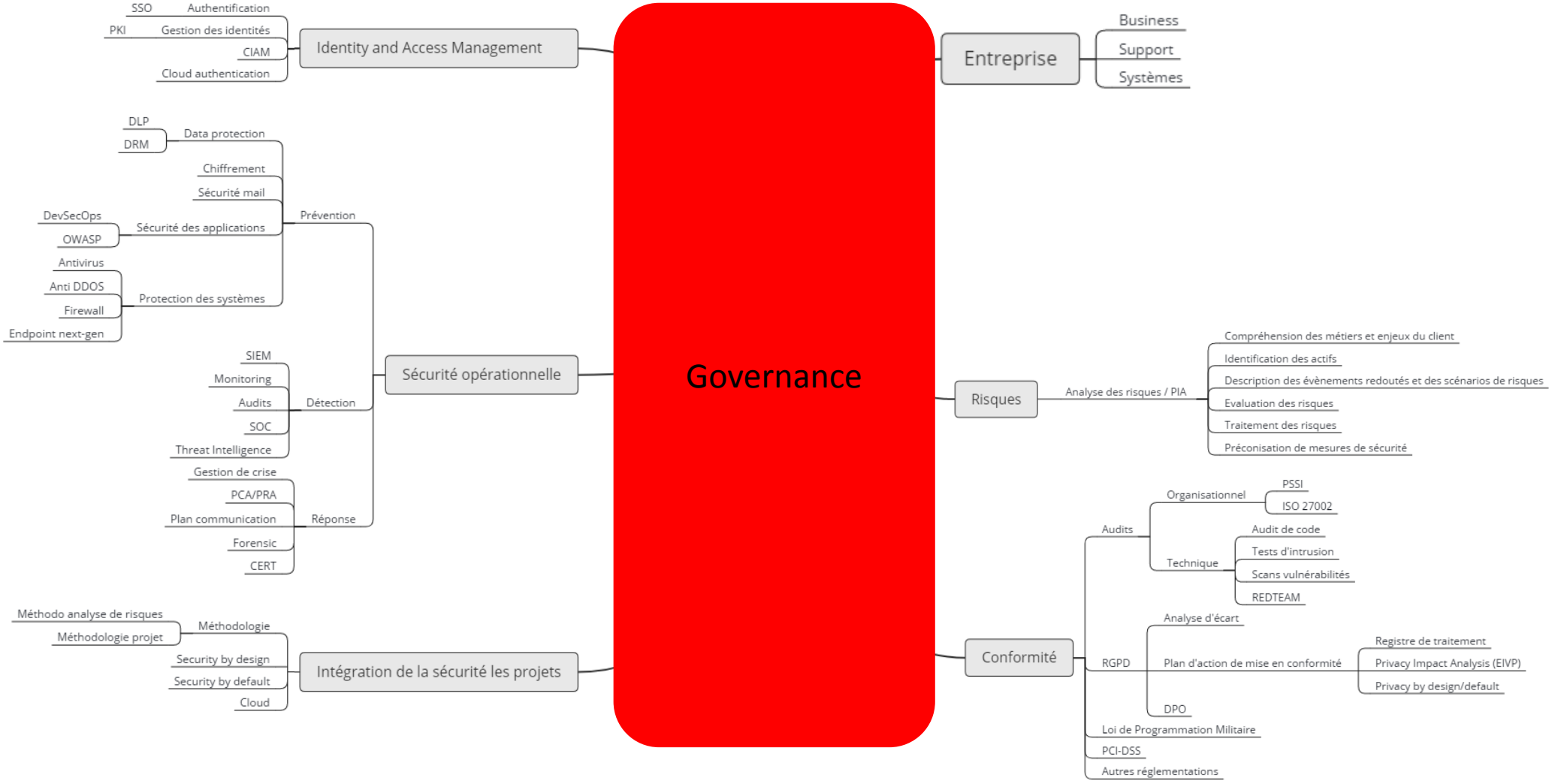
HOW TO DEFINE GLOBAL SECURITY FOR THE COMPANY ?

GOVERNANCE

INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
CENTRE VAL DE LOIRE

Example of security topics, ruled by governance



Information security policy

- Policy is an essential foundation of effective infosec program

- The success of an information resources protection program depends on the policy generated, & on the attitude of management toward securing information on automated systems.

- You, the policy maker, set the tone & the emphasis on how important a role infosec will have within your agency.

