ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

La Governance IoT

Siamo preparati a gestire l'Internet of Things ?

Alberto Piamonte - ISACA Roma

Roma 23 febbraio 2016

Agenda

- Presentazione relatore
- La compliance non basta più
- Ci vuole un Framework (possibilmente di Cybersecurity !)
- Come misurare della «capacità di dare i risultati attesi»
- Applichiamolo all'IoT
- Conclusioni e ....
- Q&A
- Sitografia

Presentazione relatore

Alberto Piamonte

Esperienze professionali

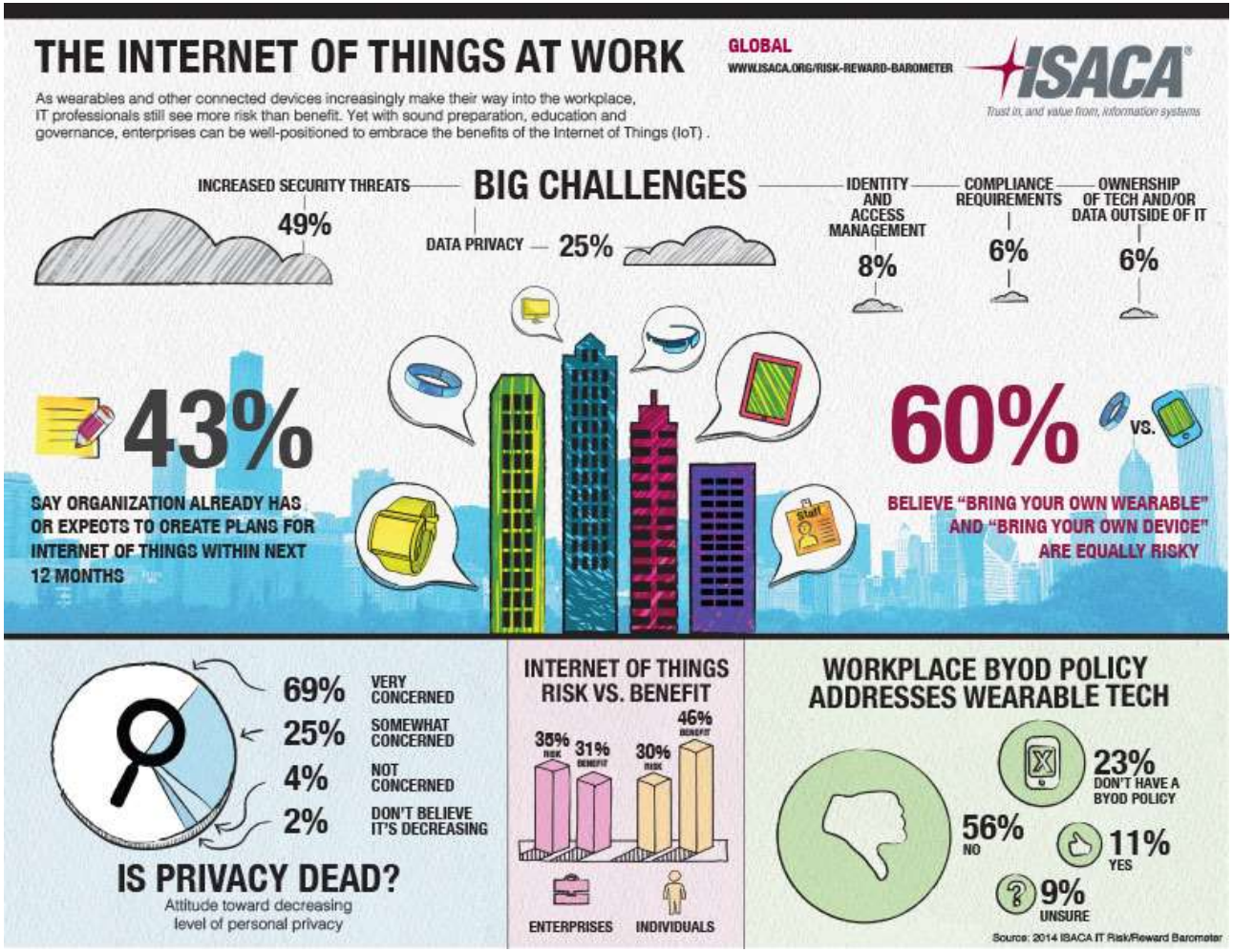
- IBM R & D : HW - Telecomunicazioni & Sicurezza
- Olivetti – Direttore Marketing Settore Pubblico
- Amdahl Corp. – Direttore Soluzioni SW Europa
- Consulente GRC

Titoli / certificazioni / attestati

- Laurea Ing. Elettronica (Univ. PD)
- COBIT5 Foundation's, COBIT5 Trainer, COBIT5 Assessor

Una realtà complessa : $10^6 \rightarrow 10^9$

Impatti su efficienza, sicurezza e privacy: la strategia di governo non può essere quella tradizionale tipo :



CERTIFICHIAMO TUTTO !

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

La semplice Compliance non basta più

"By simply trying to keep up with individual compliance requirements, organizations become rule followers, rather than risk leaders," said John A. Wheeler, research director at Gartner.

- **Direttiva (1995)** (Focus su «***cosa fare*** » per essere compliant : le Misure Minime !)
  - Legislatore definisce «**cosa fare**» (Baseline Security)
  - Il Titolare applica e fa reporting (DPS ?)
- **Regolamento** (Focus su «***cosa ottenere*** : ***risultato***» per essere compliant)
  - Legislatore definisce i «risultati (**outcomes)**»
  - Il Titolare definisce le misure di sicurezza appropriate le applica e fa reporting

Compliance

Directive

Sicurezza

Evoluzione, un esempio : ***Nuovo Regolamento Europeo per la protezione dei Dati***

- **Direttiva (1995)** (Focus su «***cosa fare*** » per essere compliant : le Misure Minime !)
  - Legislatore definisce «**cosa fare**» (Baseline Security)
  - Il Titolare applica e fa reporting (DPS ?)
- **Regolamento** (Focus su «***cosa ottenere*** : ***risultato***» per essere compliant)
  - Legislatore definisce i «risultati (**outcomes)**»
  - Il Titolare definisce le misure di sicurezza appropriate le applica e fa reporting

Sicurezza

Regulation

Compliance

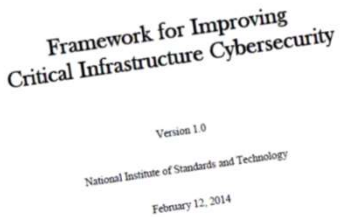
Quasi contemporaneamente al Nuovo Regolamento EU Protezione Dati Personali :

Richiesta al presidente Obama (2012) da parte di aziende USA

Vorremmo qualcosa che ci consentisse di ridurre i rischi IT :

- ✓ Non normativo
- ✓ Usato con decisione autonoma (voluntary)
- ✓ Adattabile a specifiche esigenze e priorità (no one-size fits all)
- ✓ Flessibile
- ✓ Orientato alle prestazioni
- ✓ Efficiente (costo/prestazione)
- ✓ In grado di identificare, valutare e gestire i rischi IT
- ✓ Basato sull'utilizzo o quanto meno allineato agli standards e buone pratiche già disponibili nel contesto internazionale

- ❑ EO 13636 Issued –February 12, 2013
- ❑ NIST Issues RFI –February 26, 2013
- ❑ 1st Framework Workshop –April 03, 2013
- ❑ Nel febbraio 2014 il NIST pubblica il Cybersecurity Framework (CSF) e lo rende liberam[illegible]ibile


Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

Cyber Security Framework NIST (CSF)

L'idea sembra buona, e sta avendo successo, cerchiamo di capire :

