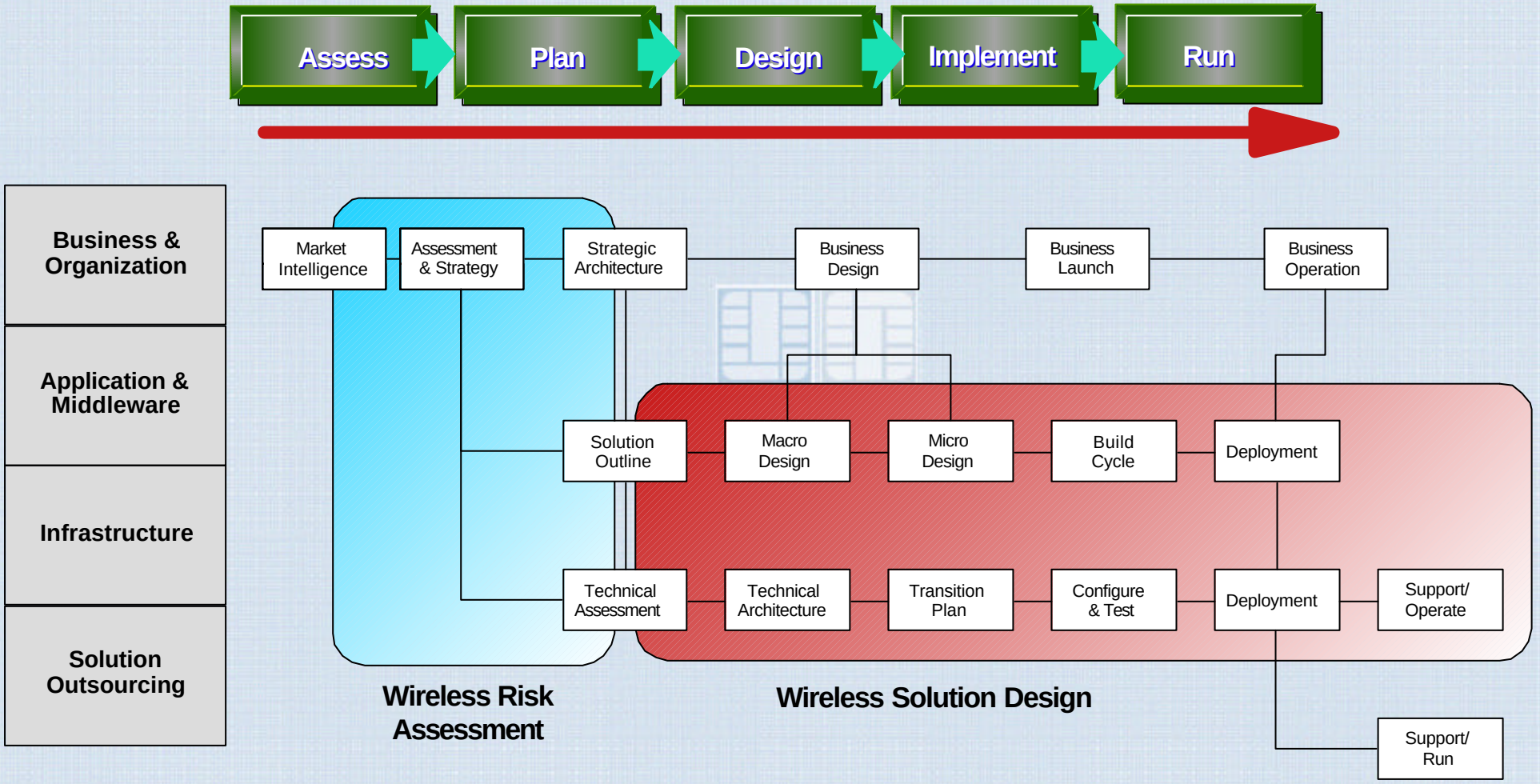


Scope

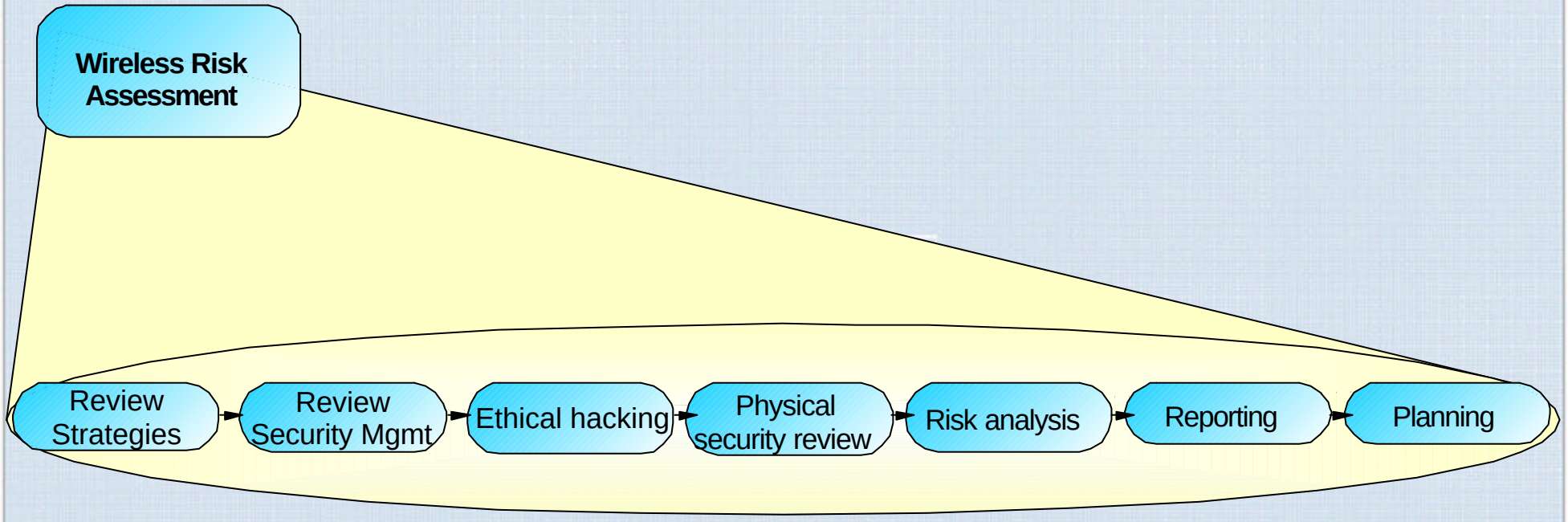
- Business process
- Governance
- Human resources
- IT Process
- Facilities
- Systems Management
- Applications and Data
- Datacommunications



New wireless security services have been announced. They are aligned with the IBM Global Services Method to enable consistent and comprehensive delivery worldwide

