E-Compliance Academy
EU GDPR INSTITUTE
E-learning platform for Insights/Online Seminars

What are the Data Security, IT Security and Cybersecurity requirements for: GDPR and CCPA compliance.

What the GDPR say about security?

GDPR, Art. 5(1)(f)

- It says that personal data shall be:
  - 'Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures'

GDPR Art. 32(1)

- States:
  - ‘Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk’

Key GDPR principles

- GDPR state that if you process personal data. You need ‘appropriate technical and organizational security measures’.
- Doing this requires you to consider:
  - Risk analysis, Organizational policies, Physical and technical measures
- Your security requirements of your data processing and also apply to data processors.
- Consider the state-of-the-art and costs of implementation when deciding what measures to take. They must be appropriate both to your circumstances and the risk your processing poses.
- Where appropriate, you should look to use measures such as pseudonymization and encryption.
- Your must ensure the ‘confidentiality, integrity and availability’ of your systems and services.
- You must also be able to restore access and availability to personal data in a timely manner - in the event of a physical or technical incident.
- You need to ensure that you have appropriate processes in place to test the effectiveness of your measures and undertake any required improvements.

What the CCPA say about security?

CCPA asks that business take part in the following activities:

- In-house data inventory, mapping of relevant personal data, and highlighting instances of selling data
- Setting up new individual rights to data access and erasure
- Setting up new individual rights to opt-out of data selling
- Updating service agreements with third-party vendors and data processors to ensure that they are also CCPA-compliant
- Identifying and eliminating information security gaps and business system vulnerabilities

To ensure CCPA compliance business should check for the following points:

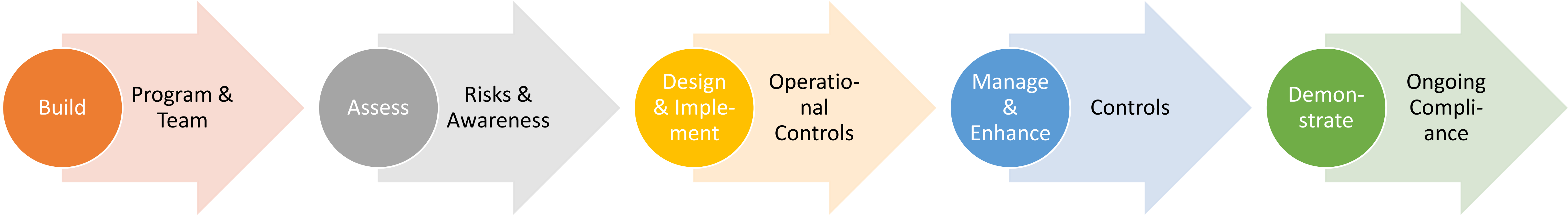
- Stringent processes and protections in place for how you collect and store customer data
- Consumer notifications of what type of information is being stored and used at the point of collection
- Strong endpoint protection and encryption
- Strong emergency processes in place in case a data breach occurs
- An Opt-Out option on your website so that consumers can request to be “forgotten”
- An updated privacy policy that you’ve shared with your third-party vendors
- An updated privacy policy posted clearly on your website

