การเตรียมความพร้อมในเรื่องทักษะทางด้านความมั่นคงปลอดภัยสารสนเทศ ในยุคดิจิทัล ให้แก่ข้าราชการและบุคลากรภาครัฐ

(Panel Discussion)

ชุดคำถาม

- จะเรียนรู้จากประสบการณ์อะไร อย่างไร?
- จะบูรณาการแนวคิดวิธีการใหม่ด้านทักษะดิจิทัลและ Cyber sec. กับสังคมโครงสร้างเดิมได้อย่างไร?
- จะสร้างภูมิคุ้มกัน และ จัดการกับการพัฒนาทักษะ Cyber sec. อย่างไร?
-
- จะจัดการทักษะในเทคโนโลยีที่คลุมเครืออย่างไร?
- ทักษะด้าน Cyber security ควรจัดวางการพัฒนาบุคลากรไว้อย่างไร?

จะเรียนรู้จากประสบการณ์อะไร อย่างไร?

- ตระหนก vs. ตระหนัก
  - —Computer: Year 2000
  - —Telecom: ISDN, ATM, Data network & Voice over Internet,..
  - —Security broken: 1G, 2G, 3G+,...
    - (มาตรฐาน ได้รับการออกแบบไว้ล่วงหน้านาน นับสิบปี ของแต่ละ generation)
  - —Ambiguous Tech: blockchain, sdn/nfv, ..

จะเรียนรู้จากประสบการณ์อะไร อย่างไร?

- กรณีเปรียบเทียบ: (นักดับเพลิงป่า กับ เครื่องมือดับเพลิงประสิทธิภาพสูงมาก)
- กรณีเปรียบเทียบ: (เหล้าเดิม ในขวดใหม่)
  - (Security) {(Physical) (Computer) (Information) (Cyber) …}
    - {(Confidential) (Integrity) (authentication)} {(non-repudiation)}
  - แก่นของ Digital transformation
  - แก่นของ Design thinking & Innovation
- สภาพแวดล้อม วัฒนธรรม สังคมขององค์กร

- **Computer security**
  - the protection of computer systems and information from harm, theft, and unauthorized use.
  - as a part of information security
- **Network security**
  - is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies.
  - consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.
- **Information security** (Infosec.)
  - is a relative term. It is effective only when it is balanced with business requirements, cost, and risk mitigation.
  - means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
  - is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

- **Cyber security**
  - Refer to Information security
  - (superset of Information security)
  - (ability to control) {(access to network system) (information)} (in effective)
    - {(prevent) (detect) (response)}
    - {(people) (process) (technology)}
    - {(confidentially) (integrity) (availability)}

- Cyber security
  - is the protection of internet-connected systems, including hardware, software and data, from cyber attacks.

Availability, Integrity and Secrecy of information systems and networks in the face of attacks, accidents and failures with the goal of protecting operations and assets

จะบูรณาการแนวคิดวิธีการใหม่ด้านทักษะดิจิทัล และ Cyber security กับสังคมโครงสร้างเดิมได้อย่างไร?

- ให้ความสำคัญ แก่นทฤษฎี และ

  แนวคิด **TEIS** (Tech, Eco, Innovation, Shared value):

  —**Telecom: ISDN, ATM, Data network &**

  Voice over Internet,..

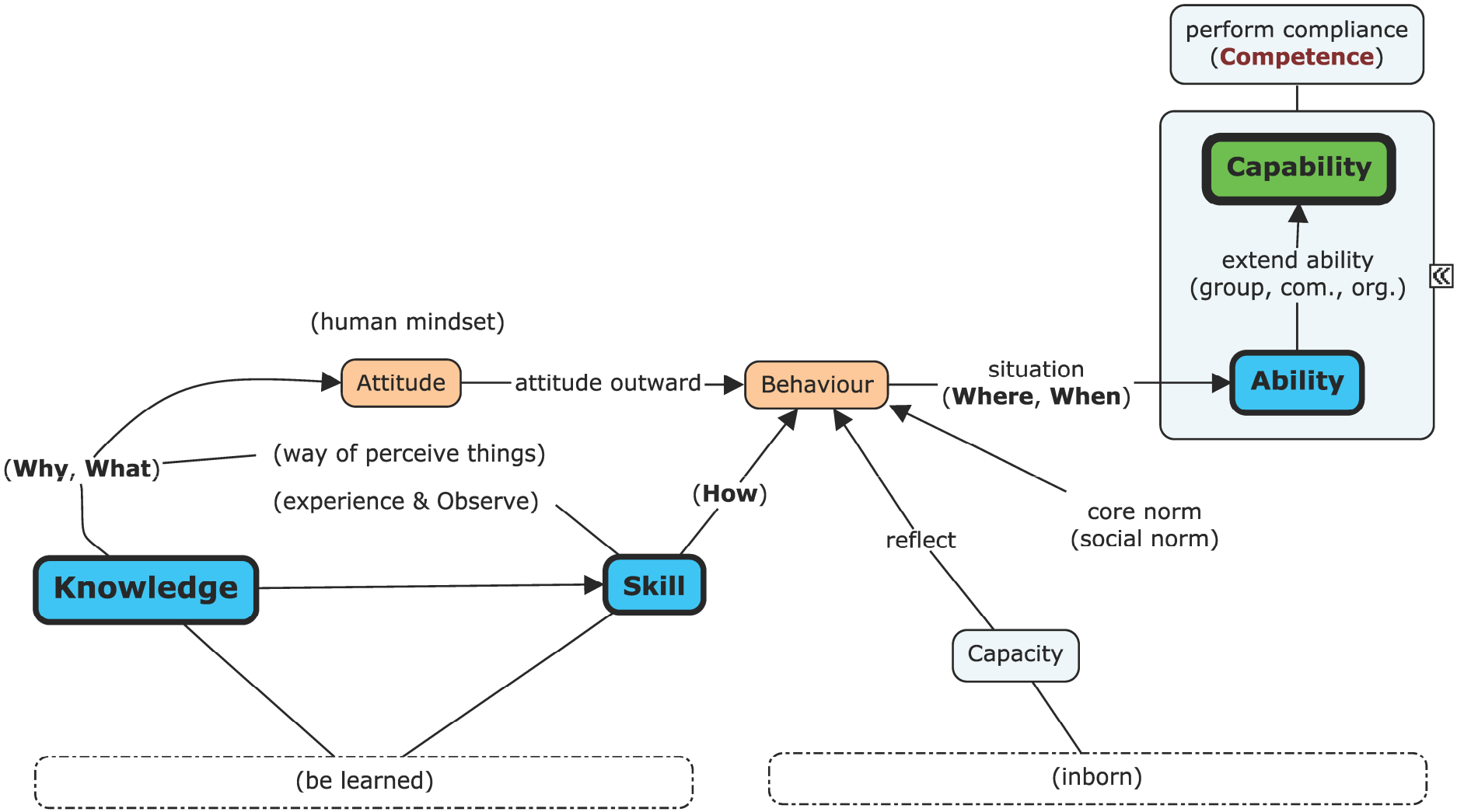
- **Digital Tsunami** กับการเตรียมความพร้อมและปรับตัว

- **(Industrial) Open platform and Cloud service**


Intelligent analytics
Things
Trusting
Telecom advance
Cloud
DIGITAL
TSUNAMI
Company
Life
THINGs
Life
Company
Company

จะสร้างภูมิคุ้มกัน และ จัดการกับการพัฒนาทักษะ Cyber security อย่างไร?

- Relative competence map



Relative Competence

จะจัดการทักษะในเทคโนโลยีที่คลุมเครืออย่างไร?

- **Digital concepts:**

  (Complexity is Simplicity) & (Insight Simplicity is Complexity)

- **Simplified Control**
  - กำหนด **Core of Business and Service (policy)**
  - ลำดับความสำคัญของปัญหา และแบ่งระยะโครงการ ระดับการพัฒนาทักษะ
  - จัดการกับความเสี่ยง และการกระจายความเสี่ยง (ทุกคนใช้รถยนต์ แต่ก็ใช่ว่าจะต้องผลิตรถยนต์เป็นกันทุกคน)
- **Standard & Guideline** สำคัญสำหรับ การสร้างฐานภูมิคุ้มกันให้กับการดำเนินองค์กรที่ดี มีคุณภาพ
- ต.ย. กรณี **Ambiguous Tech: Blockchain**

ทักษะด้าน Cyber security ควรจัดวางการพัฒนาบุคลากรไว้อย่างไร?

Conclusion

- Cyber security
  - "Availability, Integrity and Secrecy"
  - of information systems and networks
  - in the face of attacks, accidents and failures
  - with the goal of protecting operations and assets"
- Organization must have **clear objectives** first and then can create and carry out a **security policy**.

Can’t manage what Can’t measure.

No one-size-fits-all strategy.

If you measure compliance with standards, you will get compliance with standards.

