Accreditation

2015-12-08

COMBITECH

Susanne Frank

Information Security Consultant

susanne.frank@combitech.se

Agenda

- My background
- Why accreditation
- Basics of the Accreditation method
  - Standards
  - System Development Lifecycle
  - Step by step
- Difficulties
- Example – Smart phone
- Cyber Security - New Challenges

Definition

- Formal approval with regards to Information Security to go in to operation – Operation Authorization

Why accreditation?

- To ensure Information Security is handled in the system
- To do the right thing from the beginning - Information Security shall be a part of system development from the beginning to accomplish cost effectiveness
- It will be a better system in the end in the aspect of security, usability and technology
- Coordination of IT-systems in the organization
- Enhanced documentation of the system
- Record of approved applications and systems in the organization
- Standardized method in large organizations
- CC is used for products – Accreditation is used for systems

Priorities

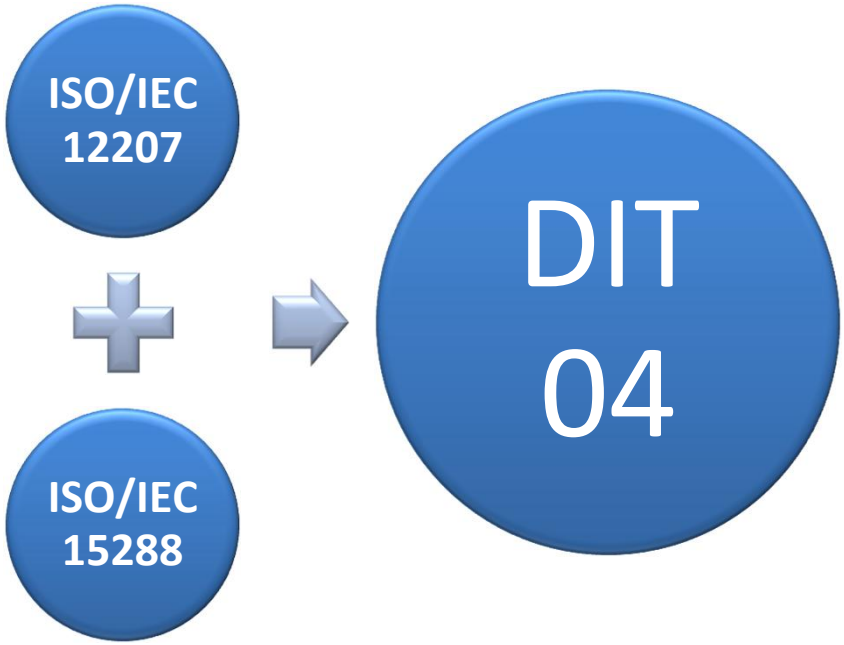
Protect the **critical** information

Technique **and** organisation

Correct protection for correct information

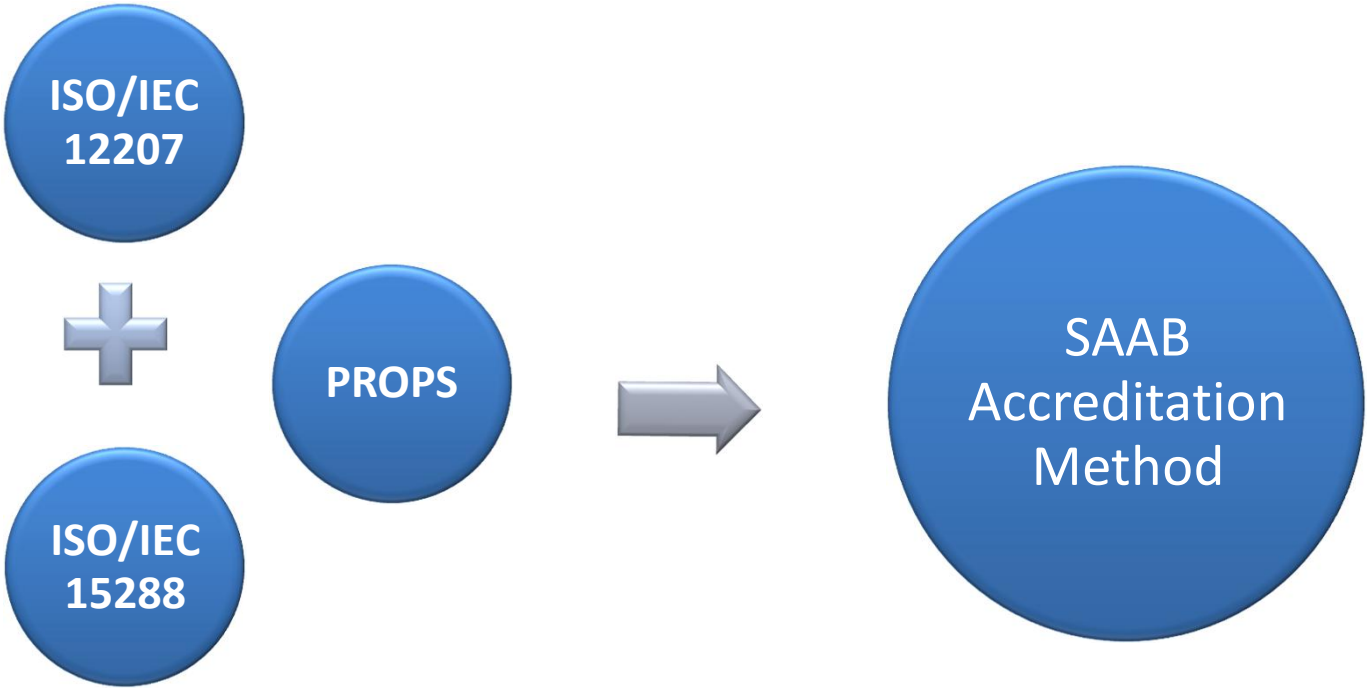
Prepare for when something happens

Method, Swedish Armed Forces

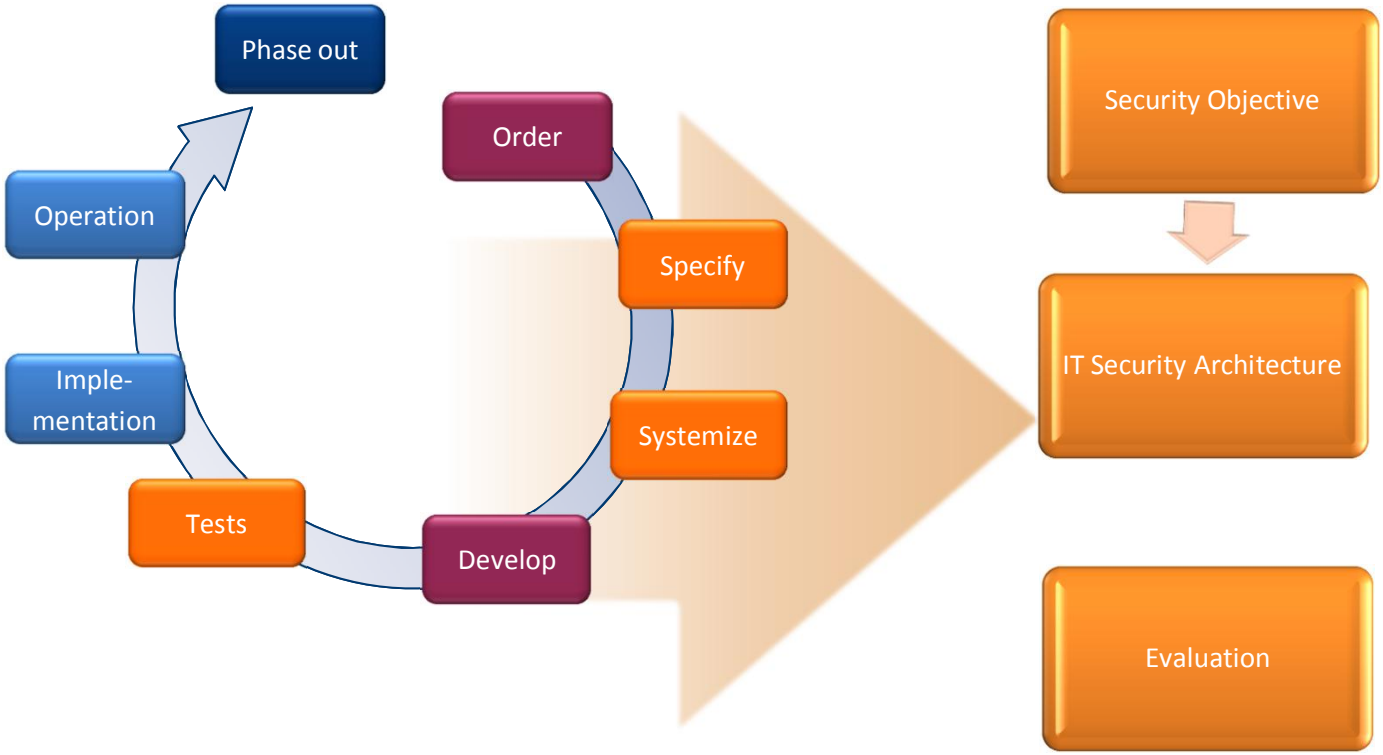


- **ISO/IEC 12207** Systems and software engineering — Software life cycle processes
- **ISO/IEC 15288** Systems Engineering standard covering processes and life cycle stages
- **DIT 04** Directives for the Swedish Armed Forces Information Technology