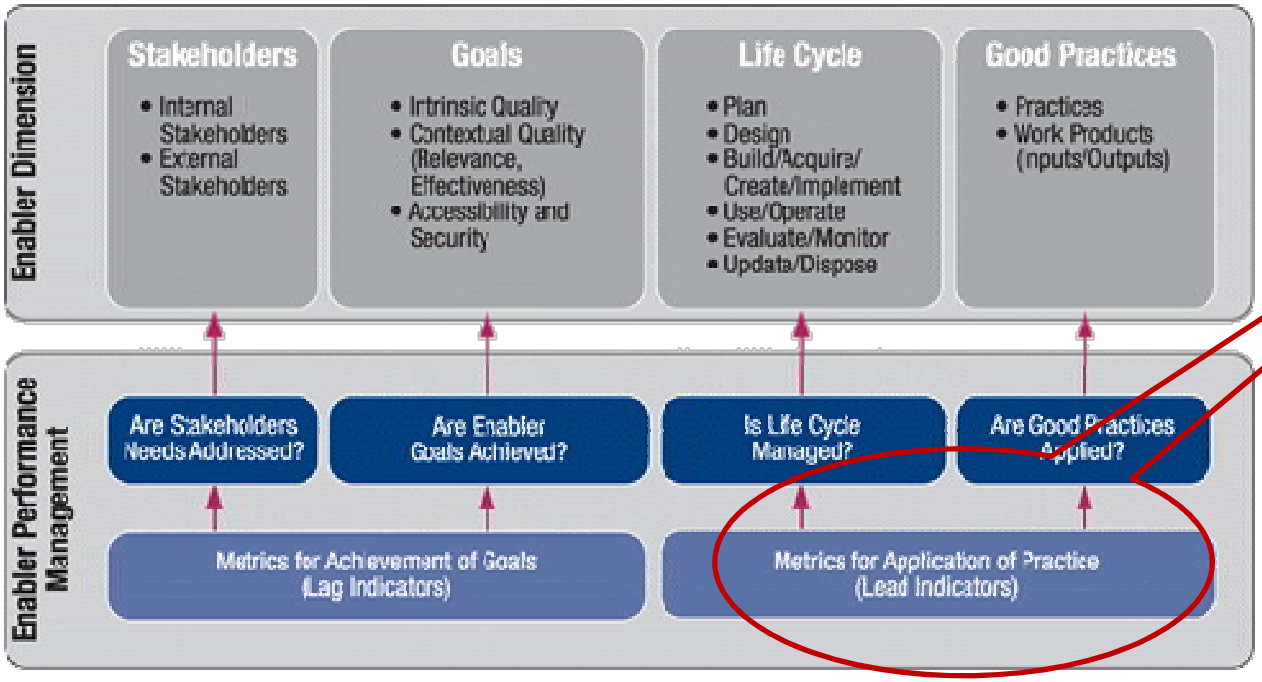
- Come nasce
- Come si sviluppa
- Come si applica

È applicabile in contesto IoT ?

- Se si, come ?

Process "Capability" *porterà i risultati attesi ?*

Misura (Lead indicators) ed azioni correttive <u>preventive</u>
(per qualsiasi fattore abilitante)



Ciclo di Vita

+

Buone Pratiche

Ciclo di vita della Sicurezza

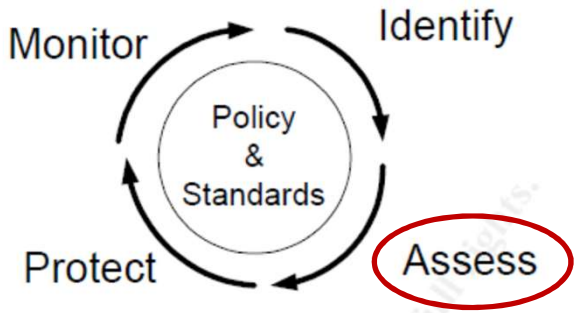
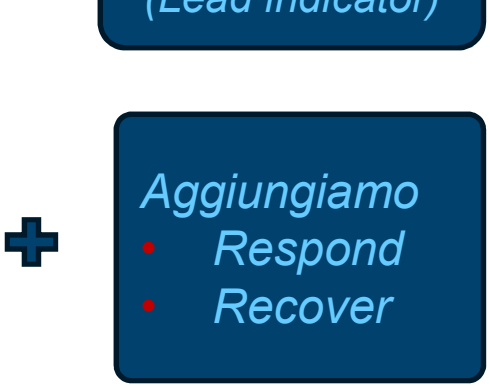
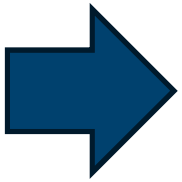
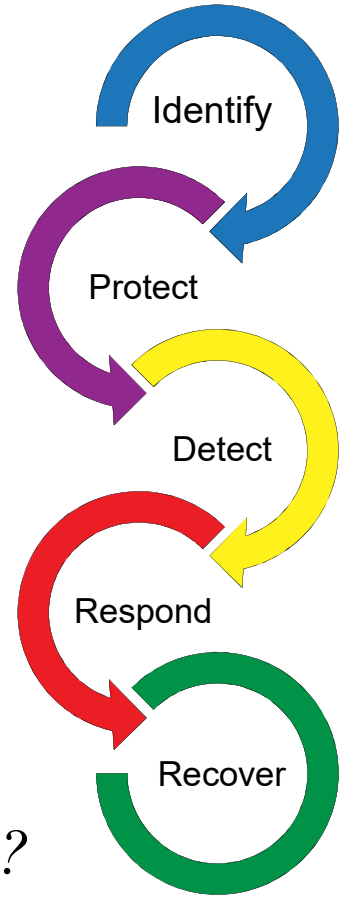


Figure 1: Security Lifecycle

NIST Framework Core :
Activities and desired outcomes



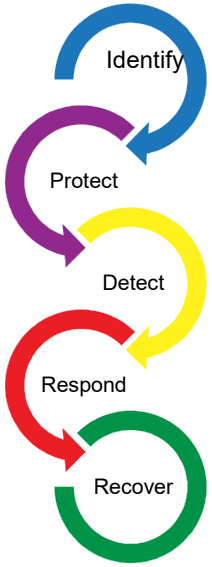




IOT ?

CSF : Struttura

NIST Framework Core



Function Unique Identifier	Function	Category Unique Identifier	Category	Subcategory
ID	Identify	AM	Asset Management	
		BE	Business Environment	
		GV	Governance	
		RA	Risk Assessment	
		RM	Risk Management	
PR	Protect	AC	Access Control	
		AT	Awareness and Training	
		DS	Data Security	
		IP	Information Protection Processes and Information	
		PT	Protective Technology	
DE	Detect	AE	Anomalies and Events	
		CM	Security Continuous Monitoring	
		DP	Detection Processes	
RS	Respond	CO	Communications	
		AN	Analysis	
		MI	Mitigation	
		IM	Improvements	
RC	Recover	RP	Recovery Planning	
		IM	Improvements	
		CO	Communications	
5		*20*		*98*