- Your primary responsibility is to set the information resource security policy for the organization with the objectives of reduced risk, compliance with laws & regulations, & assurance of operational continuity, information integrity, & confidentiality.”

Defense layer

1. Policies: first layer of defense
2. Networks: threats first meet organization's network
3. Systems: computers & manufacturing systems
4. Applications: all applications systems

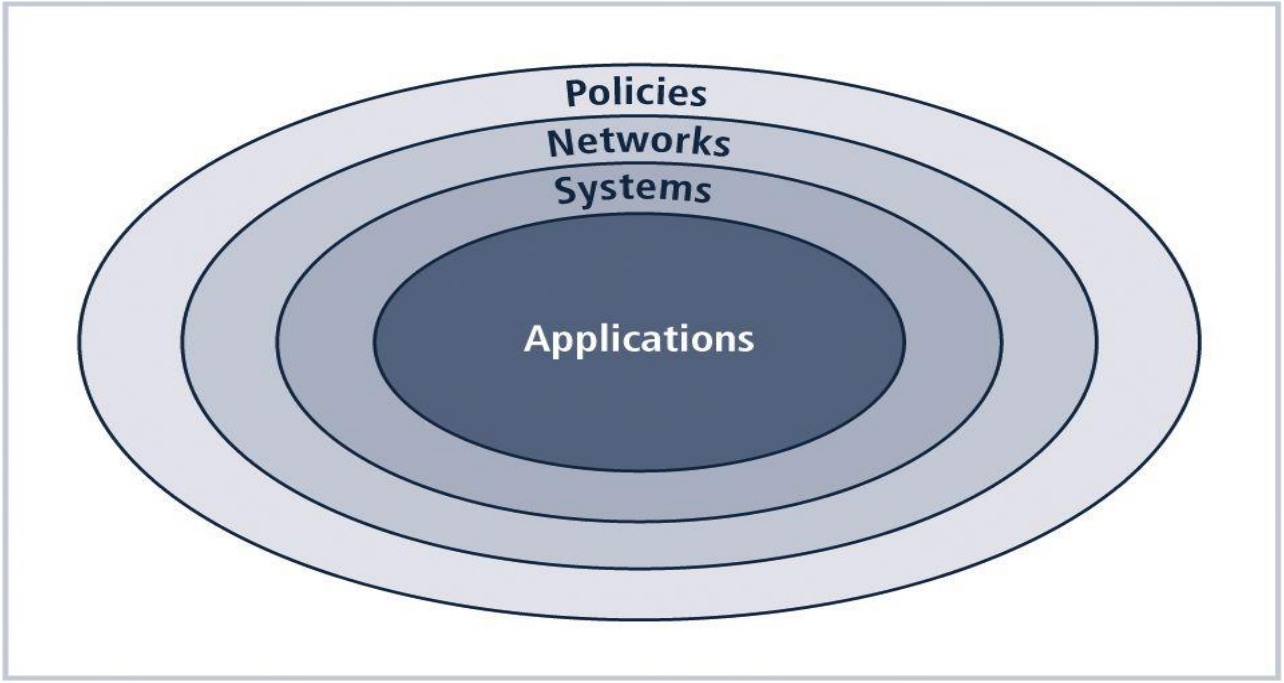


FIGURE 4-1 The Bull's-Eye Model

IS documentation organization

- Policy: plan or course of action that influences & determines decisions
- Standards: more detailed statement of what must be done to comply with policy
- Practices, procedures & guidelines:explain how employees will comply with policy

