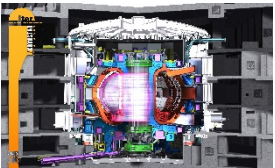

ITER organization's experience ensuring the trustworthiness of individuals accessing sensitive locations or information.

Christophe RAMU
Security, Health and Safety division head

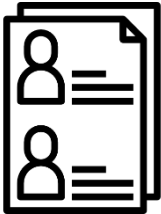
Disclaimer: The views and opinions expressed herein do not necessarily reflect those of the ITER Organization

Presentation



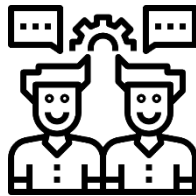
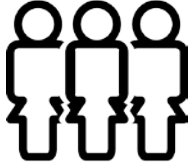
ITER Project

Identity verification



Trustworthiness assessment

New employees
Evaluation and support



Security awareness

Employee satisfaction



Confidentiality
(security of information)



Physical compartmentalization
of areas

Compartmentalization of activities



Sanctions

ITER

A multinational scientific collaboration without equivalent in history
A large-scale experiment to demonstrate the feasibility
of fusion energy



ITER Project



The way to a new, clean, safe and unlimited energy



ITER mission



To demonstrate the scientific and technological feasibility of fusion power for peaceful purposes

ITER is the only magnetic fusion device under construction aimed to produce a burning plasma.

Input (heating power): 50 MW

Output (fusion power): 500 MW

An integrated project:

Central Team & Seven Domestic Agencies

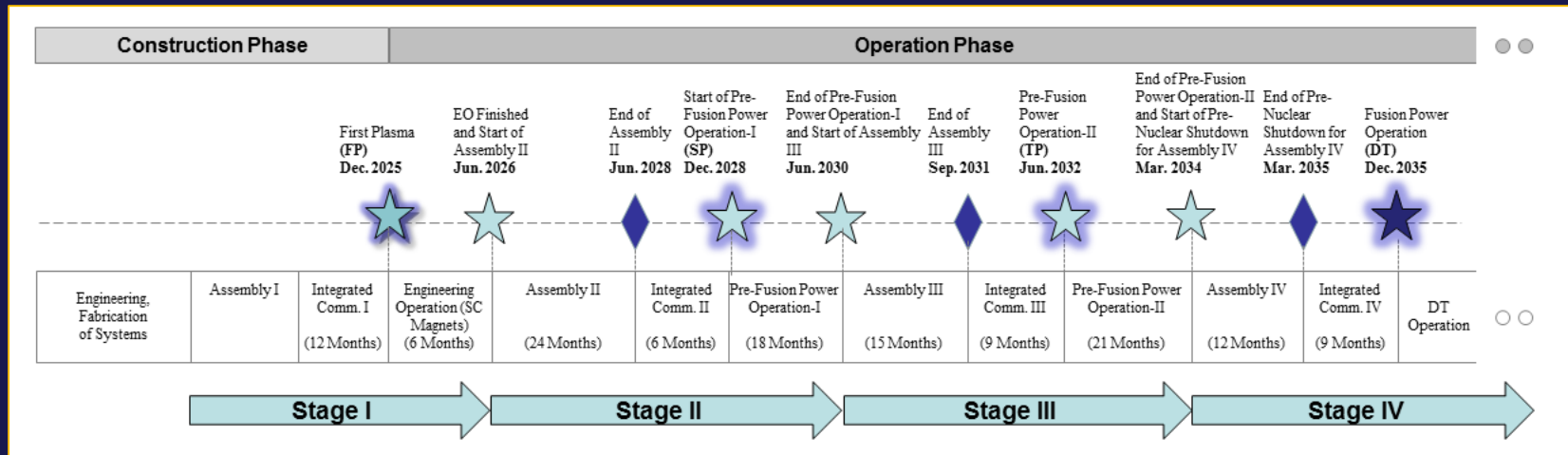
- The 7 ITER Members make cash and in-kind contributions (90%) to the ITER Project. They have established Domestic Agencies to handle the contracts to industry.
- The ITER Organization Central Team manages the ITER Project in close collaboration with the 7 Domestic Agencies.
- The ITER Members share all intellectual Property generated by the Project.