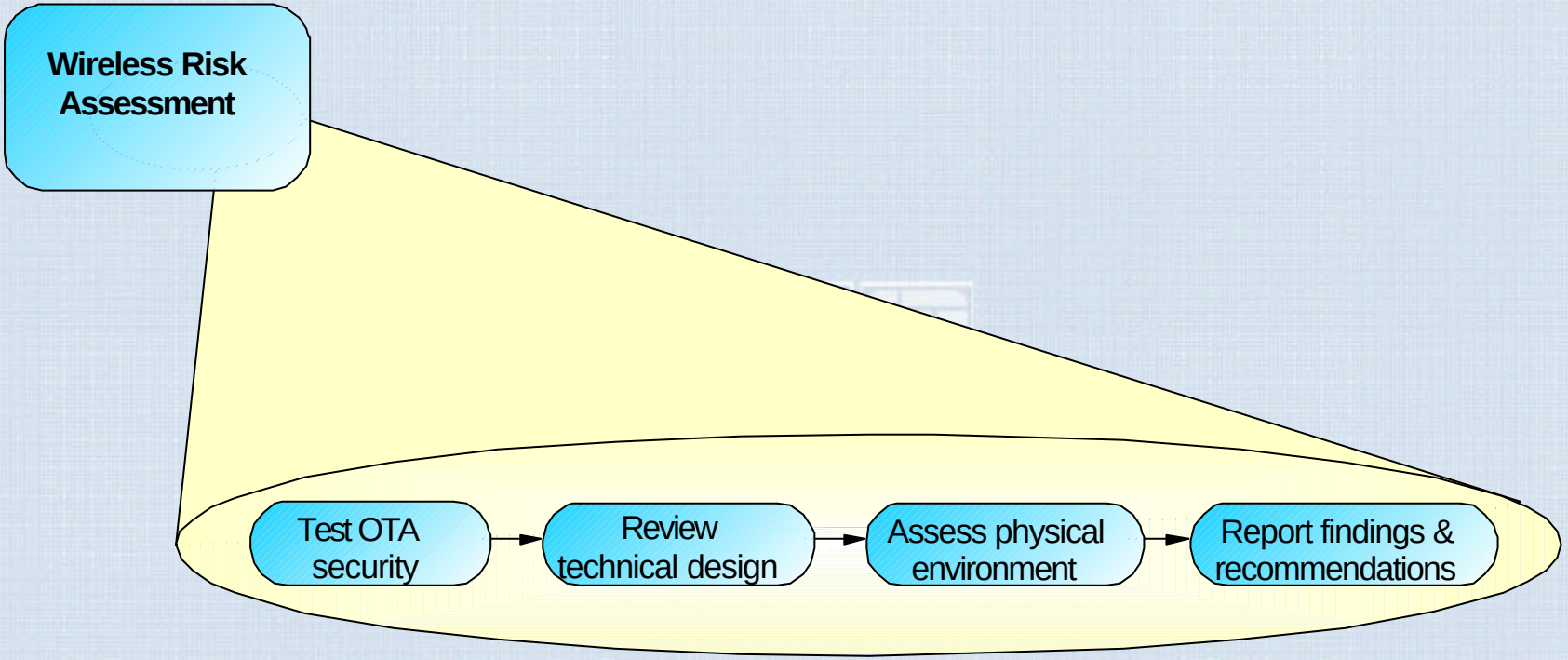


Our risk assessment services help identify and understand wireless e-business risks



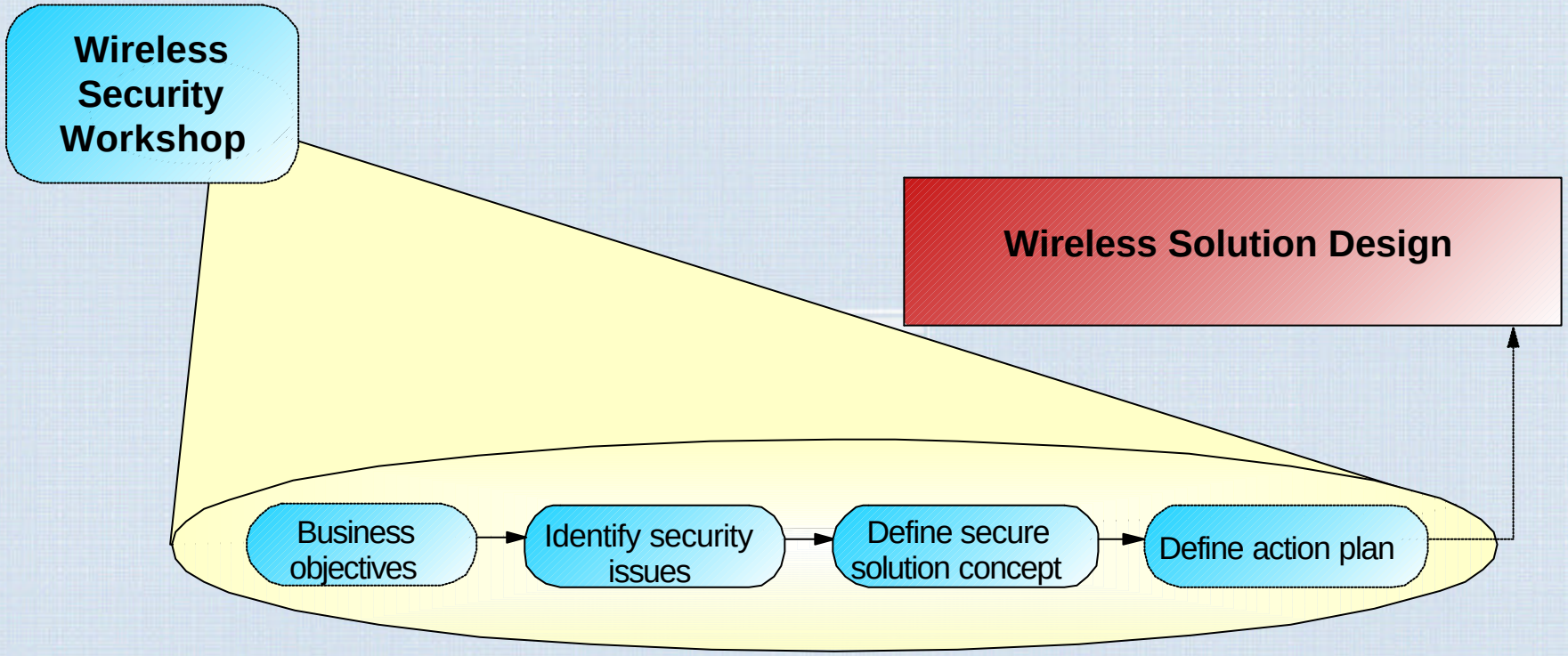
- Identify threats, vulnerabilities and risks introduced by wireless initiatives
- Assess the alignment of wireless technology to your business goals
- Report strengths, weaknesses and tactical and strategic recommendations
- Solution planning

