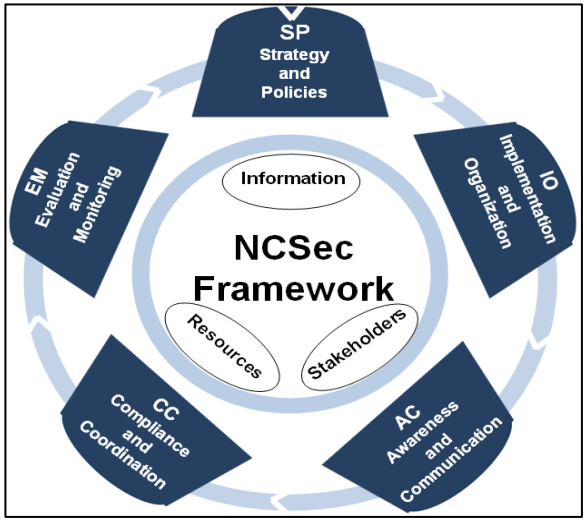
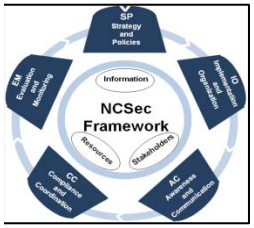
National Cybersecurity Management System:
Framework, Maturity Model and Implementation Guide



Taieb DEBBAGH, PhD, CISA
Secretary–General
Ministry of Industry, Trade and New Technologies, Morocco

ITU Regional Cybersecurity Forum for Africa and Arab States
4-5 June 2009, Tunis, Tunisia



Agenda

1 – Introduction

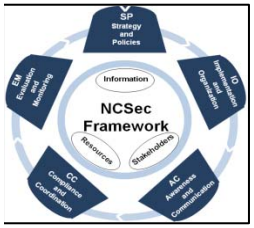
2 – National Cybersecurity Management System

- √ NCSec Framework
- √ Maturity Model
- √ Roles & Responsibilities
- √ Implementation Guide

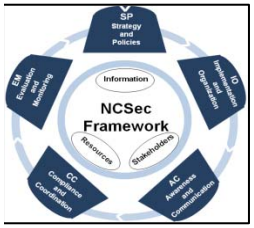
3 – Research Papers

4 – Morocco Case

- √ ICT Strategic Plan
- √ Cybersecurity Roadmap



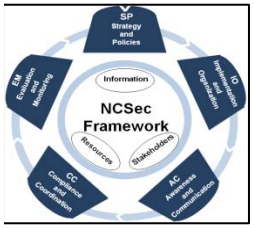
1 - Introduction



Introduction (1/2)

- Increasing computer security challenges in the world;
- No appropriate organizational and institutional structures to deal with these issues;
- Which entity(s) should be given the responsibility for computer security?
- Despite there are best practices that organizations can refer to evaluate their security status;

- **But, there is lack of international standards (clear guidance) with which a State or region can measure its current security status.**

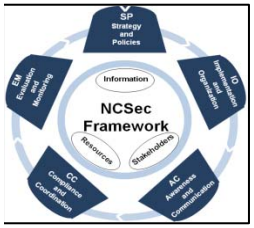


Introduction (2/2)

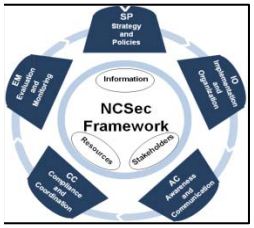
The main objective of this presentation is to propose a Roll Model of National Cybersecurity Management System (NCSecMS), which is a global framework that best responds to the needs expressed by the ITU Global Cybersecurity Agenda (GCA).

This global framework consists of 4 main components:

- NCSec Framework;
- Maturity Model;
- Roles and Responsibilities; and
- Implementation Guide.