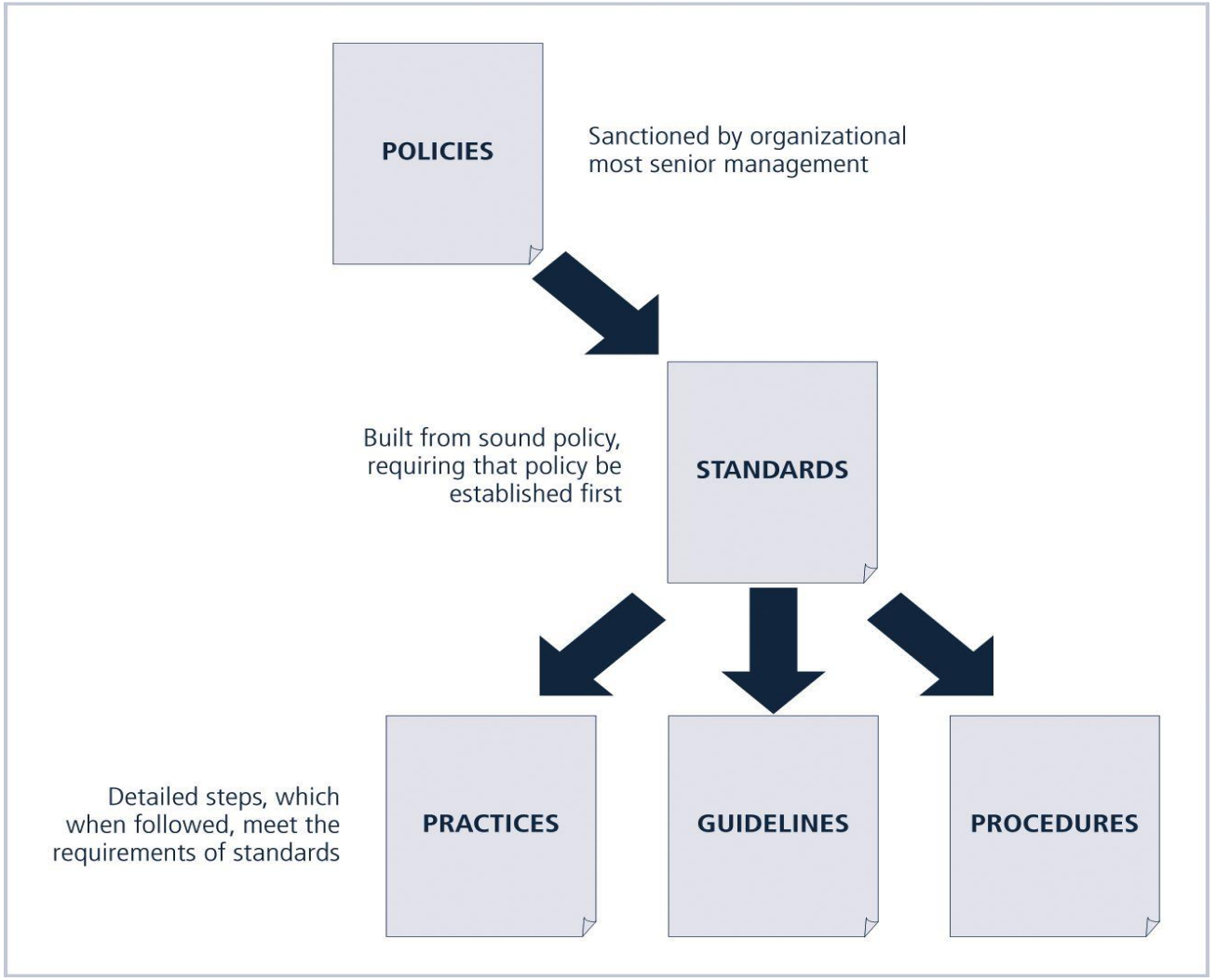


FIGURE 4-2 Policies, Standards, and Practices

- Policies are important reference documents for internal audits & for resolution of legal disputes about management's due diligence
- Policy documents can act as a clear statement of management's intent

- For policies to be effective, they must be:
  - Properly disseminated
  - Read
  - Understood
  - Agreed-to

Enterprise Information Security Policy

- Statement of Purpose:
  - What the policy is for
- Information Technology Security Elements:
  - Defines infosec
- Need for Information Technology Security:
  - justifies importance of infosec in the organization
- Information Technology Security Responsibilities & Roles:
  - Defines organizational structure
- References Information Technology standards & guidelines

Example IS documentation

Information Security Basic Regulations	Policy

Information Lifecycle Management	Policy
Data Privacy policy	Policy
Security controls for Handling Personal Information	Standard

Business Continuity Plan	

Risk Management Policy	Policy
Risk Assessment tool	Tool

Incident Management Policy	Policy
Incident Response Plan	Standard
Crisis Management	Standard
Data Breach Incident Notification	Standard

Network Infrastructure Security	Standard
Secure Application Development LifeCycle	Standard
Vulnerability and Patch Management	Standard
WebApplication Security Policy	Standard
Cryptography Standard	Standard
Logging and Monitoring	Standard
Backup and restore	Standard
Service Provider Privacy and Information Security Questionnaire	Standard
Identity and Access Management	Standard

WE NEED TO MAKE THINGS WORK

ISO STANDARD

INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
CENTRE VAL DE LOIRE

Context

- ISO
- International Standard Organization



- Independent, non-governmental international organization
- Composed of 162 national standards bodies
- AFNOR is the French org

> International Standards **make things work**. They give world-class specifications for products, services and systems, to ensure quality, safety and efficiency. They are instrumental in facilitating **international trade**.