But, will not get security goal achievement

ตัวอย่าง Competency maps

<table>
<tr><th colspan="6">Business-Service</th></tr>
<tr><td rowspan="2">Advance Business Modelling</td><td>Advance Risk Mngt.</td><td>Financial Mngt.</td><td>Stakeholder Relationship Mngt.</td><td rowspan="2">Technical Advising</td><td rowspan="3">Client Service Mngt.</td></tr>
<tr><td>Business Risk Mngt.</td><td>Service Level Mngt.</td><td>Stakeholder Mngt.</td></tr>
<tr><td rowspan="2">Business Modelling</td><td>Business Continuity Planning</td><td>Financial Maintaining</td><td>Business Process Testing</td><td rowspan="2">Technical Supporting</td></tr>
<tr><td colspan="3">Business Analysis</td></tr>
<tr><td>Business Modelling Concepts</td><td colspan="3">Risk Mngt. Concepts</td><td colspan="2">Customer Services and Supporting</td></tr>
</table>

Skill Level 3
Skill Level 2
Skill Level 1

<table>
<tr><th colspan="4">Strategic-Architecture</th></tr>
<tr><td>Sustainability Strategy</td><td>Solution Architecture</td><td>Managing Risk</td><td>Earned Value Mngt.</td></tr>
<tr><td>EA Framework and Methodology</td><td>Alternatives Analysis</td><td>Culture and Communication</td><td>Architecture Transition Mngt.</td></tr>
<tr><td>Business Technology Strategy</td><td>Technology Merging</td><td>EA establishment</td><td rowspan="3">EA Project Mngt.</td></tr>
<tr><td>EA Critical Success Factors</td><td colspan="2">Architecture Implementation</td></tr>
<tr><td colspan="2">Business IT Architecture</td><td>IT Architecture</td></tr>
</table>

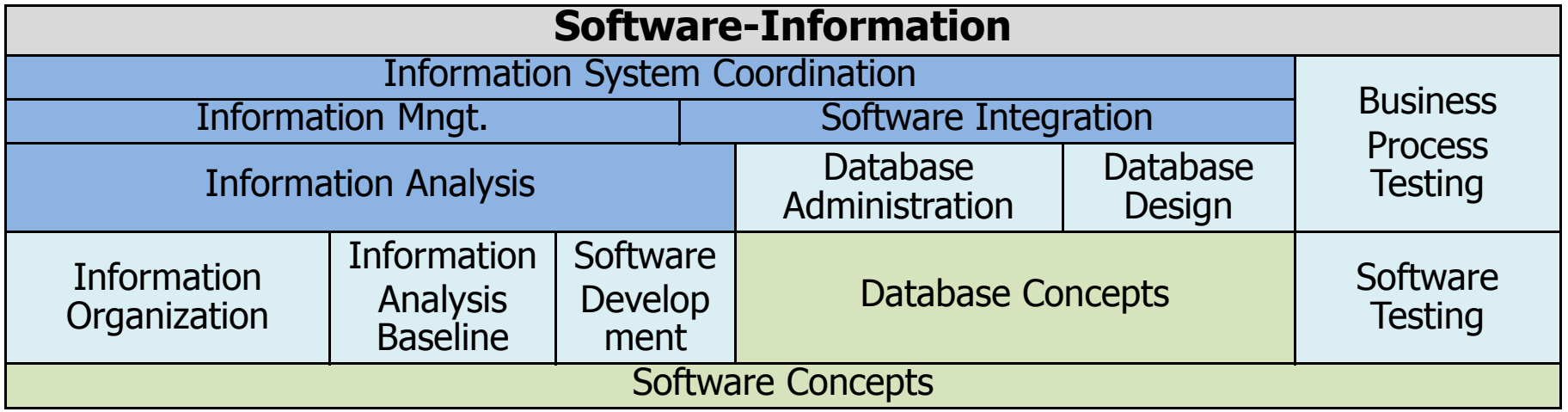
Skill Level 3
Skill Level 2
Skill Level 1

<table>
<tr><th colspan="8">Program/Project Management (Mngt.)</th></tr>
<tr><td colspan="2">Advance Project Mngt.</td><td>Project Data Service</td><td>Project Consultancy</td><td colspan="2">Project Conformance</td><td>Benefit Mngt.</td><td rowspan="2">Advance Change Mngt.</td><td rowspan="2">ICT Portfolio and Project Support</td></tr>
<tr><td rowspan="3">Project Mngt.</td><td>Cost Mngt.</td><td>Capacity Mngt.</td><td>User Experience Analysis</td><td>Problem Mngt.</td><td colspan="2">Service Level Design and Mngt.</td></tr>
<tr><td>Time Mngt.</td><td rowspan="2">Availability Mngt.</td><td>User Analysis</td><td>Release Mngt.</td><td rowspan="2">Advance Quality Assurance</td><td>Quality Mngt.</td><td rowspan="2">Change Mngt.</td><td rowspan="2">ICT and Project Support</td></tr>
<tr><td>Requirement Mngt.</td><td>Communication Mngt.</td><td>Process Release and Deployment</td><td>Project Quality Mngt.</td></tr>
<tr><td rowspan="2">PM Concepts</td><td>Scope Mngt.</td><td>Asset Mngt.</td><td>HR Mngt.</td><td>Problem Solving</td><td>Quality Assurance</td><td>Quality standards</td></tr>
<tr><td>Requirement Service Concepts</td><td>Service Transition</td><td colspan="2">Human Factor Analysis and Integration</td><td colspan="2">Software Quality Concepts</td><td>Change Mngt. Concepts</td></tr>
</table>

Skill Level 3
Skill Level 2
Skill Level 1

<table>
<tr><th colspan="5">Security</th></tr>
<tr><td colspan="5">Information Assurance</td></tr>
<tr><td rowspan="2">Information Security</td><td colspan="4">Advance Security administration</td></tr>
<tr><td>Security Access</td><td>Security Admin</td><td>Cryptography Engineering</td><td>Public Key Infrastructure</td></tr>
<tr><td>Information Security Concepts</td><td colspan="2">Roles in Security</td><td>Security Baselines</td><td>Physical Security Protection</td></tr>
<tr><td colspan="5">Security Concepts</td></tr>
</table>

Skill Level 3
Skill Level 2
Skill Level 1



Skill Level 3
Skill Level 2
Skill Level 1

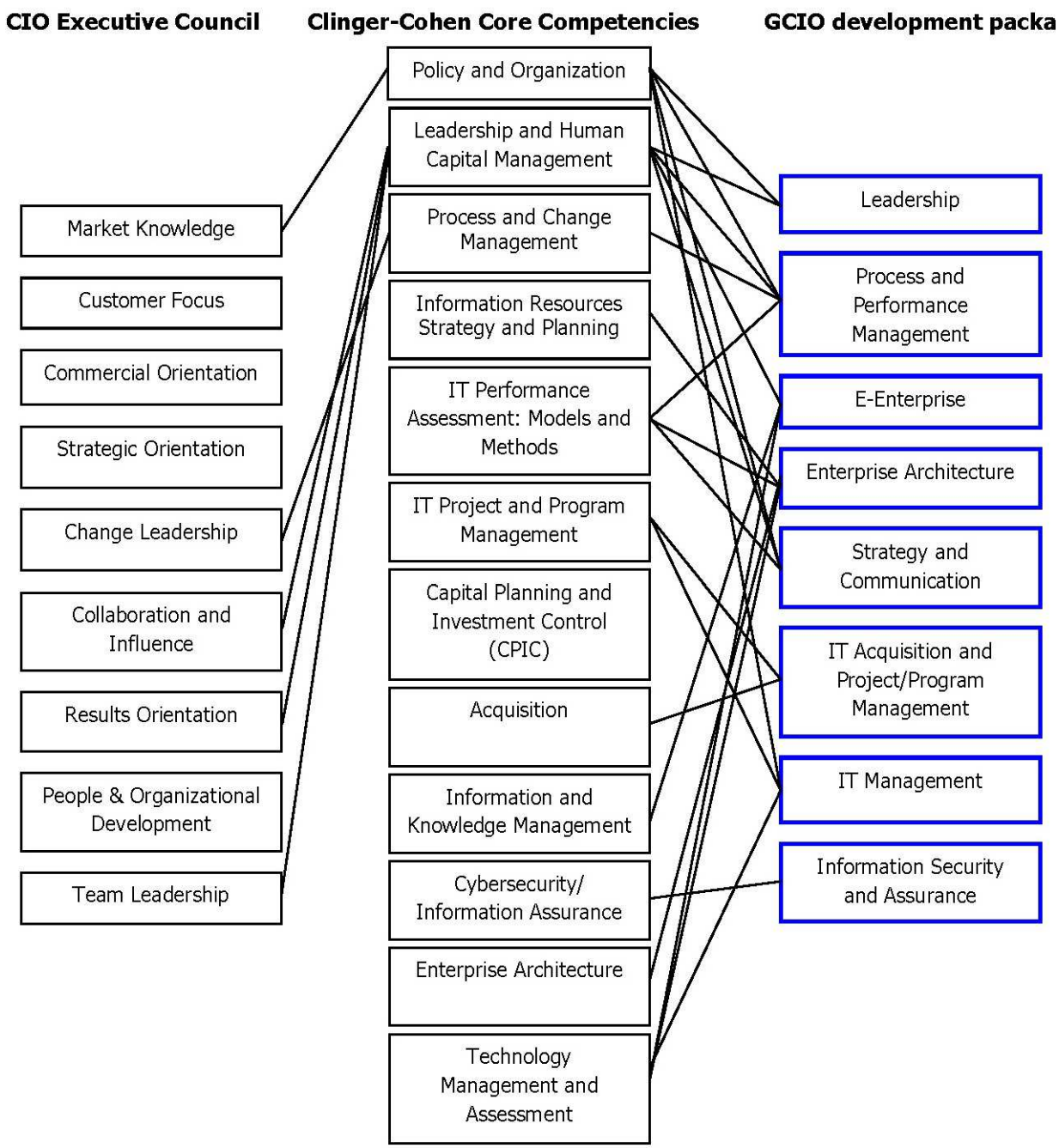
<table>
<tr><th colspan="4">System-Network</th></tr>
<tr><td colspan="2">Quality Service Mngt.</td><td colspan="2">Advance Network Integration</td></tr>
<tr><td>Data Traffic Control</td><td rowspan="2">System Design</td><td>System Integration</td><td>Advance Configuration Mngt.</td></tr>
<tr><td rowspan="2">Standards and Protocols</td><td>Storage Mngt.</td><td>Configuration Mngt.</td></tr>
<tr><td colspan="2">System Design Concepts</td><td>Configuration Mngt. Concepts</td></tr>
<tr><td colspan="4">Network fundamentals</td></tr>
</table>