MAP

Standards e Buone Pratiche

ISO International Organization for Standardization

siena NIST

Best Practices Library

AES encryption

Act Plan Check Do

NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD

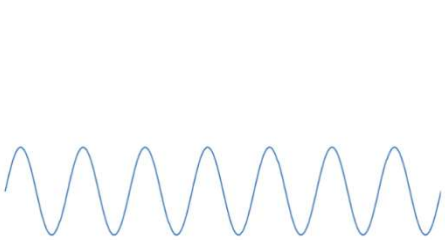
CIS Critical Security Controls

COBIT 5

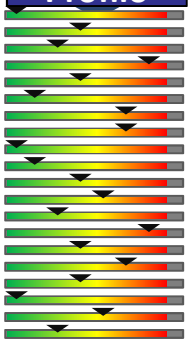
CSF : Struttura

NIST Framework Core

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

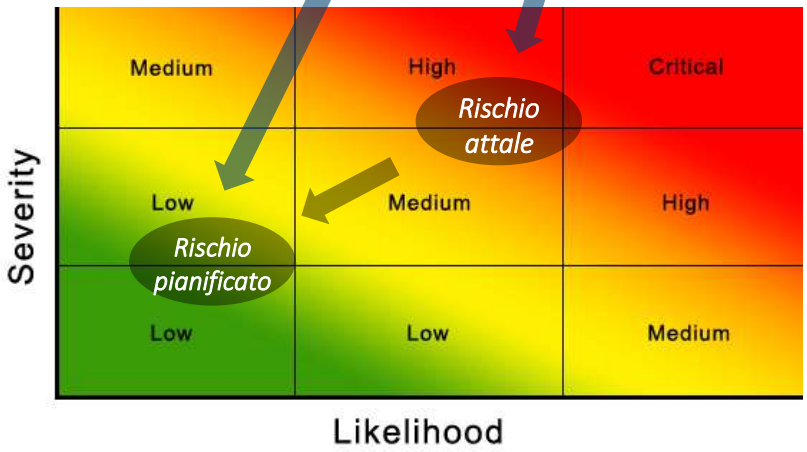


Profilo



Criticità della categoria / sottocategoria nel contesto in esame

EFFICACIA (TIER)
PIANIFICATA **ATTUALE**

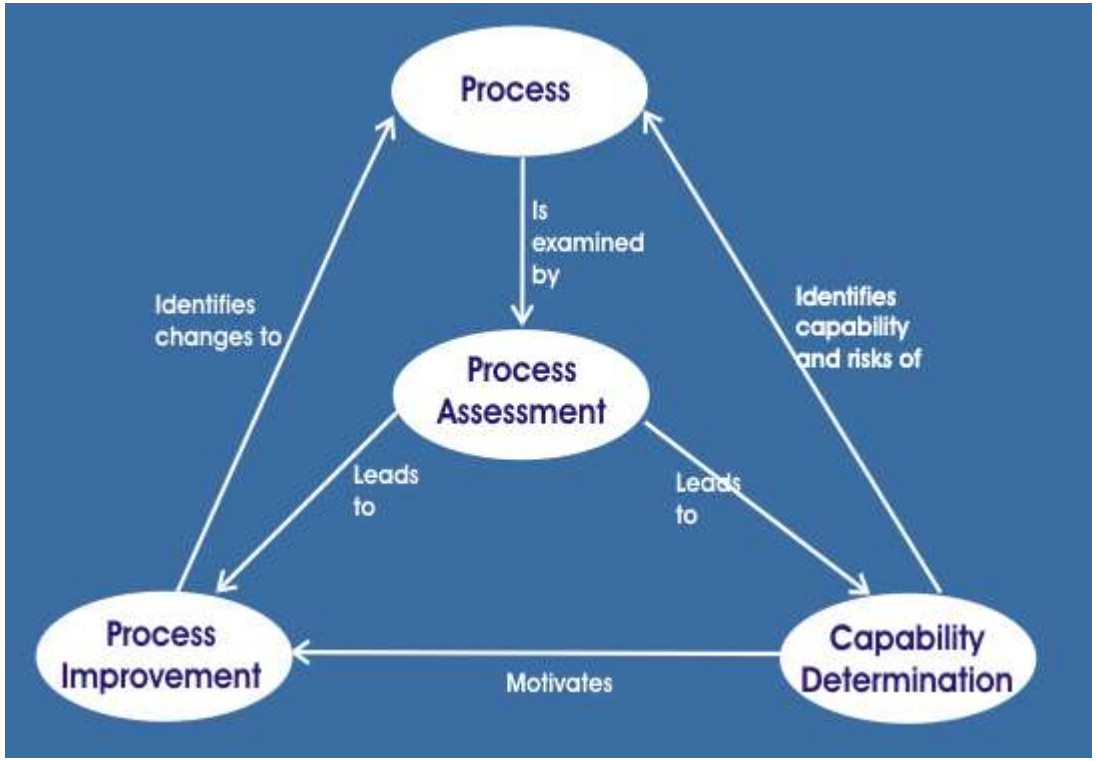


ISACA Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

La misura dell'efficacia

Indicatori

- ✓ Preventivi (Lead indicators)
- ✓ Progressivi
- ✓ Indipendenti dal controllo specifico in esame ed utilizzabili sia in fase di valutazione che di implementazione (GAP)
- ✓ Certificabili
- ✓ .....



- *CSF NIST introduce il concetto di tier (1-4) : compatibili con i primi 3 punti*
- *Esistono altri approcci al problema, ad esempio ISO/IEC ?*

ISO 15504 (-> ISO 33000)

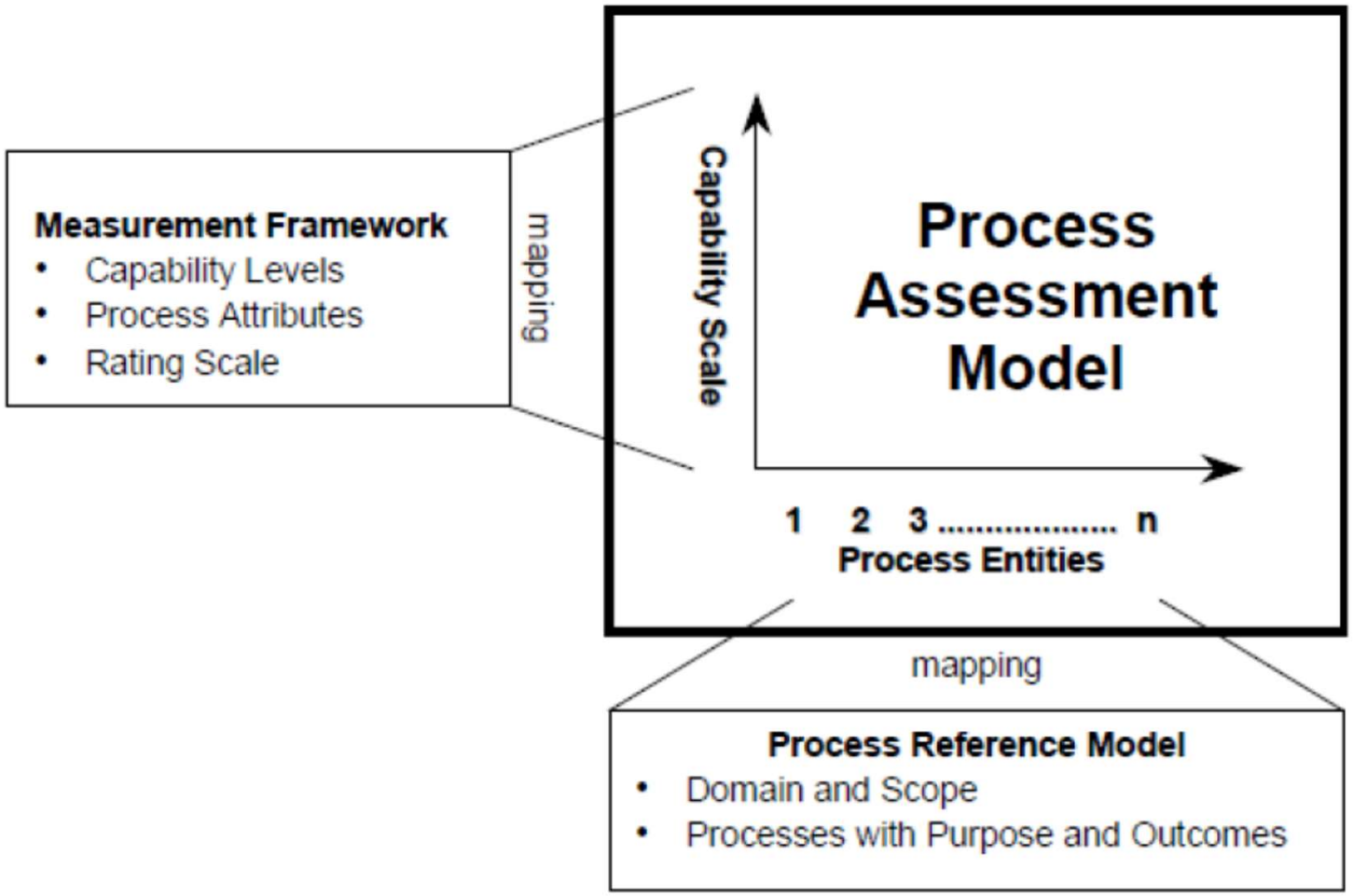
The requirements for process assessment defined in ISO/IEC 15504-2:2003 form a structure which:

- facilitates self-assessment;
- provides a basis for use in process improvement and capability determination;
- takes into account the context in which the assessed process is implemented;
- produces a process rating;
- **addresses the ability of the process to achieve its purpose;**
- is applicable across all application domains and sizes of organization; and

  may provide an objective benchmark between organizations.