ISO enables a **consensus** to be reached on solutions that meet both the requirements of business and **the broader needs of society**

ISO standards in Information Security : 27k range

"….This International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ***Information Security Management System (ISMS)*****….."**

ISO 27000
Vocabulary

ISO 27001
Requirements

ISO 27006
Requirements for bodies audit and certification

Specification

ISO 27002
Code of practice

ISO 27003
Implementation guidance

ISO 27005
Risk management

Code of conduct

ISO 27011
Telecommunications

ISO 27017
Cloud computing service

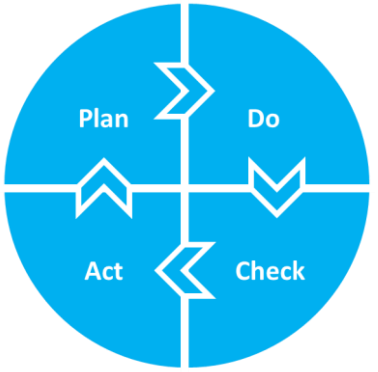
ISO 27799
Health

Specific applicability

Overview of ISO 27k range

ISO 27001

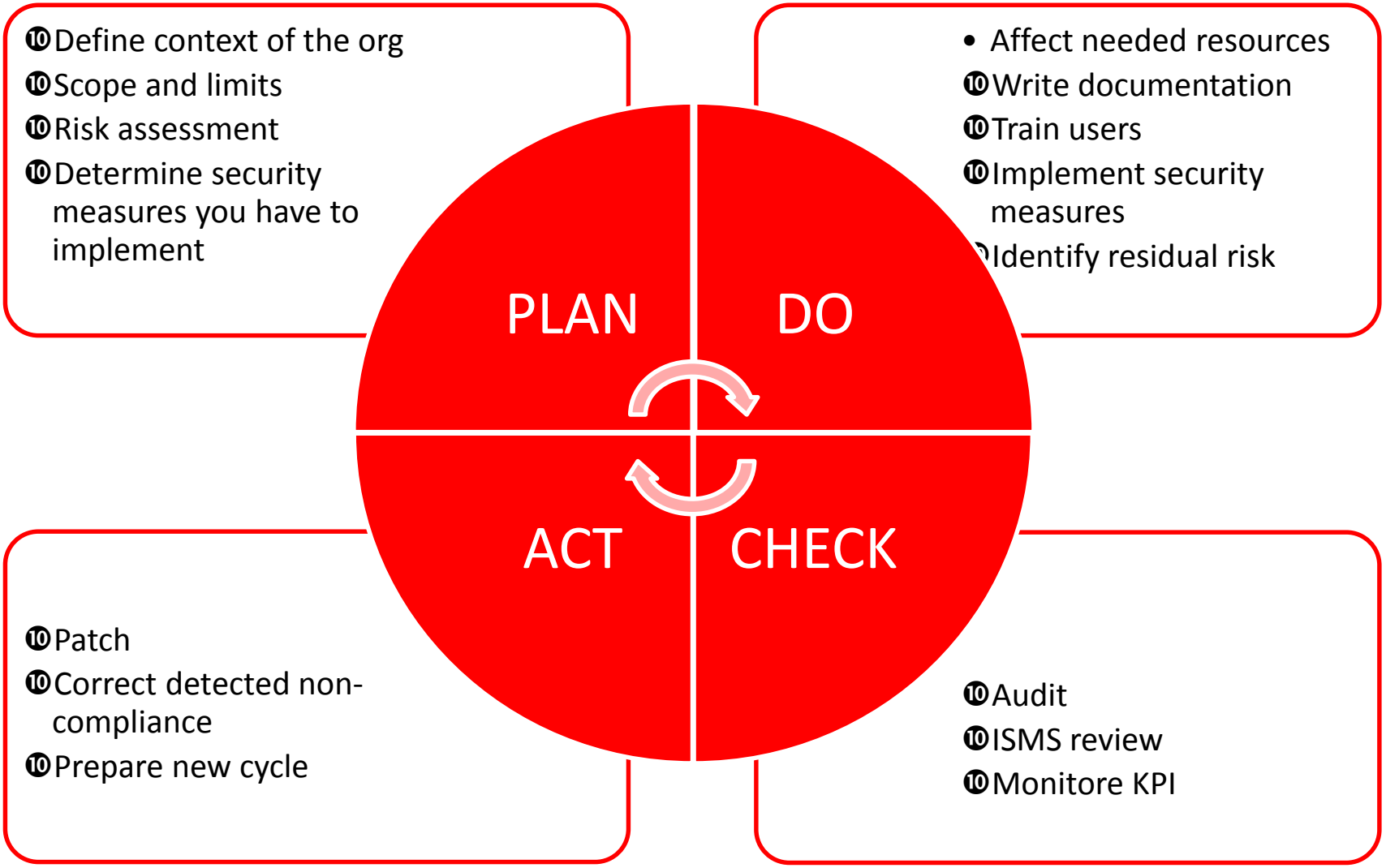
ISO270001– Information Technology – Security Techniques– Information security management systems Requirements



