WORKSHOP GARR 2018

Panel: Misure minime di sicurezza

29 maggio 2018

ISTITUTO ITALIANO DI TECNOLOGIA

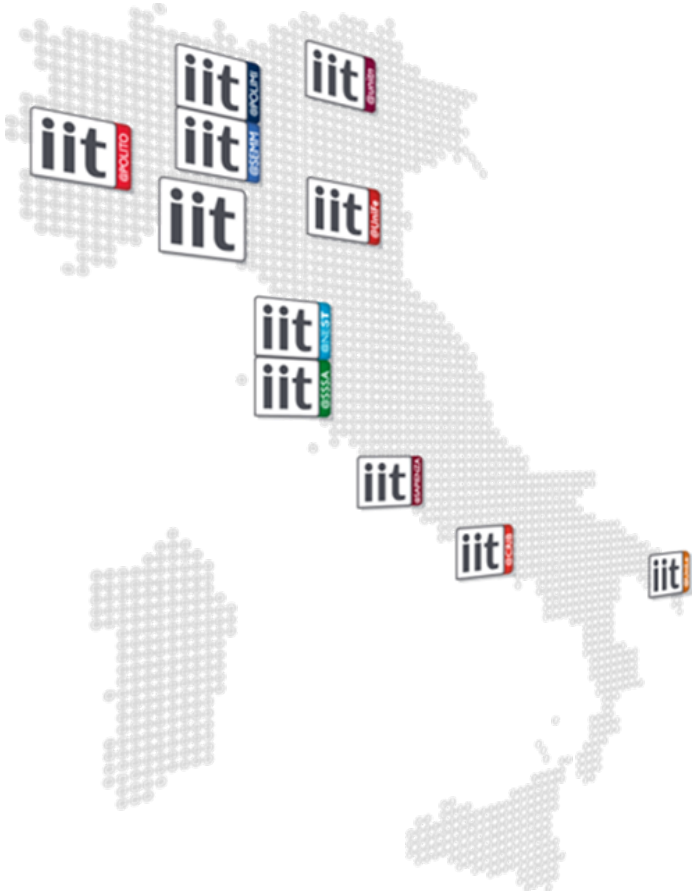
ISTITUTO ITALIANO DI TECNOLOGIA

IIT E I SUOI CENTRI

- **Center for Neuroscience e Cognitive Science, Università di Trento, TRENTO**
- **Center for Genomic Science, Campus IFOM-IEO, MILANO**
- **Center for Nano Science and Technology, Politecnico di Milano, MILANO**
- **Center for Sustainable Future Technologies, Politecnico di Torino, TORINO**
- **Center for Translational Neurophysiology, Università di Ferrara, FERRARA**
- **Center for Microbiorobotics, Scuola Superiore Sant'Anna, PISA**
- **Center for Nanotechnology Innovation, Scuola Normale Superiore, PISA**
- **Center for Life Nanoscience, Università degli Studi di Roma La Sapienza, ROMA**
- **Center for Advanced Biomaterials for Health Care, Università Federico II di Napoli, NAPOLI**
- **Center for Biomolecular Nanotechnologies, Università del Salento, LECCE**

ISTITUTO ITALIANO DI TECNOLOGIA

Central Research Laboratories, GENOVA



- **Machine Learning, MIT, BOSTON (USA)**
- **Neurobiology Dept., Harvard Univ., BOSTON (USA)**

