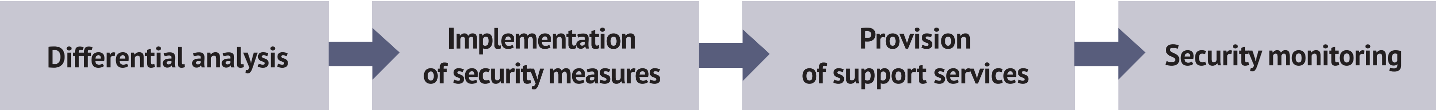
Cyber security solution

A COMPREHENSIVE CYBER SECURITY SOLUTION ACCORDING TO THE LAW NO. 181/2014 AND THE CORRESPONDING IMPLEMENTING DECREE NO. 316/2014

Cyber security solution from the company **TESCO SW a.s.** responds to the introduction of cyber law No. 181/2014 and the relevant implementing Decree No. 316/2014.

It is a comprehensive solution, which consists of the following parts, which tie in with one another:



Differential analysis → Implementation of security measures → Provision of support services → Security monitoring

Introduction to topic

On 1. 1. 2015, **Law No. 181/2014 Coll. on Cyber Security (LoCS)** came into effect. At the same time, Decree No. 316/2014 on Cyber Security (DoCS) became effective.

Their aim is to ensure on country level especially:

- Orderliness and organization in the field of cyber security.
- Unifying level of security measures on critical and important IS.
- Monitoring and evaluation of security incidents.
- Definition of procedures, how to act in emergency situations.

Authorities and persons, onto whom there are imposed obligations in the area of cyber security, are set out in section 3 of LoCS. Those are usually, but not exclusively, **providers of information and communication system of critical infrastructure and administrators of important information system**.

According to section 30 and section 31 of LoCS, they are required, within 1 year from the date of determining critical or important IS, to establish and implement security measures and keep up security documentation.

Group of major IS is formed by such systems, which are explicitly stated by Decree No. 317/2014 Dig. on important IS or which correspond to defining criteria stated in this Decree.

Similarly, it will be in the case of critical IS. The relevant decree has not yet been published.

Introduction of obligations according to LoCS and DoCS also implies the introduction or strengthening of service management processes (ITSM), such as management of events, incidents, problems, changes, release & deployment, SLA , suppliers, etc.

Cyber security solution

Cyber security solution from the company TESCO SW a.s. consists of several parts, which tie in with one another:

1) **Differential analysis** – it maps the effects of LoCS and DoCS on customer's IS in question.

2) **Implementation of organizational and technical security measures** – editing or creating security documentation, editing or creating monitoring and security software.

3) **Provision of support services** – training, consultancy, preparation for system certification according to ISO 27001.

4) **Security monitoring** – regular security audits, review of risk analysis, online 24x7 security & operation monitoring.

DIFFERENTIAL ANALYSIS

It maps the effects of LoCS and DoCS on customer's IS in question. Analysis is based on the detailed study of LoCS and DoCS. It contains:

- **Identification of administrator's obligations** – division into 3 areas: obligation is met; failure to meet it; partially met, change is necessary.
- **Product break-down** – it identifies customer needs in the form of documents, services and HW & SW deliveries necessary to ensure the fulfilment of administrator's obligations.

- **Contracting sheets** – logical division of product break-down into individual partial executions and detailed wording of assignment for implementer. Implementer may be a supplier, third party and in some cases customer himself. They also contain a price estimate and proposed date of partial execution.
- **Migration schedule or delivery timetable** – process schedule for introduction of organizational and technical measures, incl. timetable for partial deliveries.

IMPLEMENTATION OF SECURITY MEASURES

After approval of differential analysis, there follows a phase of executing organisational and technical security measures:

- **Security documentation** – Editing or creating documentation, whose subject is to define (security policy) objectives and state how to achieve them (for example IT service management strategy). Subject also includes determination of security assets (Risk analysis).
- **Other documentation** – In connection with the introduction of changes to updating of organizational and controlling documents.
- **Monitoring and security SW** – Modification or delivery of systems, monitoring and protecting the concerned infrastructure - proactive monitoring tool of IT environment (e.g. MS SCOM for operational logs), SIEM for security logs (security information and event management), firewall, IPS (Intrusion Prevension Systems) for advanced service management of network data flow filtering or HSM for advanced security operations.
- **Application SW** – Modification or delivery of Service Desk supporting processes in the area of ITSM and providing reporting tool functionality on the basis of logs and alerts from monitoring systems. According to the set rules, Service Desk notifies about reports via SMS or email.