- ISMS – Information Security Management Systems

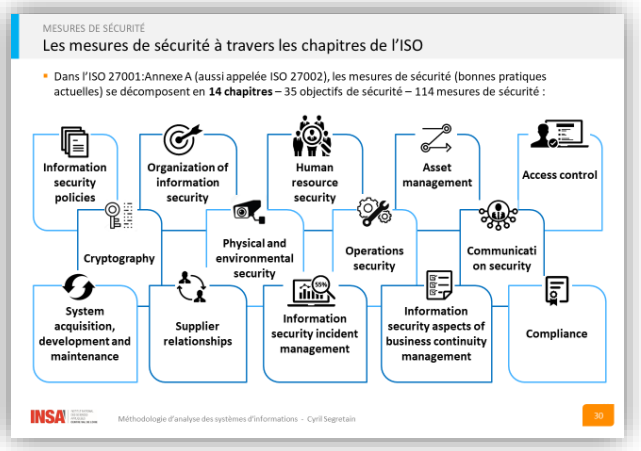
- This International Standard specifies the requirements for :
  - establishing,
  - implementing,
  - operating,
  - monitoring,
  - reviewing,
  - maintaining and
  - improving a documented information security management system within the context of the organization’s business activities and the risks it faces.

ISO 27001 : continuous improvement



ISO 27002 - Information Technology – Security Techniques – Code of practice for information security management

Chap	Title
A 5	Information security policy
A 6	Organization of information security
A 7	Human resource security
A 8	Asset management
A 9	Access control
A 10	Cryptography
A 11	Physical and environmental security
A 12	Operations security
A 13	Communication security
A 14	System acquisition, development and maintenance
A 15	Supplier relationships
A 16	Information security incident management
A 17	Information security aspects of business continuity management
A 18	Compliance