To accomodate the demand for technical reviews of existing wLANs, a "fast track" wLAN security assessment can be delivered to determine current risks



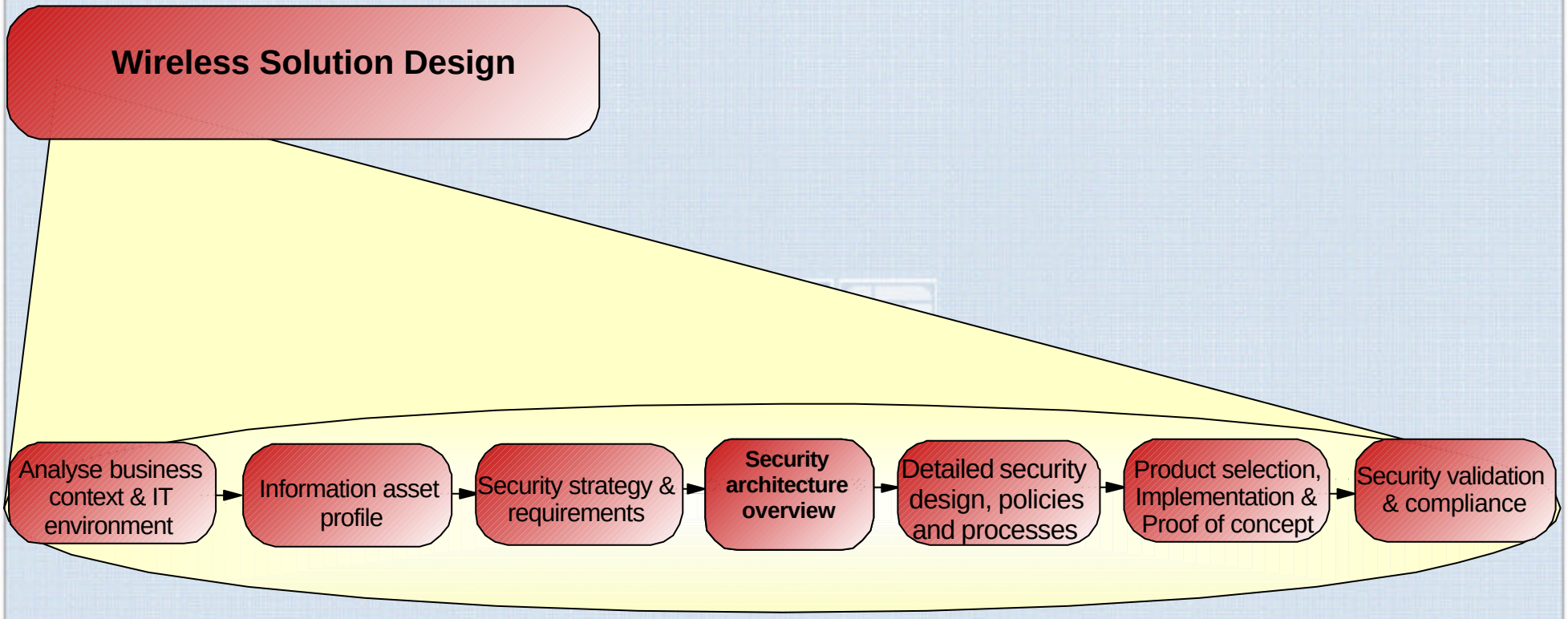
- Identify weaknesses in existing wireless LAN installations
- Provide recommendations for improvement

