IT RISK ASSESSMENT (SITE)

Secura
A BUREAU VERITAS COMPANY

At vero eos et accusamus et iusto odio dignissimos ducimus qui blanditiip-
raesentium voluptatum deleniti atque corrupti quos dolores et quas
molestias excepturi sint occaecati cupiditate non provident, similique sunt
in culpa qui officia deserunt mollitia animi, id est laborum et dolorum fuga.
Et harum quidem rerum facilis est et expedita distinctio. Nam libero
tempore, cum soluta nobis est eligendi optio cumque nihil impedit quo
minus id quod maxime placeat facere possimus, omnis voluptas assumenda
est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis
debitis aut rerum necessitatibus saepe eveniet ut et voluptates repudiandae
sint et molestiae non recusandae. Itaque earum rerum hic tenetur a
sapiente delectus, ut aut reiciendis voluptatibus maiores alias consequatur
aut perferendis doloribus asperiores repellat.

INSIGHT INTO YOUR DIGITAL SECURITY

Secura is your independent, trusted security partner. We help organisations by providing valuable insight into their digital security from a people, process and technology perspective.

Secura offers audit, test & certification services in the world of IT, IoT and OT. We link our audit and test work to international norms, standards and metrics.

The Need for Cybersecurity at your Sites

Cyber-attacks on critical infrastructure are on the increase, and are a growing concern for system operators, especially considering the increasing convergence between IT and OT. When looking back at the past, several organizations were victim of a cyber-attack on their site or plant having a significant impact on their key assets. External attackers could gain access to your plants' production network through your IT network causing ‘massive’ losses. Attacks such as these can severely affect service uptime, data integrity, compliance, and public safety. It is imperative that companies that rely on computer networks for industrial control system operations assess their current security posture, understand potential security risks, and develop effective risk mitigation strategies.

The Goal of Security Maturity Assessments

Secura has created the IT risk assessment to identify site-level risks as opposed to organizational level risks. The IT risk assessment approach uses internationally accepted standards and best practices such as the ISO 27000 family.
By performing an IT risk assessment, which can be combined with an OT risk assessment or any of the other services you will gain more control over your protection measures and its effectiveness against various threat actors. Threat actors can include organized crime, industrial spies, malicious insiders or even hacktivists. **The IT risk assessment will help you in protecting intellectual property, corporate secrets, financial information or disruption of business operations.**

Method

The identification of your organizational assets is a critical part of this assessment including people, property, and informational assets. **People assets** include more than just the employees; they include visitors, contractors, community and others that have or could have an association with business operations. **Property assets** range from building, machinery and utilities to operations, equipment and systems. **Informational assets** are computer systems, processes, and confidential business and employee information. The IT risk assessment will help you identify the risks and vulnerabilities for each category of assets. Among the identified risks are break-ins and thefts to previously overlooked risks of terrorism, espionage and sabotage.

The IT Risk Assessment of Secura adheres to internationally recognized standards on information security such as **ISO 27001, COBIT 5, and the NIST Cyber Security Framework**. The IT Risk Assessment is specifically designed to help organizations in identifying security risks at their site in an early stage and to recognize and resolve previously overlooked blind spots. The IT Risk assessment addresses the following aspects (based on and linked to ISO 27002).

1. **Assessing Environmental Security:** Equipment should be sited (placed) or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
2. **Physical Security:** Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises are assessed for security risks.
3. **Asset Management** Security: Asset management controls are assessed and it is verified that all IT equipment located within the facility is protected from unauthorized users.
4. **Access Control:** It is a fundamental concept in security that minimizes risk to the business or organization. The goal of access control is to minimize the risk of unauthorized access to physical and logical systems
5. **Privacy & Data:** 'Company Confidential' and 'Restricted' information should not be left unattended. The allocation of passwords shall be controlled through a formal management process.
6. **Human Resource Security:** The objective is that employees receive sufficient cyber security training on a regular basis that is applicable to their responsibilities and before obtaining access to the facility's critical cyber systems.
7. **Communications Security:** protection of communication technology, systems and devices.

The site assessment is performed by one of our dedicated consultants specialized in demonstrating compliance with regulations, assessing information security, providing insight into shortcomings and improvement measures, as well as giving advice. Secura supports multiple (international) clients in providing insight into the security of their offices or production sites.

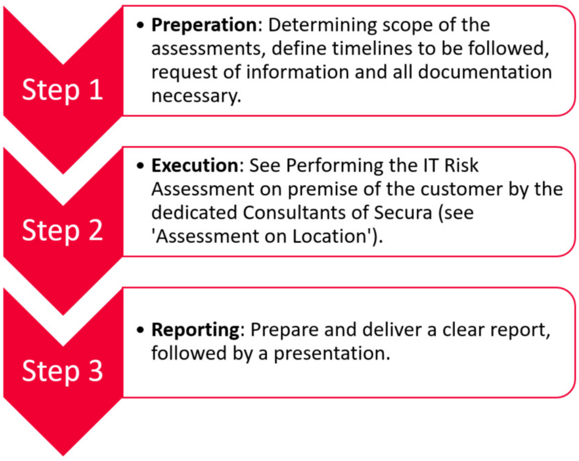
Purpose of the Assignment

An in-depth risk assessment and analysis are one of the first steps in achieving effective site security management. Secura supports in determining the quality of security measures and helps in the identification of information security risks. Secura does this by performing independent security assessments covering Information Technology (IT) facets based on the well-known ISO 27001/2 standard.