Compliance Roadmap

E-Compliance Academy

EU GDPR INSTITUTE

E-learning platform for Insights/Online Seminars



Build Program & Team

Assess Risks & Awareness

Design & Implement Operational Controls

Manage & Enhance Controls

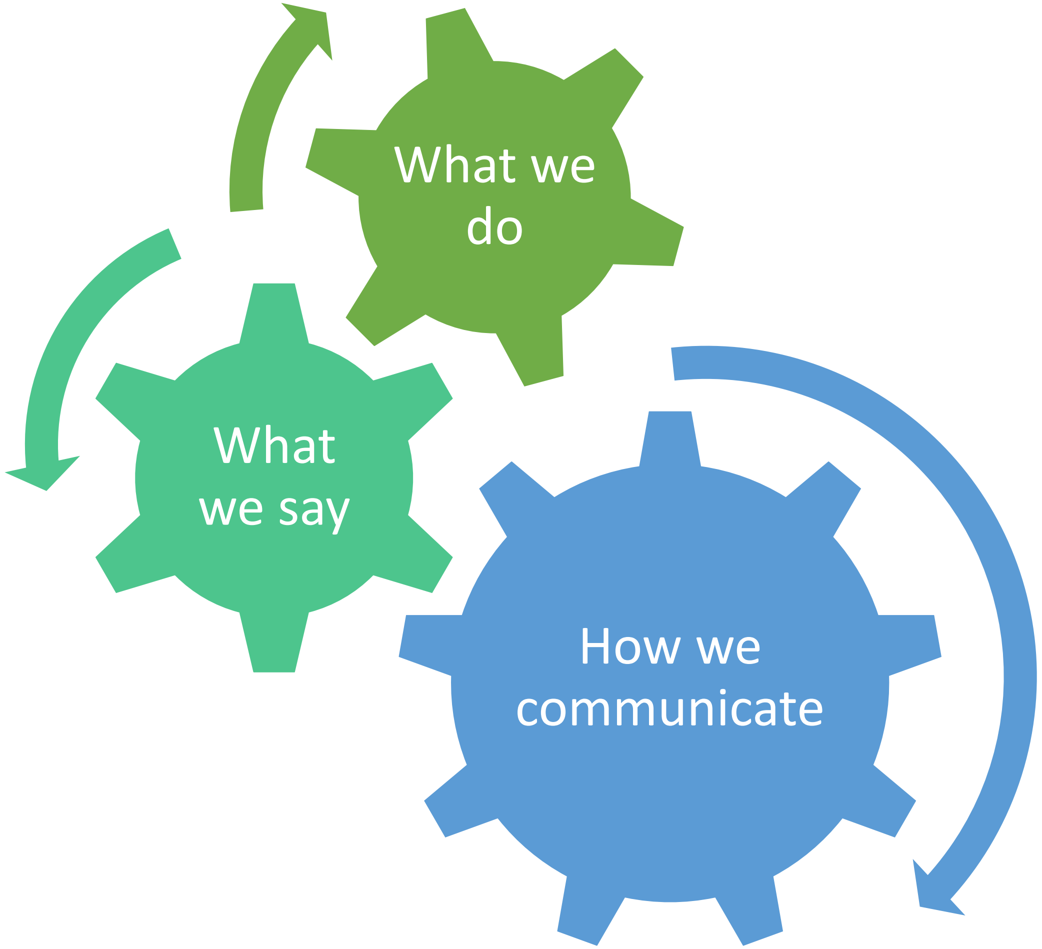
Demonstrate Ongoing Compliance

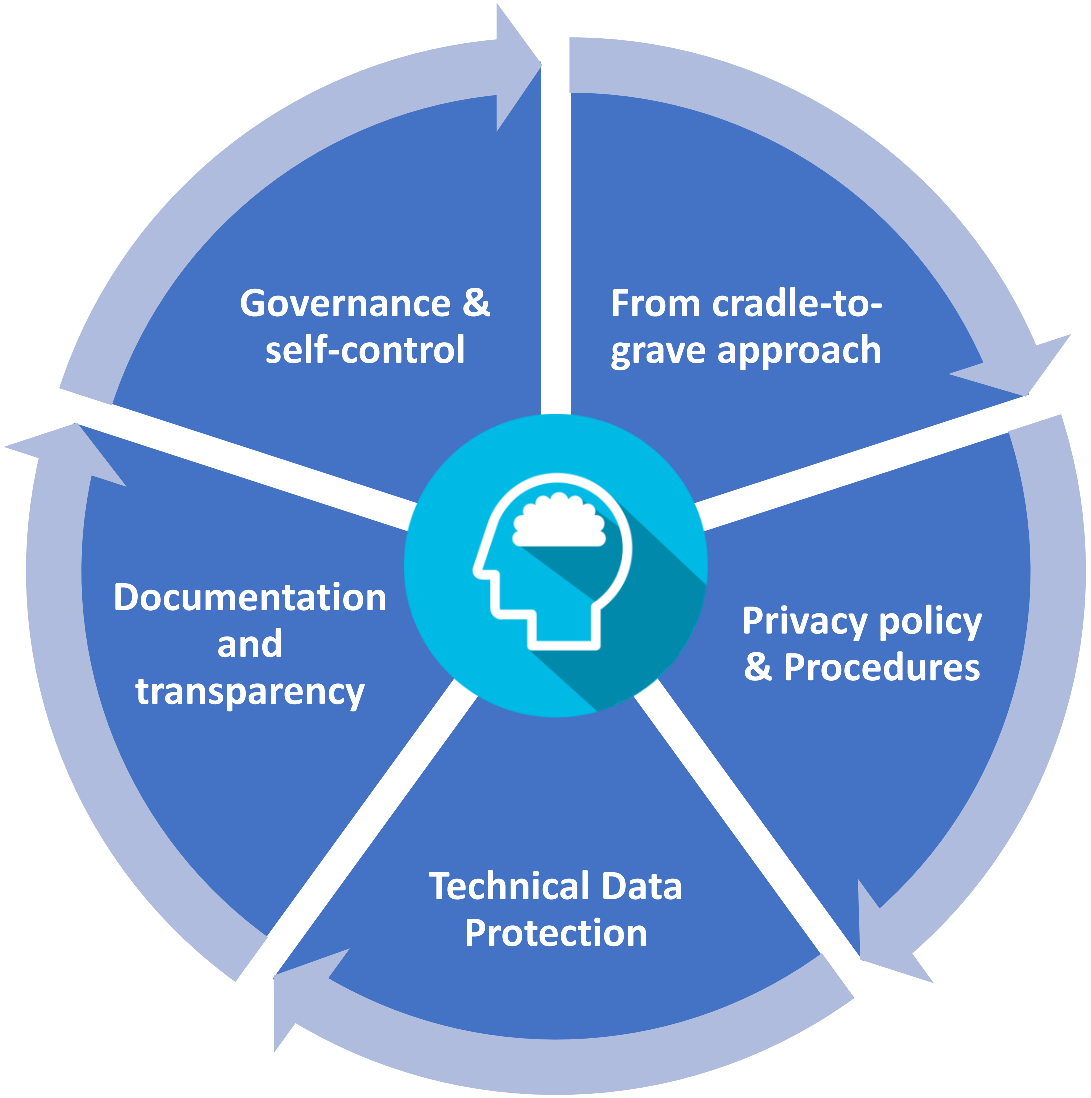
Identify Stakeholders	Conduct Data Inventory & Data Flow Analysis	Obtain & Manage Consent	**Conduct PIAs (DPIAs)**	**Evaluate & Audit Control Effectiveness**
Allocate Resources & Budget	**Conduct Risk Assessment & Identify Gaps**	Data Transfers & 3rd Party management	**Data Necessity, Retention & Disposal**	**Internal & External Reporting**
Appoint DPO (Maybe?)	**Develop Policies, Procedures & Processes**	Individual Data Protection Rights	**Data Integrity & Quality**	Privacy Notice & Dispute Resolution Mechanism
Define Program Mission & Goals	Communicate Expectations & Conduct Training	**Physical, Technical & Administrative Safeguards**	**Data Breach Incident Response Plan**	**Certification**

Securing IT and paper. Risk assessment

Article 32 of the **General Data Protection Regulation** (**GDPR**) requires Data Controllers and Data Processors to implement technical and organizational measures that ensure a level of data security appropriate for the level of risk presented by processing personal data.