The minimum set of requirements defined in ISO/IEC 15504-2:2003 ensures that assessment results are objective, impartial, consistent, repeatable and representative of the assessed processes. Results of conformant process assessments may be compared when the scopes of the assessments are considered to be similar;.

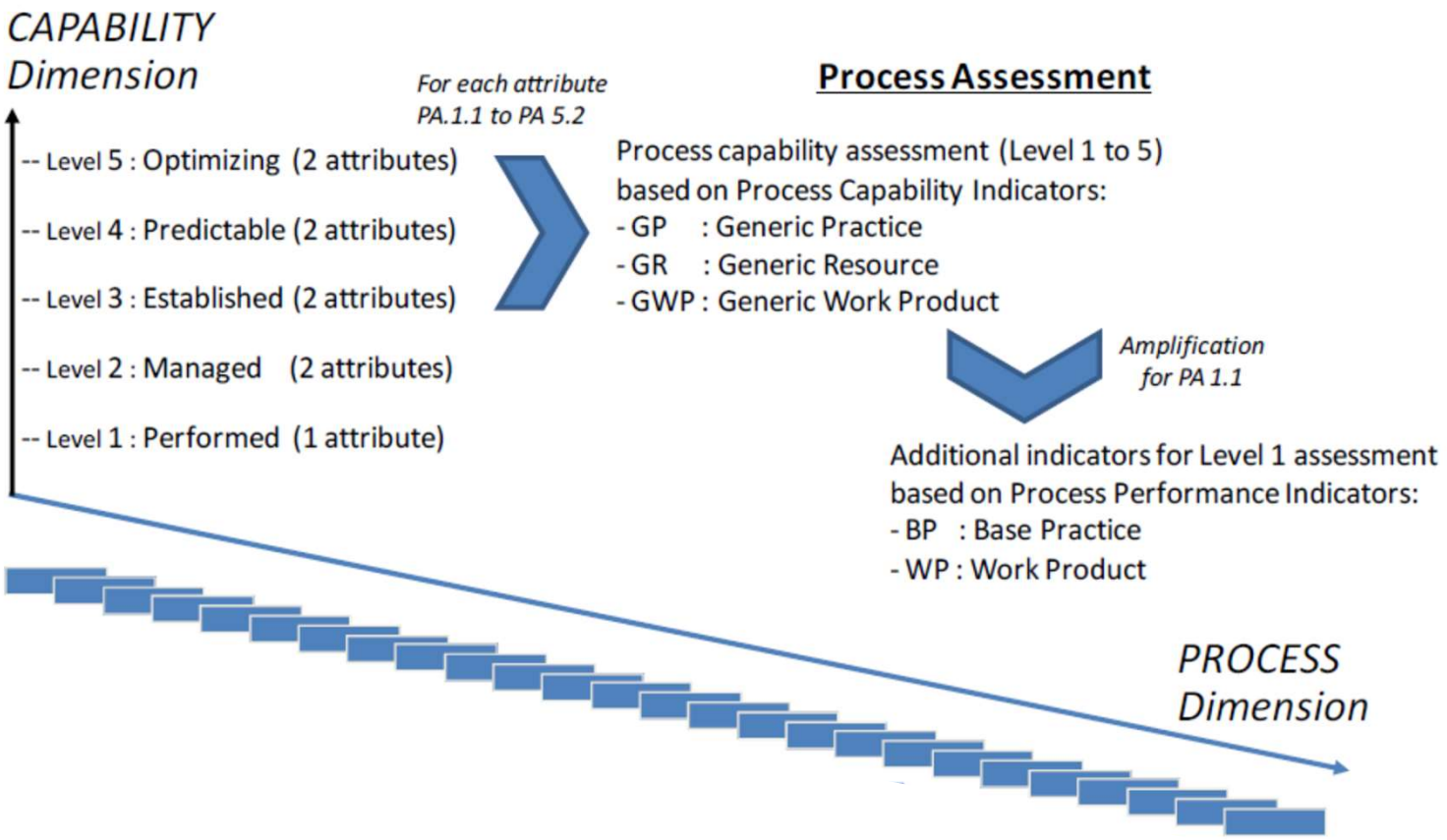
ISO/IEC 15504 – Process Assessment Model (PAM)



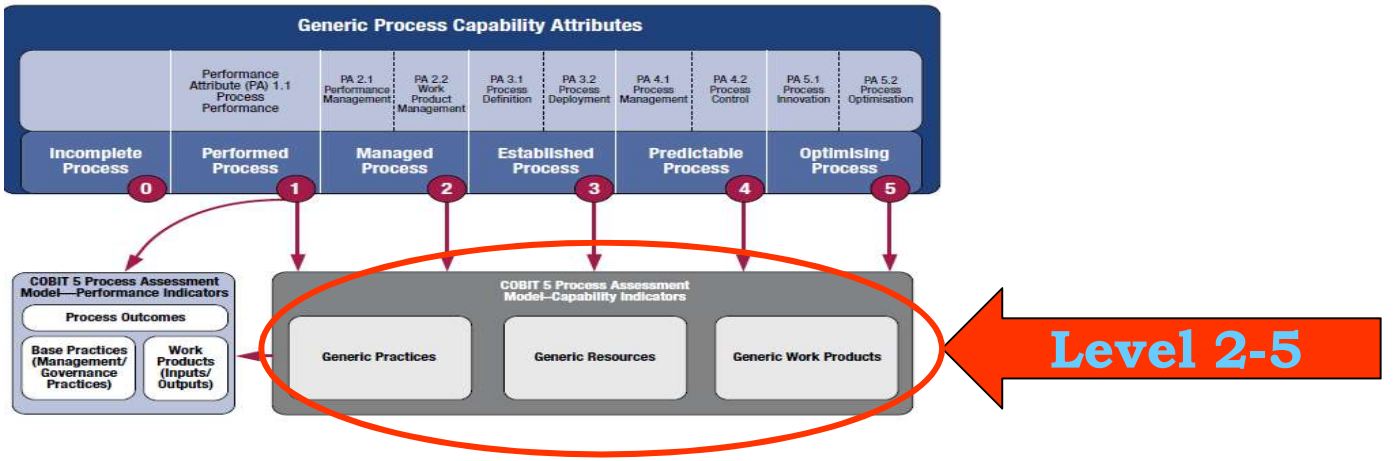
ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Process Attribute ID	Capability Levels and Process Attributes
	Level 0: Incomplete process
	Level 1: Performed process
PA 1.1	Process performance
	Level 2: Managed process
PA 2.1	Performance management
PA 2.2	Work product management
	Level 3: Established process
PA 3.1	Process definition
PA 3.2	Process deployment
	Level 4: Predictable process
PA 4.1	Process measurement
PA 4.2	Process control
	Level 5: Optimizing process
PA 5.1	Process innovation
PA 5.2	Continuous optimization

.... Indipendentemente dal processo !


