Siemens Cyber Security Consulting for ISO 27001 Certification and Beyond

Management Summary:
Siemens PTI's Energy Business Advisory supports power utilities as well as other Siemens divisions in the area of security. We have built a successful track record of customer projects over the last 4 years. Our proven subject matter expertise is recognized and requested globally.

Our consulting services are based on the internationally relevant guidelines; NERC CIP, NIST Cyber Security Framework, and BDEW white paper. We provide holistic advice on your business processes and system architecture, guiding you from strategy to implementation.

For example:

- Transparency on IT security status of the grid infrastructure
- Network structure analysis & risk analysis
- Consultancy for secure operation of SCADA

We are at your disposal, if your company faces immediate regulatory pressures and also if you proactively want to embrace the challenges, as it is in your company core interest to be prepared. We are your partner to get your organization up to speed when it comes to mastering the business threats arising from cyber attacks.

Please get in touch with us if you are interested to learn more!

Context and motivation:
Due to higher security requirements from frequently recurring and advanced IT attacks on power grid operations, critical infrastructure operators have to prove Information Security Management System (ISMS) implementation according to ISO 27001 / IT-Security Catalogue (BNA – German Regulator).

Siemens cyber security solution
More and more Siemens divisions are having their IT security management certified to ISO 27001. With this measure they are not only protecting their own IT but also their customers’ systems. To get prepared for certification, they can rely on extensive support from within the company. It ranges from sub-certificates, templates and advisory services to on-site implementation support.

“This certificate attests to you having a functioning IT security management system that knows the risks of the organization and derives rules from them, which it then clearly and correctly documents and quantifiably adheres to,” emphasizes Eric Scheer, expert for IT security management systems in Siemens Information Security & Product & Solution Security Governance.
Siemens ISMS implementation to protect grid infrastructure includes:

- Status quo assessment of IT security compliance
- Implementation based on best-practice framework
- Guidance during certification process and long-term support to ensure highest and up-to-date security in the long-run.

Early bird certificate

ISO 27001 certification became mandatory for energy suppliers in Germany at the end of January 2018. This almost inevitably means that business partners are also certified to this standard. Siemens has been exemplary in taking the initiative right from the very beginning. From June 2019, the operators of other critical infrastructures, such as transport companies, also need to be certified to ISO 27001. They, too, can rely on their business partners at Siemens to obtain the certification in good time.

Benefits to Siemens customers include:

- Transparency on IT-security status of the grid infrastructure
- Efficient implementation of ISMS true-to-life, i.e. with actual business relation
- Practical improvement suggestions and effective increase of security level
- Long-term partnership and collaboration with certifying entity.

Expert support for stress-free certification

It is essential to start the certification process as early as possible. “It takes at least six months before you can hold the certificate in your hands,” confirms Thomas Gereke, who advises internal and external clients on the subject of ISO 27001 together with his team at Siemens Energy Management. Furthermore, he can incorporate his experience gained from numerous consultation projects. To ensure that certification does not cost the Siemens divisions more effort than justified by the individual boundary conditions of business operations, Eric Scheer and his colleague Pia Utz have put together a starter package that reduces the workload significantly. They have in particular ensured that Siemens’ IT Security Governance itself is certified. “As a result, the divisions no longer need to check how Siemens defines its IT security rules and keeps them up to date,” explains Utz. “They only have to concentrate on the specifics of their own division.”

Partner support for audit preparations

The preparations for the process still represent quite a cumbersome workload. Scheer and his colleagues therefore offer support for this leg of the journey as well. “We edited all the documents that we used for our own certification so that they now only contain the Siemens-relevant parts,” explains Scheer. “The outcome was templates with explanatory texts. In addition, we have also created presentations that help prepare for the auditor’s questions. And we arrange contacts with consultants as well. These can be internal consultants like Mr. Gereke, or external consultants who are familiar with the specific Siemens’ characteristics. Of course we also support the audit in very practical terms by participating in person and explaining the overarching aspects.”

---

1 Successful Introduction of Information Security Management System (ISMS) Projects as per ISO/IEC 27001/2/19 and the German IT Security Act, Siemens PTI eNewsletter Issue 227, March 2018
Cyber security consulting
Siemens Energy Business Advisory (EBA) supports you in accomplishing the legal requirements of implementation of ISMS and certification (ISO 27001) including the specific measures for infrastructure protection:

- Infrastructure analysis (IT und OT view), documentation of network structure
- IT security concepts, incl. security assessment and risk classification
- Security concepts for action according to the current “state-of-the-art”
- Recommendation and implementation of process changes
- Transition into infrastructure conformable to law, preparation of certification.

Security remains ongoing task
Both Gottfried Putz, who coordinates Strategy and Business Development for the Digital Grid Division of the Regional Company Germany, and Christoph Roth, who develops IT security management systems at Siemens Mobility, availed the support offered by Scheer and Gereke at a time when the IT Security Governance certificate and the templates were still in the development stage. “We have already saved a lot of time with the intermediate results” confirms Putz, who completed the entire certification process on behalf of the Digital Grid Division of the Regional Company Germany in February. “With the help of what has been developed since then, along with the certificate, we will be sure to manage everything with even less work than before,” adds Roth. “ISO-27001 certification is not a one-off project. There are regular follow-up audits, for which we can benefit from the new, extended support.”

Figure 1 – Stadtwerke Ilmenau Municipal Utility Services ISO 27001 Certificate

Uwe Helfer and Christian Diez from the Stadtwerke Ilmenau municipal utility services proudly present their ISO 27001 certificate, which they received with the support of Thomas Gereke (left) and his team from Siemens Energy Management.