1865-2015

Wireless CyberSecurity Risks
Practices for policy makers and regulators

ITU

Co-organised and hosted by:

MCMC

Supported by:

KKMM
KEMENTERIAN KOMUNIKASI
DAN MULTIMEDIA MALAYSIA

Australian Government
Department of Communications

Presentation supported by:
Ronald van Kleunen

Globeron

28 August 2015

ITU International Telecommunication Union

Committed to connecting the world

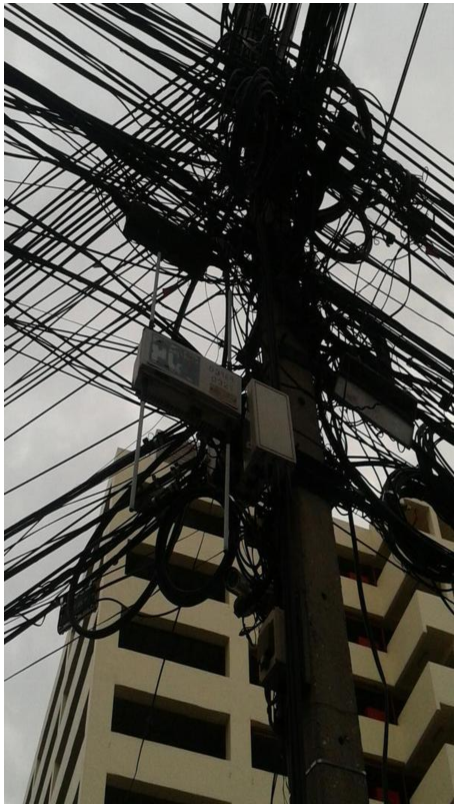
Agenda

- The Wi-Fi wireless service availability issues
- The Wi-Fi / Mobile / Cellular / other wireless security issues
- Governance – Standardization – Certification
- Examples of Governments in APAC adopting standardization and certification of personnel
- Wireless Service and Security Management System

The Wi-Fi wireless Service Availability issues

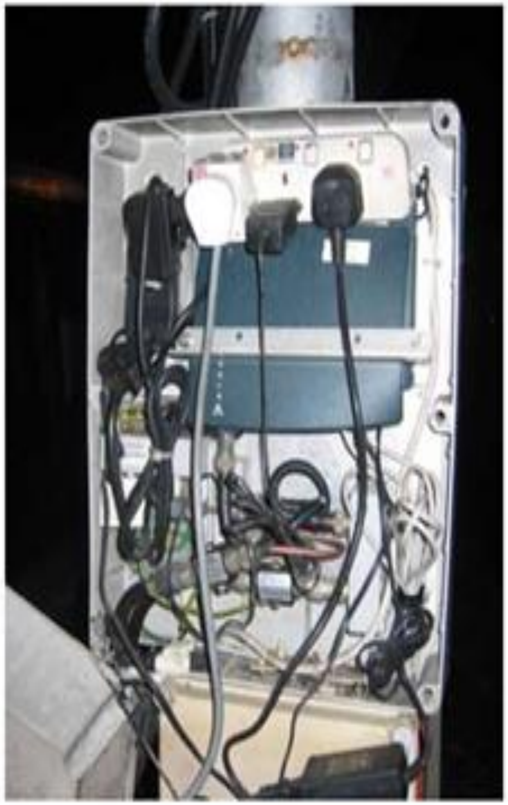
The issues - Outdoor

Ronald van Kleunen
@Globeron



Try to find the Wireless Access Points

The issues - Outdoor



Ronald van Kleunen
@Globeron

NEMA or IP-rated Enclosures

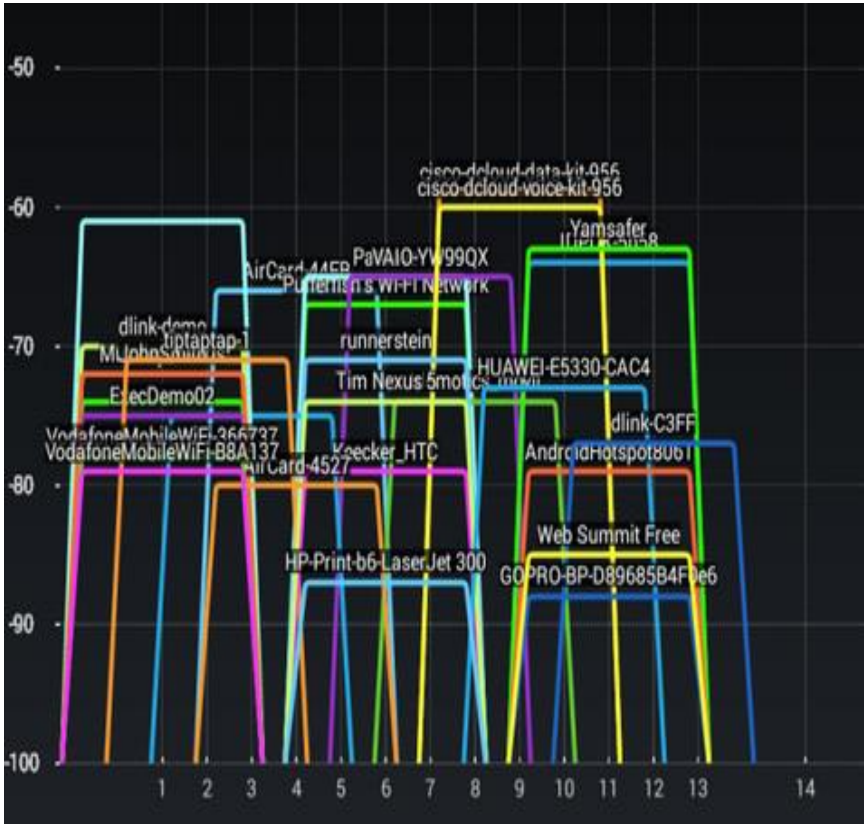
- Indoor equipment in an outdoor environment
- SoHo equipment and temperature issues
- Heat distribution ?
  - Heatsink
  - Fan

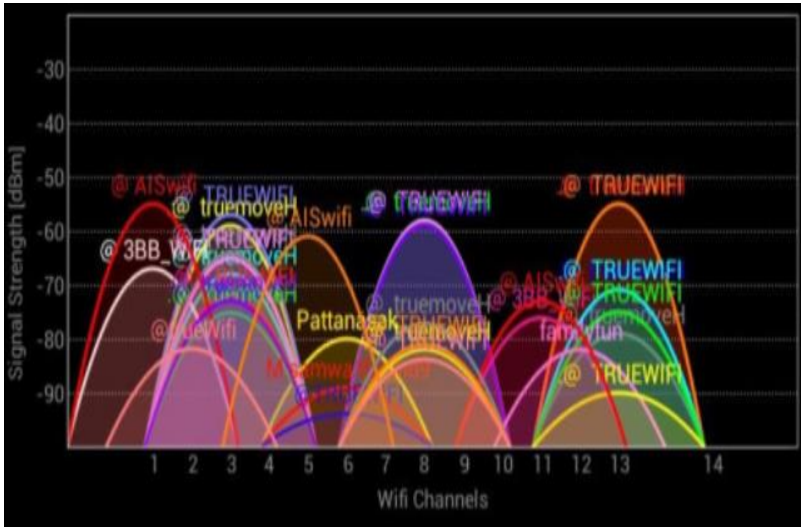
Wifi
ไปรษณีย์ไทย THAILAND POST
telic and Postage Stamp / Postal Souvenirs
ขอบคุณที่ใช้
Thank You. Please