Control and culture



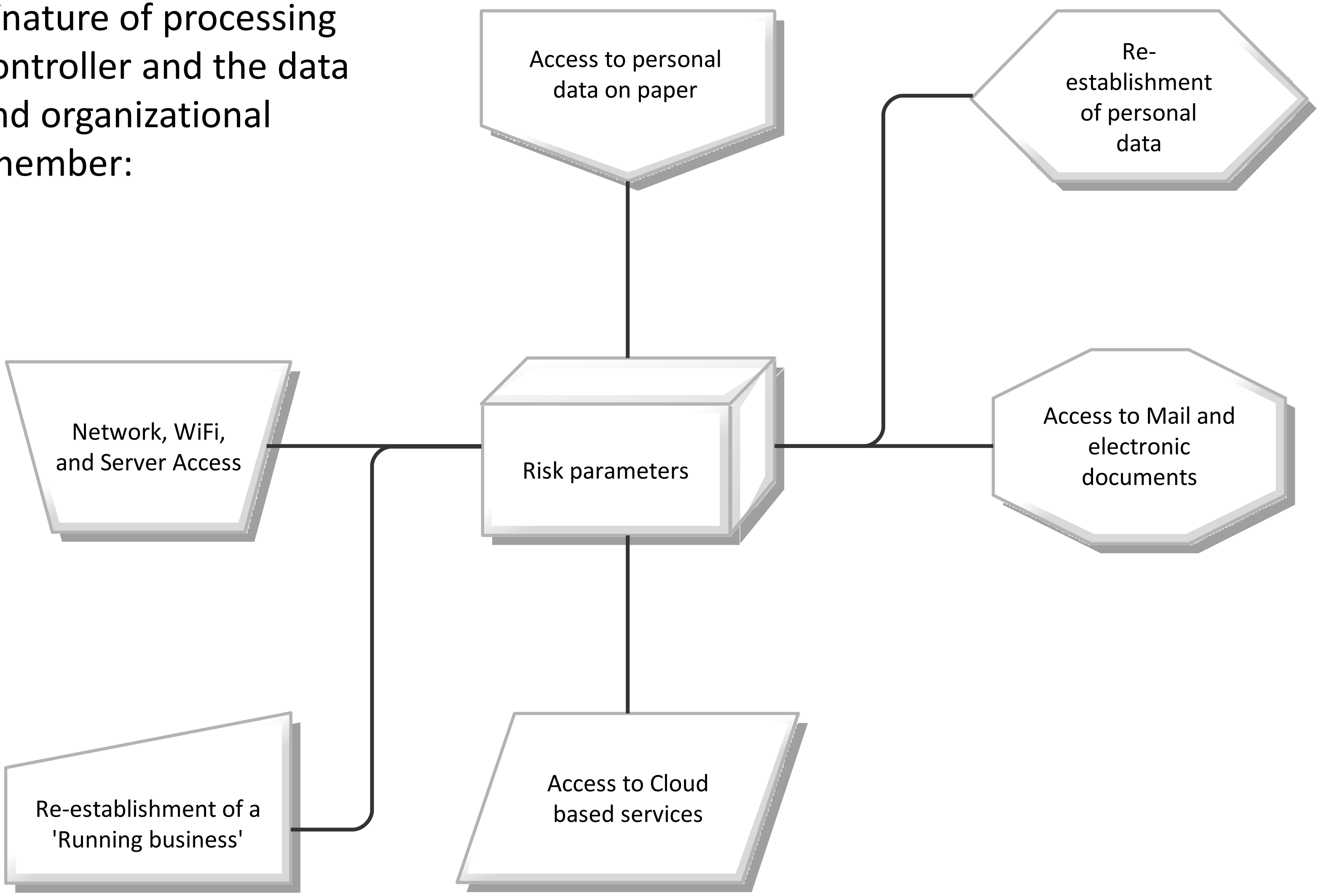

Governance & self-control
From cradle-to-grave approach
Privacy policy & Procedures
Technical Data Protection
Documentation and transparency

What is part of assessing IT risks

E-Compliance Academy
EU GDPR INSTITUTE
E-learning platform for Insights/Online Seminars

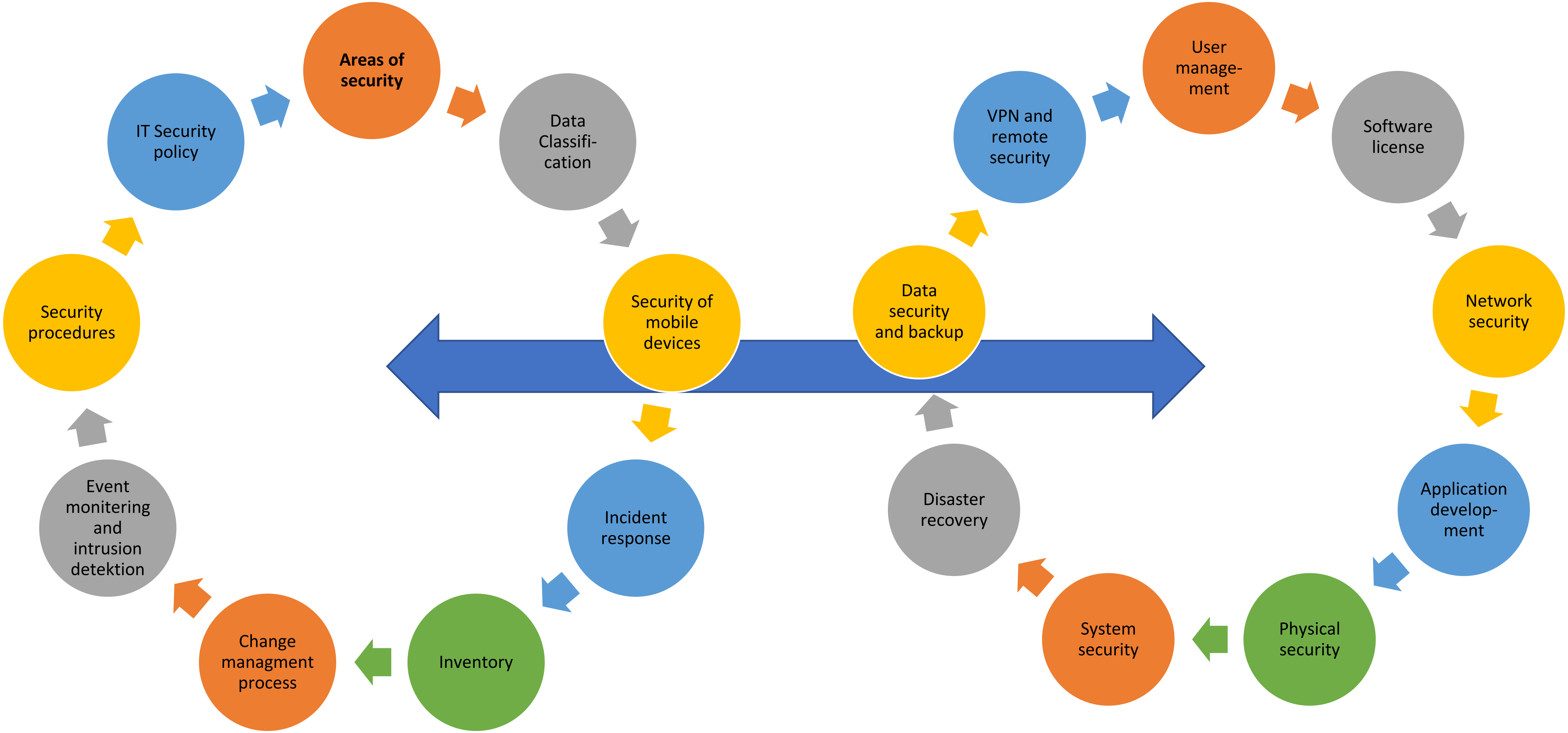
Considering the technical level, the cost and nature of processing and the seriousness of data. Both the data controller and the data processor shall have appropriate technical and organizational security levels appropriate to those risks, remember:

1. Personal data should always be behind a lock or password!
2. Use pseudonymization and/or encryption of data when possible
3. Ensure ongoing confidentiality, integrity, availability and robustness of processing systems and services
4. Can you restore access to personal data in a timely manner in the event of a physical or technical incident
5. Do you have procedure for regular testing, assessment and evaluation of the effectiveness of your technical and organizational measures


