INFORMATION SECURITY
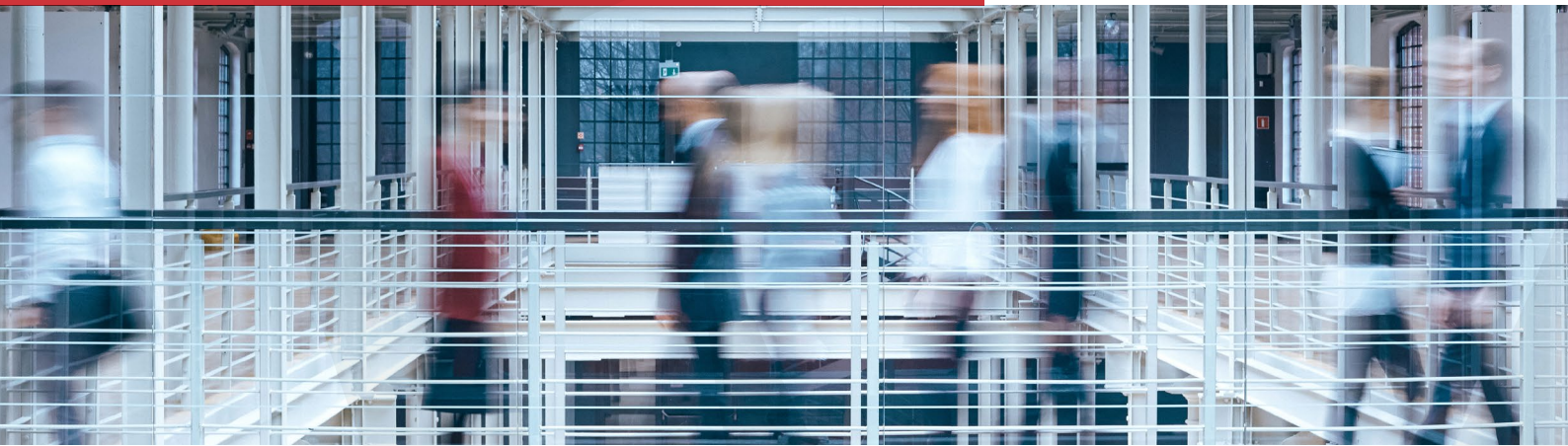
Secura

When companies mature, the question of whether or not they need to be certified for information security often arises. The most common certification is the ISO 27001 standard. Secura helps organisations with implementing such standards, as well as other similar standards and certifications such as BIR, BIG, BIWA and NEN 7510.

IN CONTROL WITH SECURA

Secura has worked in information security and privacy for nearly two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. For our customers we offer a range of security testing services varying in depth and scope.

INFORMATION SECURITY: ISO 27001, BIR, BIG, NEN 7510

Secura has been providing top-notch services for almost two decades. Our customers ask more us from than just technical security assessments. When companies mature, the question of whether or not they need to be certified for information security often arises. The most common certification is the ISO 27001 standard. Secura helps organisations with implementing such standards, as well as other similar standards and certifications such as the BIR, BIG, BIWA and NEN 7510.

Secura is specialised in the design and implementation of Information Security Management Systems (ISMS) based on ISO 27001. We work in the areas of people, processes and technology.
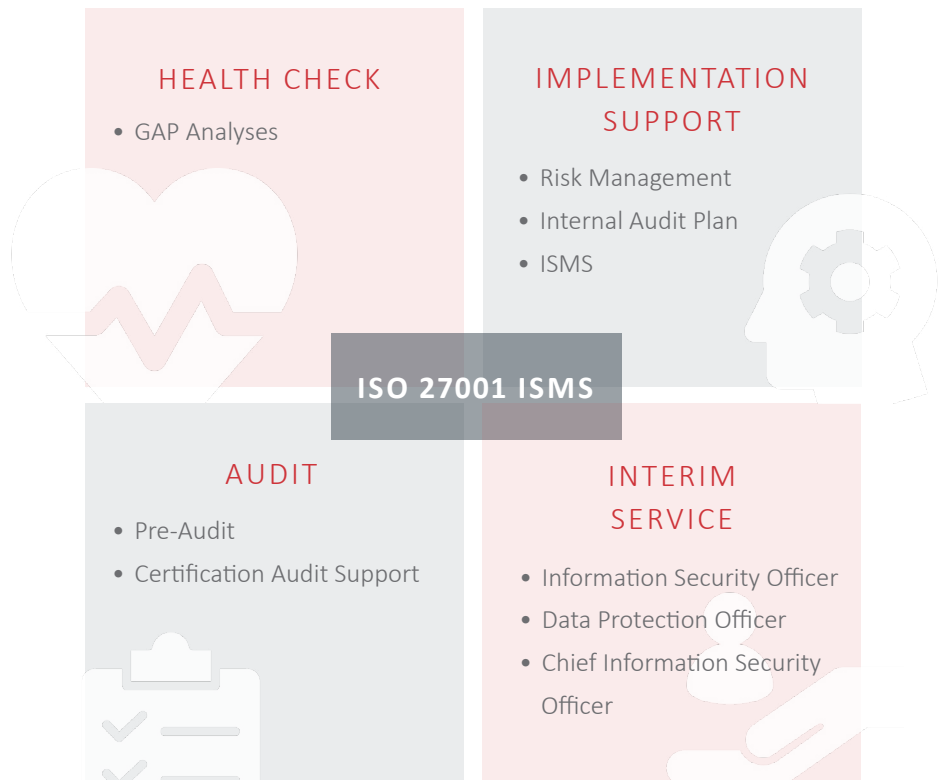
Based on our knowledge and experience we have developed various services which can help you to be 'in control' and stay that way in the area of security management. We can guide you in your path towards the ISO 27001 certification.