Skill Level 3
Skill Level 2
Skill Level 1

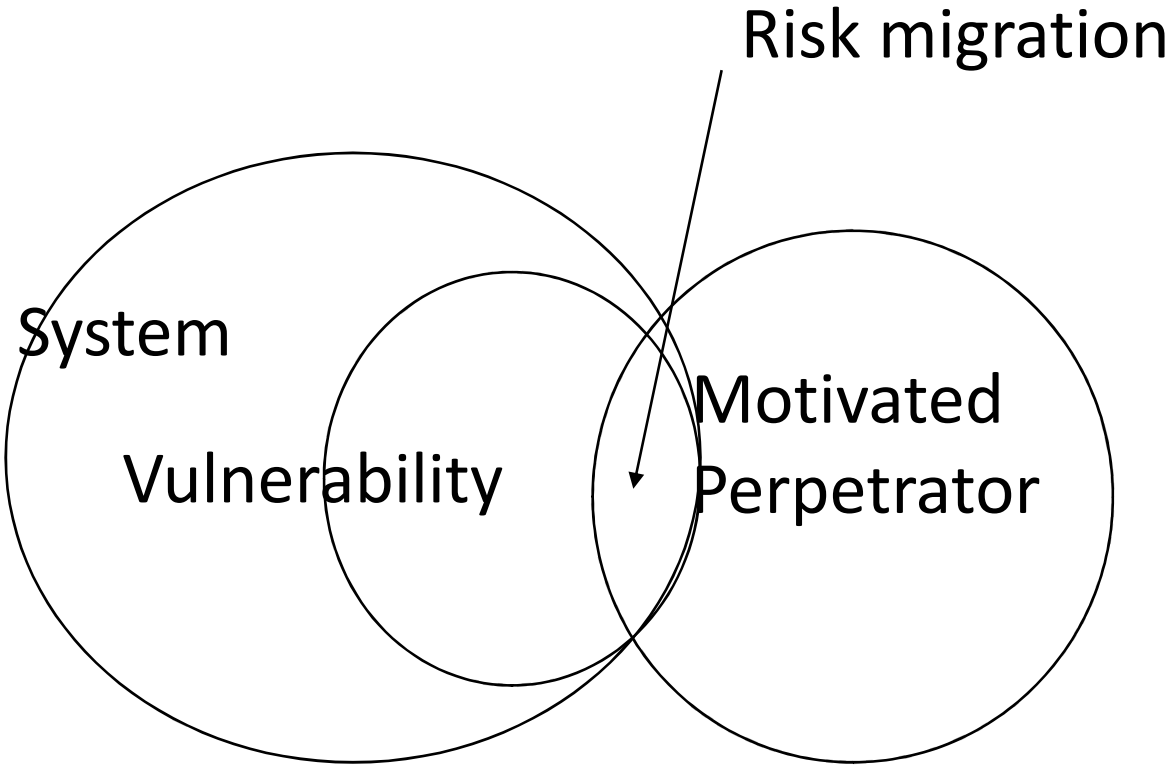
FA-XXX12	**ความปลอดภัย** (Security/Information and Application Protection)	
	มีความรู้ความสามารถจนมั่นใจได้ว่าสามารถจัดการความปลอดภัยในทางเทคนิคและการป้องกันระดับบริษัทให้สามารถดำเนินธุรกรรมของบริษัทได้อย่างต่อเนื่องผ่านระบบโครงสร้างบริการรพื้นฐานสารสนเทศอย่างปลอดภัย ด้วยการจัดให้มีนโยบายความปลอดภัยและแนวทางปฏิบัติ รวมถึงการใช้เครื่องมือเพื่อการป้องกันอย่างเหมาะสม รวมถึงการจัดให้มีความพร้อมและสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง ความรมพร้อมในการกู้คืนระบบไอที การประเมินและการปรับปรุงความปลอดภัยเป็นประจำ	
ระดับชำนาญ 4 (Value Added Level)	M	- การนำและจัดให้มีการประเมินความเสี่ยง และการจัดการควบคุมความปลอดภัย
	I	- แสดงให้เห็นถึงความเชี่ยวชาญที่หลากหลายในศาสตร์ของความปลอดภัย - แสดงให้เห็นถึงมีความรู้ใน กฎหมาย ข้อบังคับ และนโยบายความปลอดภัย และการนำไปสู่มาตรฐานวิธีปฏิบัติ - มีความชำนาญการใช้เครื่องมือและซอฟต์แวร์เกี่ยวกับการรักษาความปลอดภัย - การจัดการลดภัยคุกคามประเภทต่าง ๆ ในภาพรวมความปลอดภัยของบริษัท - การให้คำปรึกษา การให้ข้อเสนอแนะสำหรับกลยุทธ์การรักษาความปลอดภัยของบริษัท - การนำการพัฒนานโยบายความปลอดภัยและมาตรฐานการปฏิบัติของบริษัท - การนำสู่การปฏิบัติในทุกระดับพนักงาน รวมถึงการให้คำปรึกษาด้านอื่น
	E	- การนำและจัดให้มีการประเมินความเสี่ยง และการจัดการควบคุมความปลอดภัย
ระดับชำนาญ 3 (Improved Quality Level)	I	- แสดงให้เห็นถึงความเชี่ยวชาญที่หลากหลายในศาสตร์ของความปลอดภัย - แสดงให้เห็นถึงมีความรู้ในนโยบายความปลอดภัยและการนำไปสู่มาตรฐานวิธีปฏิบัติ - มีความชำนาญการใช้เครื่องมือและซอฟต์แวร์เกี่ยวกับการรักษาความปลอดภัย - การนำ การประเมินความเสี่ยง (risk assessment) - การปฏิบัติเกี่ยวกับการจัดการภายคุกคามและเหตุการณ์ที่ก่อให้เกิดผลกระทบรุนแรง - การปฏิบัติเกี่ยวกับการบุกรุก (intrusion) ในระดับเหตุการณ์ที่มีผลกระทบรุนแรง
	E	- การประเมินและการจัดการควบคุมความปลอดภัย
ระดับชำนาญ 2 (Maintenance Level)	I	- การปฏิบัติตามแผนการทดสอบความปลอดภัย - การปฏิบัติเกี่ยวกับการจัดการภายคุกคามทั่วไป - การให้การรับรองความปลอดภัย (security certificagtion) - การให้คำแนะนำการปฏิบัติตามแผน DRP (diaster recovery planning) - การร่วมปฏิบัติ การทดสอบ DRP - การให้คำแนะนำ การป้องกันความปลอดภัย - การปฏิบัติตามวิธีปฏิบัติมาตรฐานที่กำหนด
ระดับชำนาญ 1 (Operartion Level)	I	- การแสดงให้เห็นถึงความตระหนัก ความจำเป็นและความต้องการให้มีมาตรฐานความปลอดภัย - การแสดงให้เห็นถึงความตระหนัก ความจำเป็นในนโยบายการให้การรับรอง (certification policies) - การแสดงให้เห็นถึงความตระหนัก ความจำเป็นในความเป็นส่วนตัวและวิธีการปฏิบัติการจัดการข้อมูล - การแสดงให้เห็นถึงความเข้าใจในหลักการของความปลอดภัยในสารสนเทศและสถาปัตยกรรมของบริษัท

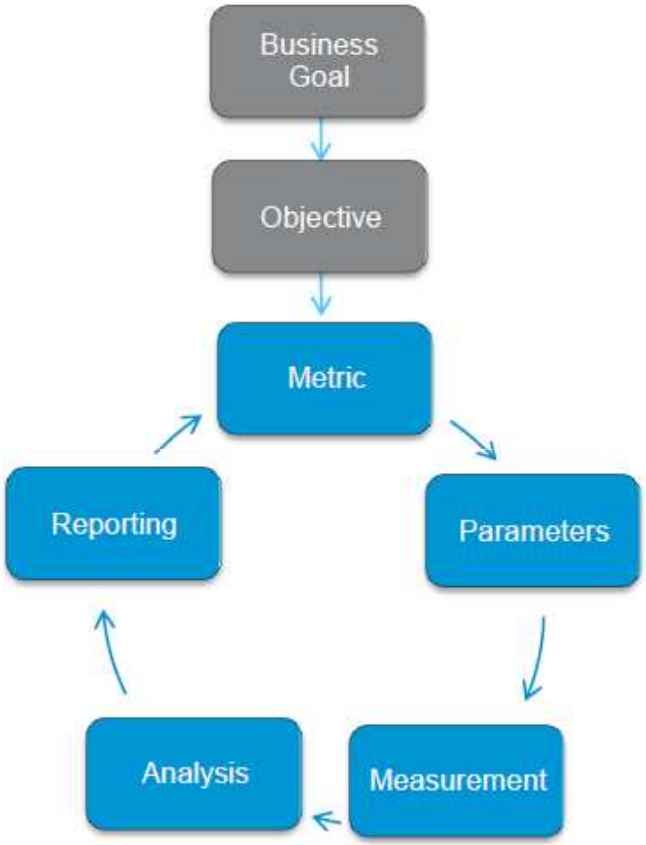
FA-XXX12	**การทดสอบ** (Testing)	
	มีความรู้ความสามารถในการทดสอบอุปกรณ์ทั้งฮาร์ดแวร์และซอฟต์แวร์อย่างเป็นระบบวิธีปฏิบัติ ตั้งแต่ขั้นการแยกทดสอบ จนถึงการรวมการทดสอบทั้งระบบ	
ระดับชำนาญ 4 (Value Added Level)	M	- การจัดกาการทดสอบรวมทั้งระบบ
	D	- การกำหนดมาตรฐานวิธีปฏิบัติสำหรับวัฐจักรการทดสอบ - การออกแบบวิธีการทดสอบ - การพัฒนามาตรฐานการทดสอบ การจัดทำ best practices และการจัดทำนโยบายการทดสอบ
ระดับชำนาญ 3 (Improved Quality Level)	M	- การจัดทำแผนการทดสอบ การจัดทำโครงการ
	D	- การพัฒนามาตรฐานการทดสอบ
	I	- การดำเนินการตรวจสอบ การทดสอบตามวิธีปฏิบัติมาตรฐาน - มีความเข้าใจถึงผลกระทบในส่วนของระบบที่สัมพันธ์กันจากการทดสอบที่เกิดขึ้น - การทดสอบ อนุกรมการทดสอบรูแบบต่าง ๆ - การทดสอบซอฟต์แวร์ การทดสอบฮาร์ดแวร์ การตรวจสอบอื่น - การทดสอบเครื่องมือทดสอบ - การให้คำแนะนำการใช้เครื่องมือและวิธีการทดสอบ
ระดับชำนาญ 2 (Maintenance Level)	I	- มีความเข้าใจในระบบรวมของการทดสอบ เช่น วิธีการ กระบวนการ รวมถึงฮาร์ดแวร์และซอฟต์แวร์ - การจัดเตรียม กรณีการทดสอบ และโปรแกรมการทดสอบ (scripts) และเครื่องมือสำหรับการทดสอบ - การทดสอบตามมาตรฐานวิธีปฏิบัติเพื่อการทดสอบ เช่น การทดสอบแบบสุ่ม การทดสอบแบบระบบรวม - การทดสอบและการยืนยันผลการทดสอบ - ความมั่นใจการลดผลกระทบในโปรแกรมคอมพิวเตอร์อื่นจากผลการทดสอบ - การพิจารณาผลตามเอกสารประกอบคู่มือการทดสอบ - การแก้ปัญหาที่อาจเกิดขึ้นขณะการรทดสอบ
ระดับชำนาญ 1 (Operartion Level)	I	- การแสดงให้เห็นถึงความตระหนักถึงหลักการ กระบวนการ และวิธีการปฏิบัติการทดสอบ - การทดสอบและการหาเหตุเสียในโมดุลซอฟต์แวร์ - การทดสอบตามโปรแกรมที่กำหนด (scripts) - การใช้เครื่องมือทดสอบ - การจัดทำรายงานผลการทดสอบ