To enable a fast-start of new secure wireless e-business initiatives, we offer a wireless security workshop



- Understand security issues within your planned wireless e-business ideas
- Understand the key security technology requirements within a high level solution concept
- Understand requirements for integration into existing infrastructure

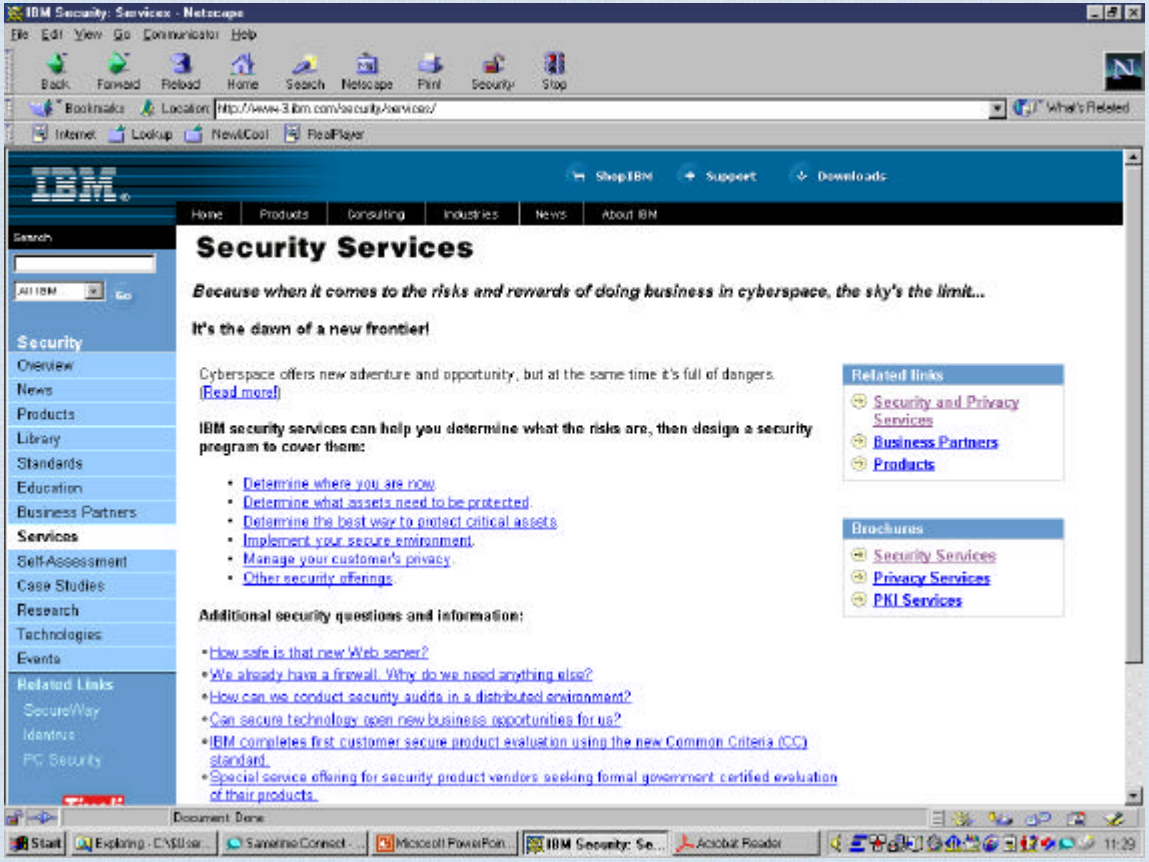
Our Solution Design service develops solutions to help leverage and protect the benefits of wireless e-business