...AND MANY OTHER CHALLENGES TO DESIGN AND DEPLOY WIRELESS NETWORKS

For example

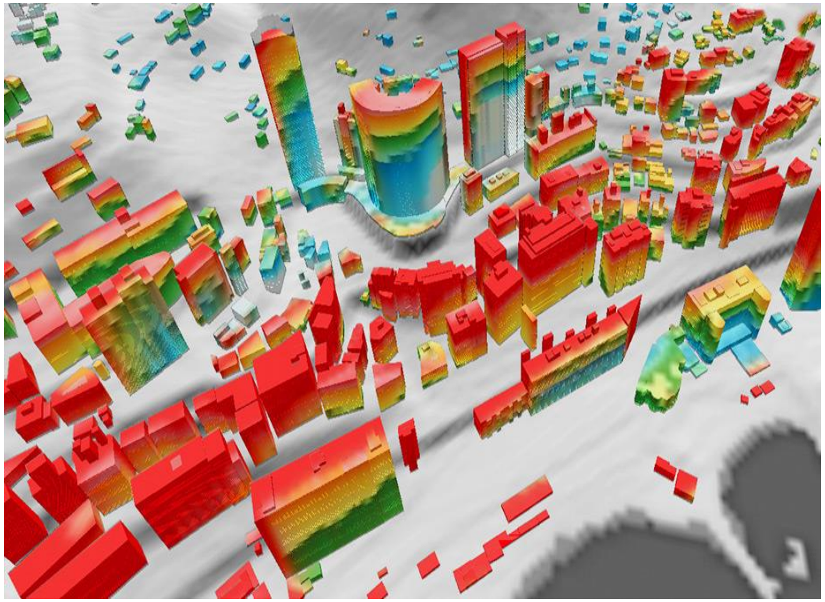
Channel mapping

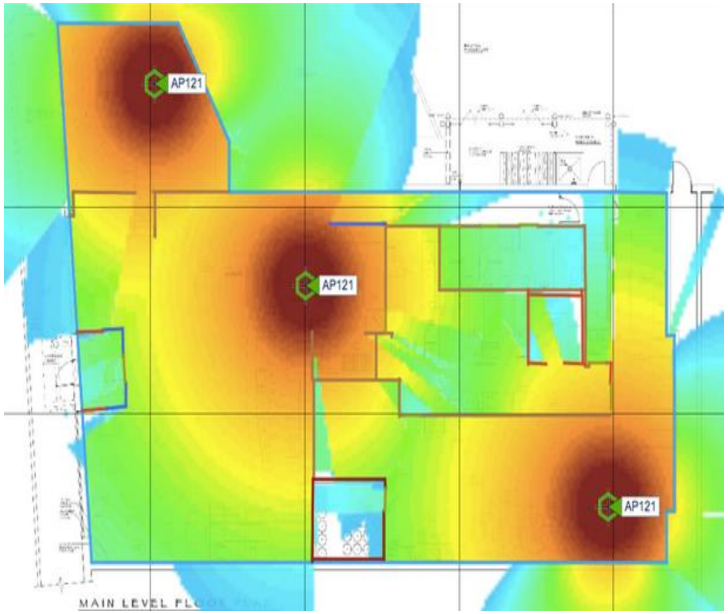




Ronald van Kleunen
@Globeron

RF Coverage planning Outdoor / Indoor

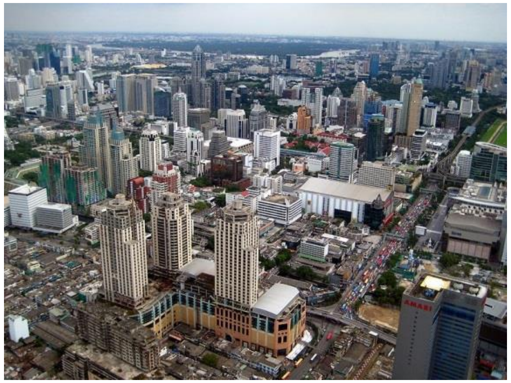




High Density

Wireless cities - millions of people

- very dense areas (apartments, hotels, houses)
- 24x hours people are on the streets (moving crowd)
- One big WiFi zone in the city,
- No channel coordination between ISPs and it is not possible with people managing their own WiFi at home both 2.4 GHz and 5 GHz are not enough, but will it ever be?



MANY OTHER ITEMS TO TAKE INTO CONSIDERATION TO DESIGN, IMPLEMENT AND OPERATE A WIRELESS LAN NETWORK

- IEEE standards, interoperability and new standards (e.g. 802.11ac)
- Modulations
- Type of Antenna’s
- Frequency selection and Channel Bandwidth
- Signal Strength and Noise values
- Channel planning
- Capacity planning (high density areas)
- Site Surveying
- Cabling requirements and Power over Ethernet (POE) requirements
- APs, MESH APs, Controllers and Cloud Controllers or Controller less
- Quality of Service (QoS) over a Wireless Network (Voice/Video/Data)
- Portability vs Mobility / Roaming
- Wireless Management tools, compliance and reporting
- Security integration

OTHER WIRELESS TECHNOLOGIES

- A Mobile/Cellular Radio Network is similar in setup
  it is also based on Radios, Antenna, RF, Protocols, etc.
  - 1G (Analog), 2G (TDMA-GSM), 2G (CDMA IS-95), 2.5G (EDGE), 3G (HSPDA), 4G (LTE), LTE-U (in Unlicensed WiFi bands), LTE-LAA (Licensed Assisted Access)

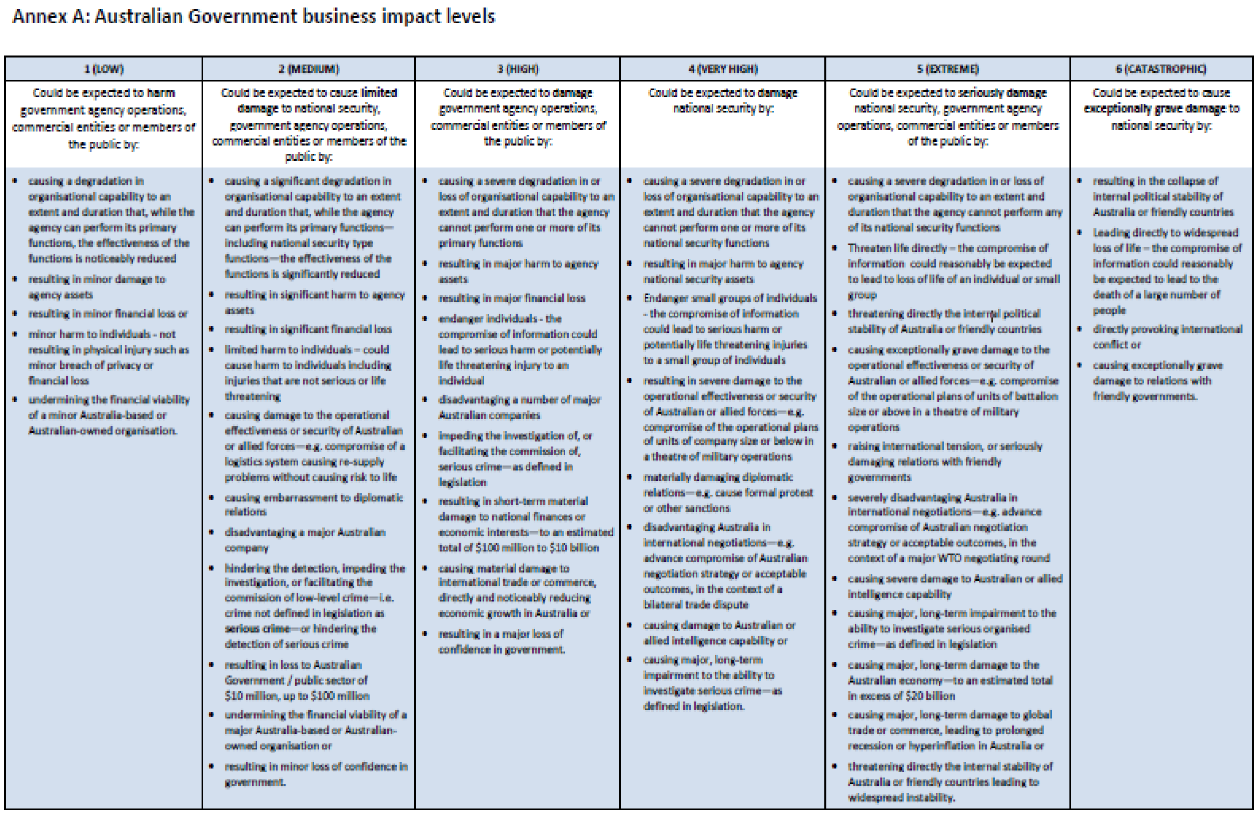
  > Network Function Virtualisation – NFV / SDN - Software Defined Networks

- And similar for any wireless network and devices:
  - Bluetooth
  - RFID
  - ZigBee
  - NFC (Near Field Communication)
  - Microwave communications
  - Satellite

The Wi-Fi / Mobile / Cellular / other wireless Security issues

Security & Business Impacts Levels
Example Australian Government

http://www.protectivesecurity.gov.au/governance/Documents/Business%20impact%20levels.pdf