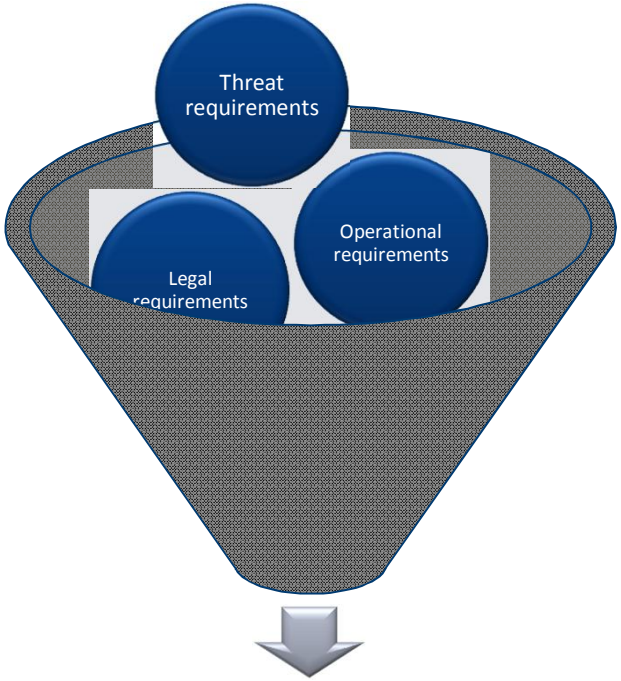
Method, Saab


ISO/IEC 12207
ISO/IEC 15288
PROPS
SAAB Accreditation Method

System Development Lifecycle



Security Objective

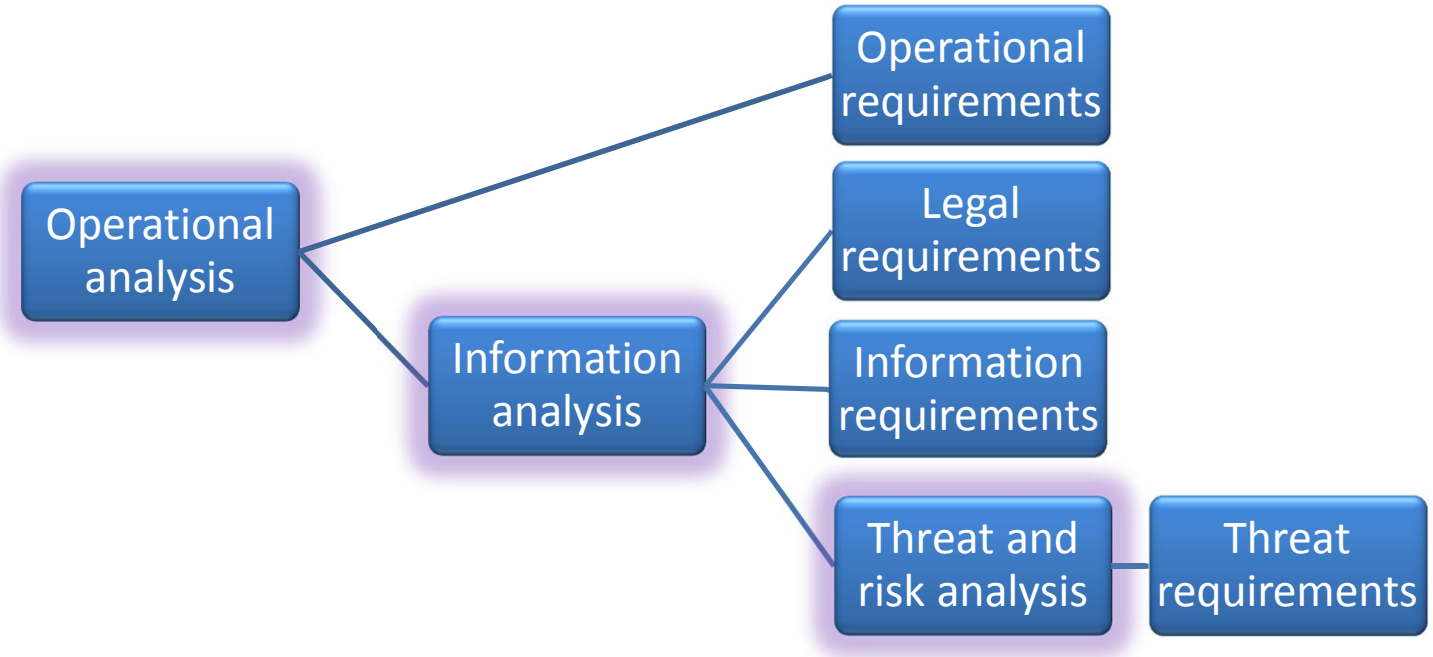


Compiles all requirements in one security objective, this includes:

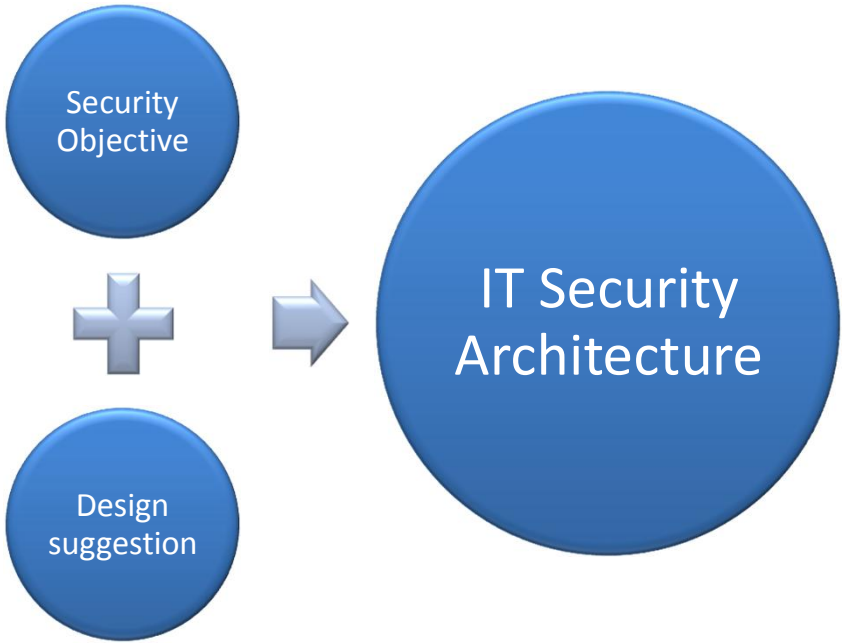
- Identify and handle contrarious requirements
- Order requirements by shall and should
- Identify requirements by technical and administrative

A compilation of all security related requirements – independent of the source

Security Objective, Method

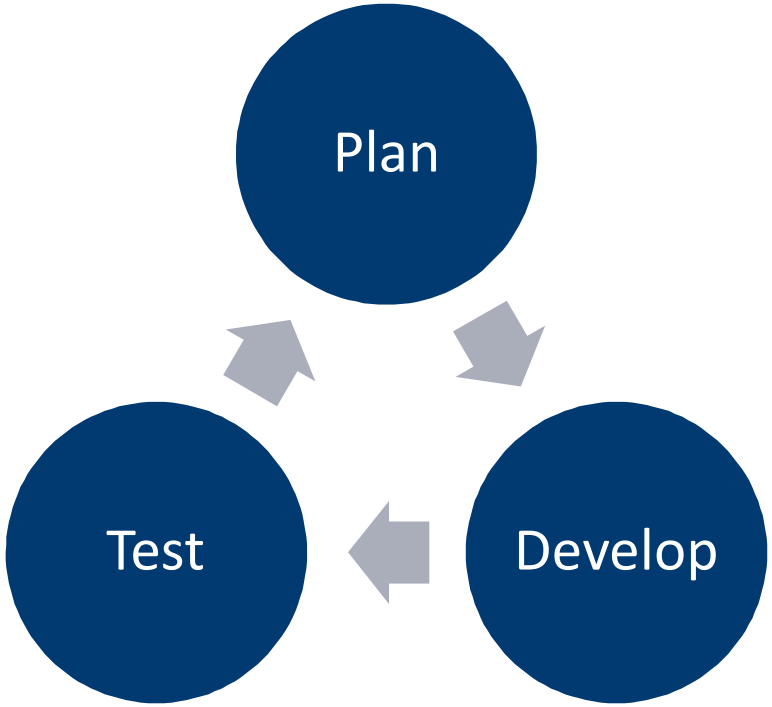


Security Architecture



The Security architecture is based on the security objective along with the design suggestion in order to describe how security shall be attained in the system.

Develop



Ensure that decided functions and solutions are implemented.