Assessment Stages

An IT risk assessment has **three main assessment stages.** The preparation and reporting phases are performed offsite while execution is performed onsite.

Figure 1. The three assessment stages



Step 1

- **Preperation**: Determining scope of the assessments, define timelines to be followed, request of information and all documentation necessary.

Step 2

- **Execution**: See Performing the IT Risk Assessment on premise of the customer by the dedicated Consultants of Secura (see 'Assessment on Location').

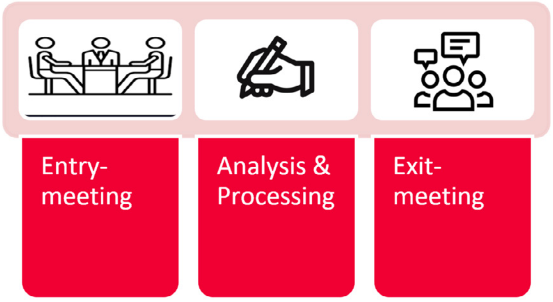
Step 3

- **Reporting**: Prepare and deliver a clear report, followed by a presentation.

Assessment on Location

At the beginning of the site visit, a quick gathering is organized with relevant personnel that is involved to align and repeat on the expectations, way of working and any other details that might be relevant. Together with a supervisor from the customer the IT risk assessment is performed. At the end of the site visit, as in the beginning a meeting is organized to give a summary of the findings.

Figure 2. A depiction of an Assessment on Location



Entry-meeting

Analysis & Processing

Exit-meeting

Result

After the assessment has been conducted in line with the selected criteria, the assessment results, conclusions and findings are summarized in an Assessment Report. Risks are presented which are linked to the various and relevant parts of the ISO 27001/2 standard. By means of the IT risk assessment identifies any threats aiming to take advantage of any vulnerabilities and/or blind spots. The IT risk assessment is performed by using a well-established framework build on state-of-the-art best practices and information security standards. Our consultants take an attacker-like mindset during

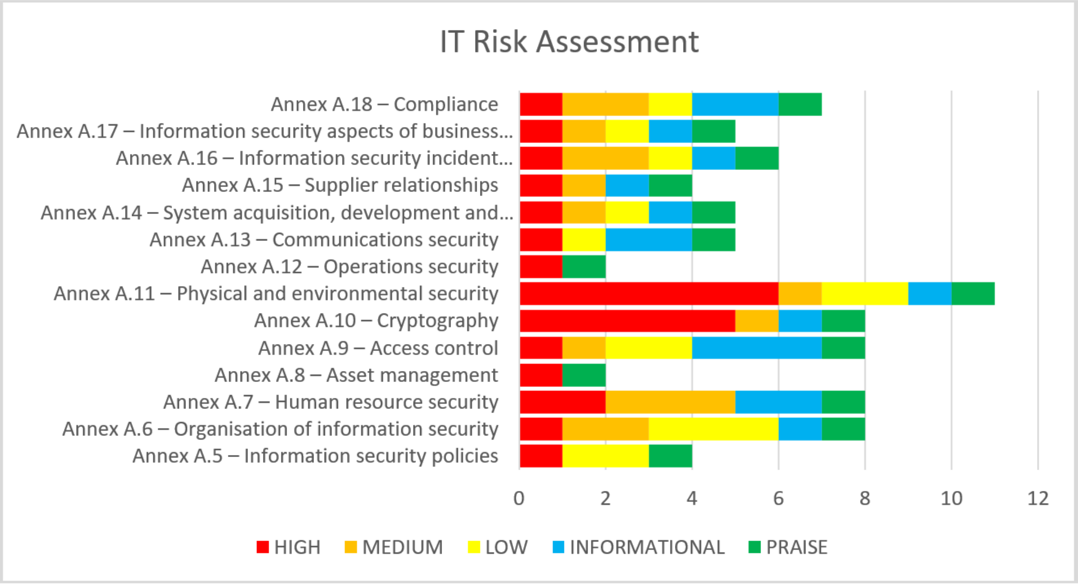
The IT risk assessment will lead to a detailed report with all the identified risks and consequent risk rating which can be aligned to your own risk management standards. Each risk will be linked to ISO 27002 controls to provide you insight into how your organization fares against internationally accepted standards. For each risk, a recommendation will be provided, on which you can count on Secura for implementing the recommendations.

Why Secura?

Since 2000, Secura has been supporting organizations with high-quality services. Secura has its origin in the technical and audit domain of IT security, which is an extremely complex and rapidly changing field in which a continuous race is going on between digital burglars and security experts.

The IT risk assessment is performed by one of our dedicated consultants who have experience in demonstrating compliance with regulations, standards and best practices. Identifying risks and providing risk mitigation strategies and recommendations are part of our core business. Our security consultants are required to have state of the art knowledge to provide you with insight into any shortcomings and improvement measures.

Figure 3. An example of an IT-risk assessment report



Secura
A BUREAU VERITAS COMPANY

Interested?

Contact us today:

Follow us:

☎ +31 88 888 31 00

✉ info@secura.com

secura.com

BUREAU VERITAS 1828

BUREAU VERITAS

Shaping a World of Trust