Annex A: Australian Government business impact levels

1 (LOW)	2 (MEDIUM)	3 (HIGH)	4 (VERY HIGH)	5 (EXTREME)	6 (CATASTROPHIC)
Could be expected to **harm** government agency operations, commercial entities or members of the public by:	Could be expected to cause **limited damage** to national security, government agency operations, commercial entities or members of the public by:	Could be expected to **damage** government agency operations, commercial entities or members of the public by:	Could be expected to **damage** national security by:	Could be expected to **seriously damage** national security, government agency operations, commercial entities or members of the public by:	Could be expected to cause **exceptionally grave damage** to national security by:
• causing a degradation in organisational capability to an extent and duration that, while the agency can perform its primary functions, the effectiveness of the functions is noticeably reduced • resulting in minor damage to agency assets • resulting in minor financial loss or • minor harm to individuals - not resulting in physical injury such as minor breach of privacy or financial loss • undermining the financial viability of a minor Australia-based or Australian-owned organisation.	• causing a significant degradation in organisational capability to an extent and duration that, while the agency can perform its primary functions—including national security type functions—the effectiveness of the functions is significantly reduced • resulting in significant harm to agency assets • resulting in significant financial loss • limited harm to individuals – could cause harm to individuals including injuries that are not serious or life threatening • causing damage to the operational effectiveness or security of Australian or allied forces—e.g. compromise of a logistics system causing re-supply problems without causing risk to life • causing embarrassment to diplomatic relations • disadvantaging a major Australian company • hindering the detection, impeding the investigation, or facilitating the commission of low-level crime—i.e. crime not defined in legislation as serious crime—or hindering the detection of serious crime • resulting in loss to Australian Government / public sector of $10 million, up to $100 million • undermining the financial viability of a major Australia-based or Australian-owned organisation or • resulting in minor loss of confidence in government.	• causing a severe degradation in or loss of organisational capability to an extent and duration that the agency cannot perform one or more of its primary functions • resulting in major harm to agency assets • resulting in major financial loss • endanger individuals - the compromise of information could lead to serious harm or potentially life threatening injury to an individual • disadvantaging a number of major Australian companies • impeding the investigation of, or facilitating the commission of, serious crime—as defined in legislation • resulting in short-term material damage to national finances or economic interests—to an estimated total of $100 million to $10 billion • causing material damage to international trade or commerce, directly and noticeably reducing economic growth in Australia or • resulting in a major loss of confidence in government.	• causing a severe degradation in or loss of organisational capability to an extent and duration that the agency cannot perform one or more of its national security functions • resulting in major harm to agency national security assets • Endanger small groups of individuals - the compromise of information could lead to serious harm or potentially life threatening injuries to a small group of individuals • resulting in severe damage to the operational effectiveness or security of Australian or allied forces—e.g. compromise of the operational plans of units of company size or below in a theatre of military operations • materially damaging diplomatic relations—e.g. cause formal protest or other sanctions • disadvantaging Australia in international negotiations—e.g. advance compromise of Australian negotiation strategy or acceptable outcomes, in the context of a bilateral trade dispute • causing damage to Australian or allied intelligence capability or • causing major, long-term impairment to the ability to investigate serious crime—as defined in legislation.	• causing a severe degradation in or loss of organisational capability to an extent and duration that the agency cannot perform any of its national security functions • Threaten life directly – the compromise of information could reasonably be expected to lead to loss of life of an individual or small group • threatening directly the internal political stability of Australia or friendly countries • causing exceptionally grave damage to the operational effectiveness or security of Australian or allied forces—e.g. compromise of the operational plans of units of battalion size or above in a theatre of military operations • raising international tension, or seriously damaging relations with friendly governments • severely disadvantaging Australia in international negotiations—e.g. advance compromise of Australian negotiation strategy or acceptable outcomes, in the context of a major WTO negotiating round • causing severe damage to Australian or allied intelligence capability • causing major, long-term impairment to the ability to investigate serious organised crime—as defined in legislation • causing major, long-term damage to the Australian economy—to an estimated total in excess of $20 billion • causing major, long-term damage to global trade or commerce, leading to prolonged recession or hyperinflation in Australia or • threatening directly the internal stability of Australia or friendly countries leading to widespread instability.	• resulting in the collapse of internal political stability of Australia or friendly countries • Leading directly to widespread loss of life – the compromise of information could reasonably be expected to lead to the death of a large number of people • directly provoking international conflict or • causing exceptionally grave damage to relations with friendly governments.

- Levels
  1. Low
  2. Medium
  3. High
  4. Very High
  5. Extreme
  6. Catastrophic

WIFI - WIRELESS VULNERABILITIES

Type	Attacks
Reconnaissance	▪ Rogue APs ▪ Open/Misconfigured APs ▪ Ad Hoc stations
Sniffing/Eavesdropping	▪ WEP, WPA, LEAP cracking ▪ Dictionary attacks / Brute Force / Rainbow Tables ▪ Leaky APs
Masquerade	▪ MAC spoofing ▪ HotSpot attacks ▪ Evil Twin / Wi-Phishing attacks
Insertion	▪ Multicast / Broadcast injection ▪ Routing cache poisoning ▪ Man in the Middle attacks (MITM)
Denial-of-Service	▪ Disassociation ▪ Duration field spoofing ▪ RF jamming

Mobile - Wireless Vulnerabilities

Type	Attacks
Reconnaissance	▪ Baseband Fuzzing (Rogue BTS)
Sniffing/Eavesdropping	▪ Telco's Protocol Analysers? ▪ Software Defined Radios SDR
Masquerade	▪ IMEI spoofing (using MTK/SDK boards)
Insertion	▪ IMSI Detach, send multiple Location Update Requests including spoofed IMSI. Prevent SIM from receiving calls and SMS (only backend HLR is off), but still can call and SMS
Denial-of-Service	▪ Request Channel Allocation (Flood BTS and possible BSC) ▪ RF jamming ▪ IMSI Flood (pre-authentication) and overload HLR/VLR ▪ IMSI Detach also disconnects user

OTHER WIRELESS SECURITY RISKS

- BlueTooth
  - Virus / Worms / Malware
  - Listening to phone calls (headset) or car audio systems
  - Changing languages (“DoS”)
  - Car Hacking via Bluetooth (Controlling the car)
- NFC (Near Field Communication)
  - Credit Cards with NFC communication
  - Transportation cards (“Bus”, “Train”)
  - Toll gates using wireless cards
  - Hotel Key cards
- ZigBee
  - Home Automation equipment
  - Floor Controllers
  - Thermostats
- Internet of Things (IoT) / Everything (IoE)
  - Limited security capabilities

Other Wireless Security Risks

- It is not only the wireless or mobile/cellular infrastructure

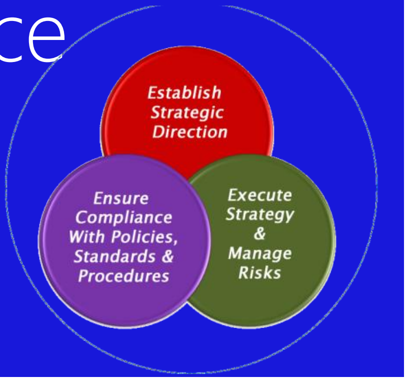
- Operating Systems
  - Android OS
  - Apple iOS
  - Etc.

- Applications
  - Access Control to the device (Camera, Storage, etc.)
  - Remote Command and Control
  - Malware