Access to personal data on paper
Re-establishment of personal data
Network, WiFi, and Server Access
Risk parameters
Access to Mail and electronic documents
Re-establishment of a 'Running business'
Access to Cloud based services

Areas of security

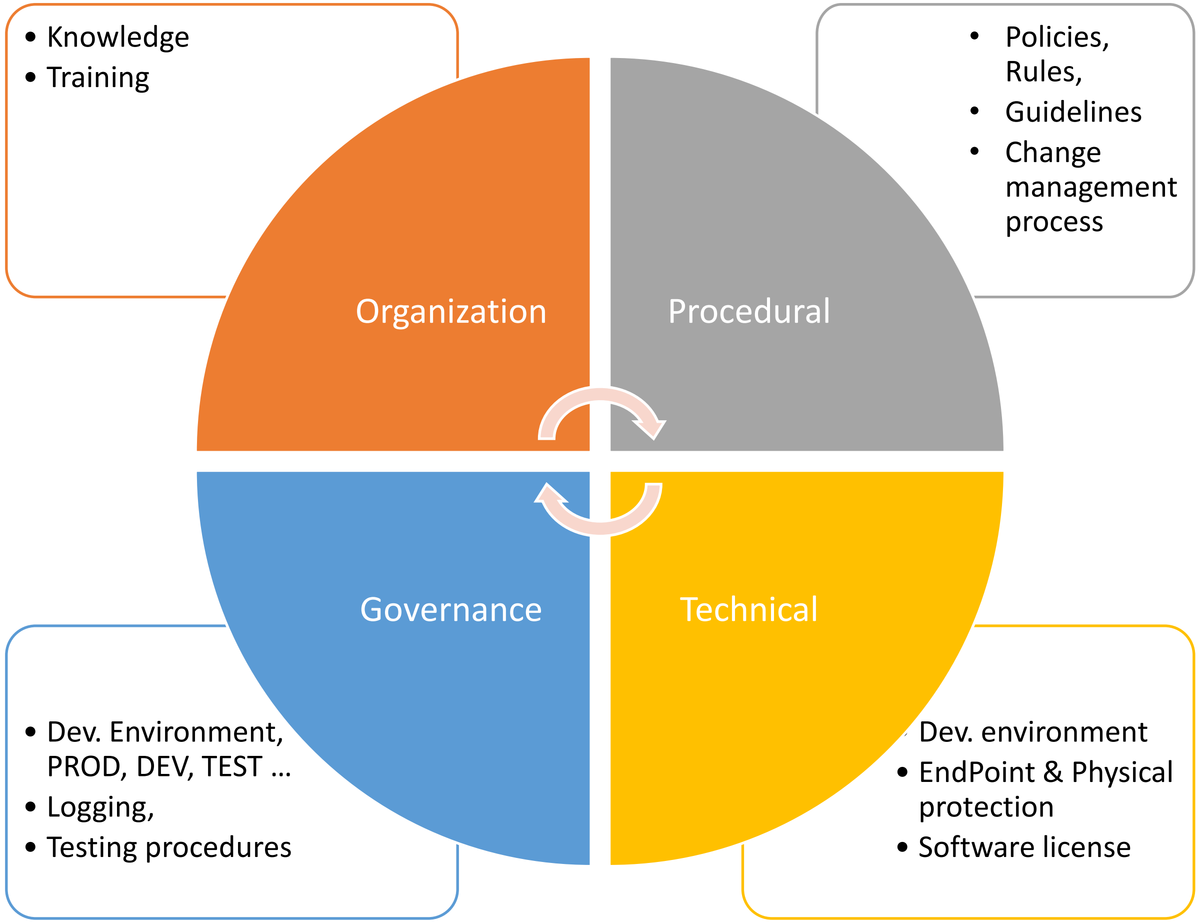
E-Compliance Academy
EU GDPR INSTITUTE
E-learning platform for Insights/Online Seminars



Application security in development

E-Compliance Academy
EU GDPR INSTITUTE
E-learning platform for Insights/Online Seminars

- Has Design by Default been incorporated into system development methods?
- Is code made Review in each stage of development?
- Are development environments separated e.g. in: Development Environment, Test and Production respectively?
  - Are production data being used in the development environment?
  - Is data anonymized?
- Are all developers informed about design by default requirements?
- Will all developed software be tested for viruses before it is put into production?



- Knowledge
- Training

- Policies, Rules,
- Guidelines
- Change management process

- Dev. Environment, PROD, DEV, TEST …
- Logging,
- Testing procedures

- Dev. environment
- EndPoint & Physical protection
- Software license

System security

- Is there a process for handling security patches and updates?
- Is there a process for identifying network, application, and operating system vulnerabilities ?
- Is an automated tool used to test system vulnerabilities?
- Is the company conducting a vulnerability analysis Pen test?
- Have all the company's systems undergone a vulnerability test?
- Does the company have an IT security and checklist for each operating system used?
- Are there regular audits where the IT security list is reviewed for each system?
- Will the IT security list be updated periodically?
- Is there a policy on how superusers get rights to use the systems?
- Are user rights regularly reviewed?
- Is there antivirus on all platforms, PC, Notebook, servers, tablets and mobile phones?
- Are the e-mail servers configured to Check all incoming and outgoing emails for viruses, spam, malware and other risks?
- Is there a procedure to ensure that Pcs And Laptops updated with the latest antivirus definitions files?
- Will files sent to and from the company be checked and virus scanned before transfer?

