Cybersecurity for Automated and Computerized Systems

Exyte – your plant design and construction partner

Exyte is a leading international engineering company specializing in the design and construction of plants and systems for the life sciences sector. Our experienced specialists develop state-of-the-art solutions spanning the entire GMP value chain for you – offering the full scope of services from consultation, concept development and design, to the delivery of qualified and validated turnkey plants and systems.

New threats – are your plants still safe?

More and more production plants and laboratory systems are being networked and connected to complex IT systems and the Internet. The growing digitalization of business processes is presenting new security challenges for machines and entire facilities. In GxP environments, data protection and data integrity have become a must – not only to safeguard operations and business continuity, but also to comply with regulatory requirements. In addition, new national and international legislation requires operators to secure their IT infrastructures. And to do this, they have to be able to trust the products they deploy to provide the requisite level of IT security.

Our services

With Exyte cybersecurity consulting services, you can be sure that you have the right levels of protection in all areas of your organization. Exyte helps you identify and implement effective security measures and processes. We also work with you to create a sustainable security governance framework.

Our solutions

- Integrated process model for cybersecurity and the introduction of information security management systems
- Planning, concept development and implementation of IT security management systems (ISO 27001, baseline protection approach developed by Germany's Federal Office for Information Security or BSI) with particular focus on pharmaceutical guidelines and measures
- IT security and vulnerability analyses of industrial control systems and interfaces at field, control, MES and ERP levels
- Definition of company-specific security objectives and risk maps, selection of relevant control standards

Consulting

- Analysis of the protection requirements of your systems
- System inventories
- Documentation of your current security status
- Industrial security strategies and concepts
- Risk analyses / risk mitigation action plans
- Development of security guidelines / SOPs / procedures
- Support in the drafting of tenders and evaluation of bids
- Managed security services
- Operation and monitoring of your industrial security environment, technical support
- Preparation for ISO 27001 and/or BSI baseline audits

Our Cybersecurity Strategy

Security Standards, Methods and GMP

Information security management systems

Information security management systems (ISMS) are at the heart of all cybersecurity processes and workflows. Spanning guidelines, procedures, instructions, resources and people, these systems need to be continually monitored, maintained, improved and evolved. Implementing an ISMS is a fundamental step in ensuring that systems and data are securely protected.

ISO 27001

The ISO/IEC 27001 standard describes an ISMS and defines the theoretical framework for its processes. As defined by ISO 27001, information security refers to the measures put in place to guarantee and maintain the confidentiality, integrity and availability of information.

IEC 62443

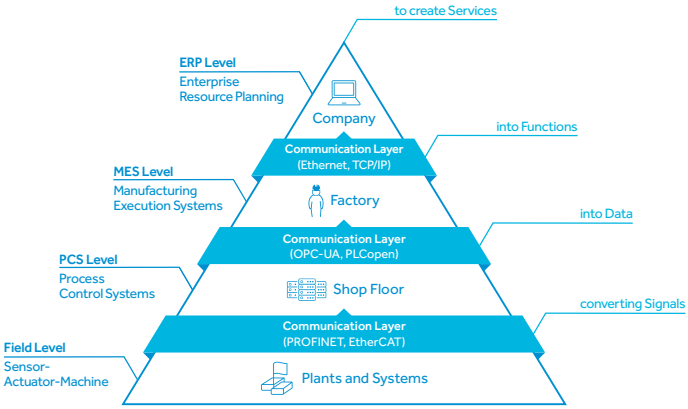
IEC 62443 is a series of international standards governing "industrial communication networks – network and system security". The new IEC 62443 standards enable companies to check for potential vulnerabilities in their control technology and develop effective preventative measures. These requirements must also be factored into ISMS implementation if a significant part of the respective company's value chain is dependent on industrial communication.

CSV & GAMP 5

The ISPE GAMP 5 Guide also provides practical, risk-based security approaches, concepts and measures for a wide range of computerized systems (IT-enabled production plants, laboratory equipment, software/hardware systems).

Our cybersecurity strategy – Integrating security standards, methods and GMP

We believe that the content and scope of IT security standards, methodologies and guidelines overlap to a large degree. So we take a 360° perspective, leveraging the resulting cost and optimization synergies to the benefit of our customers operating in regulated GxP environments.



From GAP analysis to IT compliance

We see IT and cybersecurity as a continuous process designed to protect industrial systems and infrastructures against current and future cyber threats in the life sciences sector. We support this process with a holistic service offering that builds on the broad skill set and experience base that we have established and systematically expanded over the years. We help you identify and eliminate existing vulnerabilities, analyzing your systems to eradicate external and internal system manipulations as well as finding and closing gaps in your information security management system. We define cybersecurity policies tailored to your needs and develop measures to ensure compliance.

We develop a framework capable of protecting your Industrial Control Systems (ICS) and your office and lab IT infrastructure by combining international and national guidelines such as ISO 27001 and the BSI baseline approach, incorporating industry-specific standards such as IEC 62443, complying with GMP requirements (ISPE GAMP 5, 21 CFR 11 and Annex 11) and factoring in your industry-specific needs and risk profile.

Learn more about Biopharma & Life Sciences
Contact us at **info.bls@exyte.net**
or visit **exyte.net/biopharmalifesciences**