CAPABILITY
Dimension
-- Level 5 : Optimizing (2 attributes)
-- Level 4 : Predictable (2 attributes)
-- Level 3 : Established (2 attributes)
-- Level 2 : Managed (2 attributes)
-- Level 1 : Performed (1 attribute)
For each attribute
PA.1.1 to PA 5.2
Process Assessment
Process capability assessment (Level 1 to 5)
based on Process Capability Indicators:
- GP : Generic Practice
- GR : Generic Resource
- GWP : Generic Work Product
Amplification
for PA 1.1
Additional indicators for Level 1 assessment
based on Process Performance Indicators:
- BP : Base Practice
- WP : Work Product
PROCESS
Dimension

PAM Capability Indicators (Levels 2-5)



Capability Indicators	Descrizione
Generic Practices	Attività che qualifica il livello di Capability
Generic Resources	Risorse utilizzate nella Practices
Generic Work Product	Risultato della Practices

Per evidenziare l'adeguatezza («capabilities») del Processo (livelli 2-5)

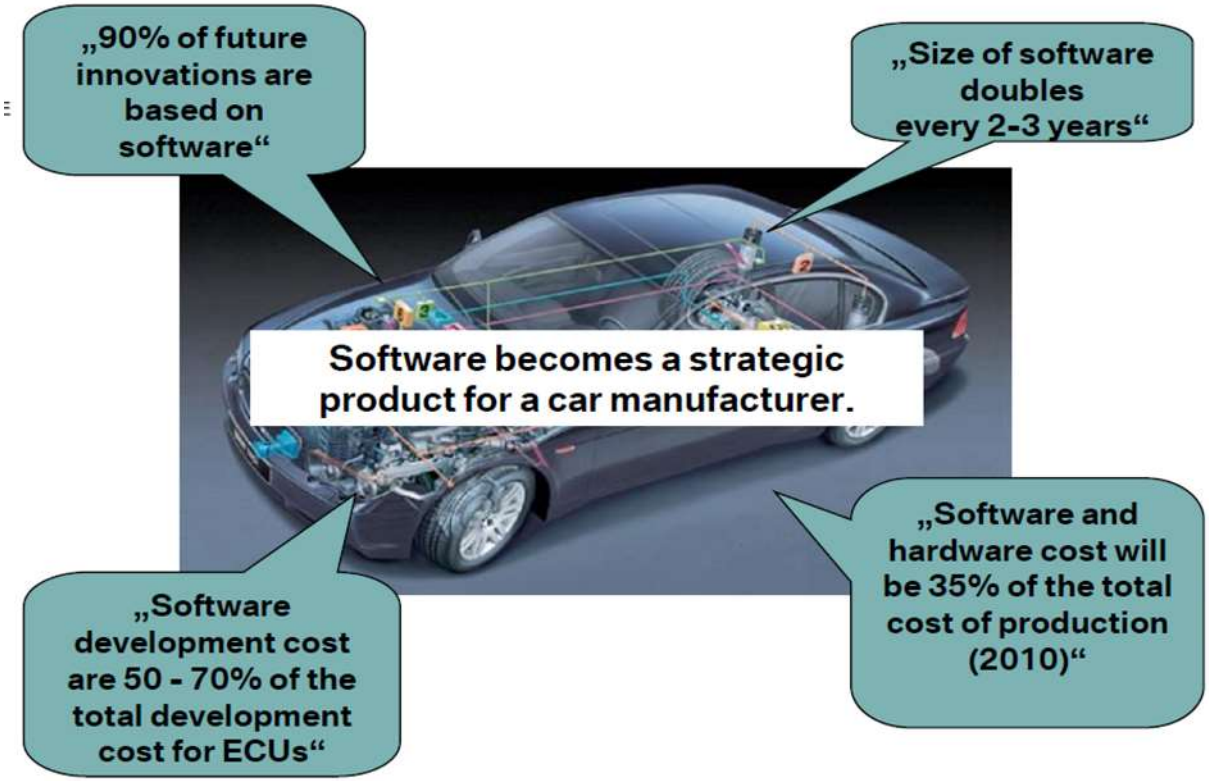
Regole semplici da spiegare ed usare ed indipendenti dal Processo (e funzionano !)

Un esempio pratico

Supplier Assessments by OEMs
Capability Levels in Automotive Software Development

Dr. Jürgen Knoblach
BOSCH, BISS-Net, 29.04.2004
BMW Group

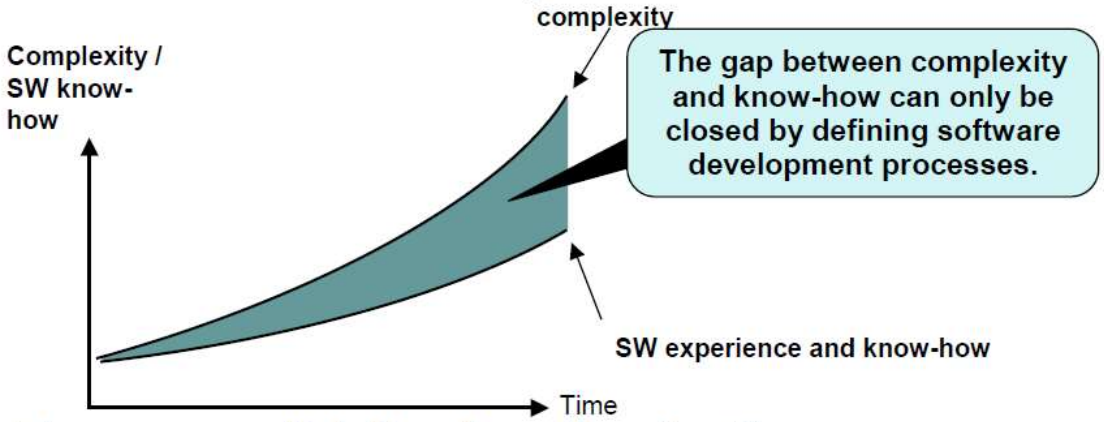
Motivation.
Position of Electrics/Electronics in Car Development.



Provate a sostituire la parola Software con IoT . . .

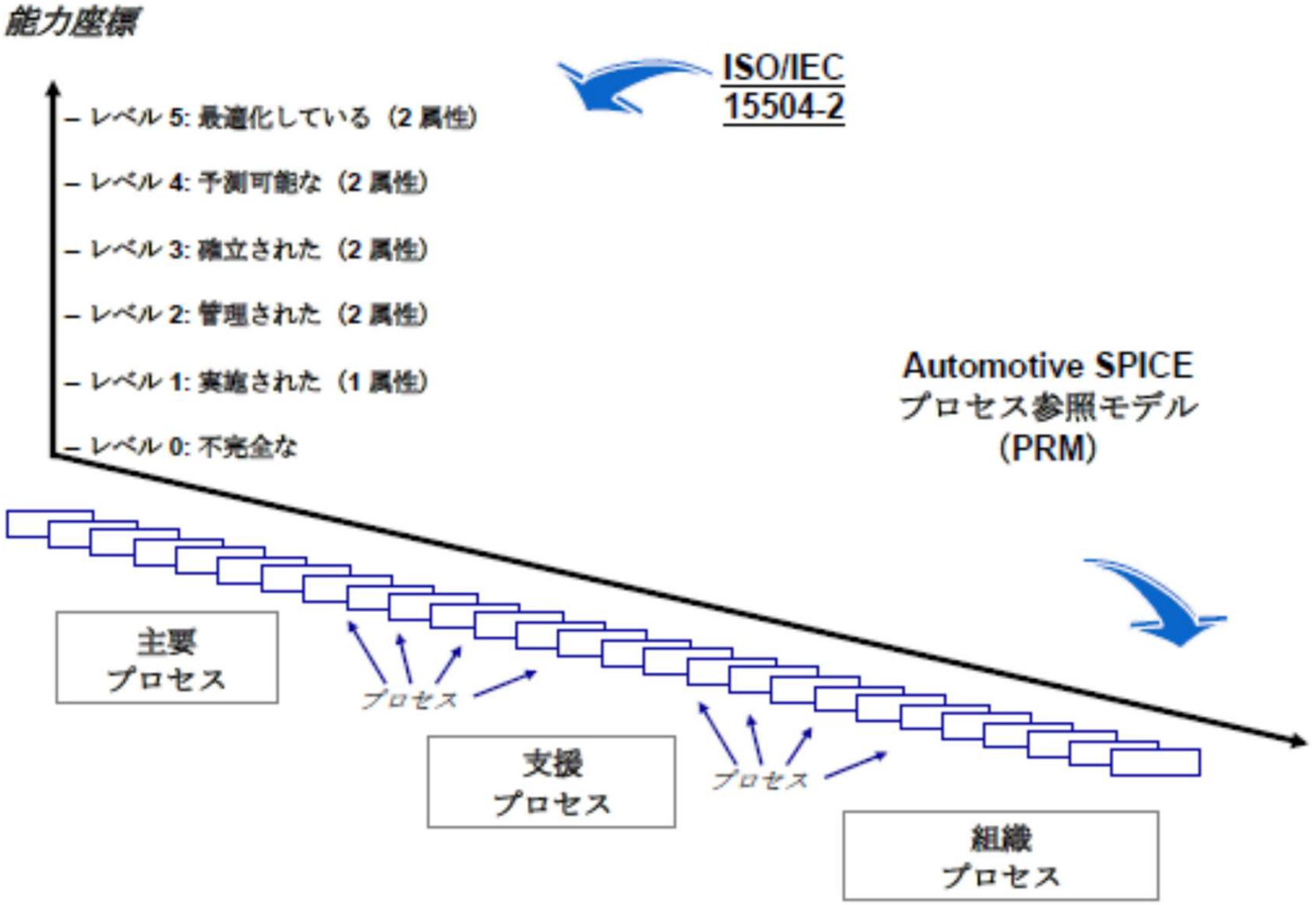
Motivation.
Increasing Complexity in Automotive Industry.