IL PIANO SCIENTIFICO 2018-2023

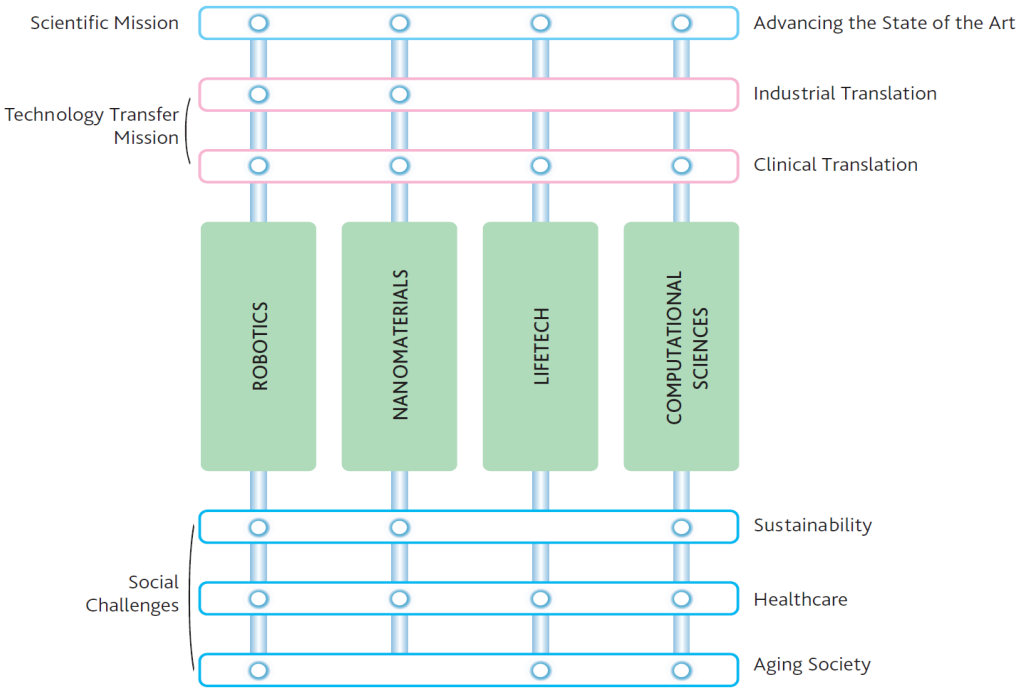
Il piano scientifico è articolato in **4 Domini di ricerca**:

Robotics contribuisce al progresso scientifico sviluppando nuove piattaforme robotiche sia in termini di hardware che di software

Nanomaterials ha come obiettivo la sintesi di nuovi materiali sostenibili e biodegradabili, lo studio di materiali nanocompositi e di materiali 2D

LifeTech si focalizza sullo sviluppo di strumenti per la genetica molecolare avanzata, l'elettrofisiologia, l'analisi computazionale e per l'imaging allo scopo di analizzare nel dettaglio i processi neurali microscopici che determinano le funzioni cerebrali

Computational Sciences incentra l'attività su estense simulazioni di sistemi fisici in grado di generare una vasta quantità di dati sui quali condurre robusti studi statistici e, dove possibile, operazioni di data mining



IL PROGETTO CYBER SECURITY DI IIT

ESIGENZE

Valutare il **livello di protezione dei dati trattati**, mediante un assessment di sicurezza.

Oltre agli aspetti privacy, oggetto di una attività parallela, è stato preso in considerazione lo **stato attuale dei processi, delle responsabilità, delle tecnologie** utilizzate dall'istituto per la gestione della sicurezza dei dati trattati nei processi amministrativi e nelle linee di ricerca.

OBIETTIVI

1. Mettere a disposizione dell'Istituto una fotografia della situazione attuale dell'organizzazione e delle contromisure in essere. **Metrica di riferimento: standard ISO/IEC 27001:2013**

2. Identificare le macro tipologie di dati e definire una **classificazione dei livelli di rischio associati** in funzione della necessità di Riservatezza, Integrità, Disponibilità e Privacy.

3. Attivare un percorso di miglioramento della sicurezza, attraverso un **piano di interventi con le azioni necessarie per la mitigazione dei rischi**, priorità di realizzazione in base agli obiettivi di sicurezza desiderati.

METODOLOGIA

- L'assessment sulla Sicurezza Informatica dei **dati trattati nell'ambito delle attività della Fondazione IIT** ha riguardato i dati trattati nell'ambito delle linee di ricerca e delle funzioni amministrative.
- Durante l'assessment, sono state svolte circa **novanta interviste alle funzioni di ricerca ed amministrative dell'Istituto**, per identificare le tipologie di dati da queste prodotte e il loro trattamento.