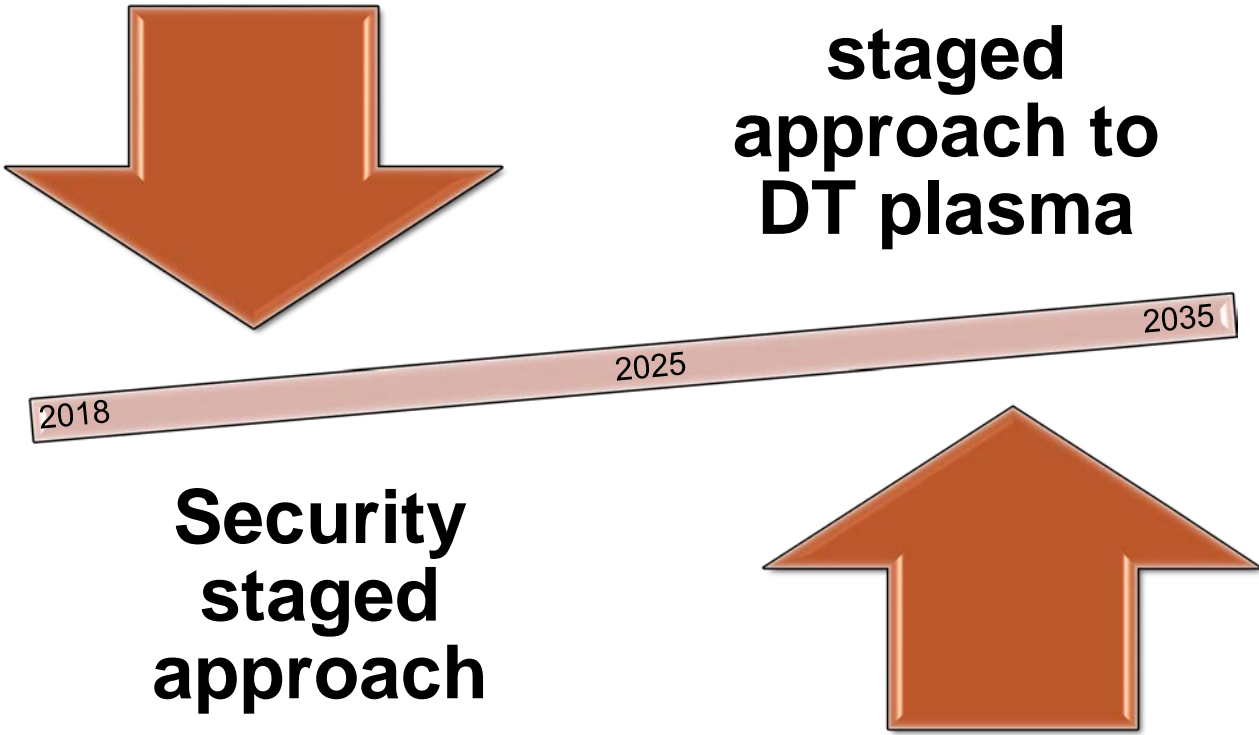
A staged approach to DT plasma

Extensive interactions among IO and DAs to finalize revised baseline schedule proposal

- ✓ Schedule and resource estimates through First Plasma (2025) consistent with Members' budget constraints
- ✓ Proposed use of 4-stage approach through Deuterium-Tritium (2035) consistent with Members' financial and technical constraints