Governance – Standardization - Certification

Governance – Standardization - Certification

Governance

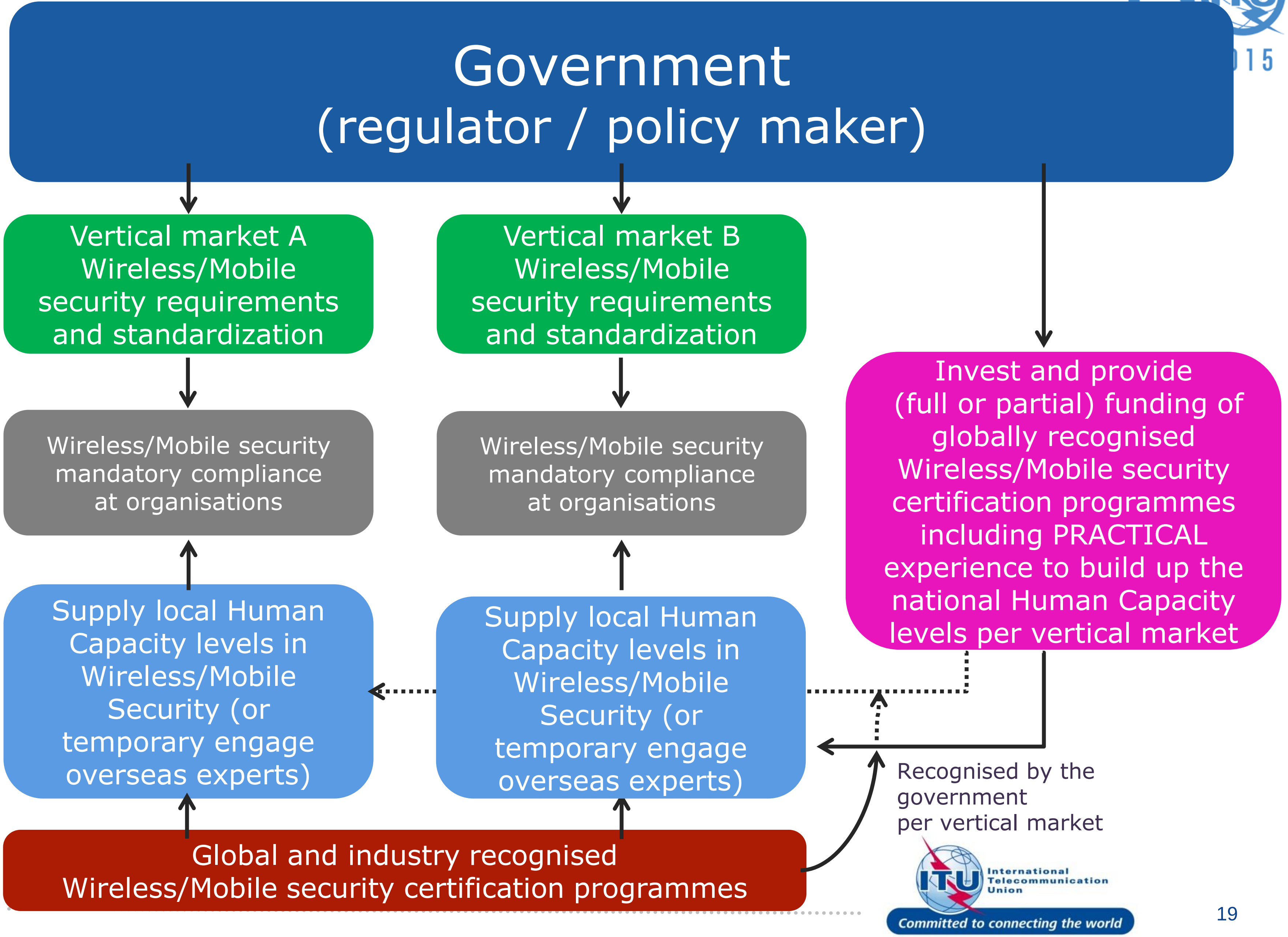

Establish Strategic Direction
Ensure Compliance With Policies, Standards & Procedures
Execute Strategy & Manage Risks

Standardization

Certified Professionals

Certified Auditors

Build Standardization At National Level per vertical market



Government
(regulator / policy maker)

Vertical market A
Wireless/Mobile
security requirements
and standardization

Vertical market B
Wireless/Mobile
security requirements
and standardization

Wireless/Mobile security
mandatory compliance
at organisations

Wireless/Mobile security
mandatory compliance
at organisations

Invest and provide
(full or partial) funding of
globally recognised
Wireless/Mobile security
certification programmes
including PRACTICAL
experience to build up the
national Human Capacity
levels per vertical market

Supply local Human
Capacity levels in
Wireless/Mobile
Security (or
temporary engage
overseas experts)

Supply local Human
Capacity levels in
Wireless/Mobile
Security (or
temporary engage
overseas experts)

Recognised by the
government
per vertical market

Global and industry recognised
Wireless/Mobile security certification programmes

Wireless Standard bodies

IEEE

IETF

ITU

ISO International Organization for Standardization

Wi Fi Alliance

IEC INTERNATIONAL ELECTROTECHNICAL COMMISSION

Wireless Broadband Alliance

3GPP A GLOBAL INITIATIVE

ISO/IEC 20000-1:2011 ITSM Standard (1st version launched :2005) and ISO/IEC 20000-2:2012 ITSM Standard (1st version launched :2005) ITSMS: Information Technology Service Management Standard

INTERNATIONAL STANDARD

ISO/IEC 20000-1

Second edition
2011-04-15

Information technology — Service management —

Part 1:
Service management system requirements

Technologies de l'information — Gestion des services —

Partie 1: Exigences du système de gestion des services

Reference number
ISO/IEC 20000-1:2011(E)

© ISO/IEC 2011

INTERNATIONAL STANDARD

ISO/IEC 20000-2

Second edition
2012-02-15

Information technology — Service management —

Part 2:
Guidance on the application of service management systems

Technologies de l'information — Gestion des services —

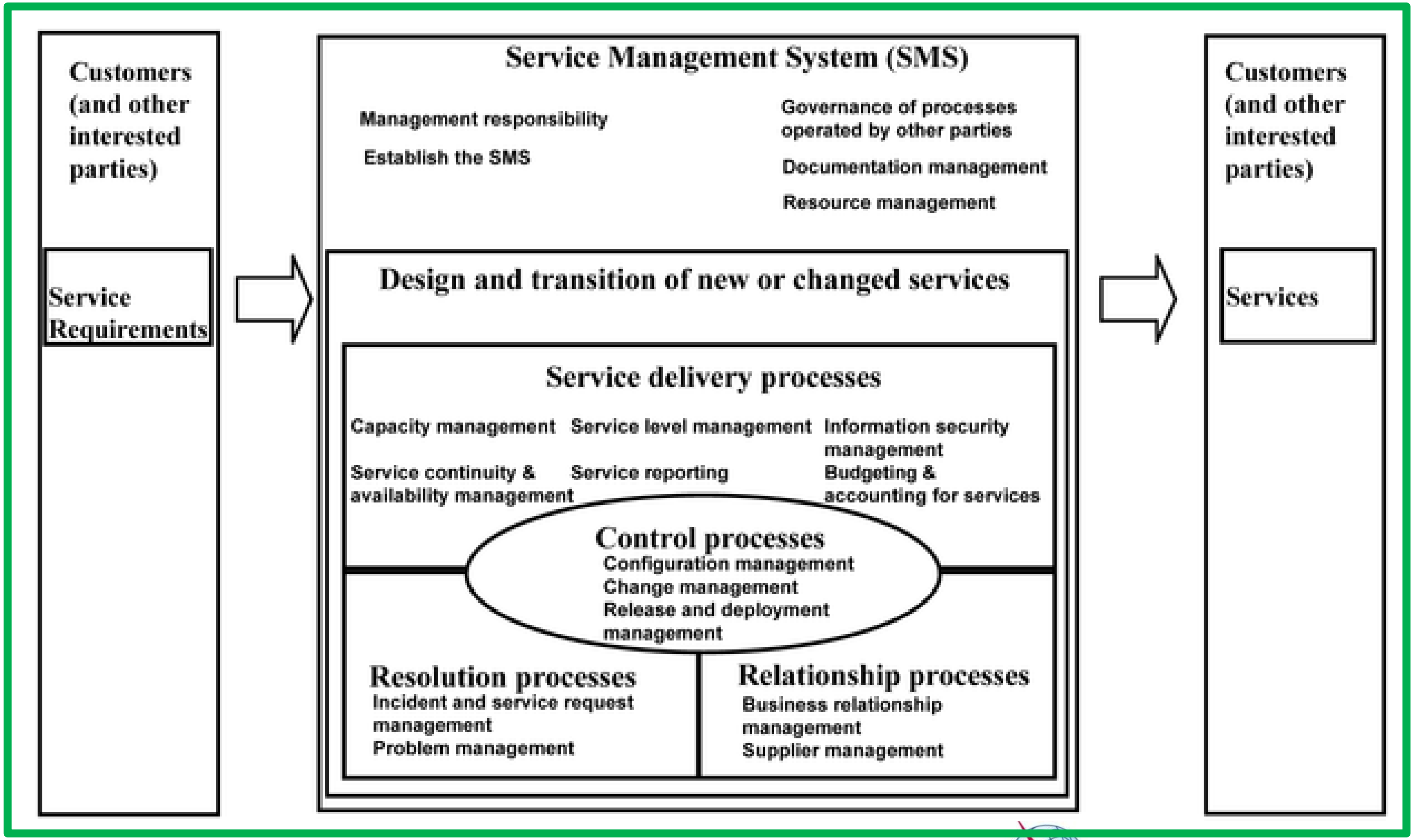
Partie 2: Directives relatives à l'application des systèmes de management des services

Reference number
ISO/IEC 20000-2:2012(E)

© ISO/IEC 2012

ITSM – Service Management System and Wireless Service Management

Wireless Service Management



Customers (and other interested parties)

Service Requirements

Service Management System (SMS)

Management responsibility

Establish the SMS

Governance of processes operated by other parties

Documentation management

Resource management

Design and transition of new or changed services

Service delivery processes

Capacity management

Service level management

Information security management

Service continuity & availability management

Service reporting

Budgeting & accounting for services

Control processes

Configuration management

Change management

Release and deployment management

Resolution processes

Incident and service request management

Problem management

Relationship processes

Business relationship management

Supplier management

Customers (and other interested parties)