Tale attività ha permesso di:

- identificare le **macro categorie di dati trattati** ed il **livello di rischio associato** rispetto a valori di Business (Riservatezza/ Integrità/ Disponibilità) e Privacy

- identificare lo stato di implementazione dei controlli dello **standard ISO/IEC 27001 «Information security management systems – Requirements»**

ISTITUTO ITALIANO DI TECNOLOGIA

DATA RISK CLASSIFICATION

Il modello di riferimento è la Risk Classification adottata dalla Stanford University

(https://uit.stanford.edu/guide/riskclassifications)

Il modello in breve:

- **Classificazione dei dati su tre livelli di rishio**: HIGH, MEDIUM, LOW in base all'impatto in termini di perdite finanziare, reputazione e mission che la perdita di Riservatezza- Integrità- Disponibilità causa all'organizzazione. Oppure obblighi di legge (privacy,…)

  Questa classificazione deriva da FIPS PUB 199- Federal Information Processing Standard Publication- Standard for security categorization of federal information ad information systems

- **Definizione delle misure minime di sicurezza per Server e End-point** in base al trattamento di dati H, M, L risk

- **Definizione delle misure minime di sicurezza per le applicazioni** in base al trattamento di dati H, M, L risk

- **Pubblicazione di un catalogo di servizi** con indicazione della rispondenza al trattamento di dati H, M, L risk

ISTITUTO ITALIANO DI TECNOLOGIA

I CONTROLLI ISO 27001 &C

- I 114 controlli totali dello standard ISO 27001:2013 sono stati raggruppati nelle **10 AREE DI INTERVENTO** riportate nella tabella
- I controlli risultati applicabili al contesto dell'Istituto e rientranti nel perimetro di **Assessment di Sicurezza ICT sono 103**
- Ciascun intervento fa riferimento ad un **dominio della norma ISO 27001** rispetto al quale è stata condotta l'attività di Assessment, meglio **adattato alle caratteristiche dell'Istituto**, in maniera tale da consentire la valutazione del livello di mitigazione dei rischi a seguito dell'implementazione degli interventi stessi
- Sono stati verificati i controlli del framework CINI
- Sono stati verificati i controlli delle Misure minime di sicurezza AGID

Aree di intervento	Controlli valutati
Sicurezza dei sistemi	20
Normativa e controlli	16
Organizzazione, formazione e consapevolezza	14
Sicurezza delle applicazioni	14
Gestione degli accessi logici	11
Protezione dei dati	9
Sicurezza della rete	6
Gestione dei log	5
Gestione sicura dei fornitori	5
Gestione degli accessi fisici	3
Totale controlli applicabili	**103**

ISTITUTO
ITALIANO DI
TECNOLOGIA

NIST

Title III of the E-Government Act (Public Law 107-347), titled the Federal Information Security Management Act (FISMA), tasked the National Institute of Standards and Technology (NIST) to develop:

- Standards to be used by all Federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;
- Guidelines recommending the types of information and information systems to be included in each such category; and
- Minimum information security requirements (i.e., management, operational, and technical security controls), for information and information systems in each such category.

FIPS 200 AND SP 800-53

IMPLEMENTING INFORMATION SECURITY STANDARDS AND GUIDELINES

FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory federal standard developed by NIST in response to FISMA. To comply with the federal standard, organizations first determine the security category of their information system in accordance with FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, derive the information system impact level from the security category in accordance with FIPS 200, and then apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. Organizations have flexibility in applying the baseline security controls in accordance with the guidance provided in Special Publication 800-53. This allows organizations to tailor the relevant security control baseline so that it more closely aligns with their mission and business requirements and environments of operation.

FIPS 200 and NIST Special Publication 800-53, in combination, ensure that appropriate security requirements and security controls are applied to all federal information and information systems. An organizational assessment of risk validates the initial security control selection and determines if additional controls are needed to protect organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. The resulting set of security controls establishes a level of security due diligence for the organization.