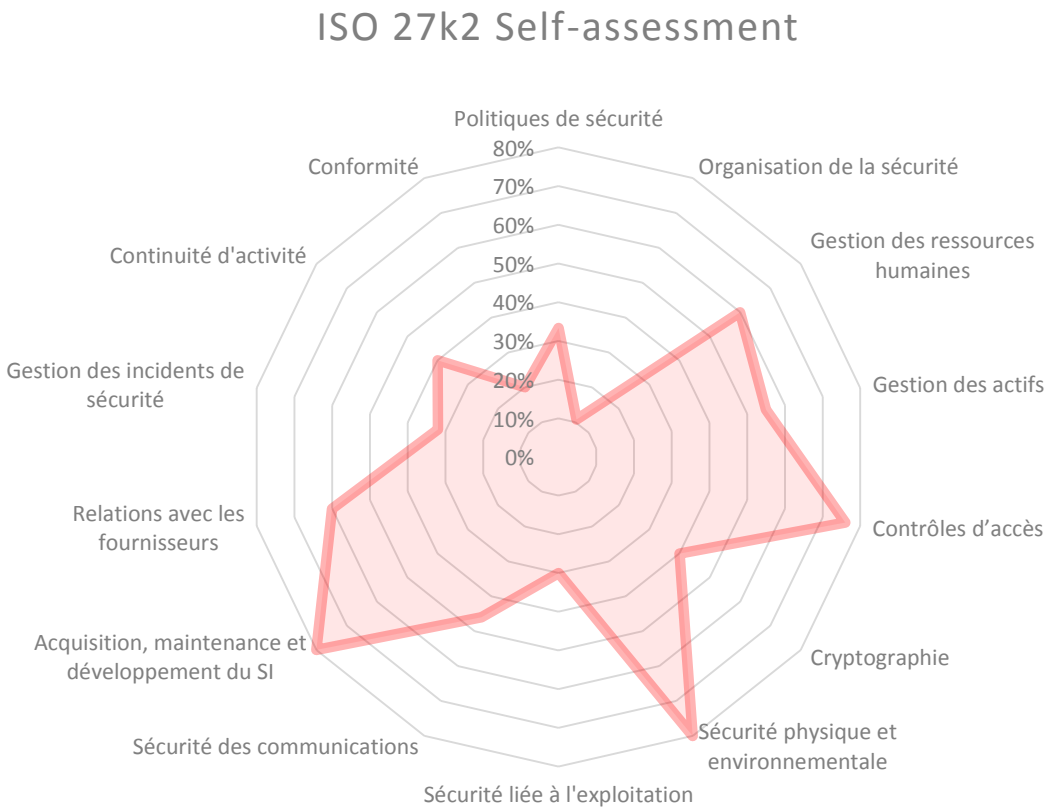


ISO 27002 Self-assessment

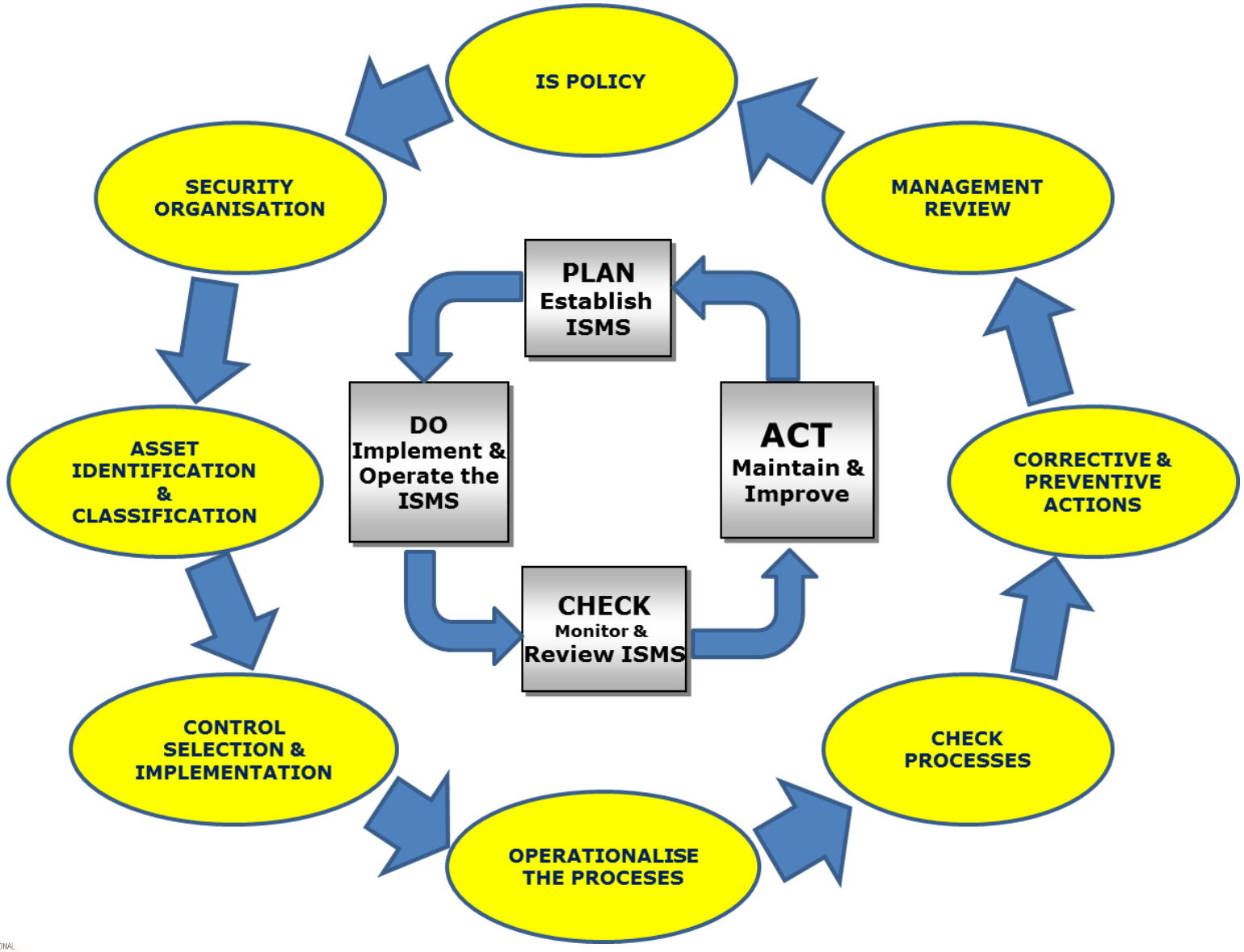
- ISO 27002 standard is used to do security self-assessment

- It allows a company to evaluate its security maturity and plan security programs.