We offer the following services:

- Health check (zero measurement or GAP analysis)
- Implementing risk management
- Support implementation;
- (Pre-) audit
- Interim Services (CISO, ISO and DPO).

HEALTH CHECK

- GAP Analyses

IMPLEMENTATION SUPPORT

- Risk Management
- Internal Audit Plan
- ISMS

ISO 27001 ISMS

AUDIT

- Pre-Audit
- Certification Audit Support

INTERIM SERVICE

- Information Security Officer
- Data Protection Officer
- Chief Information Security Officer

RELATED STANDARDS

Next to ISO 27001, there are a number of related standards in the Netherlands that have been deduced from (or strongly resemble) ISO 27001 in the sense that they all require an Information Security Management System (ISMS) and control framework based on many of the same criteria. For example:

- **Baseline Informatiebeveiliging Rijksoverheid (BIR)**
  The BIR is completely structured according to ISO 27001 and 27002. The government is mandated to meet ISO 27001 and ISO 27002. The BIR describes the interpretation of ISO 27001 for the government.

- **Baseline Informatiebeveiliging Gemeenten (BIG)**
  The BIG is the interpretation of the same standard frameaworks, speculated for the Dutch municipalities.

- **Baseline Informatiebeveiliging Waterschappen (BIWA)**
  The BIWA speculates the ISO 27001 and 27002 standard for the 22 Dutch water boards.
- **NEN 7510 (Medical care)**
  The interpretation of ISO 27001 for medical care is determined in the NEN 7510 standard. In this case a number of the standards is not optional anymore, but mandatory in the context of privacy (AVG and GDPR) and protection of patient data.