- Increasing complexity of automotive software systems.
- Relative small software experience in automotive industry.
- Defined software development processes have not yet been established until today.

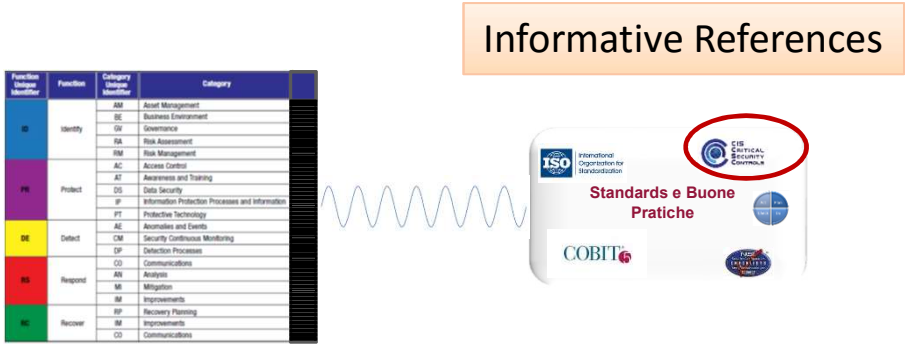


- **To ensure well defined quality of software development processes, supplier assessments are performed.**

.... Toyota


能力座標
ISO/IEC
15504-2
– レベル 5: 最適化している（2 属性）
– レベル 4: 予測可能な（2 属性）
– レベル 3: 確立された（2 属性）
– レベル 2: 管理された（2 属性）
– レベル 1: 実施された（1 属性）
– レベル 0: 不完全な
Automotive SPICE
プロセス参照モデル
(PRM)
3
主要
プロセス
プロセス
支援
プロセス
プロセス
組織
プロセス

e l'IoT ??? : c'è bisogno di un'idea !



- Scorrendo i «possibili controlli» (più di 1000 !) elencati nelle Informative References del CSF si può tentare una «macro classificazione» tra:
  - Riferimenti a «*Process assurance*»
  - Riferimenti a «*Product assurance*»
- La presenza di controlli : **CIS Critical Security Controls** indica che si sta parlando di "Product Assurance" e che quindi in quest'area è di sicuro utile (necessario?) considerare la presenza di IoT.
- La mancanza di tali controlli indica che l'attenzione è al "Process assurance" e che quindi ISO 27001 o COBIT5 costituiscono il riferimento primario.

Wow !

I controli CSC rivisti in ottica IoT

ID.AM-1: Physical devices and systems within the organization are inventoried

COBIT 5

BAI09.01	**Identify and record current assets.**	Maintain an up-to-date and accurate record of all IT assets required to deliver services and ensure alignment with configuration management and financial management.
BAI09.02	**Manage critical assets.**	Identify assets that are critical in providing service capability and take steps to maximise their reliability and availability to support business needs.

ISO 27001-2013

CSC 1 (per IoT)

+

- RACI
- PAM
- .....

ID.AM-1: Physical devices and systems within the organization are inventoried

COBIT 5

BAI09.01	**Identify and record current assets.**	Maintain an up-to-date and accurate record of all IT assets required to deliver services and ensure alignment with configuration management and financial management.
BAI09.02	**Manage critical assets.**	Identify assets that are critical in providing service capability and take steps to maximise their reliability and availability to support business needs.

ISO 27001-2013

A.8.1.1 - Inventario degli asset	Tutti gli asset associati alle informazioni e alle strutture di elaborazione delle informazioni devono essere chiaramente identificati; un inventario di questi asset deve essere compilato e mantenuto aggiornato.
A.8.1.2 - Responsabilità/Titolarità degli asset	A tutti gli asset presenti nell'inventario deve essere attribuita una "responsabilità"

CSC 1 (per IoT)

Inventory of Authorized and Unauthorized Devices

This control is especially important in the context of the IoT. Organizations must deploy technology that tracks the myriad IoT devices that will be deployed across the Enterprise.

Understanding which device types and, in some cases, which specific device instances are authorized to connect to the network is the starting point to adapting this control to the IoT.

Network scans for legacy and non--PC devices may be dangerous, putting IoT endpoints into error states; limited implementation of standard solutions possible where devices run IP stacks.

Passive line and/or RF monitoring may be required.

Proprietary communications protocols with application--specific messaging and command and control are often used in lieu of any authentication mechanism, making remote recognition of a device as “unauthorized” difficult.

This may require some combination of manual assessment, audits using sampling, and/or segregation of devices within subnets to protect legacy devices when newer or other devices can’t handle scans.

Many newer IoT devices support integration into IoT management systems via Application Programming Interfaces (APIs). Leverage systems such as these to support inventory of authorized devices on the network.

Dove bisogna «specializzarsi» IoT ?

Function		Subcategory
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 business objectives an	**ID.AM-1**: Physical devices and systems within the organization are inventoried
		ID.AM-2: Software platforms and applications within the organization are inventoried
		ID.AM-3: Organizational communication and data flows are mapped
		ID.AM-4: External information systems are catalogued
		Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value
		Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
	Business Environment (stakeholders, and acti information is used to risk management decis	The organization's role in the supply chain is identified and communicated
		The organization's place in critical infrastructure and its industry sector is identified and communicated
		riorities for organizational mission, obje icated
		ependencies and critical functions for d
		esilience requirements to support deliv
	Governance (ID.GV): Th and monitor the organi and operational requi management of cybers	and external partners
		ies obligations, are understood and managed
	Risk Assessment (ID.RA cybersecurity risk to o functions, image, or re individuals.	Asset vulnerabilities are identified and d
		Threat and vulnerability information is r es
		Threats, both internal and external, are id
		Potential business impacts and likelihoods are identified
		Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
		Risk responses are identified and prioritized
	Risk Management Strat constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Risk management processes are established, managed, and agreed to by organizational stakeholders
		Organizational risk tolerance is determined and clearly expressed
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users
		PR.AC-2: Physical access to assets is managed and protected
		PR.AC-3: Remote access is managed
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained
		PR.AT-2: Privileged users understand roles & responsibilities
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities
		PR.AT-4: Senior executives understand roles & responsibilities
		PR.AT-5: Physical and information security personnel understand roles & responsibilities
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected
		PR.DS-2: Data-in-transit is protected
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
		PR.DS-4: Adequate capacity to ensure availability is maintained
		PR.DS-5: Protections against data leaks are implemented
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
		PR.DS-7: The development and testing environment(s) are separate from the production environment
		PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained
		PR.IP-2: A System Development Life Cycle to manage systems is implemented

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

Controlli CSC per IoT !