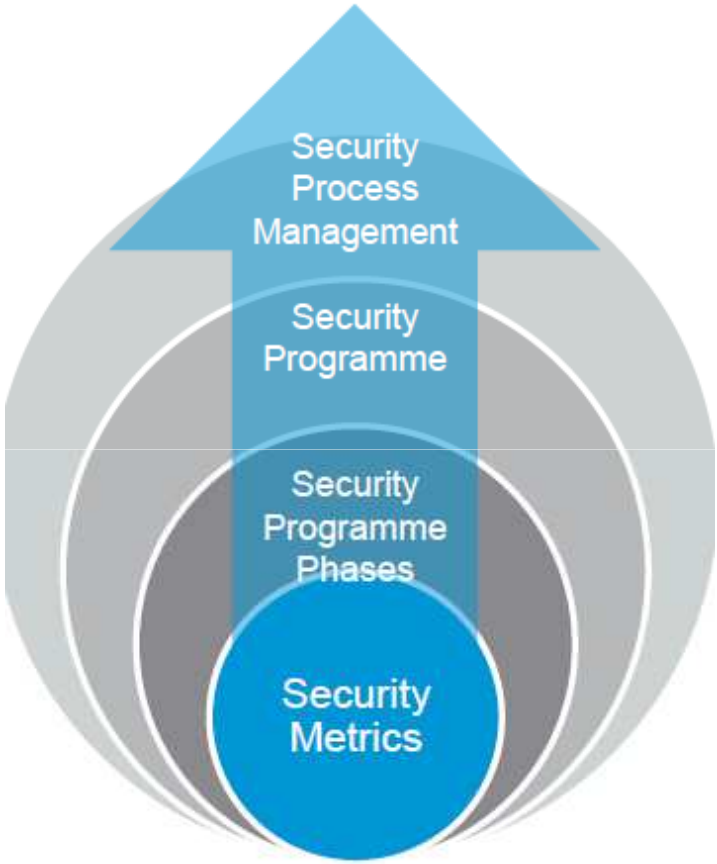
	Chief Information Officer		Digital Forensics Professional		Information Security Officer		IT Security Compliance Officer		IT Security Engineer		IT Security Professional		IT Systems O&M		Physical Security Professional		Privacy Professional		Procurement Professional	
1. การพัฒนาโปรแกรมคอมพิวเตอร์ (Application Development/Support and Maintenance)	I	D																		
	M	E																		
2. งานสถาปัตยกรรม (Architecture)																				
3. การวิเคราะห์ทางธุรกิจ (Business Analysis)																				
4. การออกแบบและจัดการฐานข้อมูล (Database Design and Management)																				
5. โครงสร้างพื้นฐาน/แพลตฟอร์ม (Infrastructure/Platforms)																				
6. การจัดหาและจัดการสินทรัพย์สารสนเทศ (IT Procurement and Asset Management)																				
7. การจัดการแผนงาน (IT Project Management)																				
8. โทรคมนาคม (Telecommunications Network)																				
9. ความปลอดภัย (Security/Information and Application Protection)																				
10.การทดสอบ (Testing)																				
11.การจัดการบริการ (Service Management)																				



รปที่ ๒.๓.๑ เปรียบเทียบการพัฒนา GCIO package บนฐานกรอบแนวทาง Clinger-Cohen และ CIO Executive Cou


Risk migration
System
Vulnerability
Motivated
Perpetrator


Business Goal
Objective
Metric
Parameters
Measurement
Analysis
Reporting

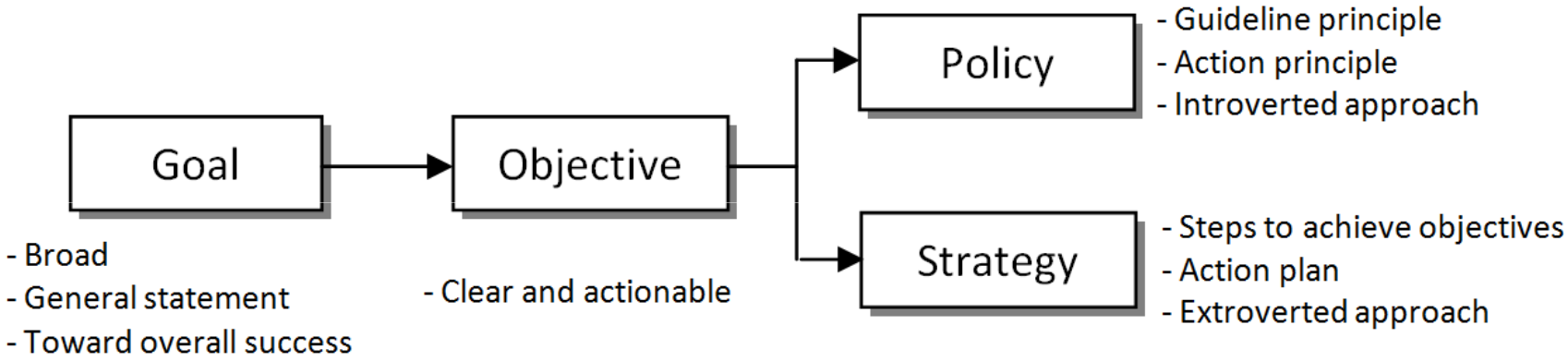

Security Process Management
Security Programme
Security Programme Phases
Security Metrics

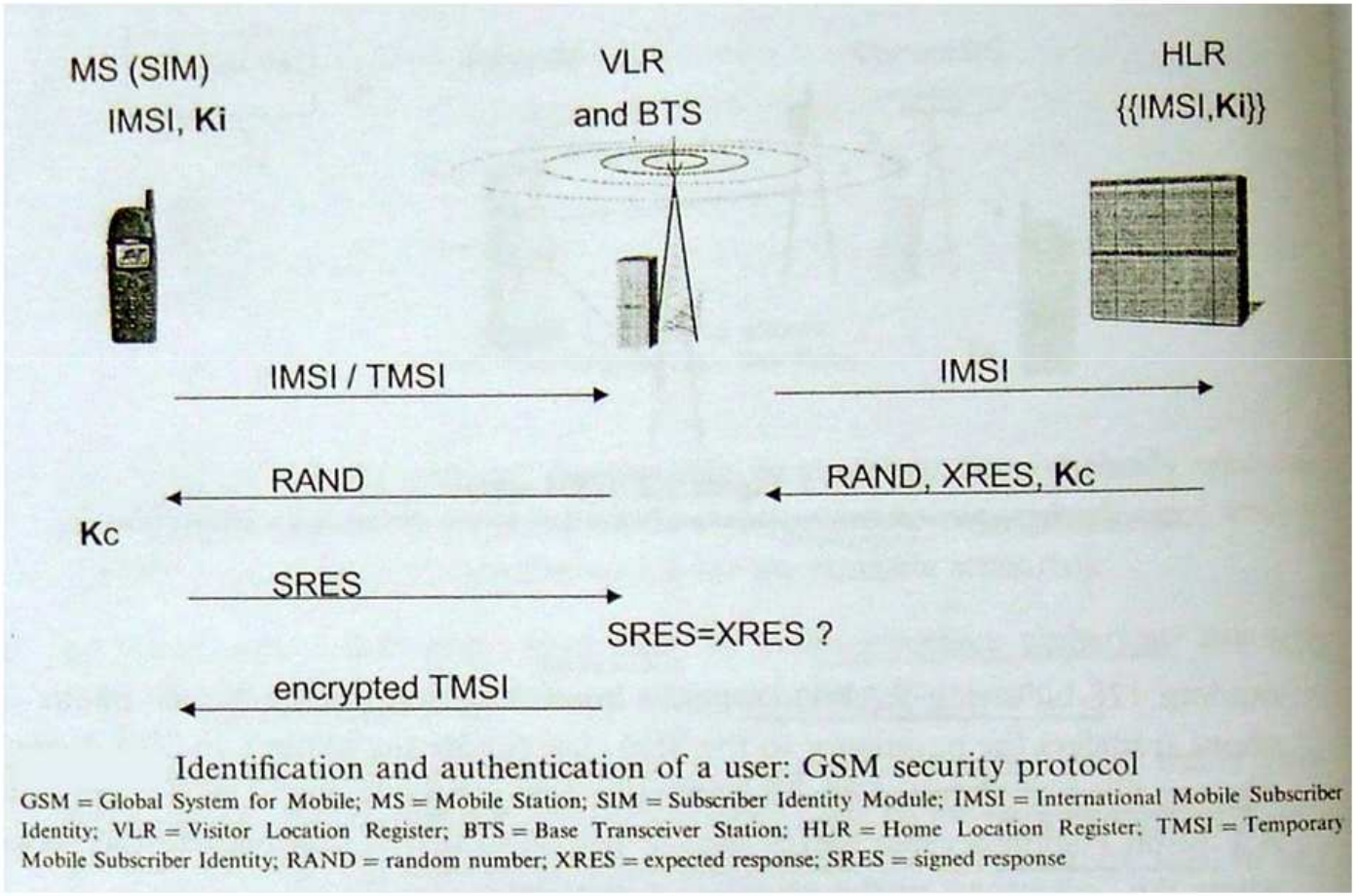
"Security leader now need to also be a business leader and to be a business leader you have to look at your peers and leadership and all of those folks have metrics that they use every day to run and manage your business you need indicators of the health of what you're doing and so if you're running a security organization and you don't have some type of metrics package then you don't really know how effective your organization is at accomplishing its mission."