2 – National Cybersecurity Management System (NCSecMS)



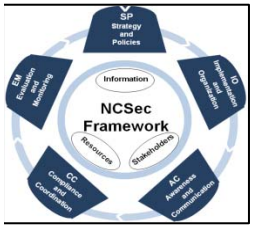
NCSecMS Components

ITU Documents + **ISO 27002** → 1 NCSec Framework → **NCSecFR** — 5 Domains, 34 Processes

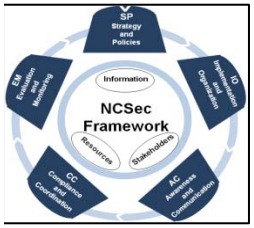
COBIT V4.1 + **NCSec Framework** → 2 Maturity Model → **NCSecMM** — For each Process

National Stakeholders + **NCSec Framework** → 3 Roles & Responsibilities → **NCSecRR** — RACI Chart by Process

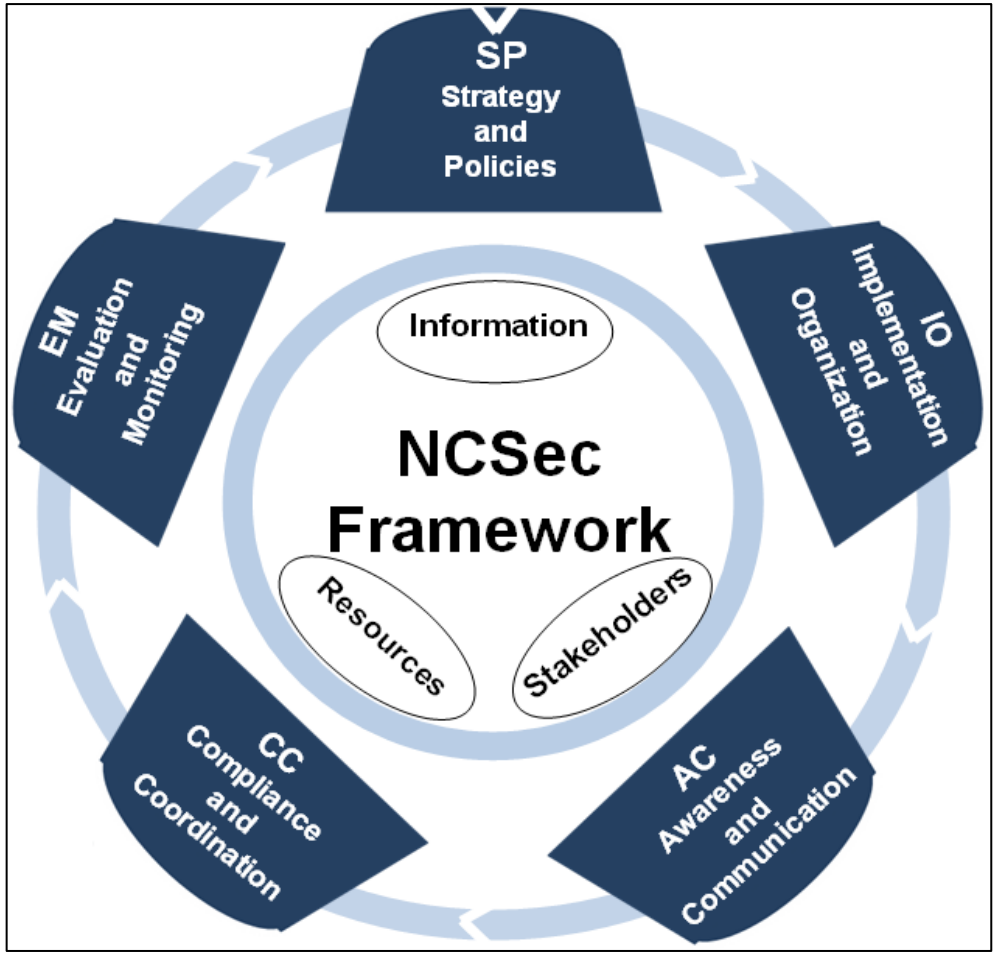
ISO 27003 + **ISO 27001** → 4 Implementation Guide → **NCSecIG** — PDCA