Colonna	Colonna2		Colonna4
CSC #	Control Name	Applicability to IoT	IoT Security Challenges and Considerations
1	Inventory of Authorized and Unauthorized Devices	This control is especially important in the context of the IoT. Organizations must deploy technology that tracks the myriad IoT devices that will be deployed across the Enterprise. Understanding which device types and, in some cases, which specific device instances are authorized to connect to the network is the starting point to adapting this control to the IoT.	Network scans for legacy and non---PC devices may be dangerous, putting IoT endpoints int error states; limited implementation of standard solutions possible where devices run IP stacks. Passive line and/or RF monitoring may be required. Proprietary communications protocols with application---specific messaging and command and control are often used in lieu of any authentication mechanism, making remote recognition of a device as "unauthorized" difficult. This may require some combination of manual assessment, audits using sampling, and/or segregation of devices within subnets to protect legacy devices when newer or other devic can't handle scans.
2	Inventory of Authorized and Unauthorized Software	Keeping control of the versions of software and firmware that drive IoT components within the enterprise will be a challenge. Identifying secure software/firmware baselines for various types of components ensures that the security team has reviewed the threats associated with a particular version of functionality.	May be able to leverage central command and control systems, which are aware of device firmware versions. Custom and restricted OSs may limit remote query capability. In genera IoT software is not patched, but loaded as a new complete flash, image, etc. Manual sampling via IoT direct maintenance port using proprietary tools may be required. In some cases, firmware must be delivered over the network to IoT devices. In these situations, use best practices for securing images, to include applying digital signatures that are evaluated by the device before loading. This requires a secured space within the devic to store credentials used for signature validation
3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	IoT components typically lack the range of configuration customization that laptops and even mobile devices offer, however when there are configuration options available, security practitioners should review and decide if any particular configurations are unallowable or if a certain configuration is required to assure the security of the component on the network. Security practitioners should baseline these controls and keep documented as security best practices.	Hardening templates may be applicable for PC---based processor OSs and other standard (e.g. ARM) host OSs. IoT devices sold as "appliances" with integrated software generally comprise proprietary software components, limiting applicability of post---development hardening or standard methods for securing configurations. Standard control implementations apply to the use of BYOD and ruggedized commodity devices that are integrated into an IoT mission system. Some newer IoT devices support Real---time Operating Systems (RTOSs) that allow for som amount of persistent storage. Oftentimes, this persistence comes in the form of startup scripts that can be modified to affect the configuration of the device at boot time. Ensure that these configurations are written in a secure manner. When IoT devices support access control via user or administrator accounts and passwords, default accounts and passwords should be changed and sound password update and streng
4	Continuous Vulnerability Assessment and Remediation	Just as with other devices on a network, regularly scheduled vulnerability assessments should be conducted to determine non---secure configurations that lead to elevated threats to the enterprise. These security holes should be remediated quickly and the processes used for remediation fed back into the best practices for secure IoT deployment kept by the organization.	Vulnerability assessments in an operational environment may be dangerous or impractical. A laboratory test environment may be appropriate for regularly scheduled assessments against new threats and new IoT software configurations. Collaborative threat laboratories (e.g., sponsored by an Information Sharing and Analysis Center, or other industry body) and IoT vendor laboratories may be the best venues for implementing this control. As with other hardware and software vulnerabilities, these should also be evaluated agains the organization's risk appetite to determine when a particular device or device class can n longer be supported on the network; or must be isolated in some fashion.
5	Controlled Use of Administrative Privileges	Some IoT components include administrative accounts for management of the system. Ensure that when evaluating IoT components for use in the Enterprise that you investigate the controls associated with administrative accounts, to include the type of authentication supported – which will most likely be passwords --- and the strength of the authentication implementation. For administrator accounts, attempt to ensure that at a minimum strong passwords are used and that account access is audited. In	Many IoT devices are deployed in insecure areas (e.g., road side units (RSUs) in the transportation sector). These devices have sometimes been deployed with shared accounts that are used by technicians to manage the devices. Consider alternative methods for restricting administrative access to devices. For legacy devices without privileged access capability, a compensating control may be applied, such as additional physical security. Newly designed IoT devices and subsystems should integrate use of this control.

Come misurarne la «IoT Governance Capability» ?

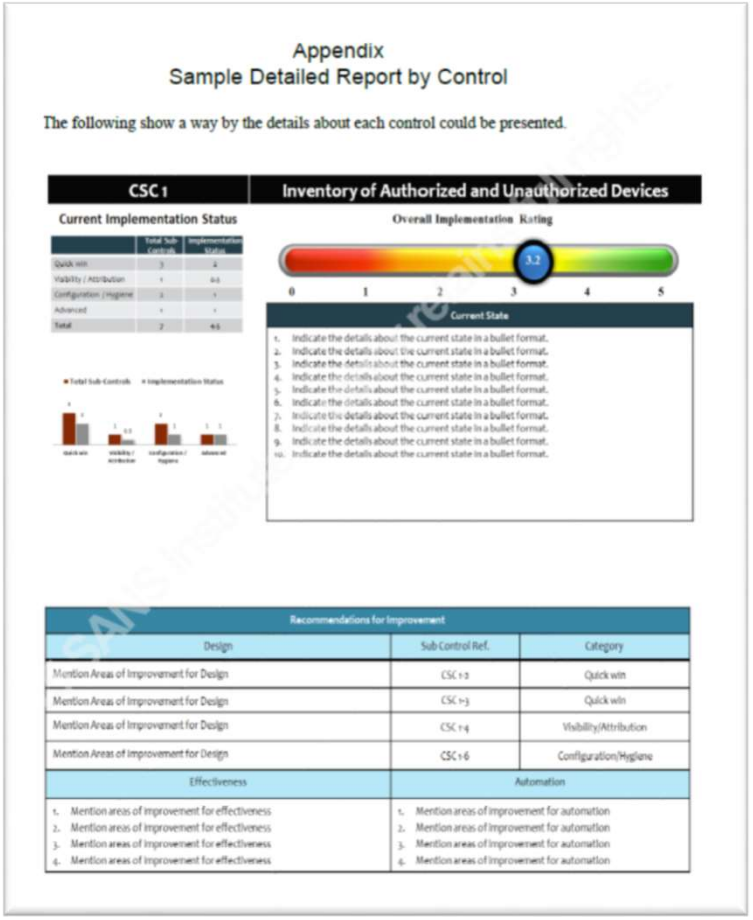
Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Framework for Assessing 20 Critical Controls Using ISO 15504 and COBIT 5 Process Assessment Model (PAM)

The 20 critical controls, maintained by the Council on CyberSecurity, present a prioritized road map for organizations to enhance their information security posture. However, an initial review that serves as a "baseline" must first be performed to know the current information security posture and to ascertain the effort required to implement the critical controls. Furthermore, assessments or audits should be performed periodically to gauge the continual improvement in information security as well as to what e...



Appendix
Sample Detailed Report by Control

The following show a way by the details about each control could be presented.

CSC 1	Inventory of Authorized and Unauthorized Devices

Current Implementation Status

Overall Implementation Rating

	Total Sub Controls	Implementation Status
Quick win	3	2
Visibility / Attribution	1	0.5
Configuration / Hygiene	2	1
Advanced	1	1
Total	7	4.5

0 1 2 3 4 5

Current State

1. Indicate the details about the current state in a bullet format.
2. Indicate the details about the current state in a bullet format.
3. Indicate the details about the current state in a bullet format.
4. Indicate the details about the current state in a bullet format.
5. Indicate the details about the current state in a bullet format.
6. Indicate the details about the current state in a bullet format.
7. Indicate the details about the current state in a bullet format.
8. Indicate the details about the current state in a bullet format.
9. Indicate the details about the current state in a bullet format.
10. Indicate the details about the current state in a bullet format.

