Oerlikon Cybersecurity Requirements for Suppliers

Oerlikon Cybersecurity Requirements for Suppliers

In adherence to our commitment to safeguarding our digital supply chain against cyber threats, we have established cybersecurity requirements that our suppliers must meet. These requirements are particularly applicable to Operational Technology (OT) components, encompassing software, services, embedded computing technologies and extend to encompass IT as well.

Our suppliers are integral to the success of our cybersecurity program, playing a vital role in fortifying the resilience of our systems. We anticipate active collaboration and support from our suppliers to enhance the overall security posture of our organization.

Supplier Adherence to Cybersecurity Performance Goals (CPGs)

In accordance with our strong commitment to cybersecurity best practices, we expressly emphasize the importance of our suppliers aligning with the Cybersecurity Performance Goals (CPGs) outlined by the Cybersecurity and Infrastructure Security Agency (CISA). These CPGs, meticulously crafted through comprehensive consultations with industry experts and government stakeholders, represent a distilled set of best practices for enhancing security in both Information Technology (IT) and Operational Technology (OT) domains.

Supplier Commitment

As a key partner in our digital supply chain, we expect our suppliers to actively embrace and implement the CISA's CPGs as part of their cybersecurity practices. By adhering to these goals, suppliers play a pivotal role in fortifying the overall security posture of our organization. This commitment is not just a regulatory requirement but a shared responsibility in ensuring the integrity and resilience of our digital ecosystem.

Integration of CPGs into Supplier Practices

We encourage our suppliers to seamlessly integrate the CPGs into their cybersecurity protocols. This integration is not only a means of compliance but a proactive measure to enhance the effectiveness of cybersecurity measures. By aligning with the CPGs, suppliers contribute to a standardized, industry-recognized framework that significantly reduces the risk of cyber threats in both IT and OT components.

Oerlikon Cybersecurity Requirements for Suppliers

Collaborative Security Efforts

Our collaborative approach extends beyond mere compliance; it embodies a collective effort to fortify the entire supply chain against potential cyber threats. We value the partnership of our suppliers in championing the cause of cybersecurity, and we are confident that, together, we can create a secure digital environment that safeguards the interests of all stakeholders.

In conclusion, we urge our suppliers to actively incorporate the CISA's CPGs into their operational practices. This shared responsibility ensures that our combined efforts result in a resilient and secure digital infrastructure.

FAQ

What are the Cybersecurity Performance Goals?

CISA's (Cybersecurity &Infrastructure Security Agency, USA) Cybersecurity Performance Goals (CPGs) represent a subset of highly impactful best practices aimed at reducing cybersecurity risks in both Information Technology (IT) and Operational Technology (OT). Developed through industry collaboration, these practices provide a focused and standardized framework to significantly enhance security posture and resilience against cyber threats.

Cross-Sector Cybersecurity Performance Goals | CISA
CISA_CPG_REPORT_v1.0.1

What is the intention of the CPG's?

The intention of the CPGs (Cybersecurity Performance Goals) is to provide a curated set of best practices for cybersecurity, encompassing both Information Technology (IT) and Operational Technology (OT). Developed through industry, government, and expert consultations, the CPGs aim to significantly reduce cybersecurity risks by offering a standardized framework for organizations to enhance their security posture, align with industry standards, and foster resilience in the face of cyber threats.

Why should suppliers adhere to CPG?

Adhering to Cybersecurity Performance Goals (CPGs) is vital for companies, ensuring risk mitigation, regulatory compliance, and industry best practices. This commitment safeguards data, builds customer trust, enhances operational

resilience, and provides a competitive edge. CPG adherence is a strategic imperative for establishing a robust cybersecurity posture in the digital landscape.

Why does Oerlikon mandate CPG adherence for suppliers when it is typically deemed mandatory only for critical infrastructure?

Oerlikon mandates suppliers to adhere to a subset of highly impactful cybersecurity practices within the well-structured CPG. This comprehensive approach ensures a uniform and elevated standard of cybersecurity across the supply chain, effectively mitigating risks, aligning with industry best practices, and strengthening the overall security posture beyond the scope of critical infrastructure requirements.

Can a supplier address all CPG practices, or are some practices specifically applicable only to Oerlikon?

The applicability of Cybersecurity Performance Goals (CPG) practices varies, and not all practices may be pertinent to every supplier. The relevance of specific practices depends on factors such as the supplier's services, technology type, and customer requirements. Alignment with and implementation of CPG practices are determined collaboratively between the customer and the supplier to enhance cybersecurity measures effectively and appropriately.

How does a provider need to fill in the answers in the CPG spread sheet?

Review CPG Documentation:

Familiarize yourself with the CPG documentation provided. Understand the context, goals, and specific practices outlined.

Assessment of Practices:

Evaluate each cybersecurity practice listed in the spreadsheet in relation to your organization's systems, processes, and technology. Determine the extent to which each practice is already implemented or needs attention.

Download the list here: Complete CPGs Matrix/Spreadsheet

Responses:

Provide detailed responses for each practice, explaining how your organization meets the requirements or any plans for implementation, by adding a new column to the spreadsheet. This may involve describing existing security measures,

policies, or plans for improvement. Additionally, clarify practices of shared responsibilities between Oerlikon and the supplier, as well as areas where Oerlikon bears sole responsibility.

Collaborate with Relevant Oerlikon Teams:

Work closely with relevant Oerlikon teams, to gather accurate and comprehensive information for each practice. Collaboration ensures a holistic and accurate representation of your organization's cybersecurity practices.

Documentation and Evidence:

Ensure that supporting documentation or evidence is attached or referenced where required. This could include policy documents, security protocols, risk assessments, or any other relevant materials.

Timely Submission:

Adhere to any deadlines for the submission of the completed CPG spreadsheet. Timely submission is crucial for compliance and effective cybersecurity management.

Continuous Improvement:

Use the CPG assessment as an opportunity for continuous improvement. Identify areas for enhancement and establish plans to address any gaps in cybersecurity practices.

By following these steps, a provider can accurately and comprehensively fill in the answers in the CPG spreadsheet, demonstrating a commitment to cybersecurity and compliance with industry best practices.