User Management

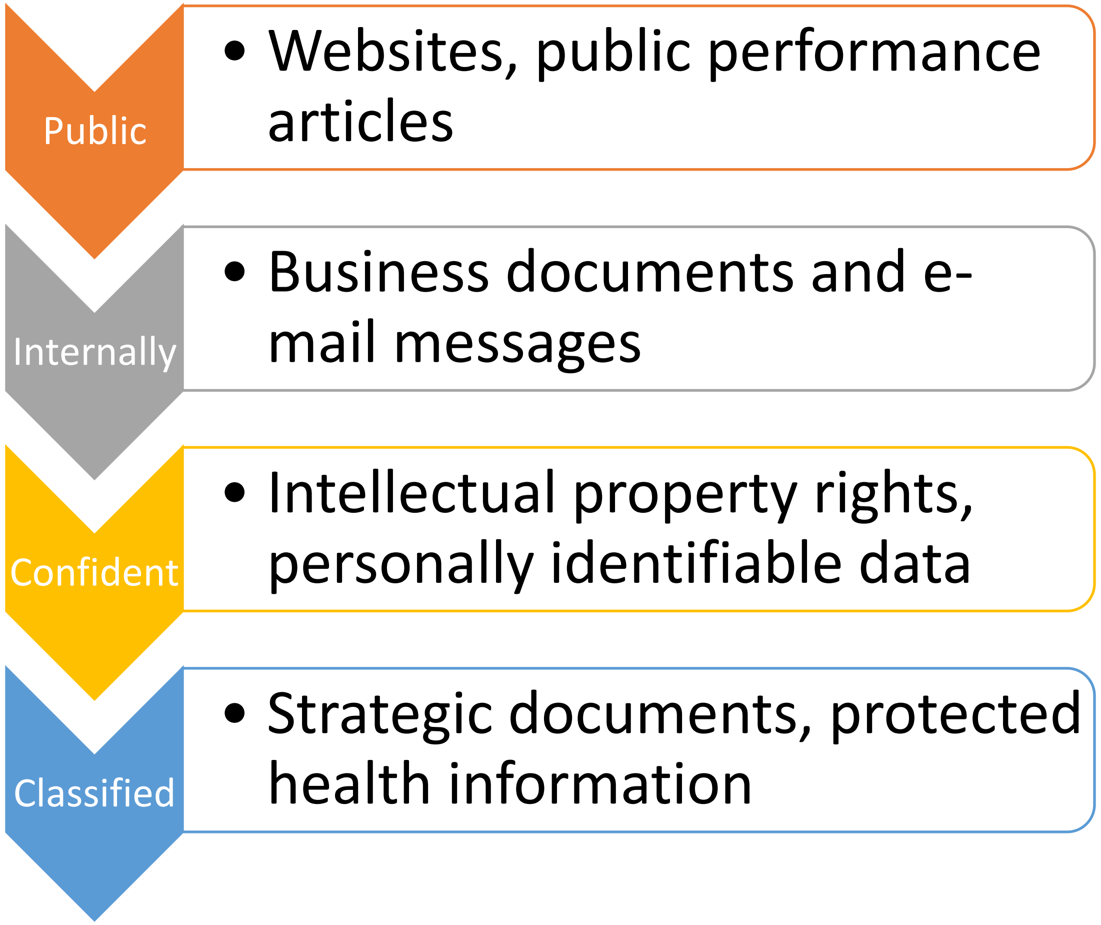
- Is there a process that controls high-security user accounts?
- Is there a policy for managing high-security accounts?
- Is simultaneous access restricted for the same user account?
- Is there a process with regard to the to delete user accounts before the user's issue date?
- Will user accounts be locked after periods of inactivity?
- Will user account be locked after X number of failed login attempts?
- Will all default accounts be disabled in the different systems e.g. Admin, Root?
- Should users change their password at first login?
- Does the password automatically expire after XX number of days?
- Is there a policy that prevents passwords from being reused?
- Is there a policy that prevents the use of easy passwords?
- Will the same USERID be used for the same person in all systems?

Change Managment Process (CMP)

- Is there a documented process for managing and updating software in development to test and production systems?
- Will the CMP check be carried out on an ongoing basis?
- Is there a formal process for approving updates to IT systems?
- Are updates documented and saved in a readable format?
- Is there a documented process for how to perform unscheduled updates?
- Is there a roll-back plan in the event of update-failuer?

Data classification

- Does all critical business data have a dedicated owner?
- Has a classification guide been prepared for the user regarding when, fx, ‘Public’, ”Internal use only’, ‘Confidential’ or ‘Restricted tag’s are to be used?
- Are file and server traffic being logged?



Public
- Websites, public performance articles

Internally
- Business documents and e-mail messages

Confident
- Intellectual property rights, personally identifiable data

Classified
- Strategic documents, protected health information

Data Security and Backup

- Are the company's critical systems and data backed up?
- Is there a process such as Checker that the backup is complete and correct?
- Is it possible to recreate parts of data from the backup?
- Will the backup be stored in a safe and controlled environment?
- Will the backup be stored in another physical location?
- Will the backup be stored in an access control area?
- Is there a process for disposing of old backup media?
- Are mobile phones and portable devices being backed up?
- Are BYOD being backed up?
- Is Laptops Encrypted?
- Is Laptops protected against theft?

Disaster Recovery

- Has a "Disaster Recovery Plan (DRP) covering partial loss or full loss of servers, applications or physical locations?
- Does the DRP plan include setting up in another location?
- Are all employees trained in DRP and carried out an annual review?
- Is DRP continuously maintained?
- Will DRP be reviewed and approved by the management/board?
- Are critical employees trained in DRP?
- Has a Business been made Impact analysis for all systems and applications?
- Are all applications and systems documented in Business Impact analysis document?