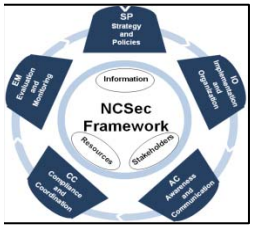


2.1 – National Cybersecurity Framework



NCSec Framework : 5 Domains

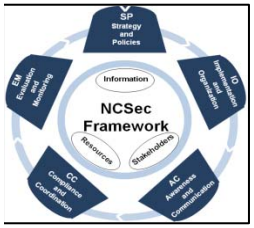




NCSec Framework : 34 processes

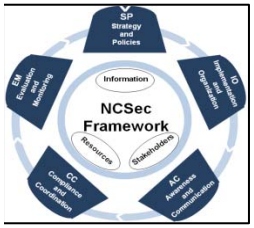
EM4 Nat Govce
IO1 NCC
AC1 GvtLeader
SP1 Cyb Strat
CC1 Coop Multi
IO2 NCA
AC10 NCyb Com
AC2 N Awar
SP2 Lead Inst.
CC2 Coop Ind
EM3 Mech Mon
IO3 N-CERT
AC9 Awer Sol
AC3 Users Syst
SP3 Policies
IO4 Privacy
AC8 Cyb Culture
AC4 COP
SP4 CIIP
CC3 Privat Sect
EM2 Ass Prog
IO5 Law
AC7 R&D
AC5 Capacity
SP5 Stackhldrs
CC4 Mng Incid
EM1 Obsevator
IO6 Institutns
AC6 ContinSce
IO10 IntExpert
IO7 Nat Exper
IO8 Training
IO9 Gov Oper
CC5 PtsContact
CC6 Reg Coop

SP: Strat & Policies
IO: Implem & Organ
AC: Awar & Comm
CC: Complian & Coord
EM: Eval & Monotor



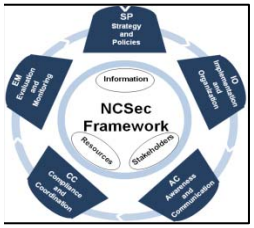
Domain 1: Strategy and Policies (SP)

Proc	Process Description
SP1	**NCSec Strategy** Promulgate & endorse a National Cybersecurity Strategy
SP2	**Lead Institutions** Identify a lead institutions for developing a national strategy, and 1 lead institution per stakeholder category
SP3	**NCSec Policies** Identify or define policies of the NCSec strategy
SP4	**Critical Infrastructures** Establish & integrate risk management for identifying & prioritizing protective efforts regarding NCSec (CIIP)
SP5	**Stakeholders** Identify the degree of readiness of each stakeholder regarding to the implementation of NCSec strategy & how stakeholders pursue the NCSec strategy & policies



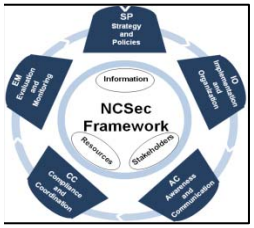
Domain 2: Implementation and Organisation (IO)

Proc	Process Description
IO1	**NCSec Council** Define National Cybersecurity Council for coordination between all stakeholders, to approve the NCSec strategy
IO2	**NCSec Authority** Define Specific high level Authority for coordination among cybersecurity stakeholders
IO3	**National CERT** Identify or establish a national CERT to prepare for, detect, respond to, and recover from national cyber incidents
IO4	**Privacy** Review existing privacy regime and update it to the on-line environment
IO5	**Laws** Ensure that a lawful framework is settled and regularly levelled
IO6	**Institutions** Identify institutions with cybersecurity responsibilities, and procure resources that enable NCSec implementation
IO7	**National Experts and Policymakers** Identify the appropriate experts and policymakers within government, private sector and university
IO8	**Training** Identify training requirements and how to achieve them
IO9	**Government** Implement a cybersecurity plan for government-operated systems, that takes into account changes management
IO10	**International Expertise** Identify international expert counterparts and foster international efforts to address cybersecurity issues, including information sharing and assistance efforts



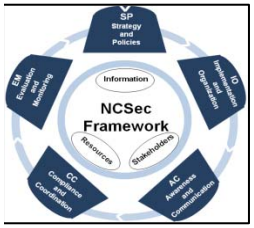
Domain 3: Awareness and Communication (AC)

Proc	Process Description
AC1	**Leaders in the Government** Persuade national leaders in the government of the need for national action to address threats to and vulnerabilities of the NCSec through policy-level discussions
AC2	**National Cybersecurity and Capacity** Manage National Cybersecurity and capacity at the national level
AC3	**Continuous Service** Ensure continuous service within each stakeholder and among stakeholders
AC4	**National Awareness** Promote a comprehensive national awareness program so that all participants—businesses, the general workforce, and the general population—secure their own parts of cyberspace
AC5	**Awareness Programs** Implement security awareness programs and initiatives for users of systems and networks
AC6	**Citizens and Child Protection** Support outreach to civil society with special attention to the needs of children and individual users
AC7	**Research and Development** Enhance Research and Development (R&D) activities (through the identification of opportunities and allocation of funds)
AC8	**CSec Culture for Business** Encourage the development of a culture of security in business enterprises
AC9	**Available Solutions** Develop awareness of cyber risks and available solutions
AC10	**NCSec Communication** Ensure National Cybersecurity Communication