PROVISION OF SUPPORT SERVICES

This part includes the following services:

- Provision of expertise according to section 6 of clause 2 of DoCS (Cyber security administrator, Cyber security architect).
- Training in accordance with the development plan of the security awareness according to section 9 of DoCS.
- Preparation for ISO 27001 certification according to section 29 of DoCS.
- Providing execution of reactive and protective measures of NSO according to section 11 of LoCS.

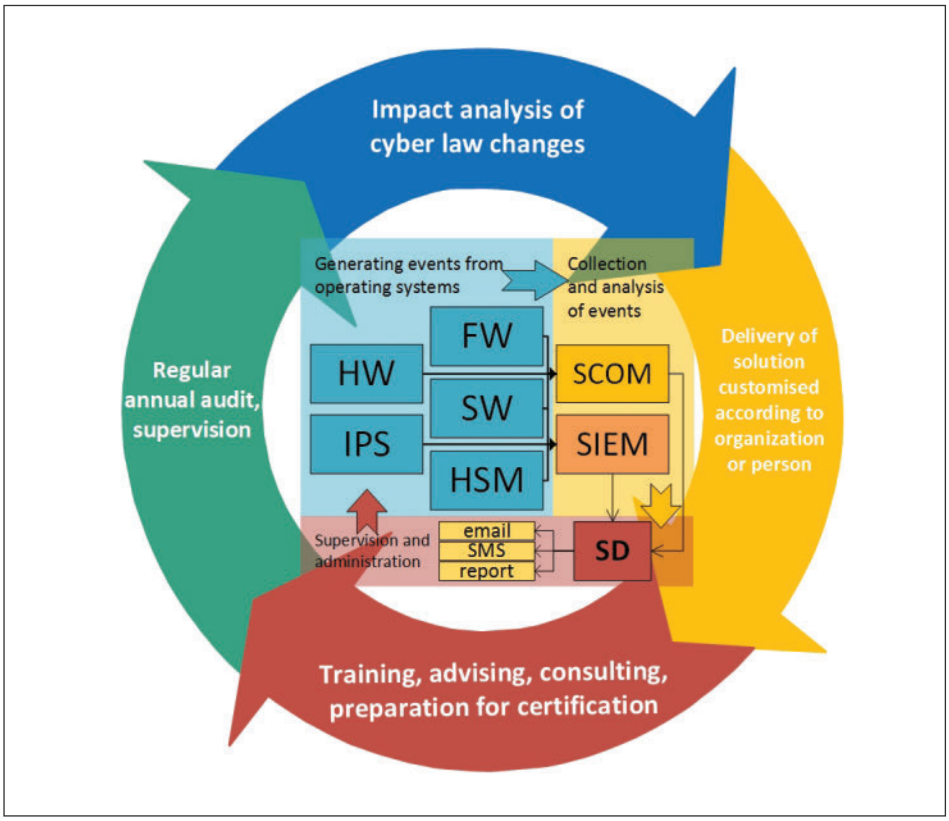
SECURITY MONITORING

It includes the following services:

- Online operation and security monitoring in 24x7 mode (continuous oversight and immediate support for the cyber security solution of events and incidents, according to section 13 of DoCS).
- Providing processes of information security management (ISMS) according to section 3 of DoCS (maintenance and update of security documentation, regular updates of risk analysis).
- Providing processes of IT service management (ITSM) according to DoCS, title I and II.
- Security audit and inspection according to section 15 of DoCS.

Goals of Cyber security solution

- ✓ Identification of necessary security measures according to section 5 of LoCS.
- ✓ Implementation of necessary security measures = fulfilling administrator's obligations according to section 4 of LoCS.
- ✓ Introduction or update of processes related to information security management system (ISMS) according to section 3 of DoCS.
- ✓ Introduction or update of processes related to IT service management (ITSM) within the meaning of DoCS, title I and II.
- ✓ Provision of support services.
- ✓ Provision of security monitorin services.


Impact analysis of cyber law changes
Generating events from operating systems
Collection and analysis of events
FW
HW
SW
IPS
HSM
SCOM
SIEM
Supervision and administration
email
SMS
report
SD
Regular annual audit, supervision
Delivery of solution customised according to organization or person
Training, advising, consulting, preparation for certification