1.3 Relationship to Other Documents

NIST Special Publication (SP) 800-60 is a member of the NIST family of security-related publications including:

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems;*
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;

---

[2] FISMA defines a *national security system* as any information system (including telecommunications system) used or operated by an agency or by a contractor on behalf of an agency, or any other organization on behalf of an agency – (i) the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapon system; or is critical to the direct fulfillment of military or intelligence missions (excluding a routine administrative or business system used for applications such as payroll, finance, logistics, and personnel management); or (ii) that processes classified information. [See Public Law 107-347, Section 3542 (b)(2)(A).]

- NIST SP 800-30, *Risk Management Guide for Information Technology Systems;*[3]
- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems;*
- NIST Draft SP 800-39, *Managing Risk from Information Systems: An Organization Perspective;*
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems;*
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*; and
- NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System.*

Table 1: Information and Information System Security Objectives

Security Objectives	FISMA Definition [44 U.S.C., Sec. 3542]	FIPS 199 Definition
Confidentiality	"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"	A loss of *confidentiality* is the unauthorized disclosure of information.
Integrity	"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…"	A loss of *integrity* is the unauthorized modification or destruction of information.
Availability	"Ensuring timely and reliable access to and use of information…"	A loss of *availability* is the disruption of access to or use of information or an information system.

Table 2: Potential Impact Levels

Potential Impact	Definitions
Low	The potential impact is **low** if—The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.[7] A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	The potential impact is **moderate** if—The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
High	The potential impact is **high** if—The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