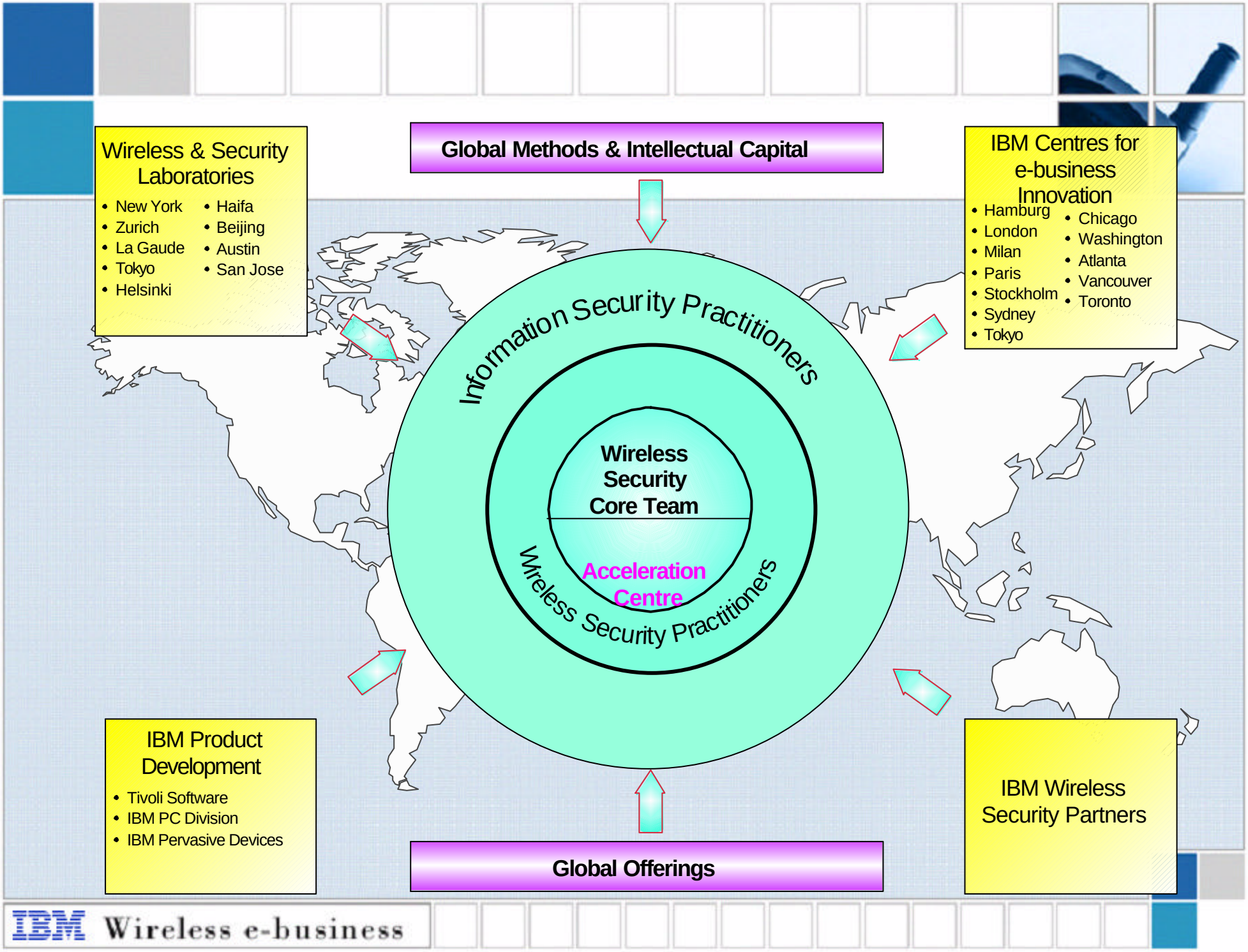


- Develop wireless e-business security strategy, requirements & policies
- Define and build secure and resilient solution architecture and design
- Build security processes
- Security out-tasking

More wireless security information is available at ibm.com

www.ibm.com/services/security




Wireless & Security Laboratories
• New York
• Zurich
• La Gaude
• Tokyo
• Helsinki
• Haifa
• Beijing
• Austin
• San Jose
Global Methods & Intellectual Capital
IBM Centres for e-business Innovation
• Hamburg
• London
• Milan
• Paris
• Stockholm
• Sydney
• Tokyo
• Chicago
• Washington
• Atlanta
• Vancouver
• Toronto
Information Security Practitioners
Wireless Security Practitioners
Wireless Security Core Team
Acceleration Centre
IBM Product Development
• Tivoli Software
• IBM PC Division
• IBM Pervasive Devices
IBM Wireless Security Partners
Global Offerings