For BIR, BIG and BIWA no certification bodies currently exist. The process of introduction however, is equal for both the government and municipalities, as well as the water boards, except for the certification audit.
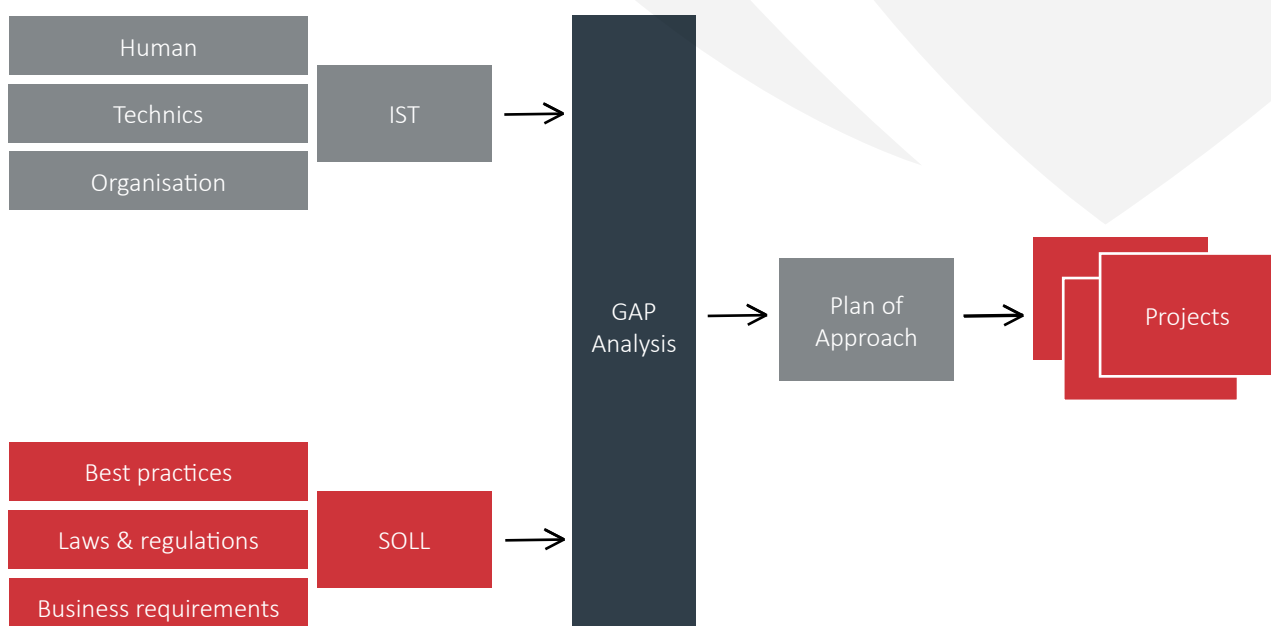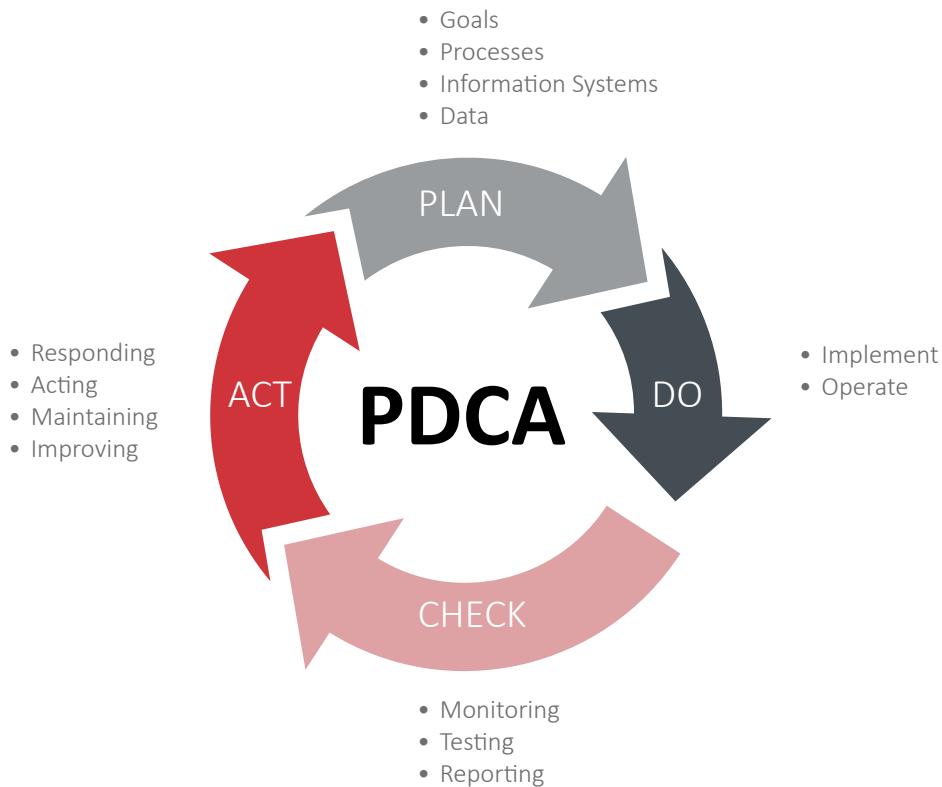
THE PROCESS

The experience of Secura teaches us that there are a couple of critical factors for a successful implementation of ISO 27001. First of all, there needs to be commitment from upper management. A precondition is that information security has the full attention of senior management. In addition, choosing the right framework for the introduction is important. Too small a framework limits the value of the standard and any certificate that can be obtained; too large a framework makes the project unnecessarily complex. Especially if the framework is chosen across multiple departments or business units, this creates greater complexity because the objectives of these departments or business units are not always in line with each other, making the scope of the ISO standard difficult to determine.

As stated above, Secura offers support in implementing the ISO 27001 (or comparable) standard or achieving the certification. Specialists from Secura play a facilitating and accompanying role. They contribute their knowledge, expertise and resources to make the implementation as efficient and effective as possible. During the project, choices will have to be made continuously and Secura can help you to make these choices based on the risks. In addition, Secura has templates and other documents available that you can use when drawing up the required documents for certification purposes. The overview below shows the process of introducing an ISO 27001 or a comparable standard outline.

For ISO 27001 and other standards, an ISMS (Information Security Management System) is implemented. This management system works on the basis of the Plan-Do-

PLAN
- Goals
- Processes
- Information Systems
- Data

DO
- Implement
- Operate

CHECK
- Monitoring
- Testing
- Reporting

ACT
- Responding
- Acting
- Maintaining
- Improving

PDCA

Check-Act cycle. If you already have a certification for quality standards (ISO9001 for example), it is useful to make use of this. The advantage is that the quality and security are managed from a single management system and as many as possible of the existing procedures and standards are reused. Secura does not carry out the final certification audit because of our independence (we can not test what we have implemented ourselves).

WHY?

An ISO 27001 certification (or implementation of BIR/BIG/BIWA/NEN 7510) supports business objectives, such as:

- market recognising that you are in control of your information security;
- compliancy with laws and regulations;
- raising awareness in own organisation;
- identifying security risks;
- cost reduction by improved process control;
- risk inventory: which matters need to be prioritized;
- avoiding fines and losses as a consequence of data leaks.

It is of course also possible that you have another question in this area. For example if you want to know how far away you are from the standards by means of a GAP analysis or audit, or that you would want thoroughly implement risk management. Even when you are more advanced, a periodical risk analysis or the execution of technical tests by an independent party is strongly advised. In all these cases you can rely on Secura's experience.