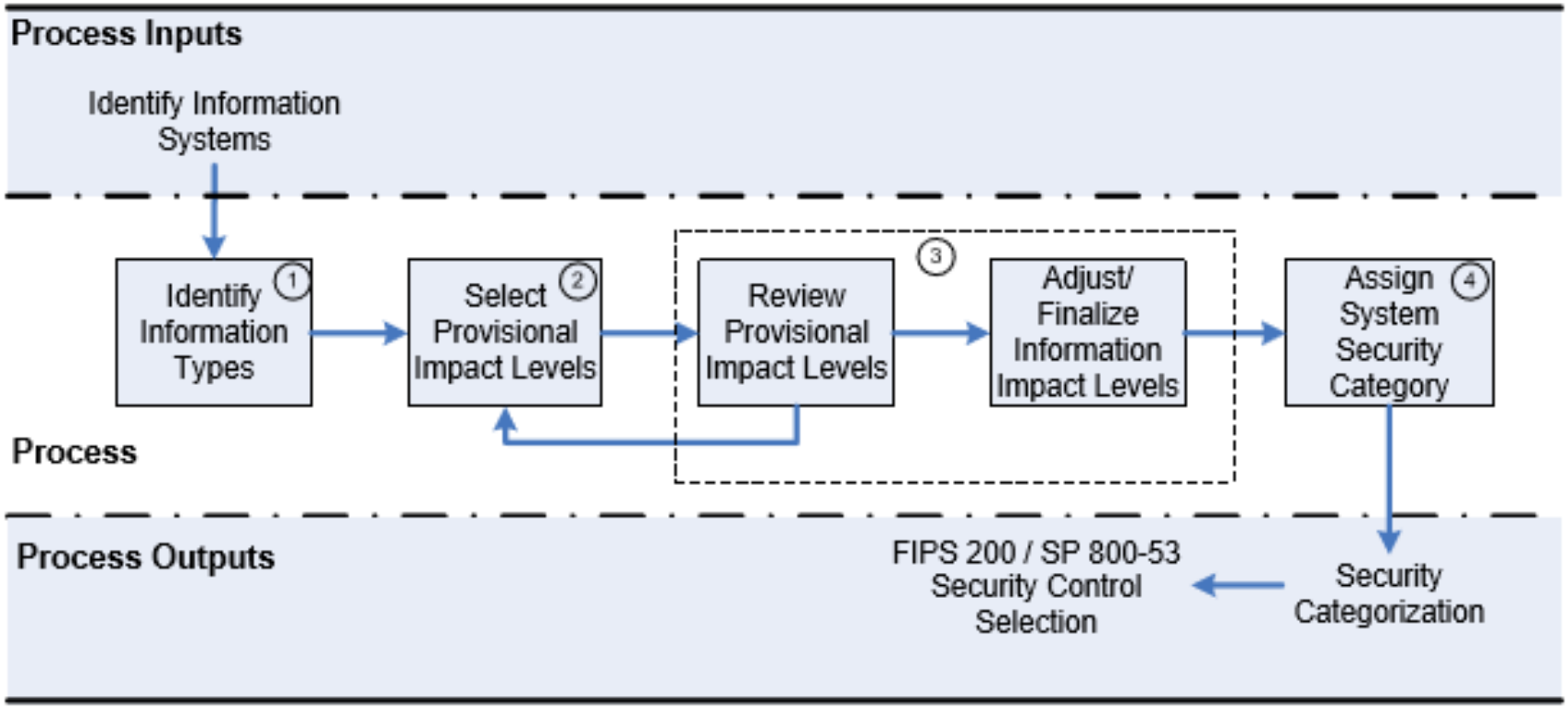


Figure 2: SP 800-60 Security Categorization Process Execution

ISTITUTO ITALIANO DI TECNOLOGIA

Table 3: SP 800-60 Process Roadmap

Process Step	Activities	Roles
Input: Identify information systems	• Agencies should develop their own policies regarding information system identification for security categorization purposes. The system is generally bounded by a security perimeter[11].	CIO; SAISO; Mission Owners

Step 1
Identify Information Types →
	• Document the agency's business and mission areas
	• Identify all of the information types that are input, stored, processed, and/or output from each system [Section 4.1]
	  ○ Identify *Mission–based* Information Type categories based on supporting FEA Lines of Business [Section 4.1.1]
	  ○ As applicable, identify *Management and Support* Information Type categories based on supporting FEA Lines of Business [Section 4.1.2]
	  ○ Specify applicable sub-functions for the identified *Mission-based* and *Management and Support* categories [Volume II, Appendices C and D]
	  ○ As necessary, identify other required information types [Sections 4.1.3, 4.1.4]
	• Document applicable information types for the identified information system along with the basis for the information type selection [Section 4.5]
		Mission Owners; Information Owners

Step 2
Select Provisional Impact Levels → ↑
	• Select the security impact levels for the identified information types
	  ○ from the recommended provisional impact levels for each identified information type [Volume II, Appendices C and D)
	  ○ or, from FIPS 199 criteria provided in Table 7 Section 4.2.1, and Section 4.2.2
	• Determine the security category (SC) for each information type: $SC_{information\ type}$ = {(confidentiality, impact), (integrity, impact), (availability, impact)}
	• Document the provisional impact level of confidentiality, integrity, and availability associated with the system's information type [Section 4.5]
		Information System Security Officer (ISSO)

Step 3
Review Provisional Impact Levels →
Adjust/ Finalize Information Impact Levels →
	• Review the appropriateness of the provisional impact levels based on the organization, environment, mission, use, and data sharing [Section 4.3]
	• Adjust the impact levels as necessary based on the following considerations:
	  ○ Confidentiality, integrity, and availability factors [Section 4.2.2]
	  ○ Situational and operational drivers (timing, lifecycle, etc.) [Section 4.3]
	  ○ Legal or statutory reasons
	• Document all adjustments to the impact levels and provide the rationale or justification for the adjustments [Section 4.5]
		SAISO; ISSO; Mission Owners; Information Owners

Step 4 Assign System Security Category ↓	• Review identified security categorizations for the aggregate of information types. • Determine the system security categorization by identifying the security impact level high water mark for each of the security objectives (confidentiality, integrity, availability): $SC_{System\ X}$ = {(confidentiality, impact), (integrity, impact), (availability, impact)} • Adjust the security impact level high water mark for each system security objective, as necessary, by applying the factors discussed in section 4.4.2. • Assign the overall information system impact level based on the highest impact level for the system security objectives (confidentiality, integrity, availability) • Follow the agency's oversight process for reviewing, approving, and documenting all determinations or decisions [Section 4.5]	CIO, SAISO; ISSO; Mission Owners; Information Owners
Output: Security Categorization	• Output that can be used as input to the selection of the set of security controls necessary for each system and the system risk assessment • The minimum security controls recommended for each system security category can be found in NIST SP 800-53, as updated	CIO; ISSO; Authorizing Officials; Developers