Event monitoring, Intrusion detection and incident Response

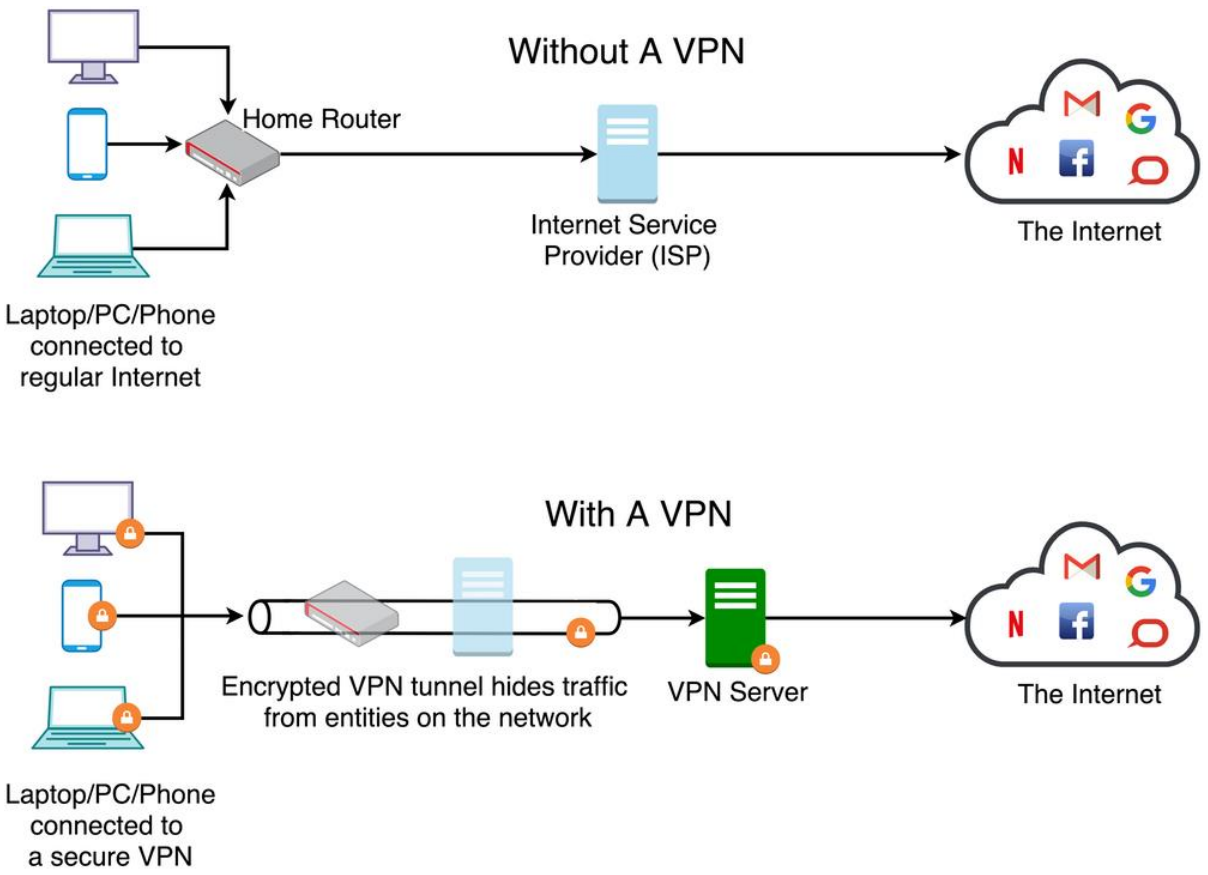
- Is security audit turned on on all systems?
- Is there a process for Review of security logs?
- Is there an automatic notification process that informs if there are irregularities?
- Do you have a Intrusion Detection software / product, on access connections, internet, web Hosting, and 3 party connections (VPN)?
- Are network penetration tests regularly carried out?
- Is there sniffer software installed and is this active?
- Is Intrusion Detection system continuously updated by new systems or changes?
- Is there a process for reporting identified viruses or malware?
- Is "Incidence Response" the process communicated to users?
- Are there any exercises that ensure that users follow the process?

Network security

- Is there an updated network diagram?
- Is ownership defined?
- Has a Stateful firewall facing the Internet?
- Is the firewall configured with a "deny all" policy, unless allowed?
- Is there a process to evaluate risks before changes are made to the configuration of the firewall?
- Is a proxy server used for outbound traffic?
- Are DMZ zones used?
- Is prohibited (Access denied) unless specifically permitted?
- Is logging enabled on all firewalls, routers, and proxy servers?
- Is there a process that periodically reads and evaluates these logs?
- Has it been hardening of all firewalls, routers and proxy servers?
- Is access to firewalls, routers, and proxy servers restricted?
- Are only employees with a necessary purpose who have access to the equipment?
- Is Remote Access to routers and firewalls protected by disposable password?
- Is access to the company's security equipment encrypted?
- Is there a process to ensure that routers/firewalls are up to date with the latest patch/software?
- Is there a process that ensures access to security Alerts from the various manufacturers?

Remote workplaces and VPNs

- Remote workplaces access via VPN
- Has a personal firewall been implemented on portable equipment
- Check that antivirus and personal firewall are active when accessed via VPN
- Is there a process to revoke a VPN access that is no longer active


Without A VPN
Home Router
Internet Service Provider (ISP)
The Internet
Laptop/PC/Phone connected to regular Internet
With A VPN
Encrypted VPN tunnel hides traffic from entities on the network
VPN Server
The Internet
Laptop/PC/Phone connected to a secure VPN

Physical security

- Will all visitors be handed an ID card?
- Will ID cards be periodically updated?
- Is there a process for handling visitors?
- Is it firefighting equipment in the building?
- Is there CCTV surveillance?
- Are there security guards?
- Are employees being security checked?
- Becoming physical security ists logged, investigated and reported to management?
- Is there a clean desk policy?
- Is there preventive maintenance e.g. a Uninterruptible Power Supply systems for IT environment and IT systems?
- Are network equipment stored in server rooms?
- Is it access control to server space?
- Will the list of employees with access to server rooms be periodically updated?
- Are there signs or markings indicating where the server space is?
- Are all servers stored in the server space?

Do the Walk-About

Inventory and Software Licenses

Inventory

- Is there a list of all IT equipment?
- Will the list be constantly updated?
- Is there a process for disposing of old IT equipment/furniture?

Software Licenses

- Is there a process for handling software licenses?
- Is the documentation constantly updated?
- Are new employees trained in the proper use of company programs?
- Are employees made aware that they are only allowed to install approved applications and software for which the company has licenses?
- Are users prevented from installing unauthorized software?

IT security policy

- Has the company developed an IT security policy?
- Is it implemented to a user who has access to the company's data, network, Pcs?
- Have all employees read and accepted the terms of the security policy?
- Are all employees trained in IT security?
- Will IT security training be repeated annually?
- Are it security policy being reviewed on an ongoing basis?
- Will the policy be updated with new guidelines for relevant topics and emerging theats?
- Is there a process that blocks sending Company Confidential data to unauthorized third party outside the company?
- Are the employees informed with regard to the to follow the copyright provision?
- Does the company have a policy that prevents user login from being shared?
- Does all company employees and others who have access to the company's data, network, Pcs signed a confidentiality agreement?
- Does the company have an email policy?
- Are employees who break e-mail rules are taken care of?
- Has the company described an internet policy?
- Have all employees read and accepted the rules of the internet policy?
- Is there detailed documentation of IT development and use?

Security procedure

- Is there access control at the company?
- Does the company have a security officer?
- Are asset protection roles and responsibilities implemented?
- Are security measures described and communicated to all departments/groups?
- Has a risk assessment process been incorporated that can help identify security threats?
- Has the company incorporated a safety training program?
- Does the company have a process that measures the effectiveness of safety training?
- Contains safety training aspects like Social Engineering attacks and industrial espionage and information gathering?
- Is the employee trained on how to intercept suspected security breaches and vulnerabilities?
- Are employees made aware of the risks and vulnerabilities that arise in connection with backup, anti-virus scanning and password selection?
- Is there a process to communicate security topics and changes to guidelines?
- Is the importance of IT security visible throughout the organization?
- Is GDPR discussed at company meetings, are there posts, etc.?