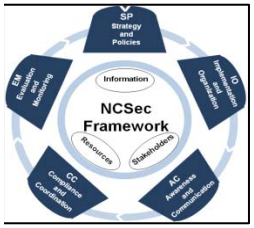
Domain 4 :Compliance and Coordination (CC)

PS	Process Description
CC1	**<u>International Compliance & Cooperation</u>** Ensure regulatory compliance with regional and international recommendations, standards …
CC2	**<u>National Cooperation</u>** Identify and establish mechanisms and arrangements for cooperation among government, private sector entities, university and ONGs at the national level
CC3	**<u>Private sector Cooperation</u>** Encourage cooperation among groups from interdependent industries (through the identification of common threats) Encourage development of private sector groups from different critical infrastructure industries to address common security interest collaboratively with government (through the identification of problems and allocation of costs)
CC4	**<u>Incidents Handling</u>** Manage incidents through national CERT to detect, respond to, and recover from national cyber incidents, through cooperative arrangement (especially between government and private sector)
CC5	**<u>Points of Contact</u>** Establish points of contact (or CSIRT) within government, industry and university to facilitate consultation, cooperation and information exchange with national CERT, in order to monitor and evaluate NCSec performance in each sector

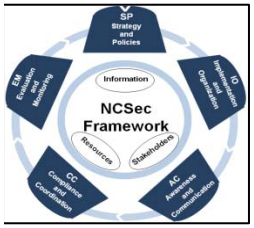


Domain 5: Evaluation and Monitoring (EM)

Proc	Process Description
EM1	**NCSec Observatory** Set up the NCSec observatory
EM2	**Mechanisms for Evaluation** Define mechanisms that can be used to coordinate the activities of the lead institution, the government, the private sector and civil society, in order to monitor and evaluate the global NCSec performance
EM3	**NCSec Assessment** Assess and periodically reassess the current state of cybersecurity efforts and develop program priorities
EM4	**NCSec Governance** Provide National Cybersecurity Governance

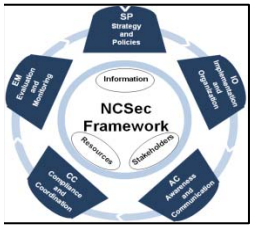


2.2 – Maturity Model

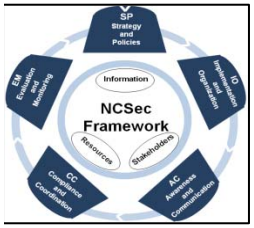


Maturity Model

PS	Process Description	Level 1	Level 2	Level 3	Level 4	Level 5
SP1	Promulgate & endorse a National Cybersecurity Strategy	Recognition of the need for a National strategy	NCSec is announced & planned.	NCSec is operational for all key activities	NCSec is under regular review	NCSec is under continuous improvement
SP2	Identify a lead institution for developing a national strategy, and 1 lead institution per stakeholder category	Some institutions have an individual cyber-security strategy	Lead institutions are announced for all key activities	Lead institutions are operational for all key activities	Lead institutions are under regular review	Lead institutions are under continuous improvement
SP3	Identify or define policies of the NCSec strategy	Ad-hoc & Isolated approaches to policies & practices	Similar & common processes announced & planned	Policies and procedures are defined, documented, operational	National best practices are applied &repeatable	Integrated policies & procedures Transnational best practice
SP4	Establish & integrate risk management process for identifying & prioritizing protective efforts regarding NCSec (CIIP)	Recognition of the need for risk management process in CIIP	CIIP are identified & planned. Risk management process is announced	Risk management process is approved & operational for all CIIP	CIIP risk management process is complete, repeatable, and lead to CI best practices	CIIP risk management process evolves to automated workflow & integrated to enable improvement



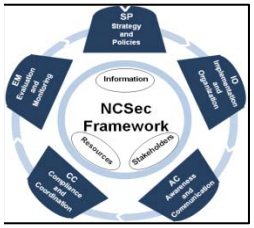
2.3 - Roles and Responsibilities
(RACI Chart)