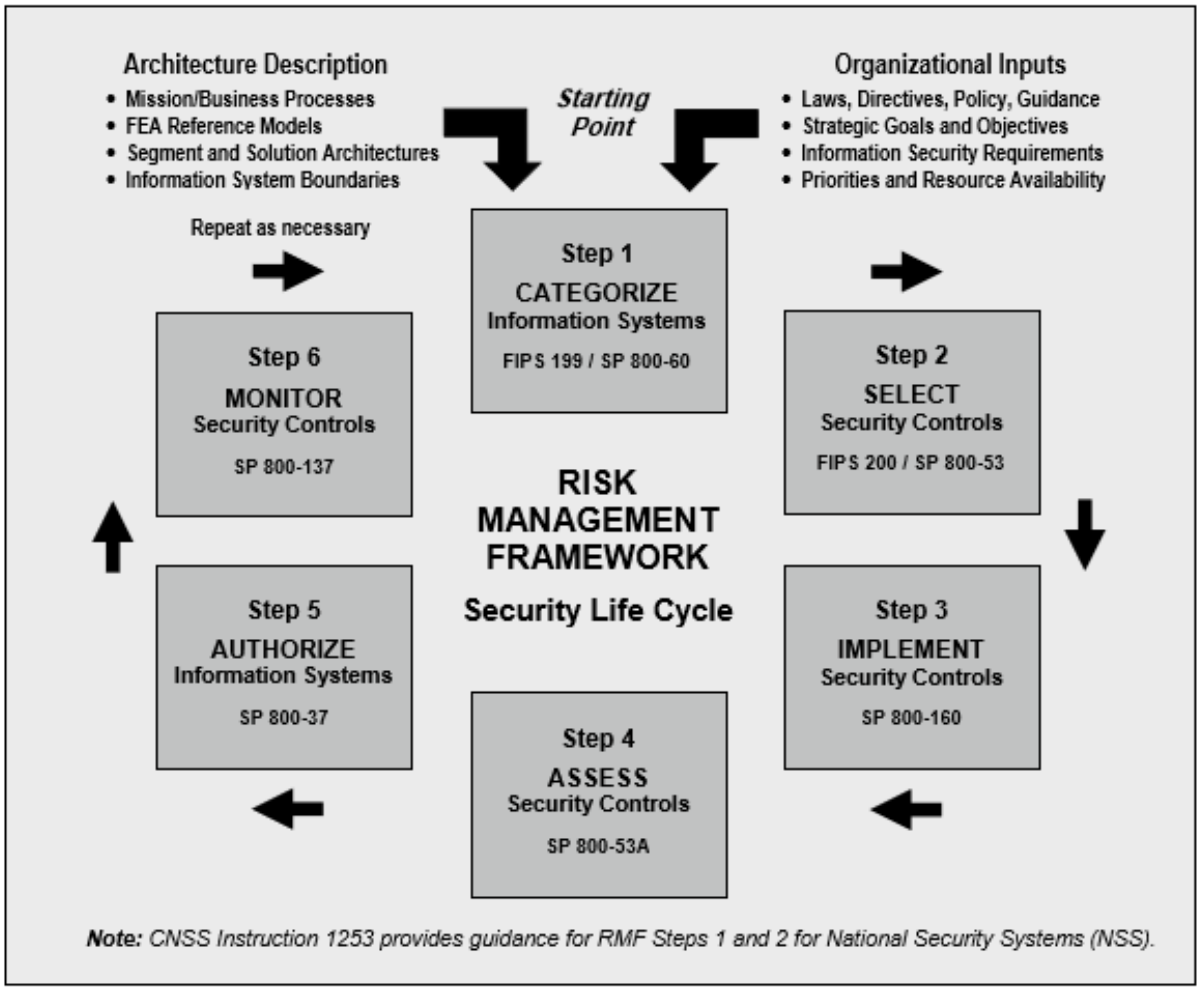


FIGURE 2: RISK MANAGEMENT FRAMEWORK

ISTITUTO ITALIANO DI TECNOLOGIA

ISO 27001 &C