David komendat VP and CSO for Boeing

3.3 Industrial Framework and Models

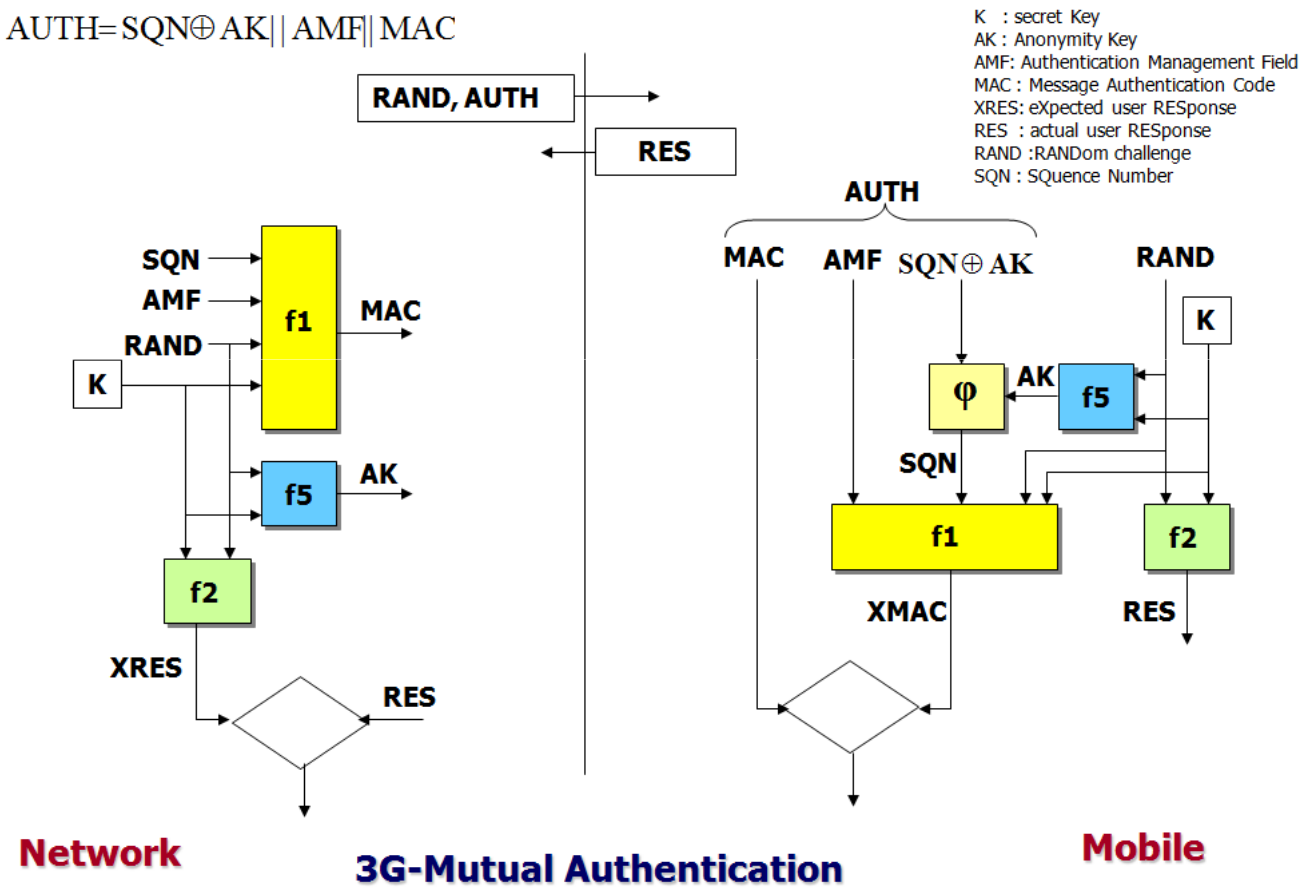
- A hybrid security framework is customized to meet business objectives, and to define policies and procedures for implementing and managing controls in the organization. It should be tailored to outline specific security controls and regulatory requirements that impact the business.
- Common Security Frameworks are such as;
  - NIST SP 800-53
  - COBIT
  - ISO 27000 Series and
  - CISQ

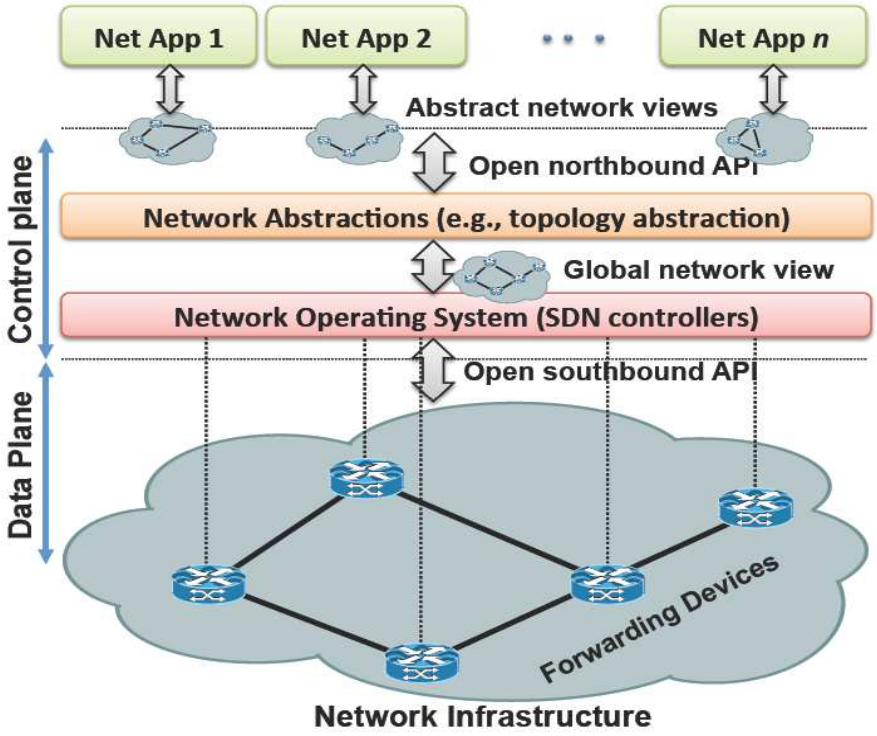

Goal
Objective
Policy
Strategy
- Broad
- General statement
- Toward overall success
- Clear and actionable
- Guideline principle
- Action principle
- Introverted approach
- Steps to achieve objectives
- Action plan
- Extroverted approach

