White Paper

enablor

Cloud based IT-solution for gap analyses, risk assessments, process change and security management.

Functional description of the enablor solution for EU GDPR projects and more.

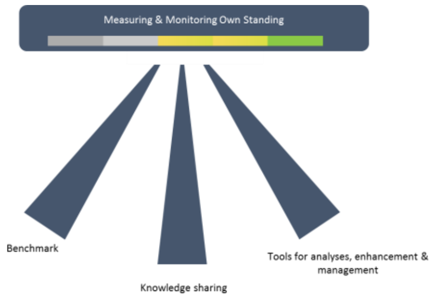
Information on the **enablor** platform for information security management

1. Behind enablor

I-Trust has long experience in helping organisations comply with legislation in the area of information security. In order to create an overview and the easiest possible progression, we have created **enablor** and placed it in the cloud.

enablor is a management and compliance portal developed to give organisations the option and opportunity to manage information security effectively, efficiently and focused. Using **enablor** the organisation can measure the status of compliance with legislations, get access to tools for analysing, improving and managing information security as well as sharing knowledge with and benchmarking against similar organisations.

enablor supports organisations' work with implementation of the EU GDPR, ISO and PCI standards. Using the benchmark tools, it is easy to monitor the outcome of the organisation's achievements – e.g. compared to resources used or actions taken.


Measuring & Monitoring Own Standing
Benchmark
Knowledge sharing
Tools for analyses, enhancement & management

*The **enablor** logo " the benchmark-symbol" refers to four functions: status, comparison, knowledge sharing and tools*

*1.1. Why Choose **enablor**?*

enablor supports the organisation's effort to comply with legislation and industry standards. At the same time, the platform provides access to reports for junior and senior management; management and implementation of best practice processes within the organisation as well as analysis, improvement and control tools for the IT manager, the information security manager and the Data Protection Officer (DPO).

The cloud-based solution offers a modern user interface that makes working with the EU GDPR and information security in general effective, efficient and easy. As everything is kept in the cloud, it is available at all times, anywhere geographically and secured against loss.

*1.2. **enablor** supports*

… an **overview** of the information security effort for the entire organisation. – From the managing director's strategic overview to the day-to-day managers' practical tasks.

… **prioritisation** of the organisation's efforts.

… **documentation** of actions, improvements and status.

… a platform in the **cloud** where all work related to the organisation's information security is kept together, *i.e.*, no more folders, file cabinets and confusing tabs. Everything can be found with a few clicks and is always nearby.

… management and reporting in an **easily available** and intuitive form.

… **effective** controls and changes to the IT organisation.

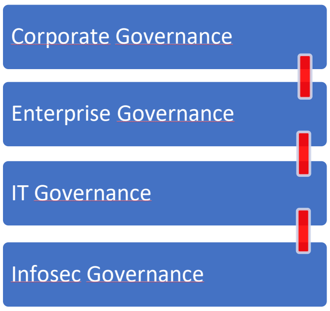
With **enablor,** it is easy to find the information needed, view graphs on progress and sustain improvements throughout the organisation.

With **enablor** the answer is certain and precise when someone asks if the organisation is compliant. **enablor** may be accessed by any single organisation as an individual information security management system (ISMS) or in a larger setup as a collaboration and knowledge-sharing platform for multiple organisations, such as groups, chains and association members.

1.3. Governance

enablor makes involving relevant personnel and levels in the organisation obtainable through reporting and inclusion in the information security processes:

- **Top management** has access to graphs on compliance and the work that is done to reach it.
- **Day-to-day management** can see whether relevant and recommended processes have been introduced.
- **IT management** has a detailed view into the coherence between processes and security efforts.
- The **information security manager** can see if all relevant controls have been introduced into the organisation and whether they are being maintained.



The keyword in having good governance is **cooperation** and **alignment** between the involved parties. **enablor** ensures that all relevant parties are involved and informed through delegation, reporting and collaboration tools.

*1.4. Acquiring **enablor***

enablor is acquired as a ”pay as you scale” solution, meaning that the price will mostly reflect the use. At the time of purchase, the needs of the organisation and the level of entry will be clarified and defined.