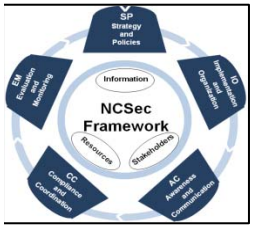
RACI Chart / Stakeholders

		Government	Head of Gov	Nat Cyb Coun	Legisl Auth	ICT Authority	Min of Int	Min of Def	Min of Fin	Min of Edu	Nat Cyb Auth	Civil Soc	Trade Union	Private Sect	Academia	Critical Infras	Nat CERT	CSIRTs	
SP1	**NCSec Strategy** Promulgate & endorse a National Cybersecurity Strategy	I	A	C	C	R	C	C	C	I	I	R		I	I		I	
SP2	**Lead Institutions** Identify a lead institutions for developing a national strategy, and 1 lead institution per stakeholder category	I	I	A	C	R	C	C	I	I		R		C	C	C	C	
SP3	**NCSec Policies** Identify or define policies of the NCSec strategy			A	C	R	C	I	C	I		R			I		I	
SP4	**Critical Infrastructures** Establish & integrate risk management for identifying & prioritizing protective efforts regarding NCSec (CIIP)			A		R	R	C	I			R				C	R	I

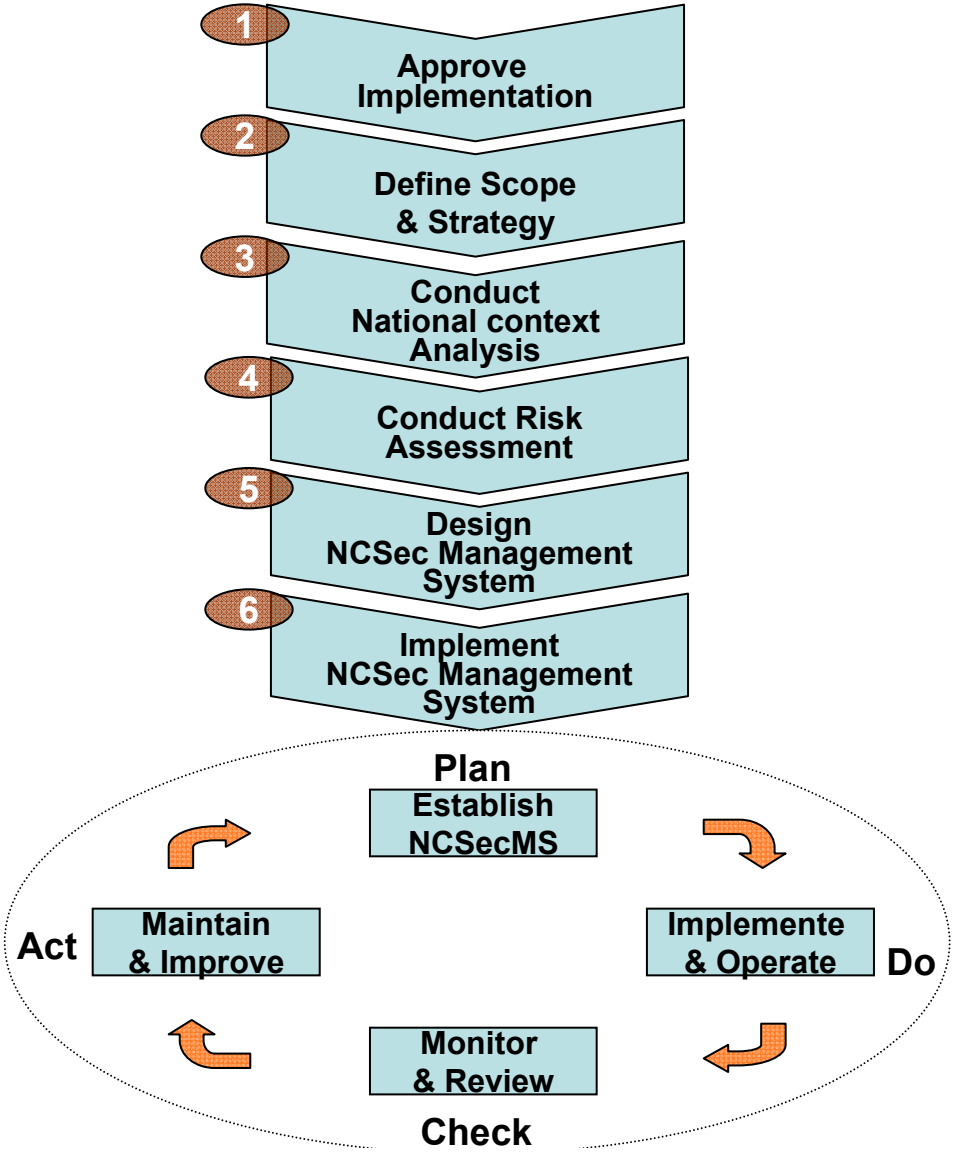
R = Responsible, A = Accountable, C = Consulted, I = Informed