- Organizational audit are mainly done with that ISO standard.



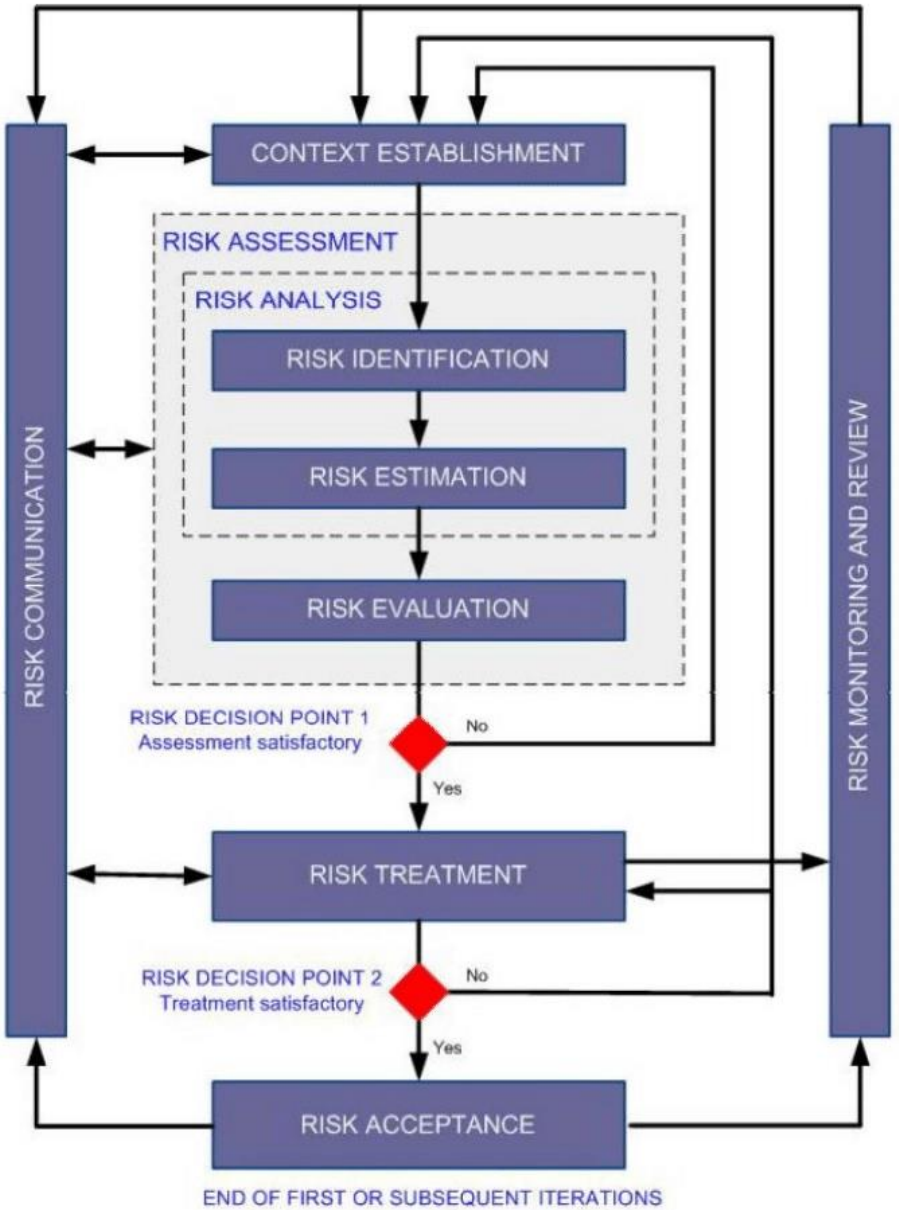
PDCA implementation



ISO 27005

- *ISO 27001 explicit a risk assessment methodology that can made comparable and redoable results.*