General consideration



General consideration - Current Risks




Site with
850 staff
and 850
contractors




High Safety
risk -
Worksite
with 2500
workers



Moderate
Security risk



Potential
targets



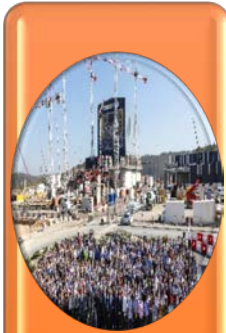
Competitive
Intelligence



Reputation
to protect



General consideration – future Risks



Site With
1000 staff
and
xxx
contractors



Lower
Safety risk



Higher
Security risk



Evolution of
Potential
targets



Competitive
Intelligence



Protection
of nuclear
materials

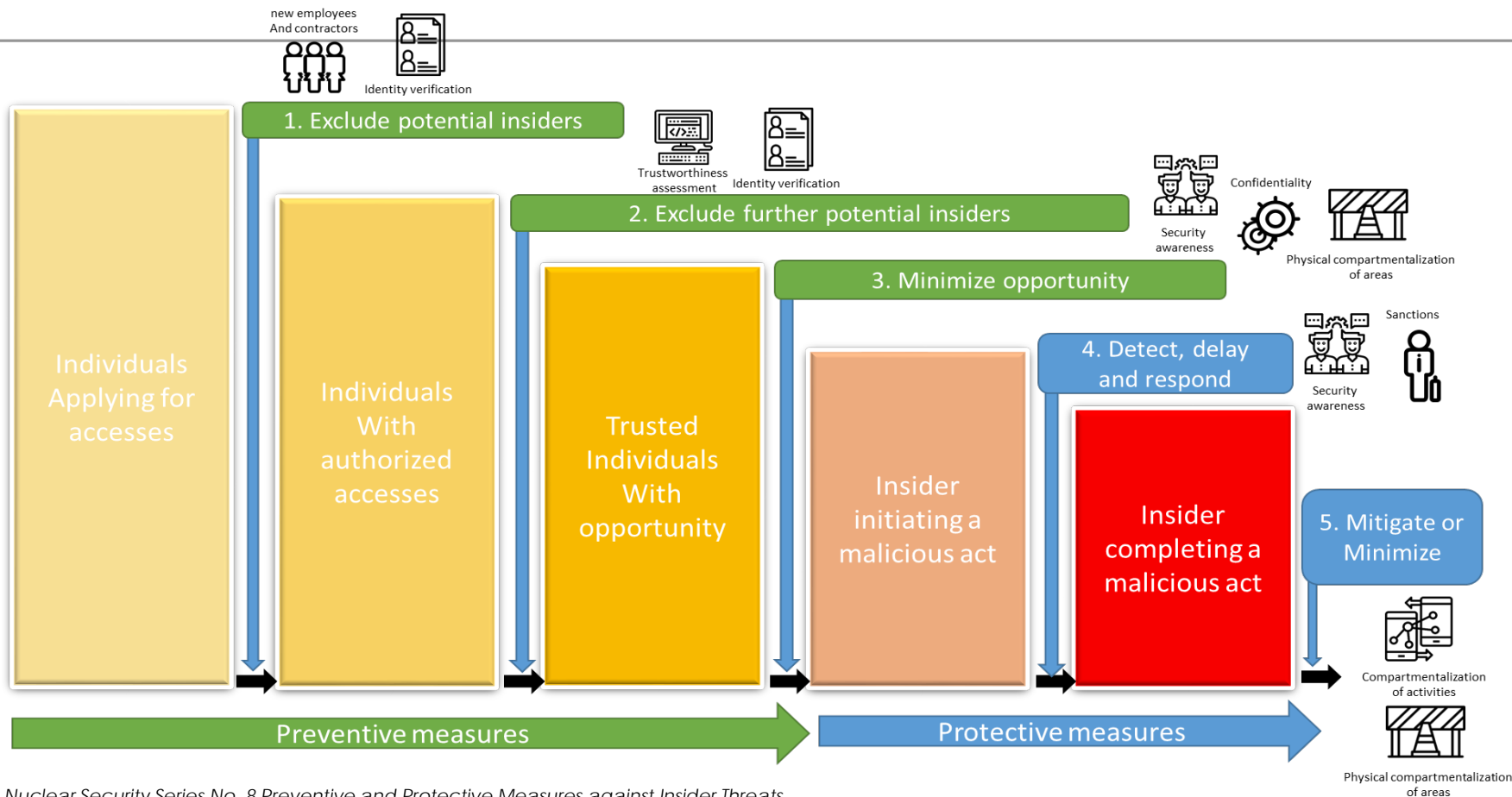


Protection
of Specific
area

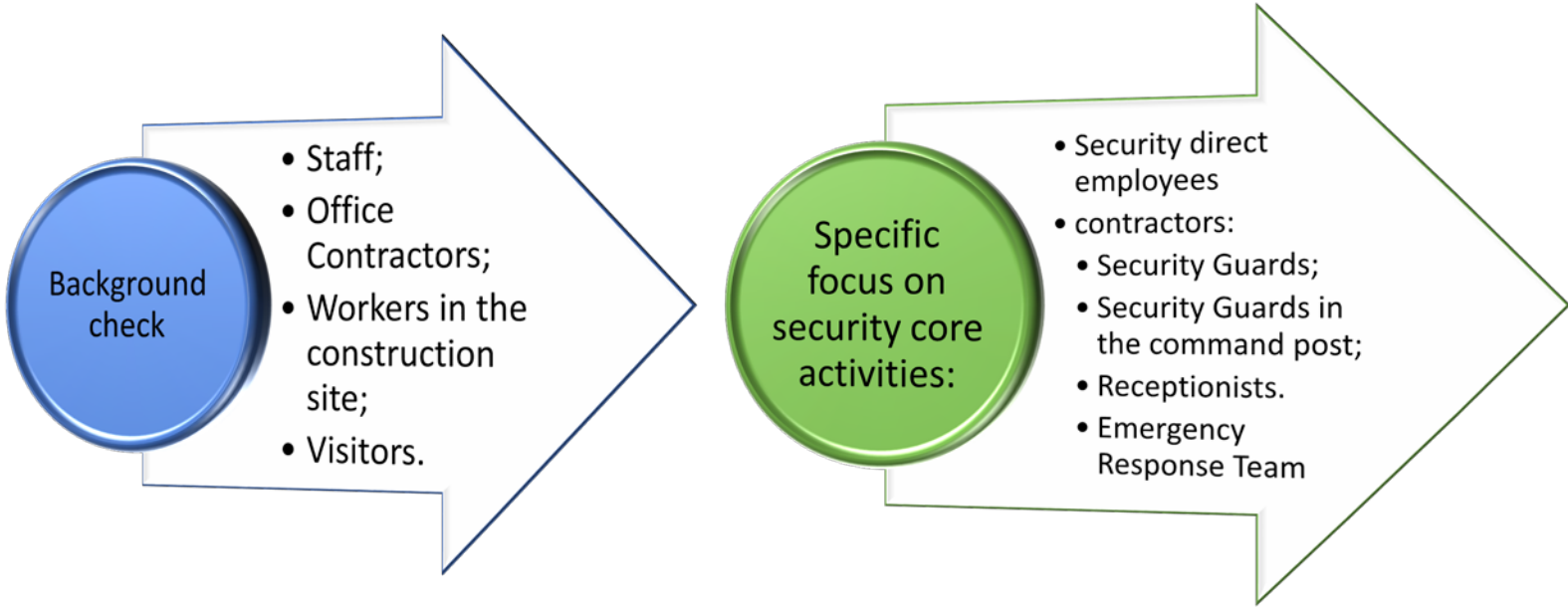


Reputation
to protect





Identity Verification



Identity Verification

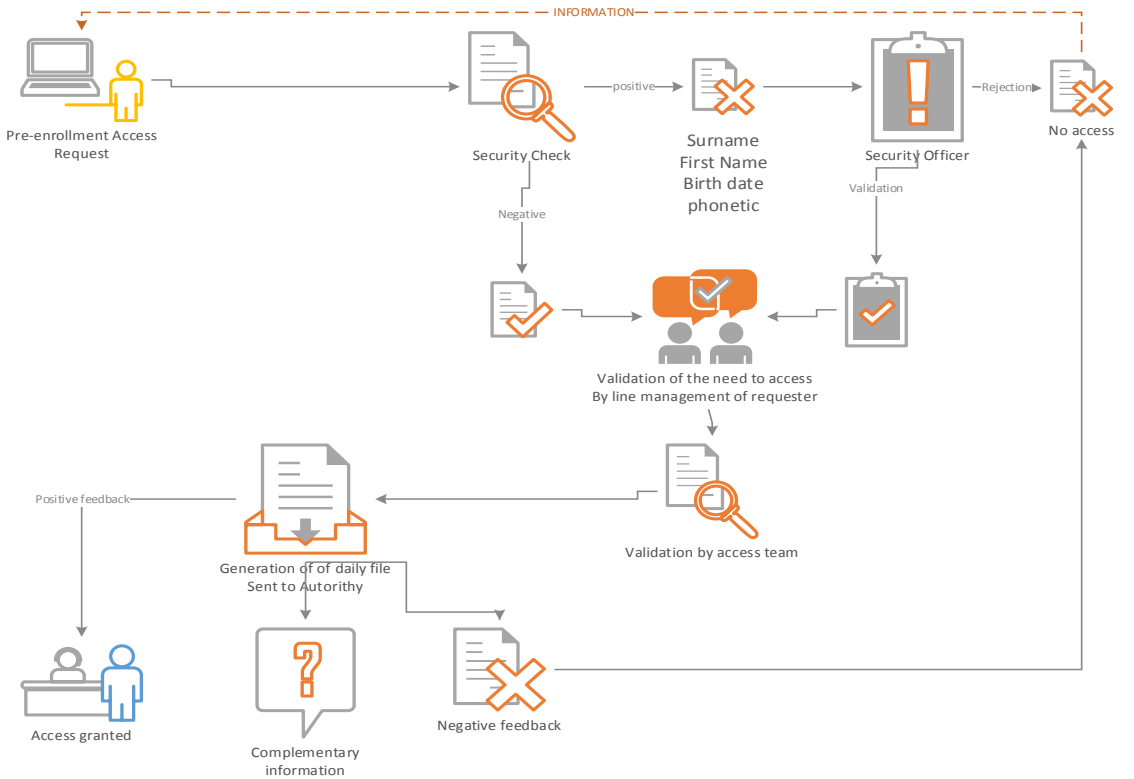


Background check

There are some rules that must be adhered to regarding the access request workflow:



- An applicant cannot submit their own access request.
- The "Submitter" and "Reviewer" of an access request cannot be the same person.
- The "Approver" cannot be the same person as either the "Submitter" or "Reviewer".



Trustworthiness assessment

New employees

Employees Satisfaction



Security awareness



- **Security induction course** provided to every new staff within the two first days of presence on site;
 - Security rules
 - Security on Site
 - Security off-site
- **Specific course** for the data protection;
- **Exercises** hold on a regular basis;
- Regular **Audit** by the providers and by the Organization.



Confidentiality (security of information)



The ITER Organization has developed a document classification system based on four levels:



Public information



Internal Use



ITER Restricted



ITER Confidential

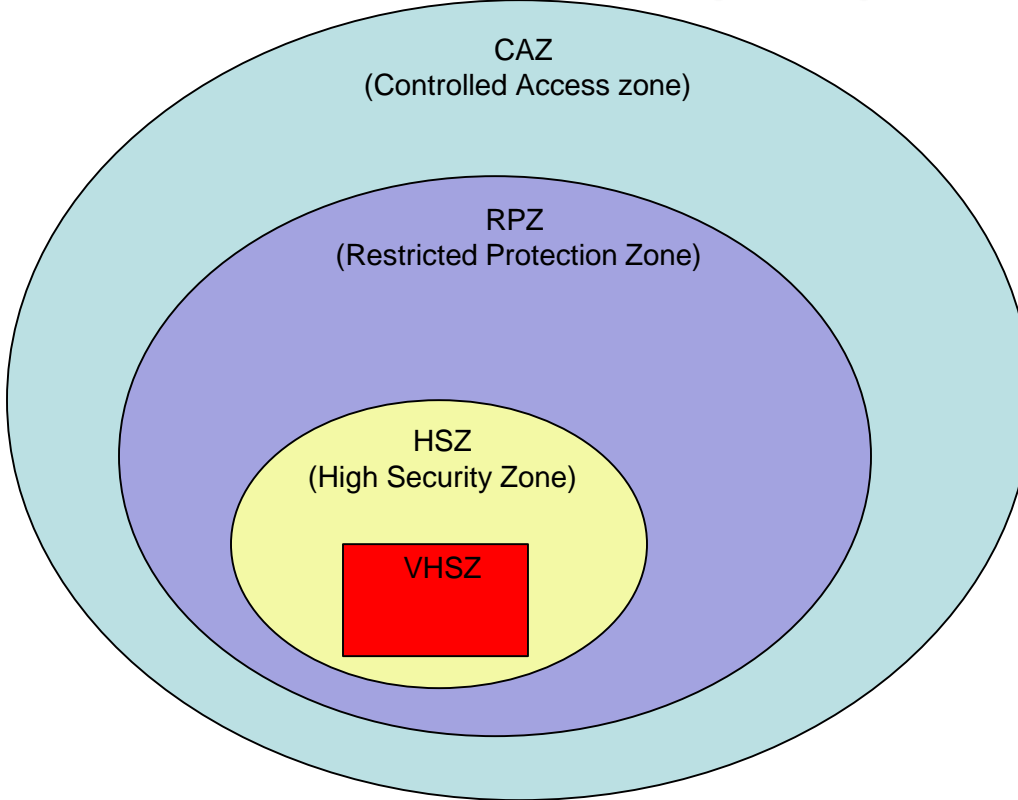
Access to the information is based on a "need to know" basis

Physical compartmentalization of areas



- Implementation of technical, human and organisational means to protect targets against malevolent action:
 - Measures based on the **defence-in-depth principle** and which will content prevention, delaying, detection, warning, follow-up of intruders and intervention measures.
 - **Graduated approach** taking into account the magnitude of the potential risks arising from the nuclear facility.
 - An **on-site response force** capability shall be maintained to deny, neutralize, contain, and/or perform recapture/recovery and pursuit missions within the required response times.
 - A **Security Command Post** shall be implemented within the HSF.