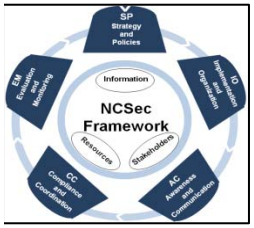


2.4 – Implementation Guide



NCSec Implementation Guide & PDCA



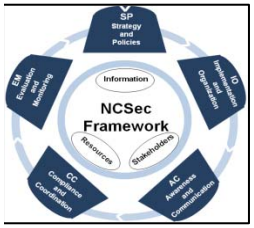


NCSec

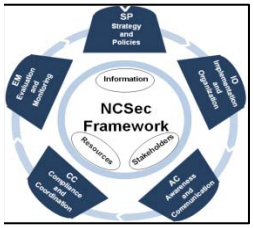
High Level Decision Makers

Implementation Guide

	HL Awarness	1 Approve Implementation	HL Commitment
HL Commitment	NCSec Framework	2 Define Scope & Strategy	NCSec Strategy
NCSec Strategy	NCSec Maturity Model	3 Conduct National Context Analysis	Nat. Inf Sec Assessment
Nat. Inf Sec Assessment	NCSec Framework	4 Conduct Risk Assessment	Processes Selected
Processes Selected	NCSec RACI Chart	5 Design NCSec Managnt System	NCSec Managnt Syst
NCSecIG	ISO 27001	6 Implement NCSec Managnt System	NCSec MS Implemt Prg



3 – Research Papers



ACM Publication

PORTAL

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ○ The ACM Digital Library ◉ The Guide SEARCH

THE GUIDE TO COMPUTING LITERATURE

Feedback

NCSec: a national cyber security referential for the development of a code of practice in national cyber security management

Full text Pdf (137 KB)

Source **ACM International Conference Proceeding Series; Vol. 351** archive
Proceedings of the 2nd International Conference on Theory and Practice of Electronic Governance table of contents
Cairo, Egypt
SESSION: Infrastructure table of contents
Pages 373-380
Year of Publication: 2008
ISBN:978-1-60558-386-0

Authors Mohamed Dafir Ech-cherif el Kettani University Mohammed V -- Souissi, Rabat, Morocco
Taieb Debbagh Commerce and New Technologies, Rabat, Morocco

Publisher ACM New York, NY, USA

Bibliometrics Downloads (6 Weeks): 39, Downloads (12 Months): 39, Citation Count: 0

Additional Information: abstract references index terms

Tools and Actions: Review this Article
Save this Article to a Binder Display Formats: BibTex EndNote ACM Ref

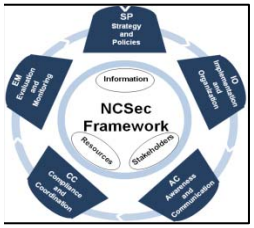
DOI Bookmark: Use this link to bookmark this Article: http://doi.acm.org/10.1145/1509096.1509174
What is a DOI?

ABSTRACT

Governments worldwide have faced computer security challenges. These challenges are serious in a context where there is an absence of appropriate organizational and institutional structures to deal with incidents. But more important which agency or agencies should be given the responsibility for computer security, is the point that some national leadership should be designated to ensure that computer security will receive government-wide attention. Therefore, sectors and lead agencies should assess the reliability, vulnerability, and threat environments of the infrastructures and employ appropriate protective measures and responses to safeguard them.

The ITU has already proposed a whole process for developing and implementing a national Cyber security plan [1]. This process requires a comprehensive strategy that includes an initial broad review of the adequacy of current national practices, and consideration of the role of all stakeholders.