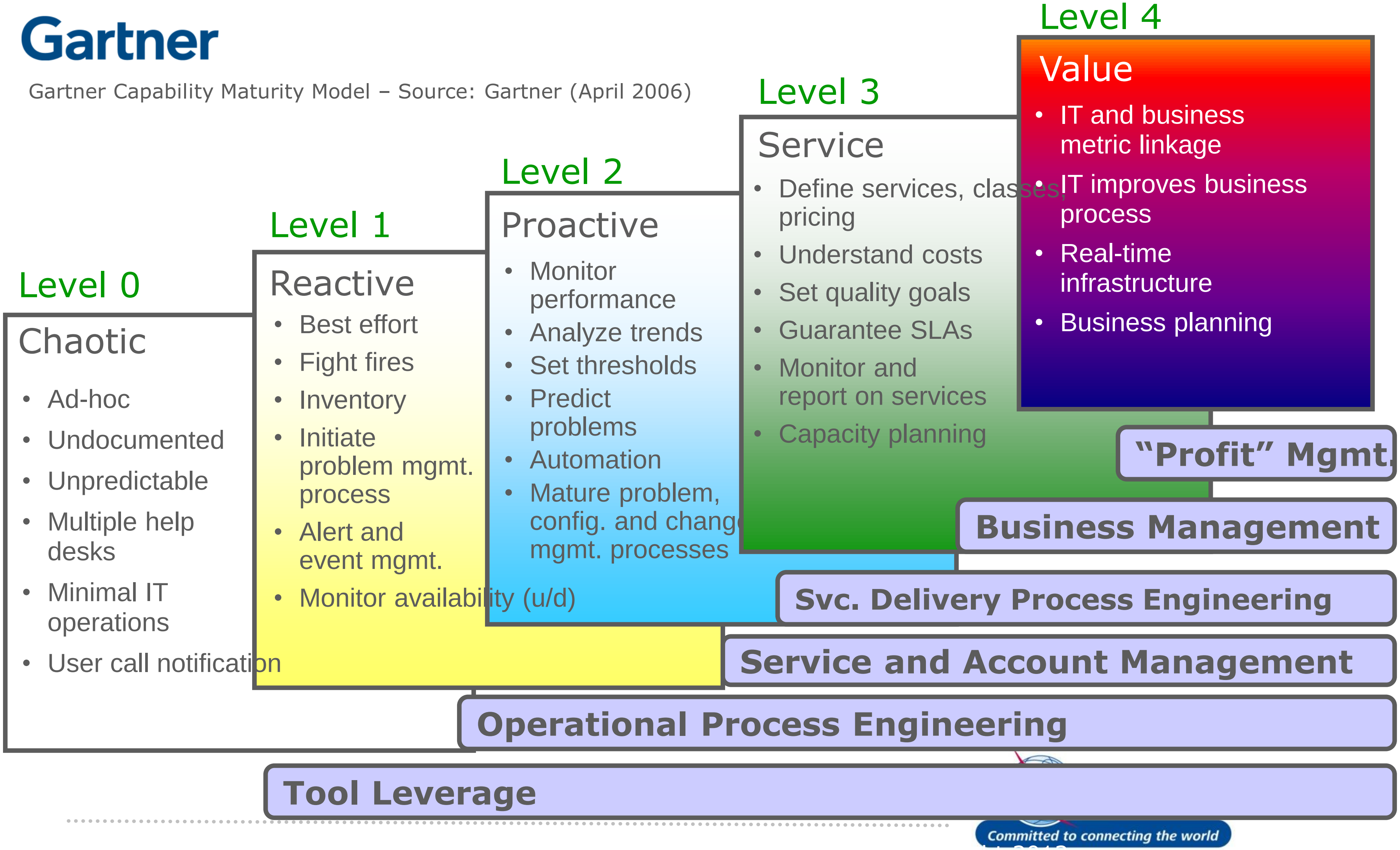
Services

Organisations' capability levels / Service Level Agreements (SLAs)

At which level do you provide wireless service management?

Gartner

Gartner Capability Maturity Model – Source: Gartner (April 2006)



Level 0

Chaotic

- Ad-hoc
- Undocumented
- Unpredictable
- Multiple help desks
- Minimal IT operations
- User call notification

Level 1

Reactive

- Best effort
- Fight fires
- Inventory
- Initiate problem mgmt. process
- Alert and event mgmt.
- Monitor availability (u/d)

Level 2

Proactive

- Monitor performance
- Analyze trends
- Set thresholds
- Predict problems
- Automation
- Mature problem, config. and chang mgmt. processes

Level 3

Service

- Define services, classes, pricing
- Understand costs
- Set quality goals
- Guarantee SLAs
- Monitor and report on services
- Capacity planning

Level 4

Value

- IT and business metric linkage
- IT improves business process
- Real-time infrastructure
- Business planning

"Profit" Mgmt.

Business Management

Svc. Delivery Process Engineering

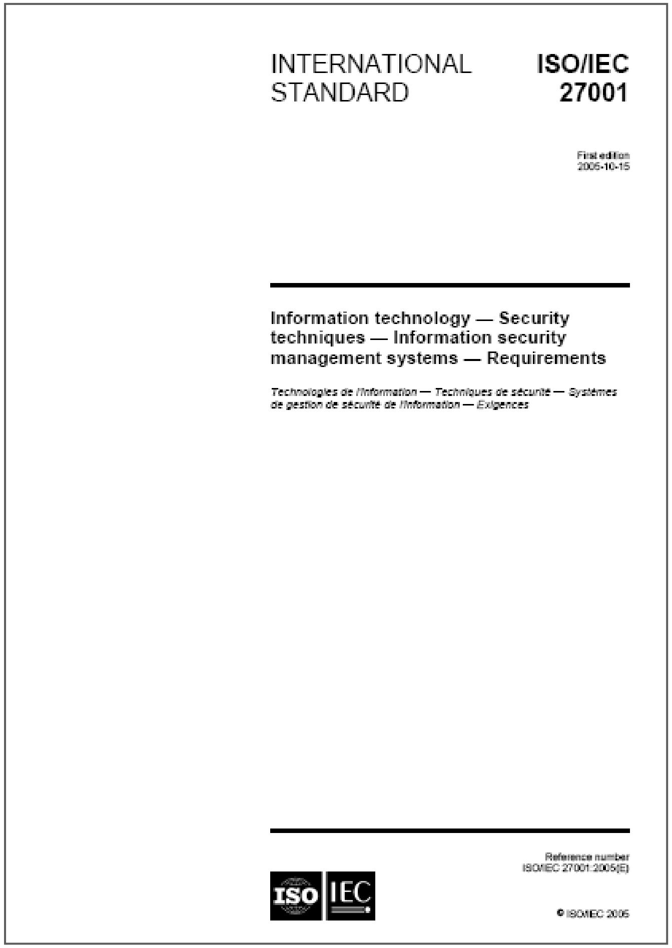
Service and Account Management

Operational Process Engineering

Tool Leverage

Committed to connecting the world

ISO/IEC 27001:2013 ISMS Standard (1st version launched :2005) and ISO/IEC 27002:2013 ISMS Standard (1st version launched :2005) ISMS: Information Security Management Systems



INTERNATIONAL STANDARD

ISO/IEC 27001

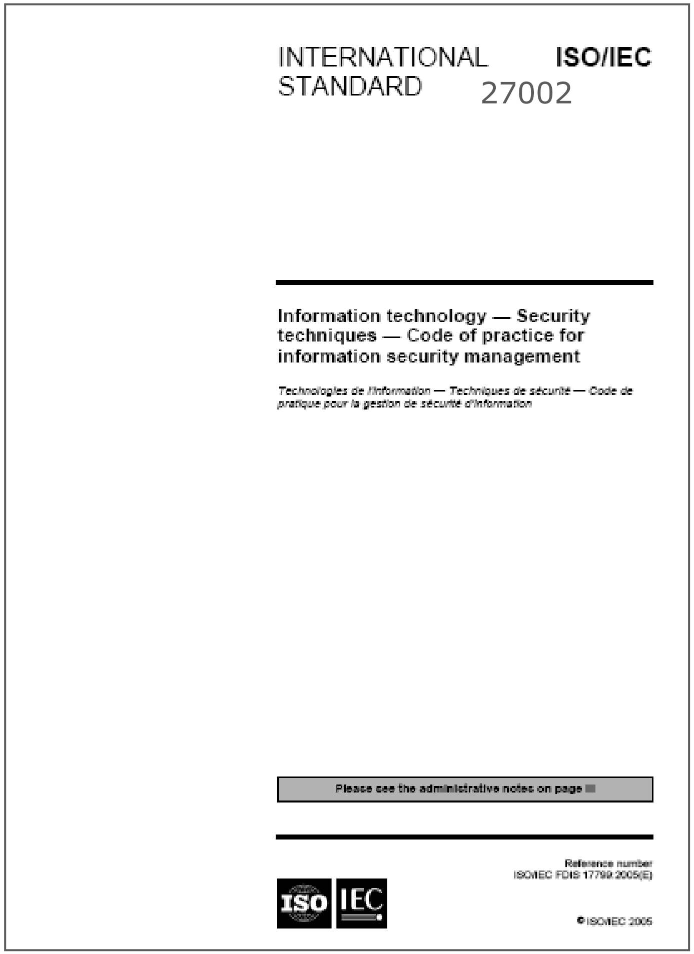
First edition
2005-10-15

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2005(E)