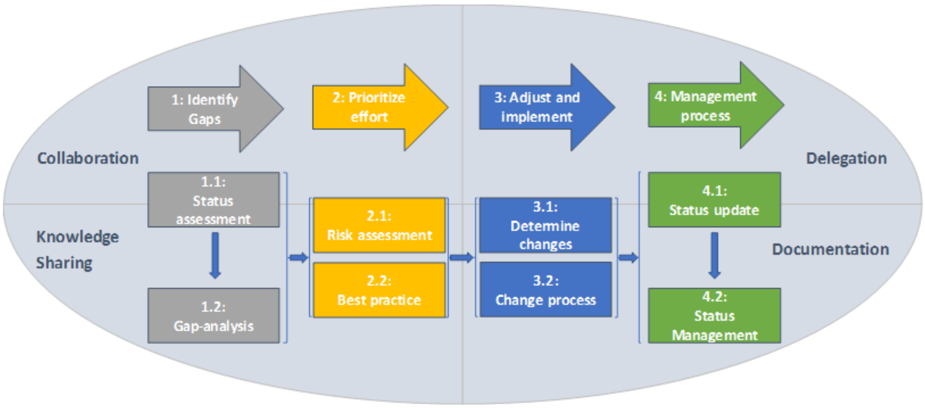
It is advised the organisation starts by making a gap analysis with focus on the EU GDPR and/or ISO 27001. After this, functions can be added to **enablor** following the progress of the organisation. Depending on the progress the organisation makes, different functions of **enablor** is taken into use.

The flexibility covers both functions and areas of collaboration as well as the number of users that are added.

The use of **enablor** as a members’ platform is advisable if a central organisation or association wishes to support its members by providing services concerning compliance such as benchmarking, best practice recommendations and legal requirements and at the same time present the members with an insight into the industry as a whole. The extent of services and functionality is defined in collaboration with the central organisation.

2. Workflow and Process Model

With **enablor,** organisations can base their work on a process model that supports managing information security, identifying specific focus areas and target improvement processes in such a manner that it involves relevant key personnel in the organisation.



The workflow and the process model is based on experience with the Plan-Do-Check-Act model, the Carnegie Mellon University IDEAL model and the continuous efforts in the Six Sigma model to achieve a workflow that covers all parameters and processes.

The organisation will work with processes in well-defined steps to achieve compliance in the focus areas. This is done by:

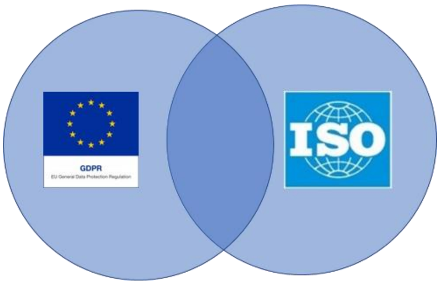
- identifying gaps in relation to legal requirements and standards based on tested and approved controls and questions that cover the organisation’s compliance level. Questions and answers overlap, so that multiple areas with partly similar demands will be answered simultaneously (*e.g.*, EU GDPR and ISO 27001),
- prioritising actions that need to be taken to fill the identified gaps using risk assessment and other organisational practice,
- documentation of information security level in a Statement of Applicability (SoA) document for auditors, shareholders and board directors.
- commissioning of change processes in the organisation based on the identified gaps or other needs,
- managing information security based in an annual work cycle containing controls with planned intervals and follow-up on the information security level.

3. Tools

All Tools in **enablor** are in the toolbox. The toolbox is augmented continuously and tools are used to the extent that is relevant for the organisation’s project and information security management.

3.1. Assessing Compliance and Status

enablor provides a status assessment tool, where compliance with EU GDPR, ISO 27001 and best practice control frames is assessed. The status assessment is done flexibly both in terms of what is assessed and when it is done. Controls and areas that are overlapping are marked as assessed everywhere when they are assessed in one place. This reduces time spent in the organisation and ensures uniform answers across frames.