This paper proposes a global framework answering the former needs expressed by the ITU. It is intended to present « ncsec », the « National Cyber security Referential », which is a guide for the development of « National Cyber security standards and effective Cyber security Management » for the creation of National Organizational Structures and Policies on Cybercrime at the national level, in order to help building regional and international cooperation for watch, warning, and incident response. We can notice a great relationship between our proposal and ISO27002 standard.



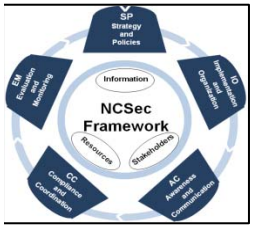
ECEG 2009
9th European Conference on e-Government
Westminster Business School, University of Westminster, London, UK
29-30 June 2009

NCSecMM: A National Cyber Security Maturity Model for an Interoperable "National Cyber Security" Framework

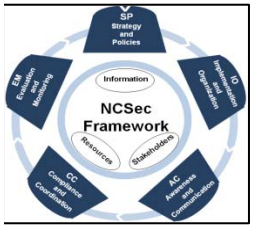
Taïeb Debbagh, Mohamed Dafir Ech-Cherif El Kettani

Abstract: Security Maturity Model is a systematic approach that replaces traditional security metrics. There is more than one Security Maturity Model (SMM, COBIT, CERT/CSO, ISM3), and each of them has only five levels of maturity, providing the blueprint for a complete security program, telling management the order in which to implement security elements (ISM3 Consortium 2007), and leading toward the use of best practice standards (e.g., BS 17799). But very few of them are dedicated to National Cybersecurity.

We propose in this paper a "National CyberSecurity Maturity Model", that will make it possible to evaluate the security of a country or a whole region, making thus comparisons between them, and pointing out its forces and threats.



4 – Morocco Case



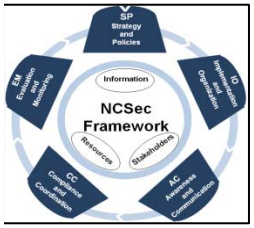
Morocco ICT Strategic Plan

5 Priorities

1. **Ensuring SMEs ICT equipment (Computerization of SMEs) to increase their productivity and contribute to their development;**
2. **Promoting Broadband Internet access (to be accessible for all citizens) and knowledge access;**
3. **Implementing an ambitious e-government programme that contributes to the efficiency and effectiveness of the Administration and Local Collectivities;**
4. **Exploiting the offshore to rapidly develop the export industry and create jobs;**
5. **Promoting the entrepreneurship and the creation of Areas of Excellence in ICT.**

3 Supporting measures

- **Implement Cyber-confidence requirements;**
- **Review/formulate HR policies to build ICT capabilities;**
- **Set up a global governance structure, a changing policy, and an ICT observatory.**



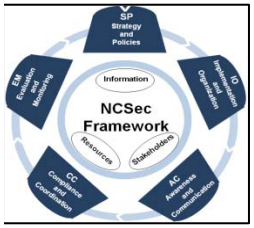
Cybersecurity Roadmap

Objectives:

Set up a National Cybersecurity policy that aims to ensure business trust, enhance security capabilities, and secure information critical infrastructures.

- Ensure Networks Security
- Ensure Information Systems Security
- Secure Electronic Data Exchange
- Ensure Private Data Protection
- Lead Fight Against Cybercrime

4 Sub-programmes have been identified to achieve these objectives



4 Sub-Programmes

Legal and Regulatory Framework

- Upgrade/update the legal and regulatory framework in order to face the Cybersecurity challenges and harmonize it with the partners countries

Structures

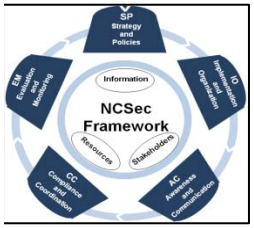
- Establish necessary Entities that will be in charge of implementing the national Cybersecurity policy

Development

- Promote the development of security capabilities

Awareness and Communications

- Arise awareness of the citizens, enterprises and administration on the Cybersecurity and cyberconfidence issues



Thank you for your attention

Contact Information:
Phone : +212 537 26 86 21/22
Email : t.debbagh@technologies.gov.ma