Handle modified requirements and conditions

- Plan – what functions and solutions shall be implemented?
- Develop– how shall the functions be realized?
- Test – validate desired functionality

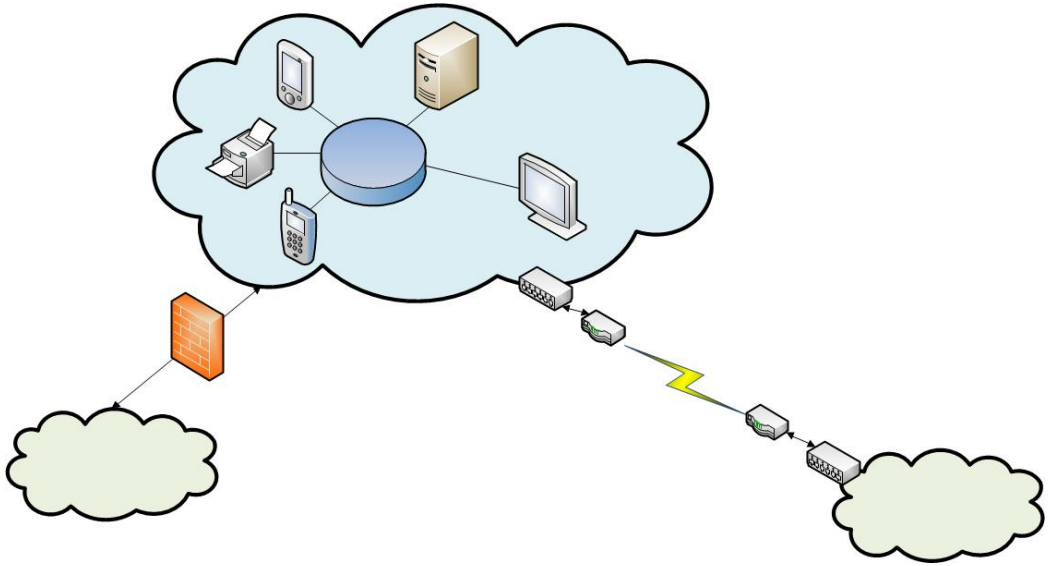
Evaluation

Can be performed during different stages in the project. Several types, depending on requests.

Difficulties

- Project Management sees cost, not profit
- Information security is generally applied late or afterwards
- Documentation is inadequate - Security functions are rarely described thoroughly in system documentation
- “System of systems” depending on other systems or components being accredited already
- Contradictive security objectives