***enablor** makes working with multiple compliance frameworks easy – without duplication of data and processes*

3.2. The Gap Analysis

The first step towards compliance is locating gaps and prioritising, which areas will be dealt with first. Even though the organisation hasn't yet worked with all focus areas **enablor** documents what is planned for the future. This documentation is important as the actual planning shows that the organisation works towards compliance. In **enablor** tasks are registered in the Analysis and the SoA Tools and information about who is in charge of the individual tasks and their progress as well as the overall process for the organisation.

3.3. Dashboard

On the organisation's **enablor** Dashboard, the current compliance-level can be viewed, and comparison with previous scores or benchmark groups can be made. Through the dashboard, the management has easy access to viewing the organisation's compliance with requirements with simply KPIs in central areas. This makes it easy to get a clear overview.

3.4. Prioritising Effort

enablor supports prioritising of the organisation's efforts with tools for registration of dataflow and risk management and by benchmarking with organisations with best practice. This is used to assess and define a desired or needed level of information security as well as expected effect based on the level of comparable organisations.

3.5. Benchmark

With **enablor,** the organisation's efforts can be measured and compared with other organisations to determine if the organisation works cost-effectively. In the Analysis Tool benchmark data can be filtered to show comparison with previous assessments, subsidiaries or comparable organisations based on, *e.g.*, size or geographical location. **enablor** provides a range of business intelligence functionality that ensures substantiated processing of the status assessment. This includes gap analyses, Best-In-Class/Worst-In-Class, result predictions and more.

The outcome of benchmarking increases the likelihood of locating the best areas for improvement and using best practice experience from other organisations.

3.6. Statement of Applicability - SoA

While doing the gap analysis – perhaps supported by risk assessment and/or benchmark – the status of the organisation can be summed up in a SoA document that draws data from other parts of the system. The SoA sums up the status of the organisation's compliance goals and milestones. This helps make working with information security more manageable and accessible. The document is a key step in the compliance process with ISO 27001. The SoA works as a declaration of intent for the organisation and document the planned steps towards compliance.

The SoA provides a place for noting the considerations that have been included in determining the prioritisation of efforts and goals. A management-approved Statement of Applicability guaranties that the information security manager knows the priorities of the top management and is made available so that it can be used in auditing or given to board members, other stakeholders and managers in general.

3.7. Status Improvement

The identified gaps and SoA goals can be collected in improvement tasks, which are the described, prioritised and collected in the annual work cycle. Each task can be assigned to persons, who will receive an e-mail invitation that grants access to a mini-**enablor** where all the person's tasks are collected and managed. In this way, tasks can be assigned to relevant personnel in different departments (also outside IT) without having to grant access to the entire ISMS. The person assigned to the task can then document change and change status of the tasks and the areas involved.

As tasks area are performed and finished, the status assessment will be updated and the information security manager can monitor and react to the development in the Status Management tool.

3.8. Status Management

The annual work cycle is automatically created and updated in Status Management. From here the information security manager can manage and follow up on tasks and controls to maintain regularity.

Apart from creating and managing tasks, **enablor** also supports creation and management of controls of recurring information security events. The controls ensure that the improvements made are functioning according to plan. Documentation of these controls is readily available, so that progress and status of every task and control are always known.

Managing tasks and controls in Status Management can be achieved with focus filtering, so that a focus on, *e.g.*, ISO 27001 can be made to follow only the tasks and controls related to this specific area. This helps reporting on progress on specific areas right down to the single questions of the status assessment.

Tasks in the annual work cycle can be filtered by individuals so that periods with too many deadlines can be avoided and ensure that tasks are evenly distributed between available personnel.

With Status Management, the organisation's information security manager and top management gain control over how many tasks are in progress and the status of each.

3.9. Documentation

In **enablor**'s Archive all finished tasks and controls are collected so that they can be used as documentation when talking to authorities and external parties.

4. Risk Management

Risk Management is a tool that is built for action and progress. Risks and their consequences for the organisation's business and processes are assessed. The tool helps ensure identification, creation and description of the risk profile and by focusing on close relationships between data resources and processes maintenance of the risk library becomes much easier.