ISO27005 – Risk management



ANNEXES

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

Annexes - Liste normes ISO famille 27000

Norme	Intitulé
ISO/CEI 27000	Introduction et vue globale de la famille des normes, ainsi qu'un glossaire des termes communs (mai 2009)
ISO/CEI 27001	Norme d'exigences des SMSI, permettant la certification (publiée en 2005, révisée en 2013)
ISO/CEI 27002	Guide des bonnes pratiques en SMSI (précédemment connu sous le nom de ISO/CEI 17799, et avant BS 7799 Partie 1 (renuméroté en ISO/CEI 27002:2005 en juillet 2007, dernière révision en 2013)
ISO/CEI 27003	Guide d'implémentation d'un SMSI, publié le 3 février 2010 (Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information)
ISO/CEI 27004	Norme de mesures de management de la sécurité de l'information (publiée le 12 juillet 2009)
ISO/CEI 27005	Norme de gestion de risques liés à la sécurité de l'information (publiée le 4 juin 2008, révisée le 19 mai 2011)
ISO/CEI 27006	Guide de processus de certification et d'enregistrement (publié (en) le 1er décembre 2011)
ISO/CEI 27007	Guide directeur pour l'audit des SMSI (publié (en) le 14 novembre 2011)
ISO/CEI 27008	Lignes directrices de vérification en matière de mesures de sécurité (publiée (en) le 15 octobre 2011)
ISO/CEI 27010	Gestion de la sécurité de l'information des communications intersectorielles et interorganisationnelles
ISO/CEI 27011	Guide pour l'implémentation de ISO/CEI 27002 dans l'industrie des télécommunications (publié le 15 décembre 2008)
ISO/CEI 27013	Guide sur la mise en œuvre intégrée de l'ISO/CEI 27001 et de l'ISO/CEI 20000-1
ISO/CEI 27014	Gouvernance de la sécurité de l'information
ISO/CEI 27015	Lignes directrices pour le management de la sécurité de l'information pour les services financiers
ISO/CEI 27016	Management de la sécurité de l'information -- Économie organisationnelle
ISO/CEI 27017	Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/CEI 27002 pour les services du nuage
ISO/CEI 27018	Guide de pratiques pour la protection des données à caractère personnel (PII - personally identifiable information) dans les clouds publics (publié le 29 juillet 2014)
ISO/CEI 27019	Lignes directrices de management de la sécurité de l'information fondées sur l'ISO/CEI 27002 pour les systèmes de contrôle des procédés spécifiques à l'industrie de l'énergie
ISO/CEI 27031	Lignes directrices pour mise en état des technologies de la communication et de l'information pour continuité des affaires (publiée le 1er mars 2011)
ISO/CEI 27032	Lignes directrices pour la cybersécurité (publiée le 7 juillet 2012)
ISO/CEI 27034	Sécurité des applications
ISO/CEI 27035	Gestion des incidents
ISO/CEI 27036	Sécurité d'information pour la relation avec le fournisseur
ISO/CEI 27037	Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques (publié le 15 octobre 2012)
ISO/CEI 27038	Spécifications pour la rédaction numérique
ISO/CEI 27039	Sélection, déploiement et opérations des systèmes de détection d'intrusion (publié le 11 février 2015)
ISO/CEI 27040	Sécurité de stockage (publié le 5 janvier 2015)
ISO/CEI 27799	Guide pour l'implémentation de ISO/CEI 27002 dans l'industrie de la santé (publié le 12 juin 2008), sera probablement renommé en 2701x

Annexes – Termes ISO/EBIOS

NORME	METHODE
ISO 27005	EBIOS 2010
Appréciation des risques	Appréciation des risques
Actif	Bien
Actif primordial	Bien essentiel
Actif de support	Bien support
Propriétaire	Dépositaire / Propriétaire
Critère de risque (C,I,D)	Critère de sécurité
Source de la menace	Source de menace
Menace	Menace
Vulnérabilité	Vulnérabilité
Evénement	Evénement / Menace
Incident	Incident
Scénario d'incident	Risque / Evénement redouté/ scénario de menace
Impact	Impact
Conséquence	Conséquence
Objectif de sécurité	Objectif de sécurité
Mesure de sécurité	Mesure de sécurité
Vraisemblance	Vraisemblance
Vraisemblance de la menace	Force d'occurrence

Politique de Sécurité des Systèmes d'Information de l'Etat - PSSIE

Politique de Sécurité des Systèmes d'Information de l'Etat - PSSIE

Politique de Sécurité des Systèmes d'Information de l'Etat - PSSIE

Politique de Sécurité des Systèmes d'Information de l'Etat - PSSIE