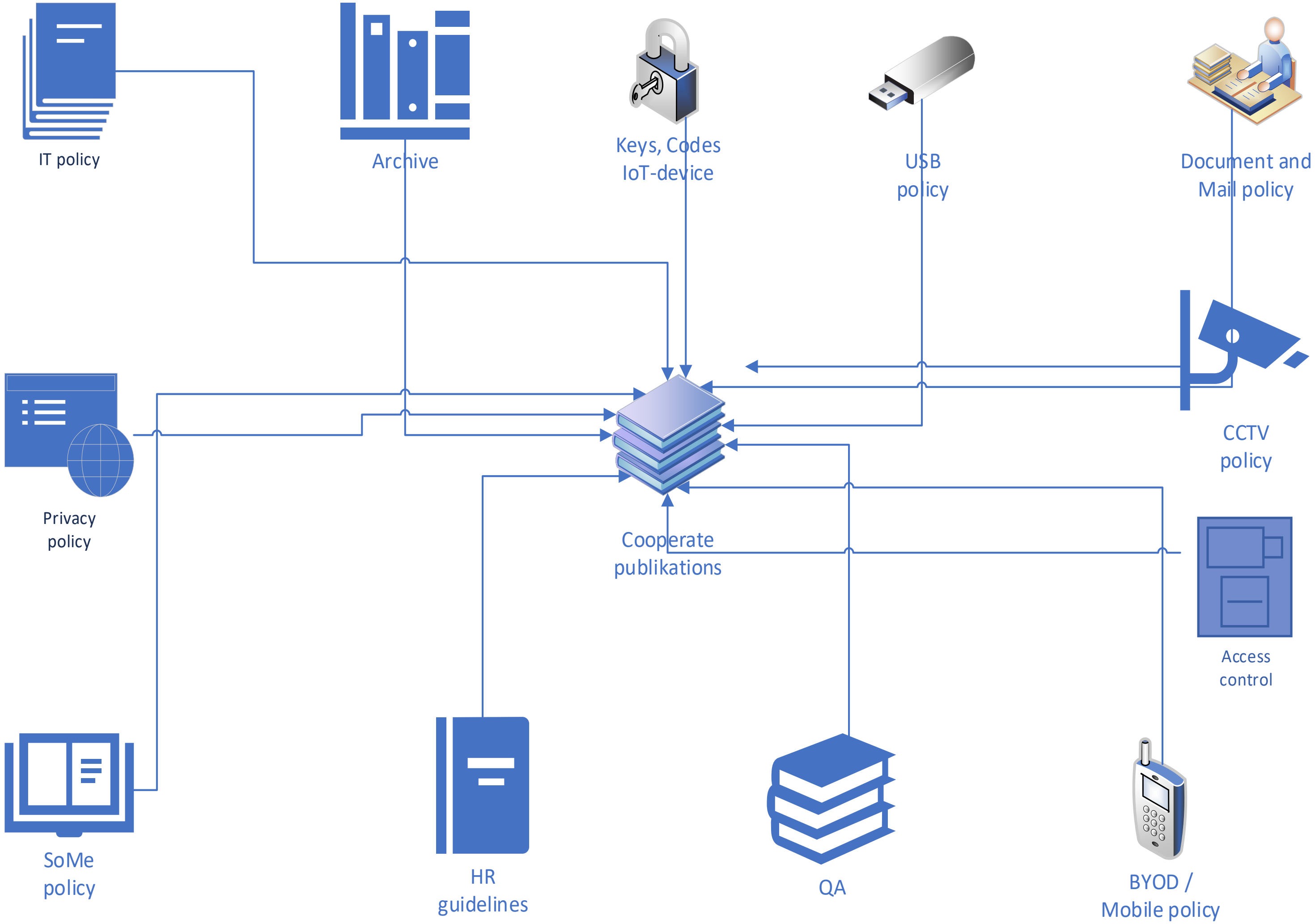
Security procedure

- Are employees informed that business and customer data may only be available on the company's equipment?
- Are employees informed of the penalties for not complying with the IT policy?
- Is there a policy that deals with unaccompanied visitors, use of common area?
- Is there periodic follow-up to the workplace to ensure that employees comply with IT policy?
- Do a background check of new employees be carried out e.g. check of references, criminal record?
- Will new employees get an IT security training?
- Is there a process that notifies the IT manager when an employee changes departments or leaves the company?
- Is there an exit interview involving IT assets, admission cards and the company's property?
- Is there a process that can immediately involve access to the company and IT systems?
- When an employee leaves the company, is it checked whether he has multiple passes or has handed over a pass to others?

Policies and documentation

E-Compliance Academy
EU GDPR INSTITUTE
E-learning platform for Insights/Online Seminars

- IT Security Policy
- Training and information on IT security
- Business Continuity Level
- IT Contingency Plan
- Disaster Recovery plan