Physical compartmentalization of areas - *defence-in-depth principle*



Level of SCZ	Name of SCZ	Description
SCZ-Level 1 (L1)	CAZ (Controlled Access Zone)	Unrestricted IO staff and contractor access with restricted public access area. Delimited by the site boundary fence which is the first line of defence against malevolent actions and a first step for detection. Storage of information and physical assets with negligible impact level.
L2-SCZ	RPZ (Restricted Protection Zone)	Limited and controlled employee and contractor access with escorted or closely controlled visitors only. Surrounding the INB perimeter and delimited by the High Security Fence (HSF).
L5-SCZ	High Security Zones (HSZ)	Limited and strictly controlled employee and contractor access. Storage of information and physical assets of which the compromise, loss of integrity or unavailability would have an impact up to critical is permitted.
L6-SCZ	Very High Security Zone (VHSZ)	Limited and strictly controlled employee access with the two-man access rule. Storage of information and physical assets where the compromise, loss of integrity would have a crisis impact.

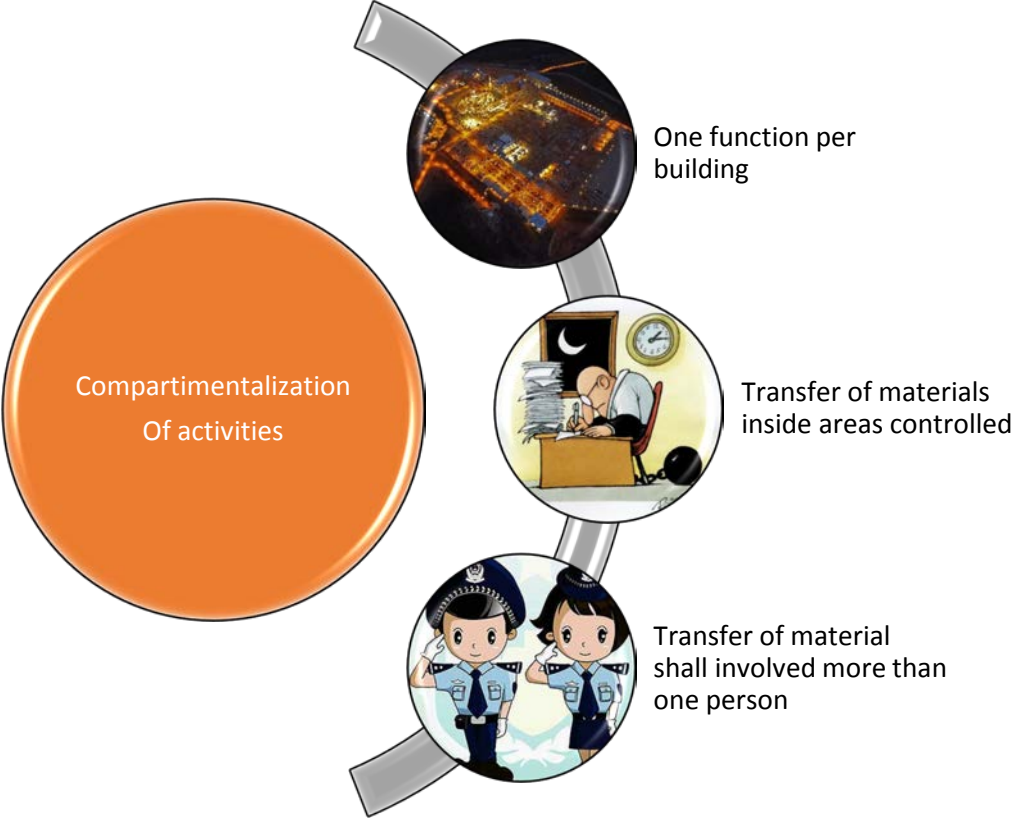
Physical compartmentalization of areas – *On site and off site response force*



- Internal response composed by guard unarmed;
- Composition of the response will be assessed at different stages of the project;
- External response by Gendarmerie with specialized armed team at 4km from the Site.



compartmentalization of activities



Physical compartmentalization of areas – Security command post



- Monitor the security and the physical protection of the whole ITER Site.
- Inform and communicate on security purposes.
- Assess and process all alarms in the field of security and physical protection
- Ensure the protection and availability of needed resources and means in all circumstances



- Development of an incentive procedure:
 - Ensure rapid response to infringements
 - Applies on Staff and contractors
 - Access to the site can be denied temporary / definitively
- Internal regulations:
 - More in depth response following incentive procedure