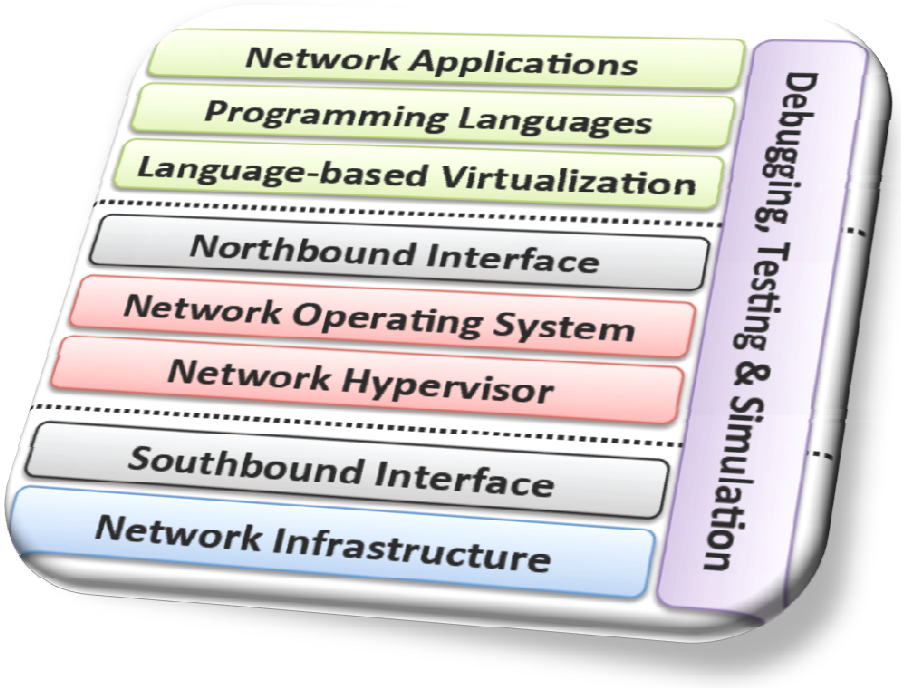


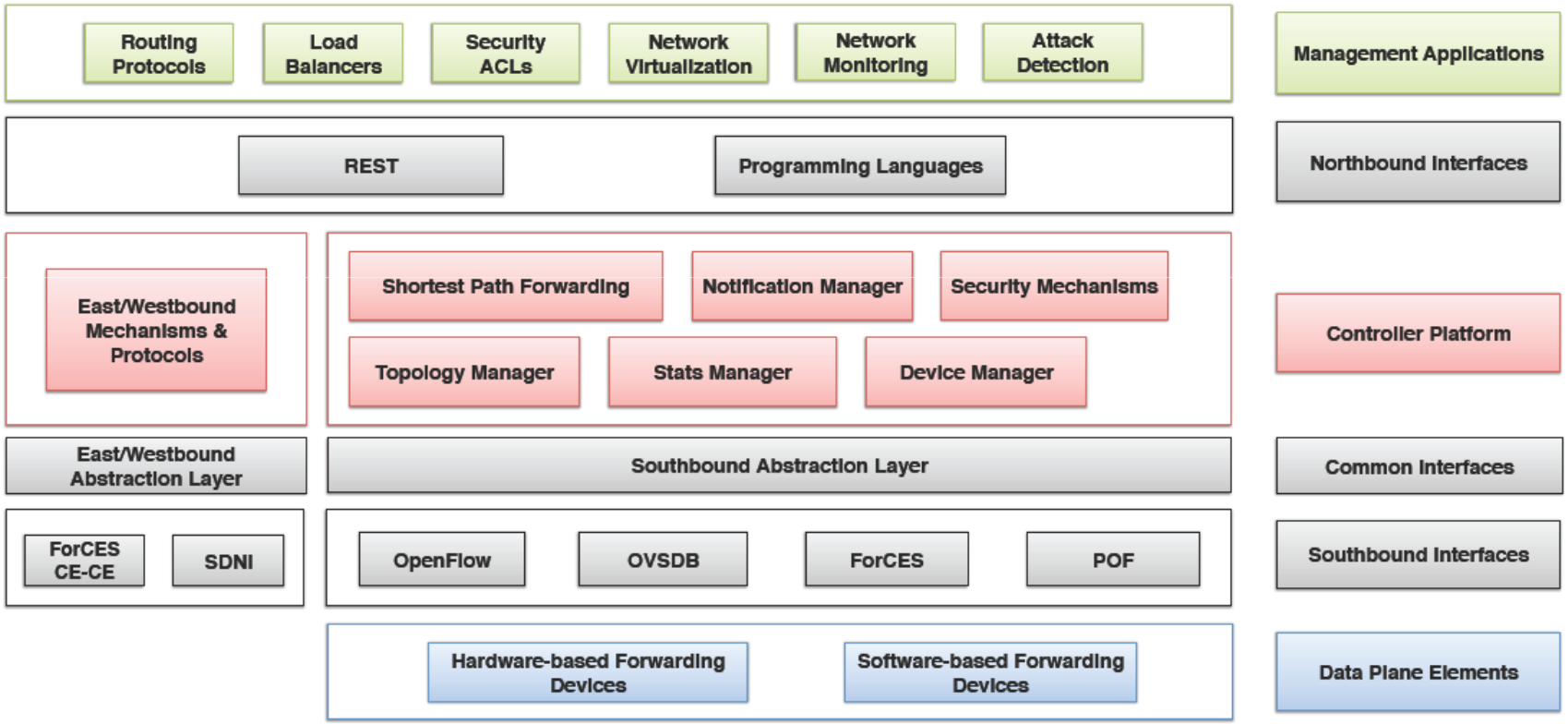
Identification and authentication of a user: GSM security protocol

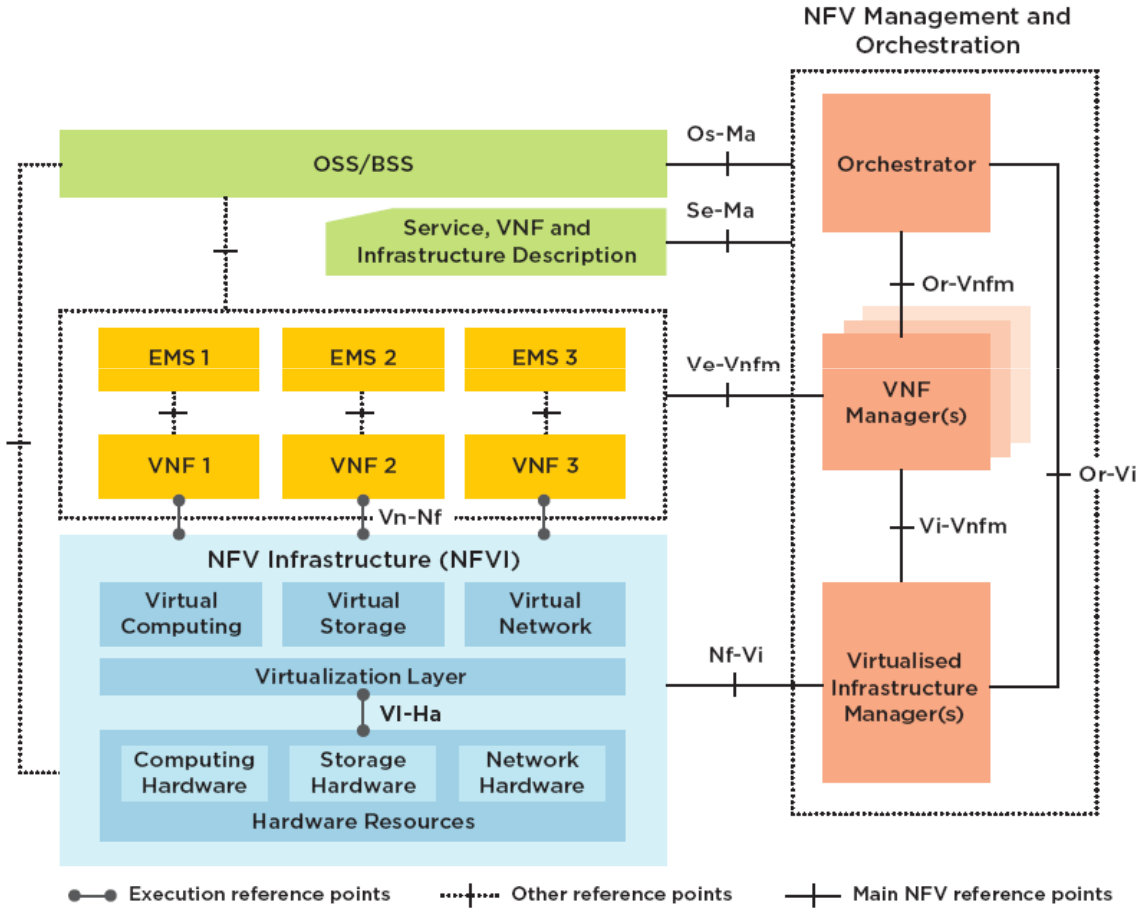
GSM = Global System for Mobile; MS = Mobile Station; SIM = Subscriber Identity Module; IMSI = International Mobile Subscriber Identity; VLR = Visitor Location Register; BTS = Base Transceiver Station; HLR = Home Location Register; TMSI = Temporary Mobile Subscriber Identity; RAND = random number; XRES = expected response; SRES = signed response


AUTH= SQN⊕AK||AMF||MAC
K : secret Key
AK : Anonymity Key
AMF: Authentication Management Field
MAC : Message Authentication Code
XRES: eXpected user RESponse
RES : actual user RESponse
RAND :RANDom challenge
SQN : SQuence Number
RAND, AUTH
RES
SQN
AMF
RAND
K
f1
MAC
f5
AK
f2
XRES
RES
AUTH
MAC
AMF
SQN⊕AK
RAND
K
φ
AK
f5
SQN
f1
f2
XMAC
RES
Network
3G-Mutual Authentication
Mobile


Net App 1
Net App 2
Net App n
Abstract network views
Open northbound API
Network Abstractions (e.g., topology abstraction)
Global network view
Network Operating System (SDN controllers)
Open southbound API
Control plane
Data Plane
Forwarding Devices
Network Infrastructure


Network Applications
Programming Languages
Language-based Virtualization
Northbound Interface
Network Operating System
Network Hypervisor
Southbound Interface
Network Infrastructure
Debugging, Testing & Simulation


Routing Protocols
Load Balancers
Security ACLs
Network Virtualization
Network Monitoring
Attack Detection
Management Applications
REST
Programming Languages
Northbound Interfaces
East/Westbound Mechanisms & Protocols
Shortest Path Forwarding
Notification Manager
Security Mechanisms
Topology Manager
Stats Manager
Device Manager
Controller Platform
East/Westbound Abstraction Layer
Southbound Abstraction Layer
Common Interfaces
ForCES CE-CE
SDNI
OpenFlow
OVSDB
ForCES
POF
Southbound Interfaces
Hardware-based Forwarding Devices
Software-based Forwarding Devices
Data Plane Elements


NFV Management and Orchestration
OSS/BSS
Os-Ma
Orchestrator
Service, VNF and Infrastructure Description
Se-Ma
Or-Vnfm
EMS 1
EMS 2
EMS 3
Ve-Vnfm
VNF Manager(s)
VNF 1
VNF 2
VNF 3
Or-Vi
Vn-Nf
Vi-Vnfm
NFV Infrastructure (NFVI)
Virtual Computing
Virtual Storage
Virtual Network
Nf-Vi
Virtualised Infrastructure Manager(s)
Virtualization Layer
VI-Ha
Computing Hardware
Storage Hardware
Network Hardware
Hardware Resources
Execution reference points
Other reference points
Main NFV reference points

Security in SDN infrastructure

Security risks in implementing a technology {(still in its fancy)}
Challenge (SDN's vulnerability: not exploited) {(by malicious attacks), (learning cases)}

SDN: {(simple network programming), (opportunity for attacker)}
Both more and less secure risk {(more: because of attack layer), (less: no longer need physical access)}

Three main points of vector for attack and problem in layers:

- **Data layer**
  - Southbound API and protocols {(OpenFLow: OF), (Open vSwitch Database Management: OVSDB), (Application Centric Infrastructure: ACI), ..}
    (new : may not fully developed with security in mind.)
  - API {(more **friendly**-user management **interface**) -> **increase** (**attack** surface)},
    {(add own flow table), (spoof traffic), (disallow network),..}

  - **Secure in data layer** {(TLS secure to control plane), (reduce session life time of TLS), (use **out of band** for signaling control)}

- **Control layer**
  - (interest to hacker) {(**high value target** for bad attack), (single point of failure),..}
  - (**network component**) (now open to control from controller) (could be a way in for cyber attacker)}
  - (new types of attacking) {(**DDoS** to scale limits of SDN infrastructure), ..}

  - **Secure in control layer** {(**prevent unauthorized** activity access), (set up Role Base Access Control: **RBAC policy**), (continuous **monitor** and **audit**)}
    {high availability (**redundant**) controller}...
  - (first critical to secure SDN controller with architecture), (**strong access control**), (**trust zone**), (**DDoS protection**), (**anti-virus** and other threat)

- **Application layer**
  - northbound protocol and API {(also a target for attacker)}
  - **API** {(Java), (JSON), (Python),..} (could gain control of SDN infrastructure)
    risk to{(set SDN policies by attacker),..}

  - **Secure in application layer** : {(**authenticated application**), (use **TLS communication**), (make sure **coded securely** for northbound application)

Improved security:

- With these overlay schemes (virtual network) require defined **clear rules for communication**.
- (it is important to bake **security into SDN from the start**.)
  {(flow traffic) {(northbound), (southbound), (service delivery),..}

- Flow rule control {(traffic through security device)}
- **Network topology** {(virtualization)}
  Require (**completed trust** in) {(application), (controller)} and (trust in) {(data plane)}

Which factors shall be consideration to an effective IT security strategy?
Consideration of AN EFFECTIVE IT SECURITY STRATEGY:

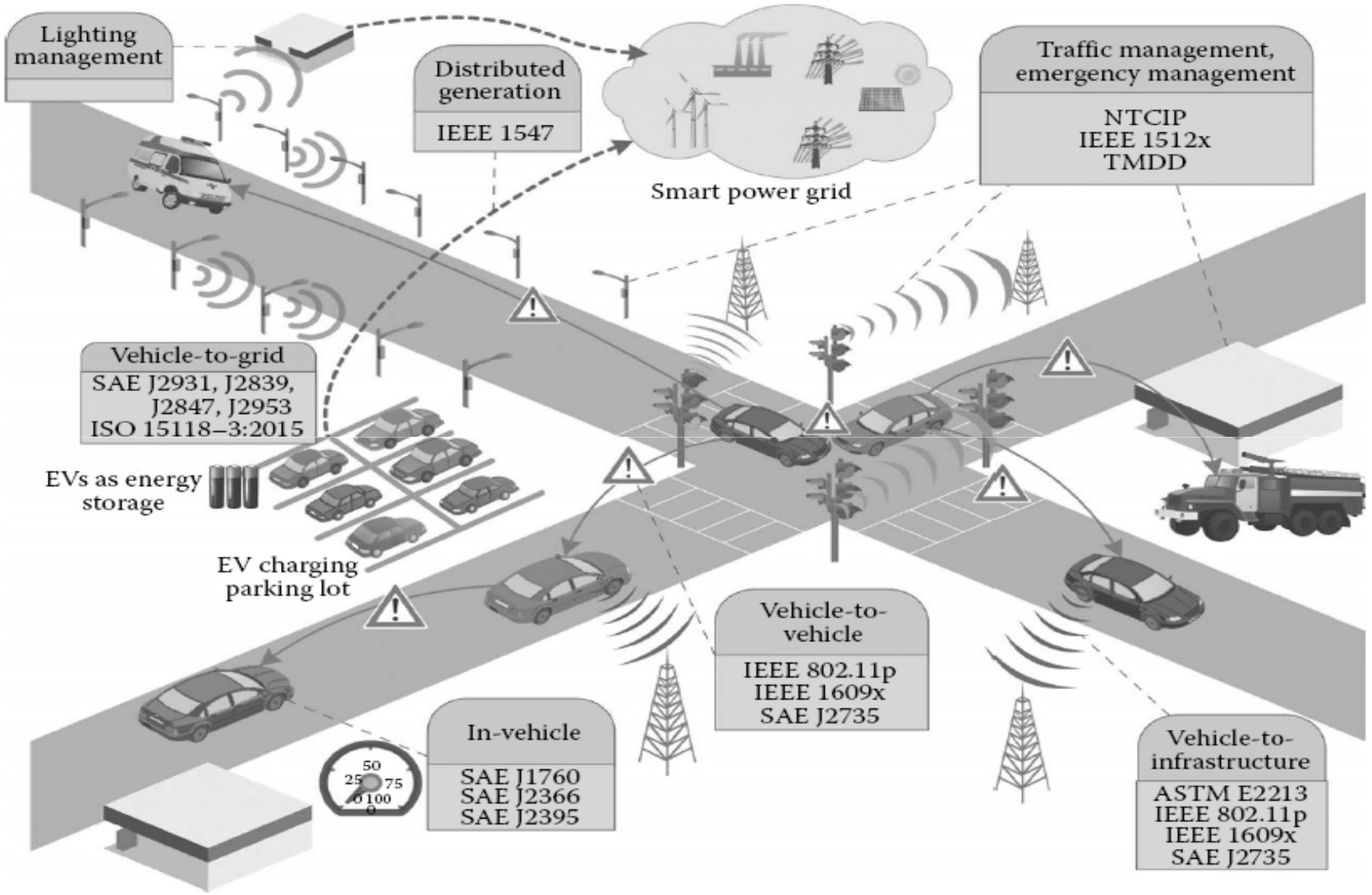
People:
Security must start with people. Most of the security decisions we make are based on emotion, like whether we choose to click on a malicious email and open ourselves up to attack. Cyber criminals are able to piece personal information leaked on social media networks.

Policy: An information security policy is the foundation for protecting an organization's assets.
It should provide a thorough understanding of your business and be concise documents that identify best practices vs. required practices. If employees can't understand, therefore legal can't enforce.

Process: Cyber self-defense is more about psychology than it is about technology and our biggest adversary may in fact be ourselves. As an organization, you need to think like an attacker, train and test relentlessly, and measure results over time.

The goal should be a reduction in risk, and continuous process monitoring will help you better understand your security posture. If your IT security system is simple to both technical and non-technical people, with multiple layers of diverse security to protect data, and is limited to only those who need access, your risks of a breach are severely lowered.

AN EFFECTIVE IT SECURITY STRATEGY shall be considered in People, Policy and Process together.


Lighting management
Distributed generation
IEEE 1547
Smart power grid
Traffic management, emergency management
NTCIP
IEEE 1512x
TMDD
Vehicle-to-grid
SAE J2931, J2839, J2847, J2953
ISO 15118–3:2015
EVs as energy storage
EV charging parking lot
Vehicle-to-vehicle
IEEE 802.11p
IEEE 1609x
SAE J2735
In-vehicle
SAE J1760
SAE J2366
SAE J2395
Vehicle-to-infrastructure
ASTM E2213
IEEE 802.11p
IEEE 1609x
SAE J2735

ตัวอย่างการจัดกลุ่ม Security

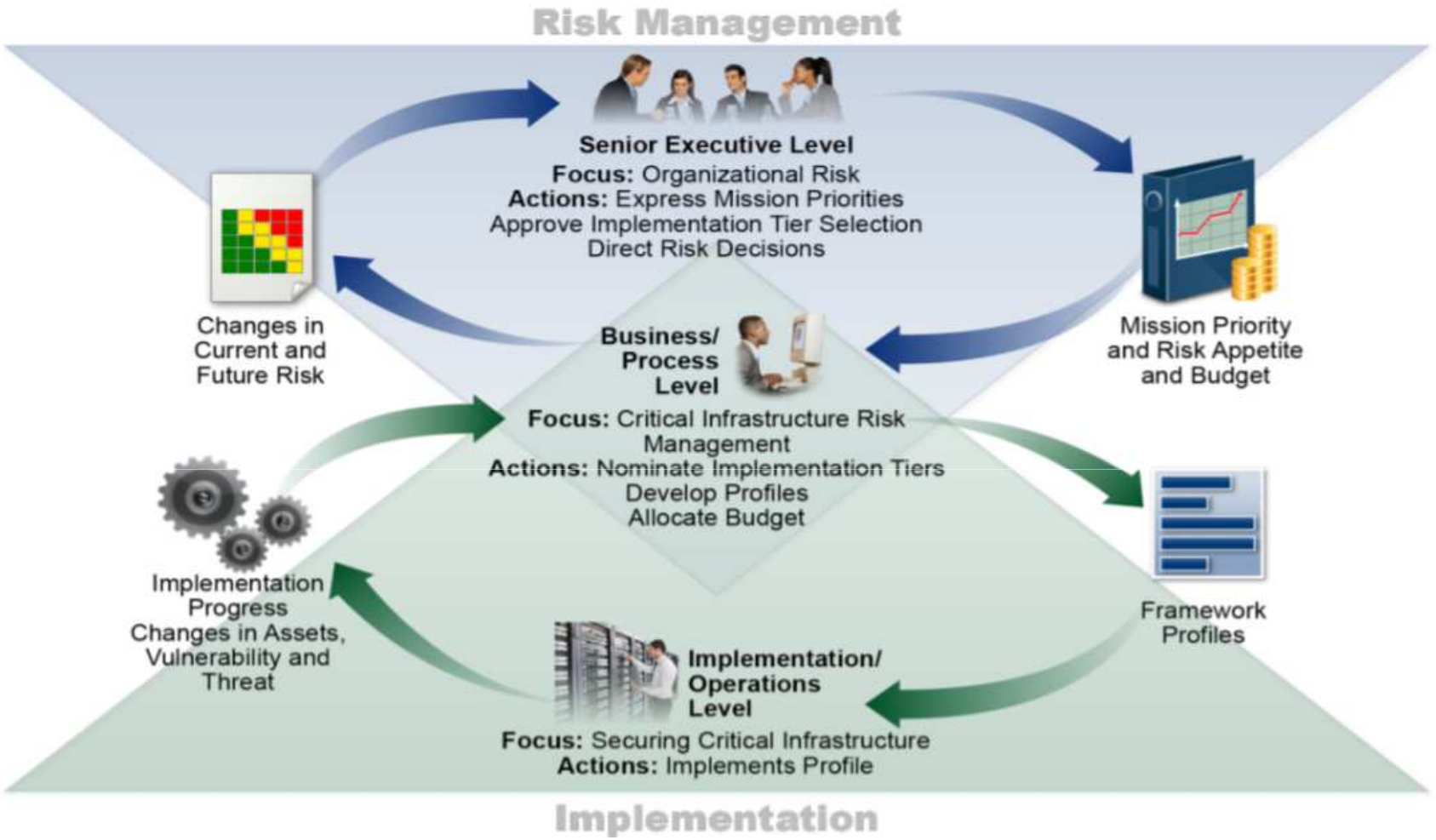
Group	Sub-group
Entity-Level Policies and Procedures	Information Security Policy Management
	Human Resources Security
	Acceptable Use
	Data Classification and Document Retention
	Regulatory Compliance
	Physical and Environmental Security
Access-Control Policies and Procedures	Logical Access
	Password Management
	Wireless, Mobile Computing, and Teleworking
Change Control and Change Management	Software Development
	Change Management
	Patch Management
System Information Integrity and Monitoring	Firewall and Router Security Administration
	Network Security and Monitoring
	Audit Logging Controls
	Antivirus and Mobile Code Protection
	Encryption
	System Configuration and Hardening
System Services Acquisition and Protection	Vendor and Third-Party Agreements
	System Interconnections
	Electronic Commerce
Informational Asset Management	Media Handling
	Asset and Capacity Management
Continuity of Operations	Data Backup and Recovery
	Disaster Recovery (DR) and Business Continuity Planning (BCP)
	Incident Response Plan and Procedures