FKK 520
SECTRA

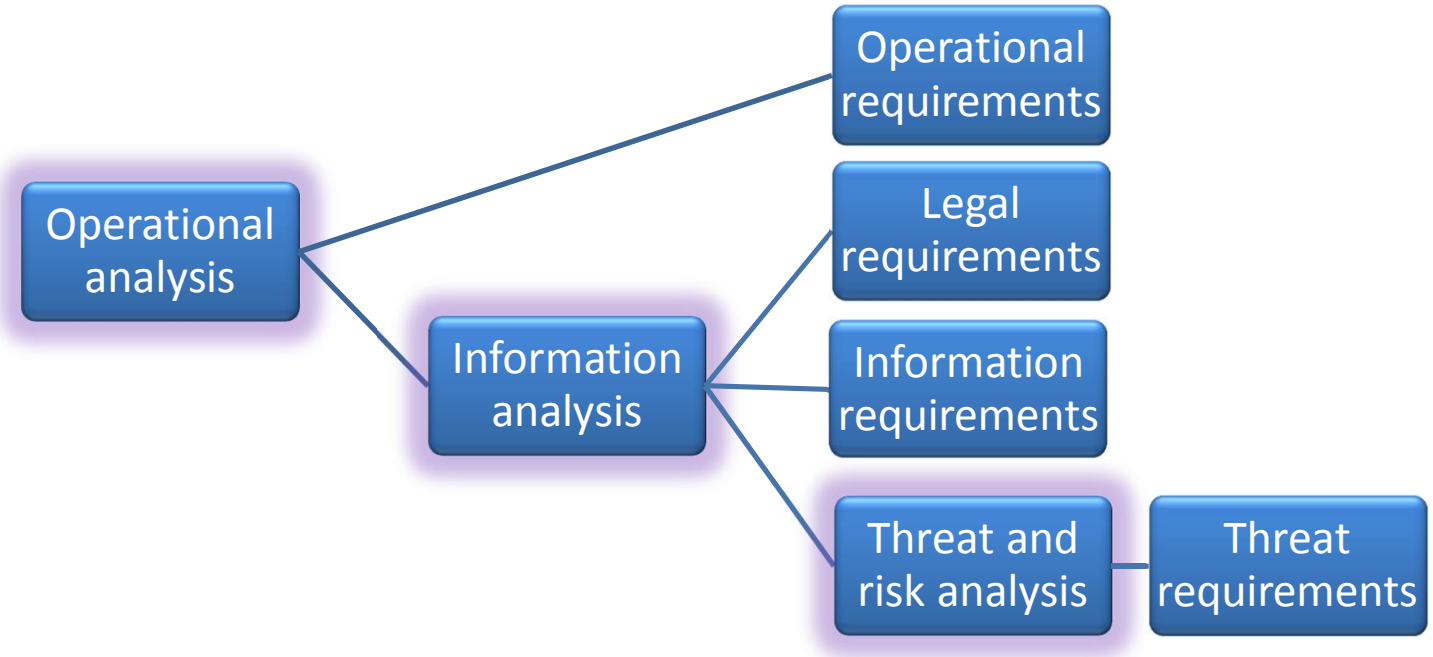


Example - Smart phone

Assessment/Evaluation

- Technical Evaluation/Penetration test
- Code review
- Validation and verification

Security Objective



COMBITECH

Camera:

I want to be able to take photos and store a lot of photos

SMS/MMS:

I want to be able to send texts including pictures.

WIFI:

I want WIFI

Contacts:

I want both customers, family and friends in my contacts

E-mail:

I want to be able to send both private and company e-mails

Calendar:

I want both my private calendar and work calendar.

The calendar shall synchronize automatically.

GPS:

I want Facebook and google maps to know my position

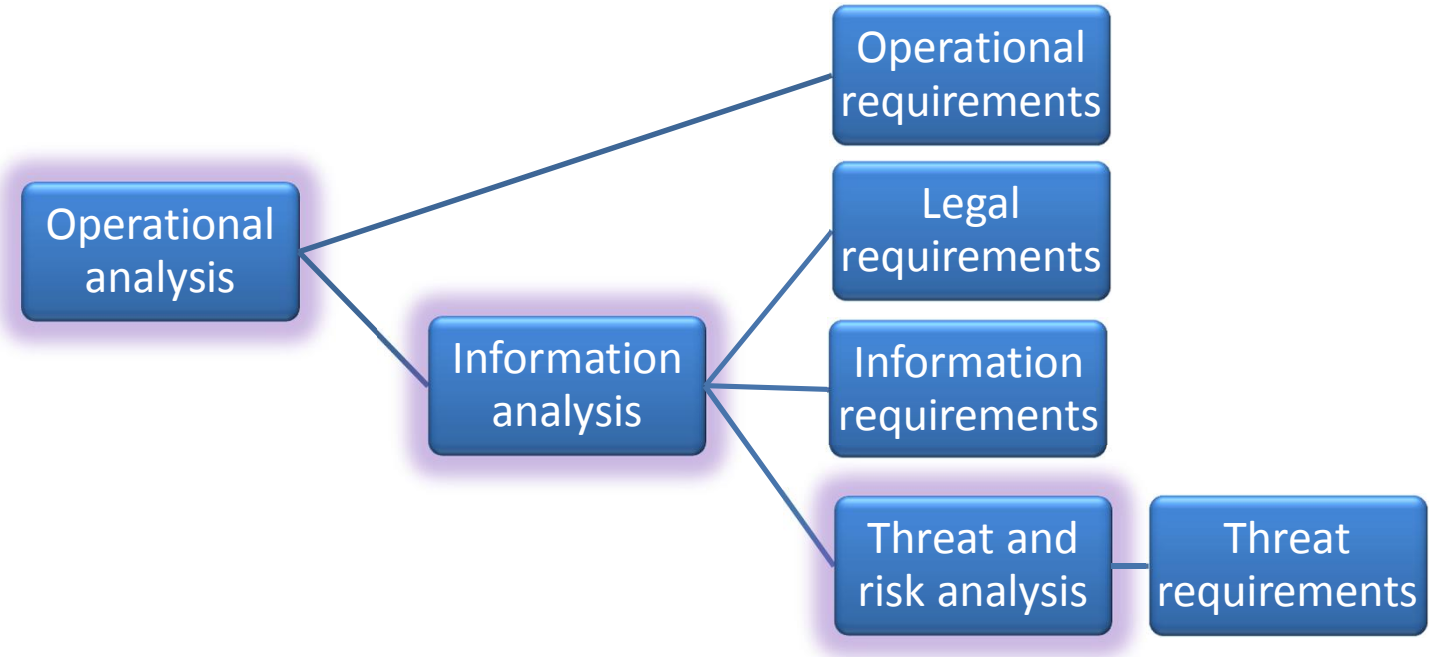
APP:

I want Facebook, Instagram, LinkedIn.

Internet:

I want to be able to connect to Internet.