© ISO/IEC 2005



INTERNATIONAL STANDARD

ISO/IEC 27002

Information technology — Security techniques — Code of practice for information security management

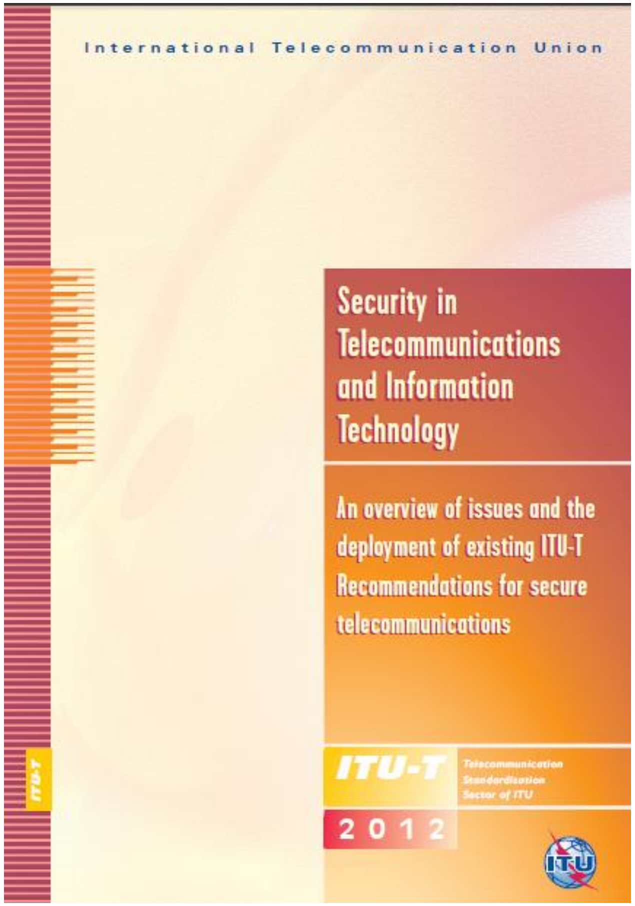
Technologies de l'information — Techniques de sécurité — Code de pratique pour la gestion de sécurité d'information

Please see the administrative notes on page

Reference number
ISO/IEC FDIS 17799:2005(E)

© ISO/IEC 2005

Security in Telecommunications and Information Technology



International Telecommunication Union

Security in Telecommunications and Information Technology

An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications

ITU-T Telecommunication Standardization Sector of ITU

2012

2012: The purpose of the ITU-T Manual on Security in Telecommunications and Information Technology is to provide a broad introduction to the security work of ITU-T. It is directed towards those who have responsibility for, or an interest in, information and communications security and the related standards, and those who simply need to gain a better understanding of ICT security issues and the corresponding ITU-T Recommendations.

ITU / IMPACT / GLOBERON
WIRELESS SECURITY
DISTANCE LEARNING FOR GOVERNMENTS IN APAC

ANNEX 1: Distance Learning Course On *WIRELESS SECURITY PRACTICES FOR POLICY MAKERS AND REGULATORS*

ITU ASIA-PACIFIC CENTRES OF EXCELLENCE

Distance Learning Course

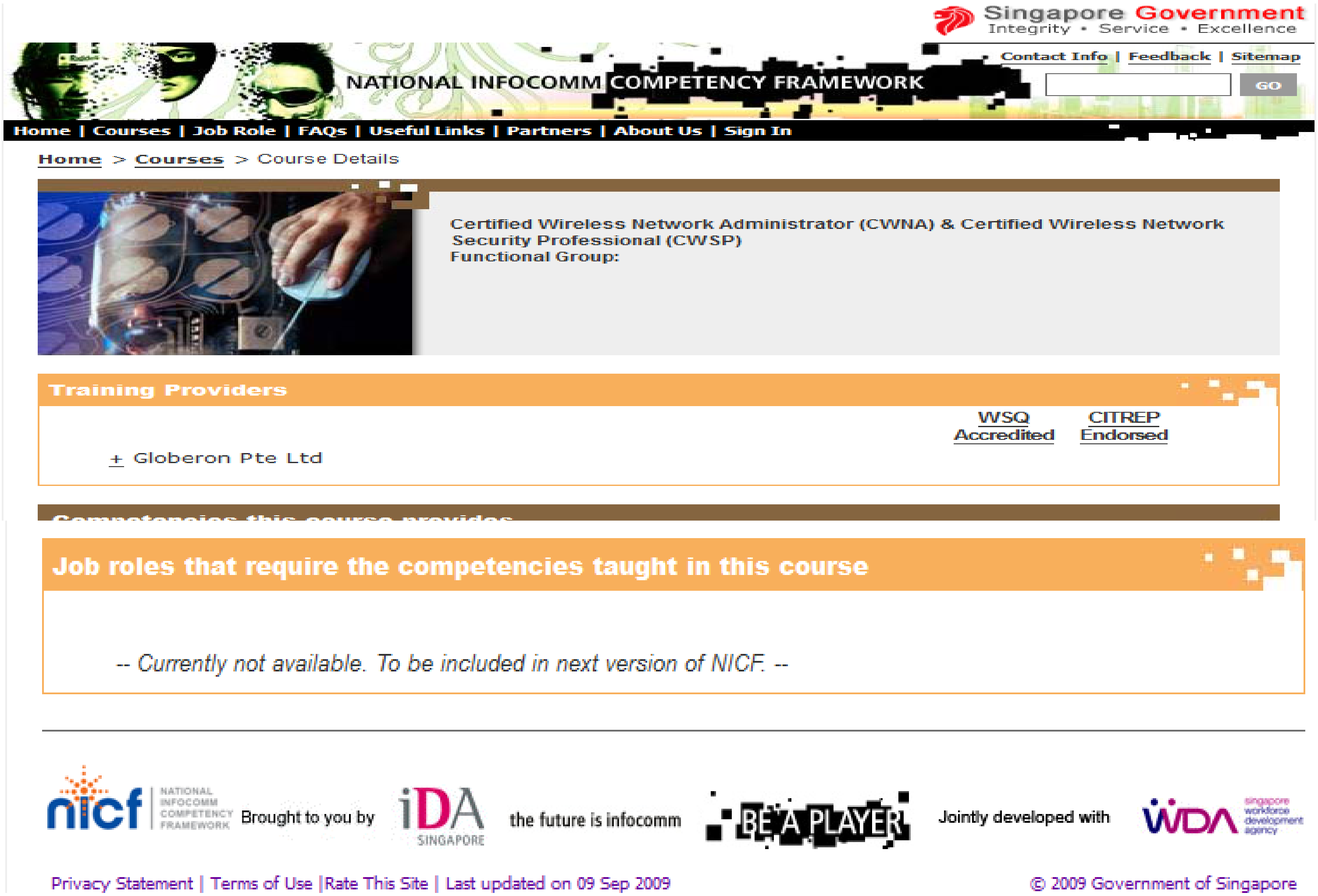
WIRELESS SECURITY PRACTICES FOR POLICY MAKERS AND REGULATORS

Supported by:

Examples of Governments in APAC adopting standardization on certification for personnel

Singapore: National Infocomm Competency Framework

https://www.idaicms.gov.sg/nicf/course/courseDetails.do?CourseID=NICF-COUR-0158



Singapore Government
Integrity • Service • Excellence

Contact Info | Feedback | Sitemap

NATIONAL INFOCOMM COMPETENCY FRAMEWORK

GO

Home | Courses | Job Role | FAQs | Useful Links | Partners | About Us | Sign In

Home > Courses > Course Details

Certified Wireless Network Administrator (CWNA) & Certified Wireless Network Security Professional (CWSP)
Functional Group:

Training Providers

	WSQ Accredited	CITREP Endorsed
+ Globeron Pte Ltd		

Competencies this course provides

Job roles that require the competencies taught in this course

-- Currently not available. To be included in next version of NICF. --

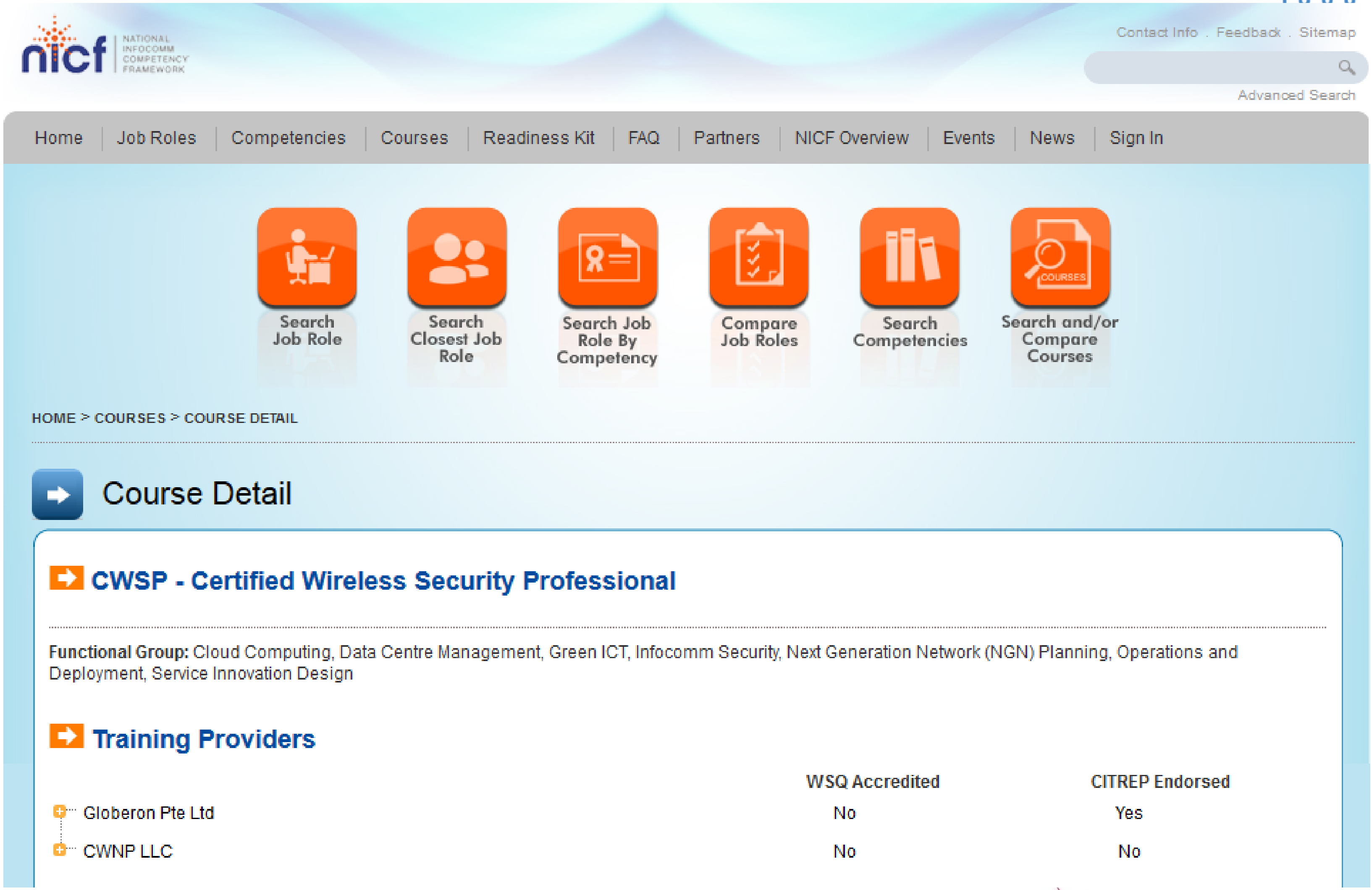
nicf NATIONAL INFOCOMM COMPETENCY FRAMEWORK Brought to you by iDA SINGAPORE the future is infocomm BE A PLAYER Jointly developed with WDA singapore workforce development agency

Privacy Statement | Terms of Use |Rate This Site | Last updated on 09 Sep 2009

© 2009 Government of Singapore

Certified Wireless Security Professional (CWSP) recognised by Singapore government

CITREP – Critical Skill development programme



Course Detail

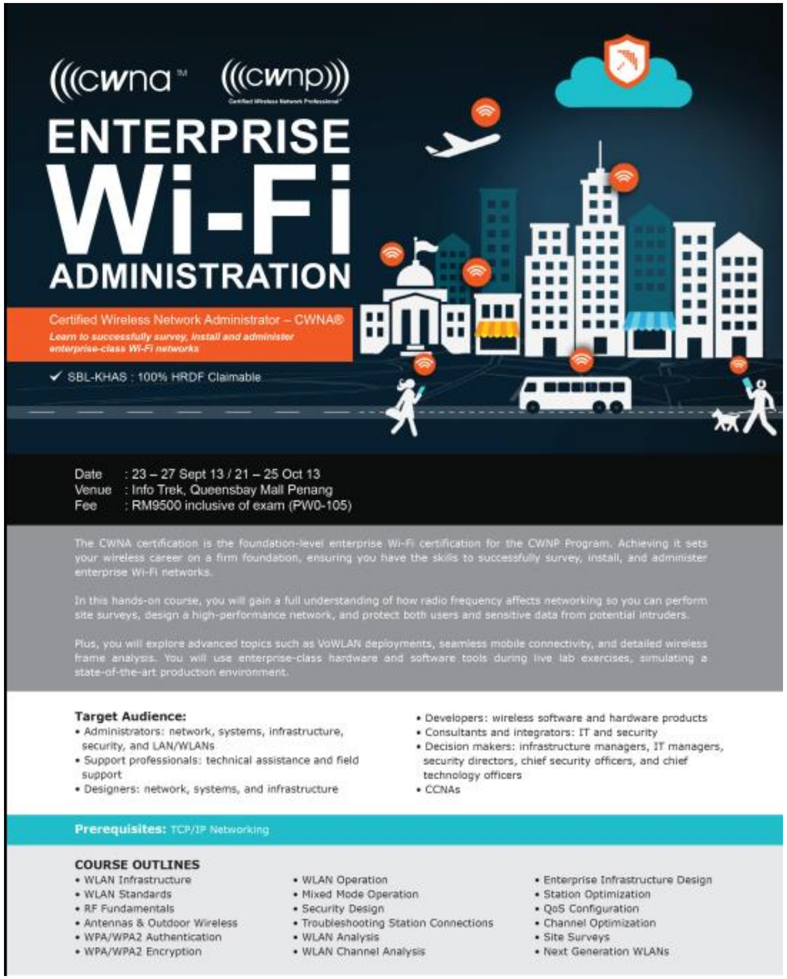
CWSP - Certified Wireless Security Professional

Functional Group: Cloud Computing, Data Centre Management, Green ICT, Infocomm Security, Next Generation Network (NGN) Planning, Operations and Deployment, Service Innovation Design

Training Providers

	WSQ Accredited	CITREP Endorsed
Globeron Pte Ltd	No	Yes
CWNP LLC	No	No

Malaysia: PSMB / HRDF
Human Resource Development Fund


((cwna™
((cwnp))
Certified Wireless Network Professional

ENTERPRISE Wi-Fi ADMINISTRATION

Certified Wireless Network Administrator – CWNA®

Learn to successfully survey, install and administer enterprise-class Wi-Fi networks

✓ SBL-KHAS : 100% HRDF Claimable

Date : 23 – 27 Sept 13 / 21 – 25 Oct 13
Venue : Info Trek, Queensbay Mall Penang
Fee : RM9500 inclusive of exam (PW0-105)

The CWNA certification is the foundation-level enterprise Wi-Fi certification for the CWNP Program. Achieving it sets your wireless career on a firm foundation, ensuring you have the skills to successfully survey, install, and administer enterprise Wi-Fi networks.

In this hands-on course, you will gain a full understanding of how radio frequency affects networking so you can perform site surveys, design a high-performance network, and protect both users and sensitive data from potential intruders.

Plus, you will explore advanced topics such as VoWLAN deployments, seamless mobile connectivity, and detailed wireless frame analysis. You will use enterprise-class hardware and software tools during live lab exercises, simulating a state-of-the-art production environment.