Recommendations for Improvement

Design	Sub Control Ref.	Category
Mention Areas of Improvement for Design	CSC 1-1	Quick win
Mention Areas of Improvement for Design	CSC 1-3	Quick win
Mention Areas of Improvement for Design	CSC 1-4	Visibility/Attribution
Mention Areas of Improvement for Design	CSC 1-6	Configuration/Hygiene

Effectiveness	Automation
1. Mention areas of improvement for effectiveness	1. Mention areas of improvement for automation
2. Mention areas of improvement for effectiveness	2. Mention areas of improvement for automation
3. Mention areas of improvement for effectiveness	3. Mention areas of improvement for automation
4. Mention areas of improvement for effectiveness	4. Mention areas of improvement for automation

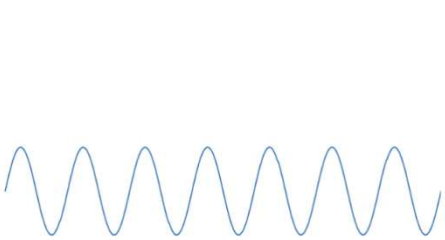
Abbiamo esteso il CSF NIST anche all'IoT
(ci scappa un'articolo sull'ISACA Journal !)

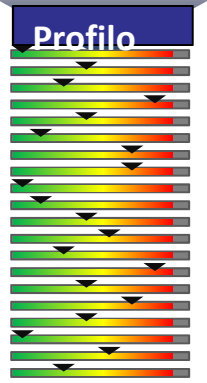
ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

CSF : si può usare per sistemi (complessi) che includano dispositivi IoT

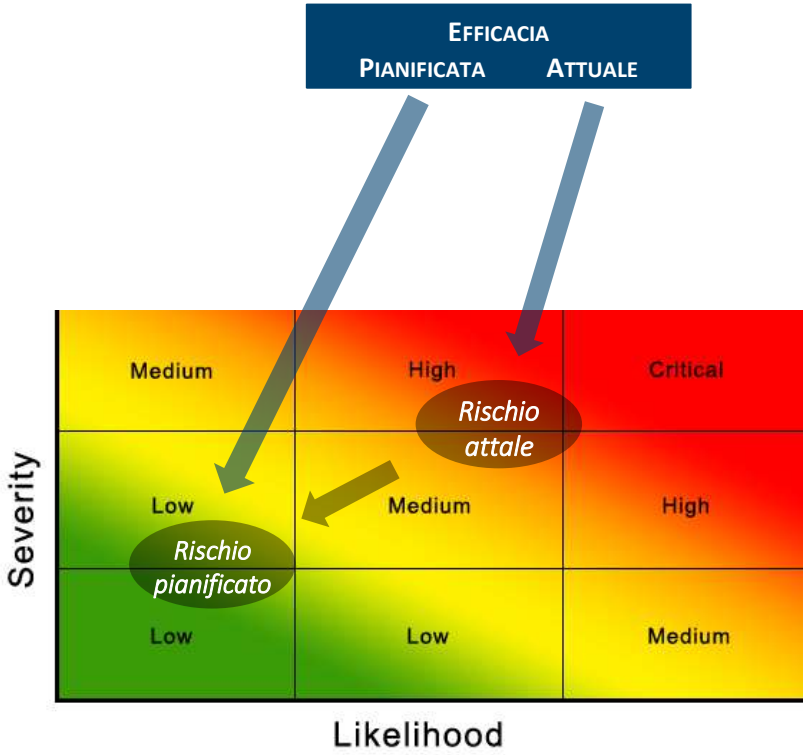
NIST Framework Core

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





Criticità della categoria / sottocategoria nel contesto in esame



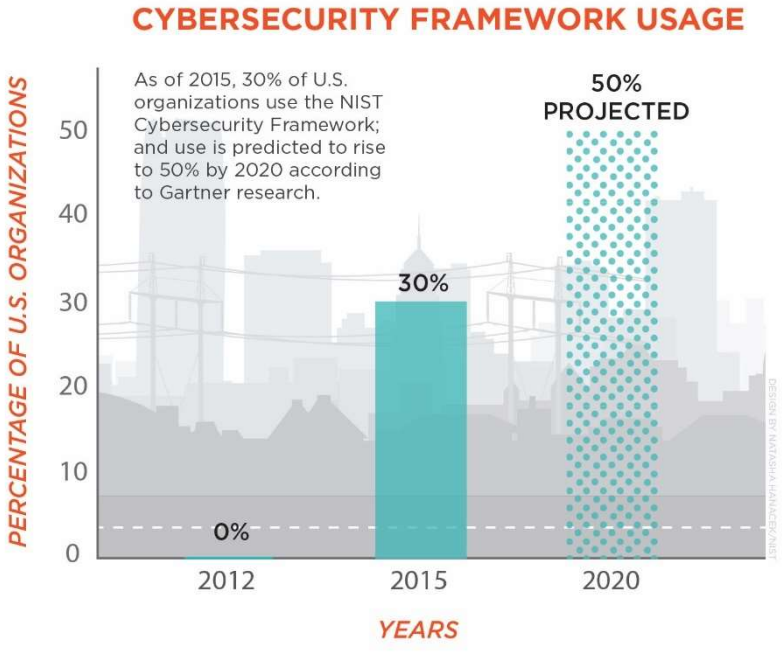
ISACA Sistemi informativi: averne fiducia e trarne valore Rome Chapter

Tre osservazioni finali

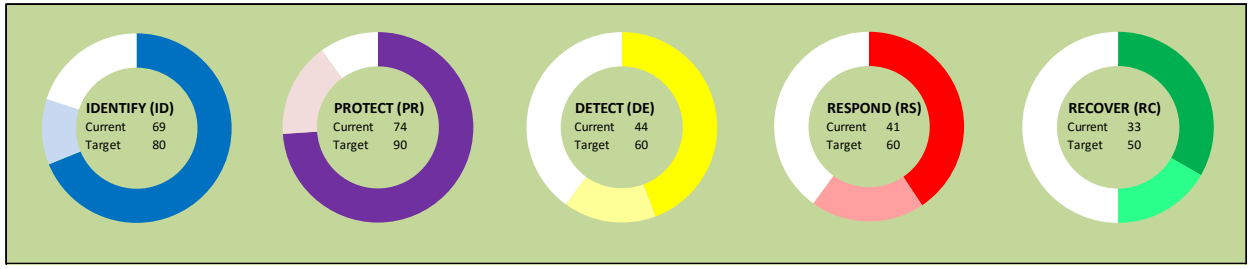
1. Non pensiamo (*osiamo*) di usare solo il CSC per IoT: otterremmo al massimo dei processi di controllo di tier 1 : si ricadrebbe nella «Compliance». Usiamo il «full» CSF NIST !
2. Il metodo è facilmente estensibile ad esempio :
    1. Mobile
    2. Cloud
    3. Data Protection (Data Protection by Design …….)
    4. Contesti speciali
3. e .....

... dal sito NIST:

- **Cybersecurity "Rosetta Stone" Celebrates Two Years of Success**
  February 18, 2016
- .... users include critical infrastructure giants Bank of America, U.S. Bank, and Pacific Gas & Electric, as well as Intel, Apple, AIG, QVC, Walgreen's and Kaiser Permanente. Universities and other organizations also rely on its guidance. In addition to private organizations in other countries, other governments, ***such as Italy***, are using it as the foundation for their national cybersecurity guidelines.
- ISACA, a global nonprofit association of information system professionals, participated in the framework process and now offers a course and related professional certification.
- .... riutilizzo dati assessment disponibili (AP)



NIST National Institute of Standards and Technology U.S. Department of Commerce



Azienda X

Cyber Security 2016

Planned Maturity

ISACA Sistemi informativi: averne fiducia e trarne valore Rome Chapter

Sitografia

http://www.nist.gov/cyberframework
https://www.sans.org/critical-security-controls
http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Assessment-Programme-FAQs.aspx
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=37458
http://www.nist.gov/itl/acd/cybersecurity-rosetta-stone-celebrates-two-years-of-success.cfm

Contatti

- alberto.piamonte@alice.it

Grazie...