Security Objective



COMBITECH

Photos:

Whiteboard from job meeting

Embarrassing photo from Saturday night party…

SMS/MMS:

Here is your password…

I'll be away on a trip all of next week…

WIFI:

Net and password

Contacts:

Customers

Family, friends

E-mail:

Log in information…

Tickets…

Calendar:

Away…

GPS

History

Location

Phone log:

Customers

Social media:

Family, friends

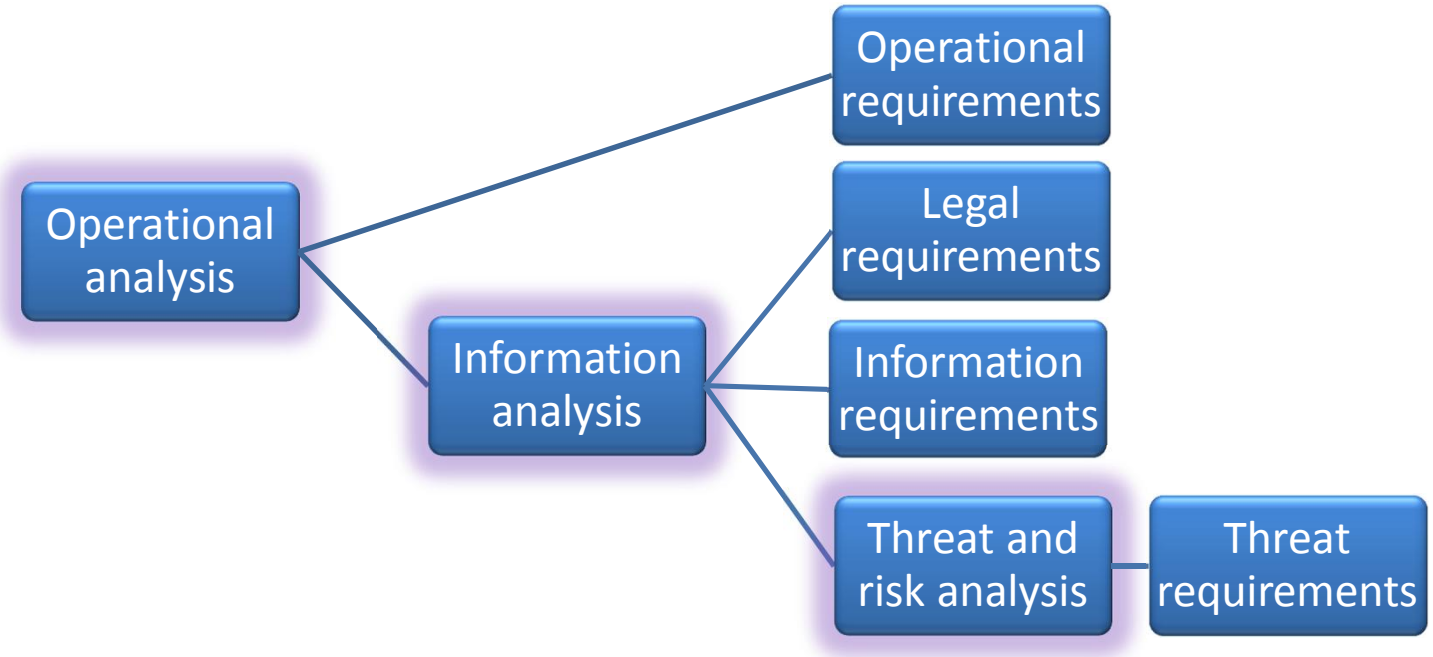
Pictures, status updates…

Internet:

Web history

Favorites

Security Objective



COMBITECH

SMS/MMS:

Text in your name to customers/friends

E-mail

Send e-mails in your name

Phone

Call in your name

App

Control your online characters

Train-tickets

Spend money on online games

Settings on Spotify/Netflix/Skype

Social media:

Facebook posts/Instagram in your/the company's name

Twitter in your/the company's name

What differs a smart phone from a laptop?