Target Audience:

- Administrators: network, systems, infrastructure, security, and LAN/WLANs
- Support professionals: technical assistance and field support
- Designers: network, systems, and infrastructure
- Developers: wireless software and hardware products
- Consultants and integrators: IT and security
- Decision makers: infrastructure managers, IT managers, security directors, chief security officers, and chief technology officers
- CCNAs

Prerequisites: TCP/IP Networking

COURSE OUTLINES

- WLAN Infrastructure
- WLAN Standards
- RF Fundamentals
- Antennas & Outdoor Wireless
- WPA/WPA2 Authentication
- WPA/WPA2 Encryption
- WLAN Operation
- Mixed Mode Operation
- Security Design
- Troubleshooting Station Connections
- WLAN Analysis
- WLAN Channel Analysis
- Enterprise Infrastructure Design
- Station Optimization
- QoS Configuration
- Channel Optimization
- Site Surveys
- Next Generation WLANs

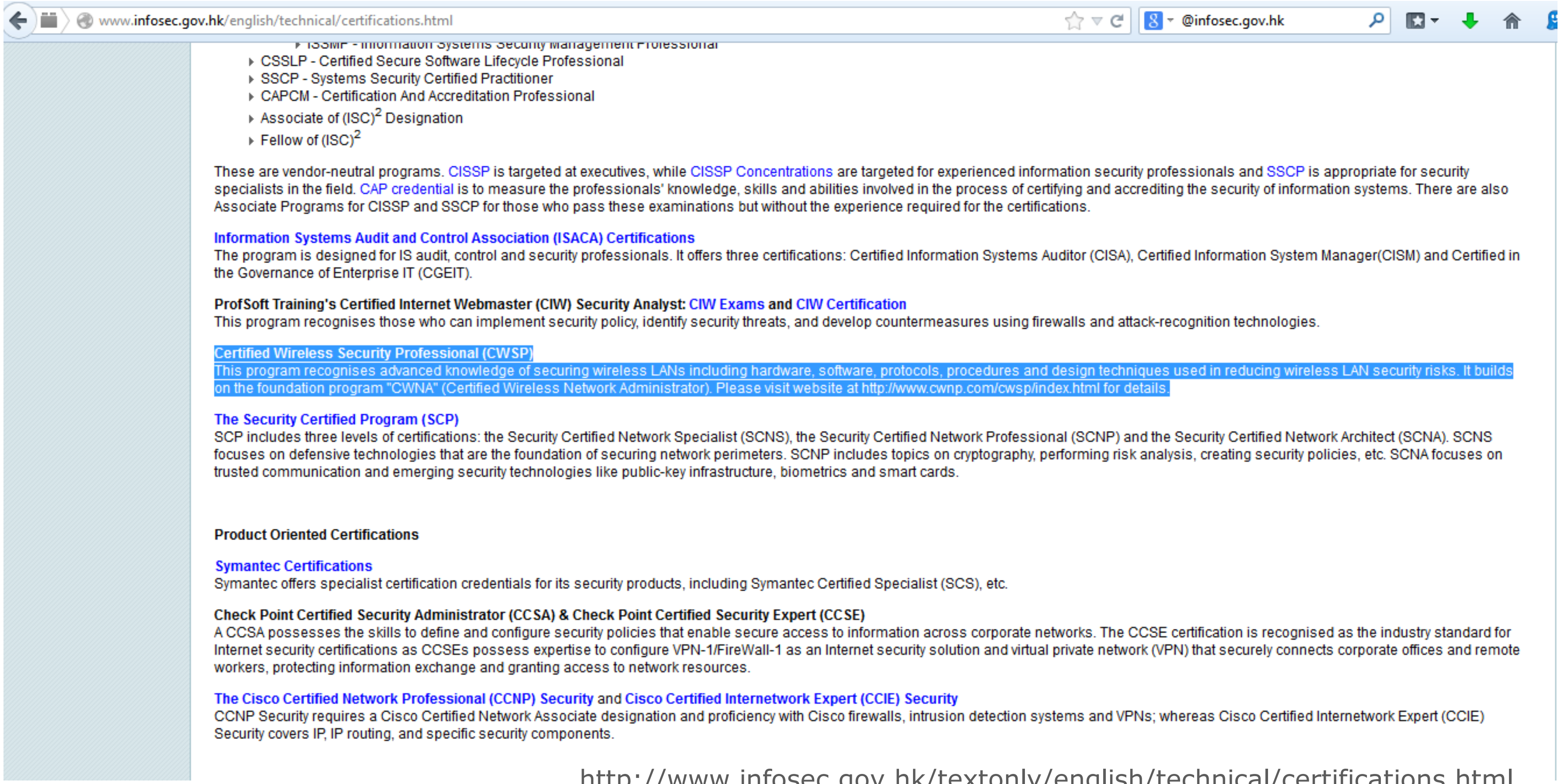
✓ SBL-KHAS : 100% HRDF Claimable

registered with

HRDF
MALAYSIA

INFOSEC HONG KONG (CWNA+CWSP)

This InfoSec website is produced and managed by the Office of the Government Chief Information Officer of the Government.



- ISSMP - Information Systems Security Management Professional
- CSSLP - Certified Secure Software Lifecycle Professional
- SSCP - Systems Security Certified Practitioner
- CAPCM - Certification And Accreditation Professional
- Associate of (ISC)^2 Designation
- Fellow of (ISC)^2

These are vendor-neutral programs. CISSP is targeted at executives, while CISSP Concentrations are targeted for experienced information security professionals and SSCP is appropriate for security specialists in the field. CAP credential is to measure the professionals' knowledge, skills and abilities involved in the process of certifying and accrediting the security of information systems. There are also Associate Programs for CISSP and SSCP for those who pass these examinations but without the experience required for the certifications.

Information Systems Audit and Control Association (ISACA) Certifications
The program is designed for IS audit, control and security professionals. It offers three certifications: Certified Information Systems Auditor (CISA), Certified Information System Manager(CISM) and Certified in the Governance of Enterprise IT (CGEIT).

ProfSoft Training's Certified Internet Webmaster (CIW) Security Analyst: CIW Exams and CIW Certification
This program recognises those who can implement security policy, identify security threats, and develop countermeasures using firewalls and attack-recognition technologies.

Certified Wireless Security Professional (CWSP)
This program recognises advanced knowledge of securing wireless LANs including hardware, software, protocols, procedures and design techniques used in reducing wireless LAN security risks. It builds on the foundation program "CWNA" (Certified Wireless Network Administrator). Please visit website at http://www.cwnp.com/cwsp/index.html for details.

The Security Certified Program (SCP)
SCP includes three levels of certifications: the Security Certified Network Specialist (SCNS), the Security Certified Network Professional (SCNP) and the Security Certified Network Architect (SCNA). SCNS focuses on defensive technologies that are the foundation of securing network perimeters. SCNP includes topics on cryptography, performing risk analysis, creating security policies, etc. SCNA focuses on trusted communication and emerging security technologies like public-key infrastructure, biometrics and smart cards.

Product Oriented Certifications

Symantec Certifications
Symantec offers specialist certification credentials for its security products, including Symantec Certified Specialist (SCS), etc.

Check Point Certified Security Administrator (CCSA) & Check Point Certified Security Expert (CCSE)
A CCSA possesses the skills to define and configure security policies that enable secure access to information across corporate networks. The CCSE certification is recognised as the industry standard for Internet security certifications as CCSEs possess expertise to configure VPN-1/FireWall-1 as an Internet security solution and virtual private network (VPN) that securely connects corporate offices and remote workers, protecting information exchange and granting access to network resources.

The Cisco Certified Network Professional (CCNP) Security and Cisco Certified Internetwork Expert (CCIE) Security
CCNP Security requires a Cisco Certified Network Associate designation and proficiency with Cisco firewalls, intrusion detection systems and VPNs; whereas Cisco Certified Internetwork Expert (CCIE) Security covers IP, IP routing, and specific security components.

http://www.infosec.gov.hk/textonly/english/technical/certifications.html

Wireless Service and Security Management System

Wireless Service and Security Management System

Wireless Service Management Standard (WSMS)

Note: Wireless = Mobile/Cellular, WiFi and indoor/outdoor mission/business critical wireless technologies

WSMS auditor / Certified Wireless Service Auditor is a wireless services professional with the knowledge and skills required to assess the conformance of an organization's wireless services management system as part of the ISO/IEC 20000 ITSM standard.

Wireless Service Security Management Standard (WSSMS)

Note: Wireless = Mobile/Cellular, WiFi and indoor/outdoor mission/business critical wireless technologies

WSSMS auditor / Certified Wireless Security Auditor is a wireless security professional with the knowledge and skills required to assess the conformance of an organization's wireless services management system as part of the
ISO/IEC 27001 ISMS standard.

Together we need to get better quality wireless networks for mission and business critical services

1. Click here

   Wireless Service management & audit aligned with ITSM / ISO/IEC 20000:2011

2. Click here

   Wireless Security management & audit aligned with ISMS / ISO/IEC 27001:2013

3. **Standardization is needed for:**
   - Design
   - Analysis
   - Security
   - Audit (end to end service & security management)

4. **Accreditation Body for wireless services/technology**

   Cellular/Mobile, WiFi, etc.

Wireless CyberSecurity Risks
Practices for policy makers and regulators

Co-organised and hosted by:

Supported by:

28 August 2015

Committed to connecting the world