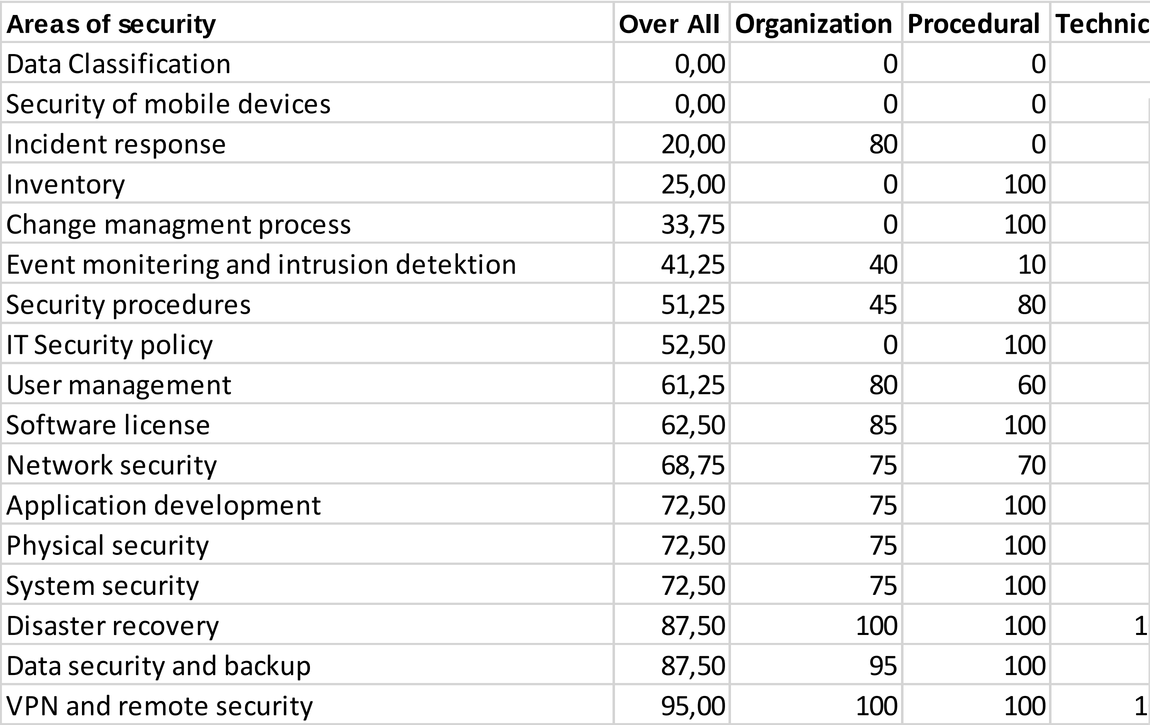
Security checklist

- We undertake an analysis of the risks presented by our processing and use this to assess the appropriate level of security we need to put in place.
- When deciding what measures to implement, we take account of the state of the art and costs of implementation.
- We have an information security policy and take steps to make sure the policy is implemented.
- Where have additional policies and ensure that controls are in place to enforce them.
- We make sure that we regularly review our information security policies and measures and, where necessary, improve them.
- We have put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.
- We may also need to put other technical measures in place depending on our circumstances and the type of personal data we process.
- We use encryption and/or pseudonymization where it is appropriate to do so.

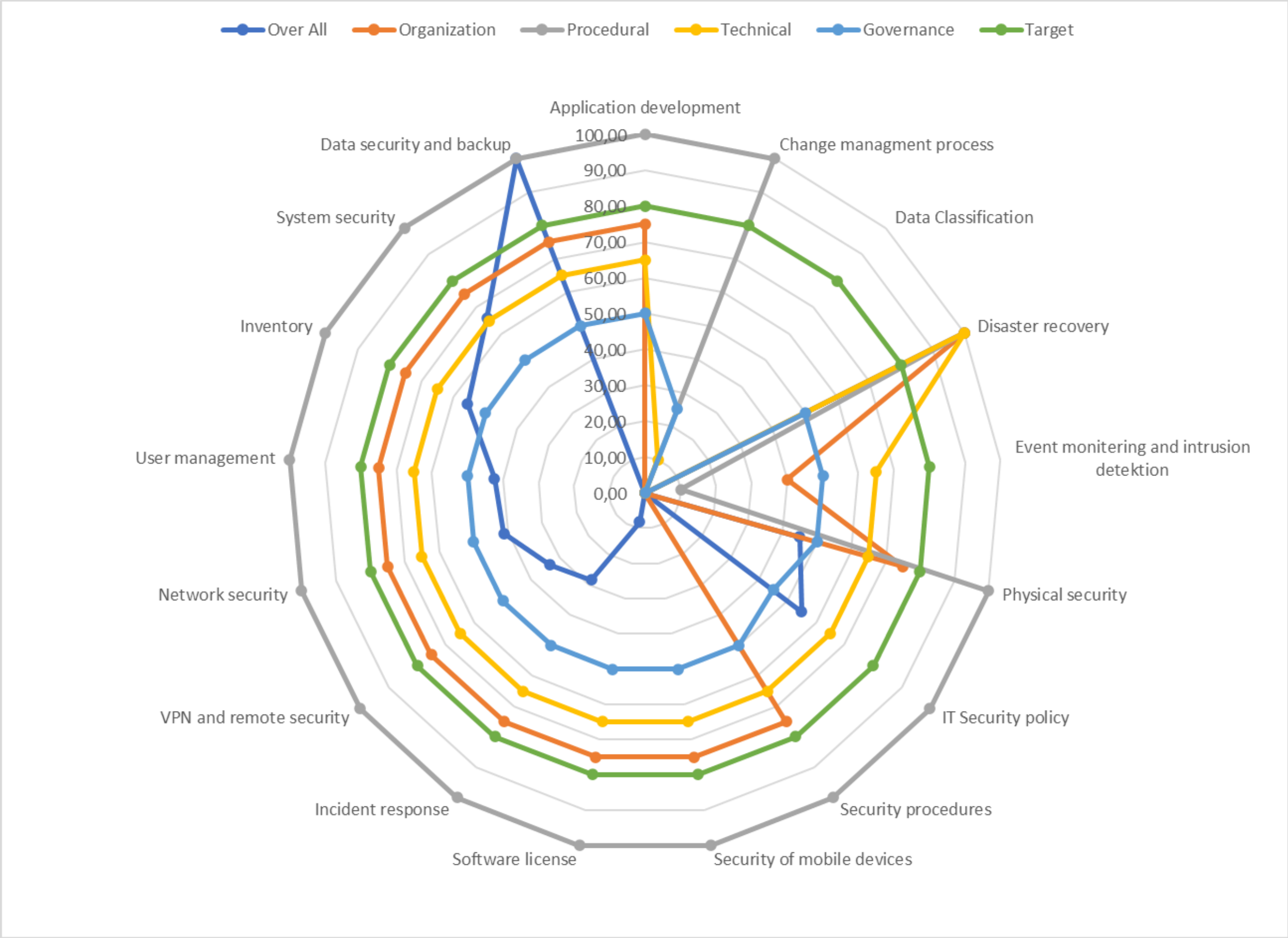
Security checklist

- We fulfill the requirements of confidentiality, integrity and availability for the personal data we process.
- We can restore access to personal data in the event of any incidents and have appropriate backup process.
- We conduct regular testing and reviews of our security measures and act on the results of those tests where they highlight areas for improvement.
- Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism.
- We ensure that any data processor we use also implements appropriate technical and organizational measures.

How this is prioritized …



Areas of security	Over All	Organization	Procedural	Technical	Governance	Target
Data Classification	0,00	0	0	0	0	80
Security of mobile devices	0,00	0	0	0	0	80
Incident response	20,00	80	0			
Inventory	25,00	0	100			
Change managment process	33,75	0	100			
Event monitering and intrusion detektion	41,25	40	10			
Security procedures	51,25	45	80			
IT Security policy	52,50	0	100			
User management	61,25	80	60			
Software license	62,50	85	100			
Network security	68,75	75	70			
Application development	72,50	75	100			
Physical security	72,50	75	100			
System security	72,50	75	100			
Disaster recovery	87,50	100	100	1		
Data security and backup	87,50	95	100			
VPN and remote security	95,00	100	100	1		


Over All
Organization
Procedural
Technical
Governance
Target
Application development
Change managment process
Data Classification
Disaster recovery
Event monitering and intrusion detektion
Physical security
IT Security policy
Security procedures
Security of mobile devices
Software license
Incident response
VPN and remote security
Network security
User management
Inventory
System security
Data security and backup