- You often use it both for work and in your spare time
  - Different focus on protection
- Easier to carry
  - Easier to loose, easier to steel
  - More opportunities to surf on unprotected WiFi networks
- Many more and easy to get applications
- Children and friends use it for games, films and music

Suggested requirements

- Use password (not just the SIM-code)
- Encrypt the content, if possible
- Control app permissions
- Always use HTTPS
- Avoid unencrypted/unsecure networks
- Install updates

Suggested requirements

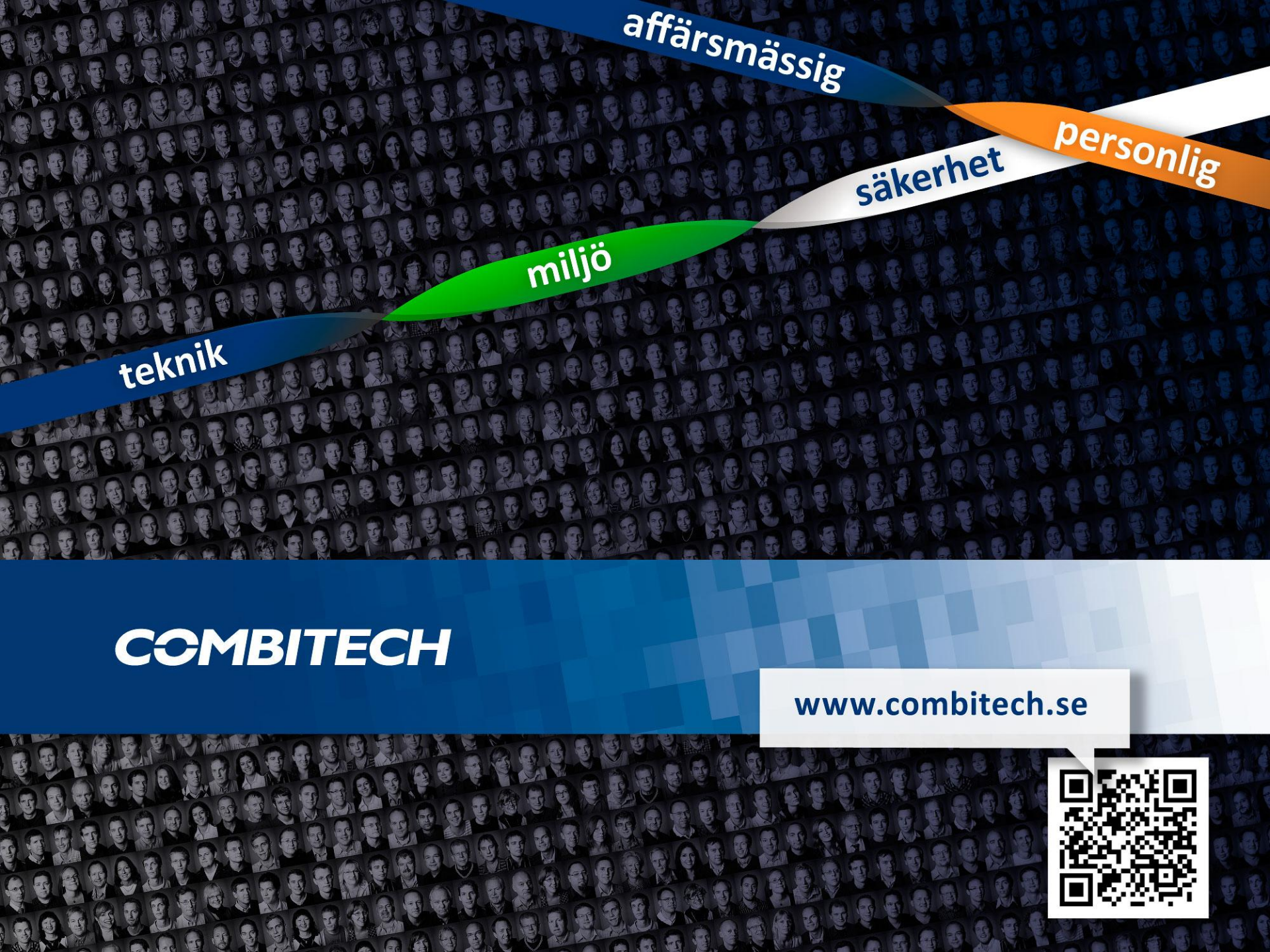
- No root or jailbreak
- Contact information outside of the locked content
- Backup
- No unknown chargers/cables
- Turn off interfaces that is not needed
- Be aware that photos may contain time and position
- Reset old mobile phones, in combination with encryption

Security functions

- Access control
  (user name, password, certificates, etc.)
- Logging of security related events
  (log in, configuration changes, access of information etc.)
- Protection of stored information
  (checksums, encryption, key handling, revocation, etc.)
- Redundancy
- Intrusion detection/prevention
  (firewalls, IDS/IPS, etc.)
- Protection of information in transmission
  (HTTPS, VPN, TLS, i.e. encryption)
- Protection against malware
  (virus, worms, trojans, etc.)

Evaluation


Validation and verification
Technical evaluation /Penetrati on tests
Assessment/ Evaluation
Accreditation
Code review


affärsmässig
personlig
säkerhet
miljö
teknik
COMBITECH
www.combitech.se