4.1. Process Description

In **enablor**'s Risk Management processes are registered and assessed in accordance with their importance to the organisation. To ensure a correct and manageable assessment, the processes are divided into three levels: process area (the overall area), business process (typically with a process owner) and process (the actual task that is done).

The division in levels ensures that organisational changes (new/updated processes, new software, etc.) can easily and effectively be registered and inserted into the existing structure.

For every process, dependency to other processes and software or other resources is registered.

Consequences for the business, Business Impact Assessment (BIA), and the data subject, Data Privacy Impact Assessment (DPIA), are evaluated for each process and both dependent processes as well as the supporting assets inherit this consequence assessment.

During the registration of processes, documents and files that are being used are identified with focus on those containing privacy data and all registered data will be classified according to commonly used classification types.

4.2. Dataflow and Resource Registration (Privacy)

Dataflow and resource registration related to privacy is a new requirement introduced by the EU GDPR. It is required that organisations create and maintain consequence assessments for data relating to all personal data.

If the organisation wished to be ISO 27001 compliant it is a first step to register and maintain dataflow as well as registering resources in the form of assets and IT systems involved in processing data. This is part of creating an organisational overview and organising the ISMS.

Dataflow and resource registration is an overview of all possible placements of documents and data, which, when done correctly, create a map of places where potential security breaches can happen. Location and classification of data are done in the organisation mapping.

4.3. Consequence Assessment

The consequence assessment is the foundation of the consequence analysis on processes as well as data and resources. In this assessment, consequences in the event of a breach of both the data subject and the business are considered. This is the foundation of the organisation’s Data Privacy Impact Assessment (DPIA) and its Business Impact Assessment, both being dynamically updated when processes and resources are changed.

5. Support for Multiple Organisation Structures.

enablor supports knowledge sharing, which is an important part of developing the organisation’s information security and processes. There are several possible ways of involving, delegating and sharing knowledge within the organisation and with external organisations as well.

5.1. Internal Task Delegation

Tasks, controls and risk assessments can be delegated to the personnel that are directly responsible. Individuals can access and document changes for their tasks using mini-**enablo**r.

The task responsible individual receives an invitation by e-mail that grants access to all his tasks in mini-**enablor**. In this way, tasks can be assigned to relevant personnel in different departments (also outside IT) without having to grant access to the entire ISMS. The person assigned to the task can then document change, and change status of the tasks and the areas involved.

5.2. Chat

enablor’s chat helps keeping the dialogue about information security between the involved parties, instead of spreading it through e-mail and other channels. The chat can be set up to cover different levels: internally in the organisation as well as within communities or to external partners.

5.3. Library

The Library enables sharing of files – guidelines, policies, templates, etc. – internally, in communities and with external organisations.

5.4. Group structure

Organisation setup with subsidiaries or underlying institutions enables sharing and collaboration within a joint effort between main organisations and their subsidiaries. Benchmark can be made for the group as a whole or against and amongst the individual subsidiaries.

5.5. Collaborations

Collaboration and formal groupings of organisations can be setup on several levels between organisations that work together on the information security area. The organisation can benchmark within the collaboration as well as share information and knowledge.

5.6. External DPO

The use of external consultants and Data Protection Officers is supported by **enablor**. The cloud-based solution is ideal for giving an external consultant or the rented DPO access to **enablor**.

6. enablor For Projects with Multiple Participants

enablor's functions support projects where a central project owner or organisation supports a number of organisations. Through business intelligence tools, the project owner can follow development of the project and observe whether set goals are reached. The central project owner has access to knowledge-sharing tools for chatting and for distributing files targeted at the participating organisations.

6.1. enablor As a Collaboration and Knowledge Sharing Tool

enablor can be used as a knowledge sharing and survey tool, where participants have access to one or more questionnaires. The organisations can follow their own status on the **enablor** Dashboard and compare with other participating organisations. The survey will then become the basis of individual status assessments and the continuing work with information security, as well as being the foundation of analyses and guides created by the central organisation to support the participating organisations.