Appendix A: ISO/IEC 27001 (Annex A) Controls

A.5	Security Policy
A.6	Organization of Information Security
A.7	Asset Management
A.8	Human Resources Security
A.9	Physical and Environmental Security
A.10	Communications and Operations Management
A.11	Access Control
A.12	Information Systems Acquisition, Development, and Maintenanc
A.13	Information Security Incident Management
A.14	Business Continuity Management
A.15	Compliance

Descriptions	ISO 27001
Entity-Level Policies and Procedures: **Information Security Policy Management**	
Describe management's commitment to develop and maintain formal, documented, and approved information security policies and procedures that encompass information values, information protection, and an overall organizational commitment.	(A.5.1.1) (A.6.1.1)
Define the individual or group assigned the responsibility of ensuring that the information security policy is regularly reviewed, documented, and approved. This assignment should be defined in the overall security policy	A.6.1.3
Describe the security policy review and approval process.	A.5.1.2
Define the frequency of the security policy review (annually at a minimum) to ensure its continuing stability, adequacy, and effectiveness.	A.5.1.2
Describe how the security policy document is communicated to all employees (e.g., upon hire, annual awareness training, or intranet).	A.5.1.1
Describe management's intent and support of the goals and principles of information security.	A.6.1.1
Define the compliance requirements (legislative, regulatory, and contractual requirements) that the information security policy is designed to address.	A.5.1.1
Define the security education, training, and awareness requirements for every employee and contractor with access to the organization's information resources.	A.8.2.2
Describe the formal sanction process for personnel failing to comply with the organization's information security policies and procedures.	A.8.2.3
If applicable, describe the use of a cross-functional group of management representatives (e.g., a steering committee) from relevant parts of the organization to coordinate the implementation of information security controls.	A.6.1.2
Describe how management approves assignment of specific roles and responsibilities for information security across the organization.	A.6.1.3
Describe how appropriate contacts with special interest groups or other specialist security forums and professional associations are maintained. Management should support such associations and memberships as a matter of policy.	A.6.1.7
Describe the use of independent, outside organizations to periodically review the organization's approach to managing information security and its implementation.	A.6.1.8
Describe the organization's risk assessment (RA) and risk management process. Output from the assessment should include a formal RA document that is submitted to management for review.	A.14.1.2
Define the information security roles and responsibilities to include each of the following: • Responsibility for creating and distributing **security policies** and **procedures** • Responsibility for monitoring and analyzing **security alerts** and distributing information to appropriate information security and business unit management personnel. • Responsibility for creating and distributing security **incident response** and escalation procedures. • Responsibility for administering user **account** and authentication management. • Responsibility for monitoring and controlling **access to data**.	A.8.1.1

ตัวอย่าง Cyber Security Framework


Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget
Implementation Progress
Changes in Assets, Vulnerability and Threat
Framework Profiles
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

The Five Functions

- Highest level of abstraction in the core
- Represent five key pillars of a successful and wholistic cybersecurity program
- Aid organizations in expressing their management of cybersecurity risk at a high level

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 2: Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

ตัวอย่าง CIS

Center for Internet Security

CIS Benchmarks

You now have access to all of our CIS Benchmark PDFs. Feel free to download as many as you like!

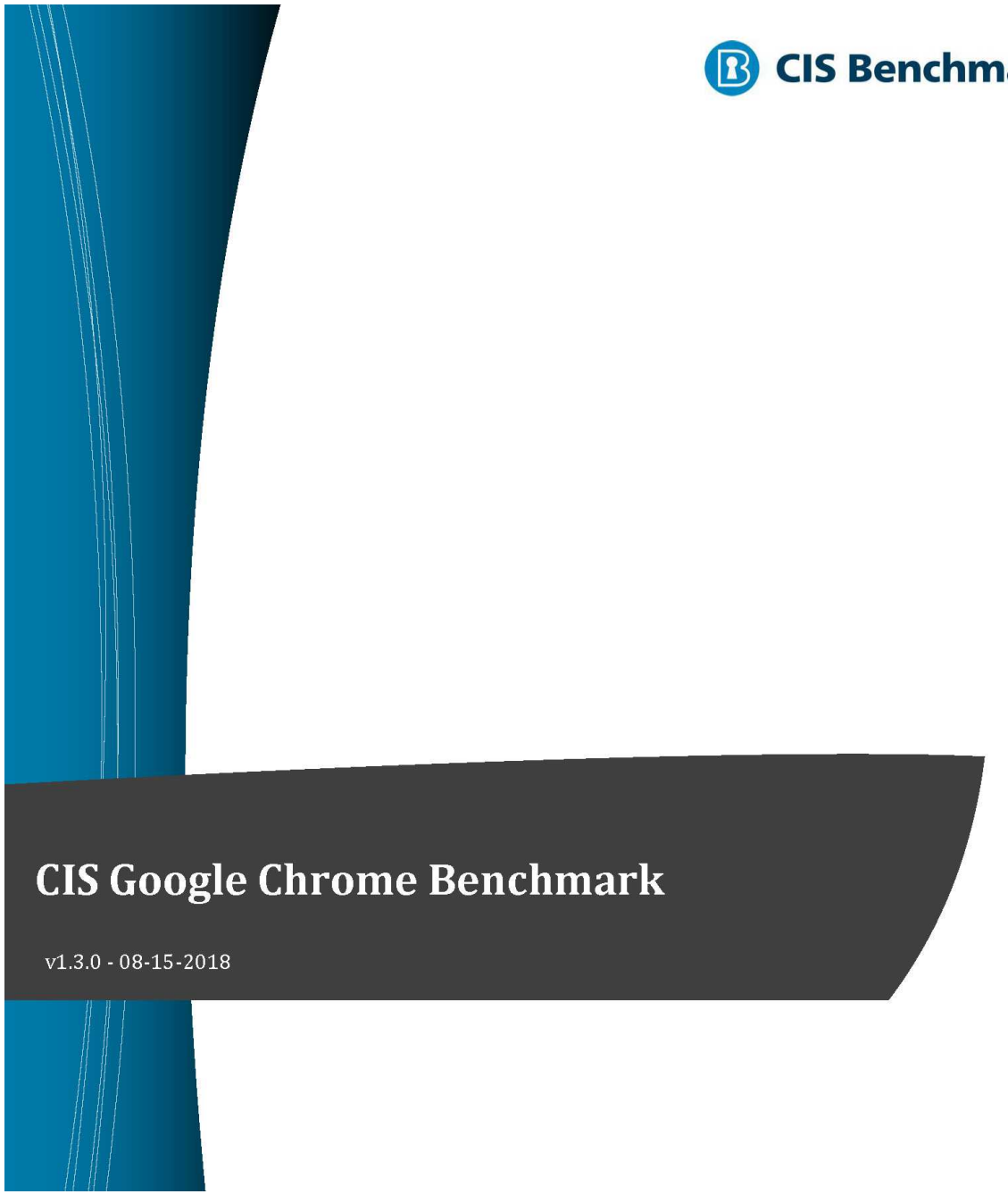
If you have any issues accessing the files, please let us know at learn@cisecurity.org.

Looking for a previous version of a CIS Benchmark? See our ***archive***.

Operating Systems

Distribution Independent Linux Linux

CIS Distribution Independent Linux Benchmark v1.1.0



CIS Benchmarks

CIS Google Chrome Benchmark

v1.3.0 - 08-15-2018

Recommendations

1 Computer Configuration

The following structure of this guide mirrors how it is structured in the Google Chrome Group Policy template.

1.1 Google Chrome

This section contains recommendations for Google Chrome.

1.1.1 Configure Remote Access Options

This section contains recommendations for Configuring Remote Access Options

1.1.1.1 (L1) Ensure 'Configure the required domain names for remote access hosts' is set to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

Chrome allows the user to configure a required host domain that is imposed on remote access hosts. When enabled, hosts can only be shared using accounts that are registered to the specified domain.

Rationale:

If this setting is disabled or not set, then hosts can be shared using any account.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as