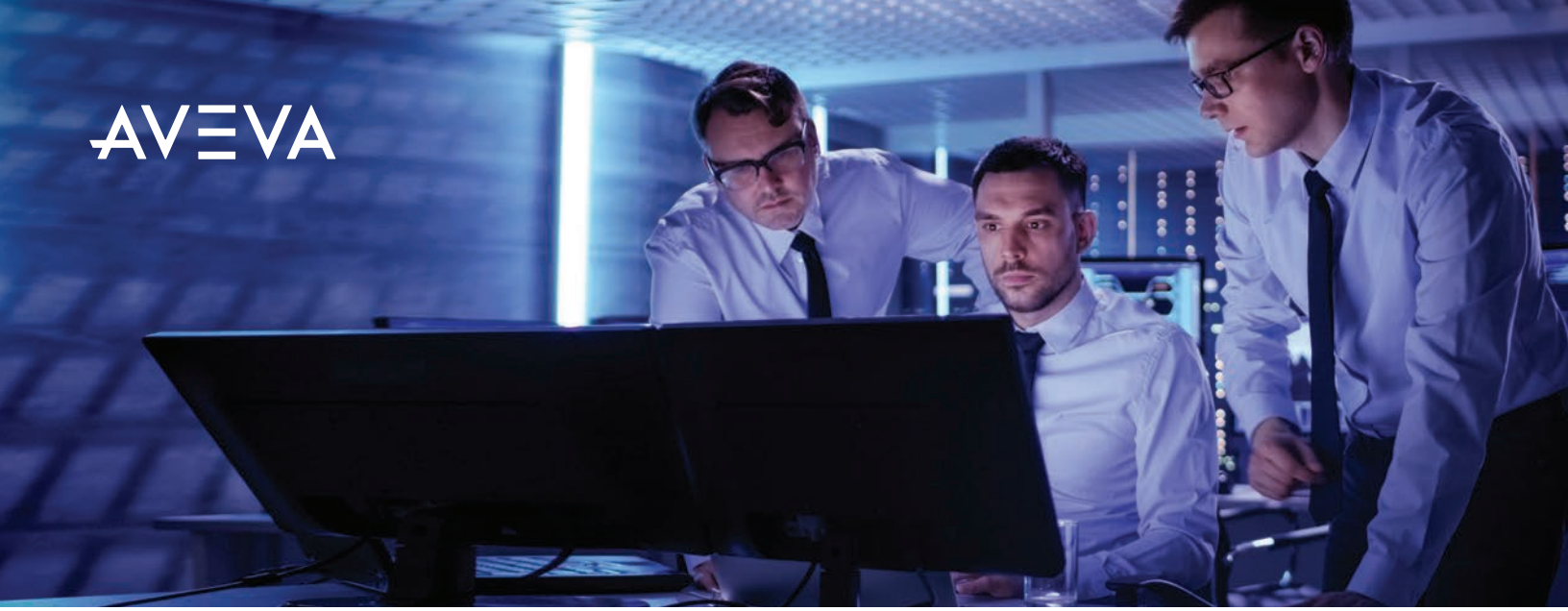


SERVICES PROFILE

Industrial Control System (ICS) Security and Risk Assessments

As industrial operations become more digital, the need to provide safeguards against cyber security threats becomes increasingly critical. A comprehensive security strategy requires a thorough assessment of the current state of your ICS environment, including policies, procedures, technologies, and practices. Our ICS cyber security offering includes both a Security Assessment and a Risk Assessment to help you effectively identify the highest priority security concerns and recommendations for your control system environment.

Industrial Control Systems are Vital

Virtually all industries today – power, water & wastewater, oil & gas, chemicals, manufacturing, food & beverage, and others – rely on industrial control systems to perform critical operations. As industrial operations become more digital, the need to provide safeguards against cyber security threats becomes increasingly critical. While they were once stand-alone systems, they are now commonly connected to an organization's IT infrastructure and face the same cyber security threats as corporate networks.

It is extremely important to protect these systems from a dynamic threat environment that could cause, to varying degrees, loss of proprietary data, IT assets, and trade secrets, and system downtime that could lead to major risks such as bodily injury, loss of life, production interruption, equipment damage, unnecessary costs or loss of revenue. A comprehensive security strategy requires a thorough assessment of the current state of your ICS environment, including policies, procedures, technologies, and practices. Our ICS cyber security offering includes both a Security Assessment and a Risk Assessment to help you effectively identify the highest priority security concerns and provide recommendations for your control system environment.

As a global leader in engineering and industrial software, AVEVA is pleased to provide cyber security success accelerator options as part its AVEVA Customer FIRST Program. These include Security and Risk Assessments, both performed in partnership with BlackBerry Cylance, recognized experts in ICS security.

ICS Security Assessment

While many considerations must be taken when addressing the nature of ICS environments, an ICS Security Assessment involves a range of activities focused on analyzing the effectiveness of the organisation's security programs. It looks into vulnerabilities and solutions to mitigate their critical risks/impacts by collecting information about the organisation's security practices, policies, and procedures through survey responses, staff interviews, tools, company documentation, and site walk downs.

Based on the results, the assessment can help guide decisions on corporate best practices to enhance the organization's overall cyber security posture. An associated strategic security roadmap helps you build and prioritize the governance and remediation of critical vulnerabilities surrounding people, processes, and technologies.

Value

- Enhance your cyber security understanding, including best practices for securing ICS with integrated IT/OT (information and operational technology) systems. The awareness helps improve your planning and preparations for a better overall company strategy and reduce risk.
- Develop a systematic and repeatable approach to assessing and maintaining your ICS security posture – including legacy architectures, systems and devices – without replacement. Our expert consultation provides a blueprint for assessing your systems in a cost-effective, repeatable way.
- Support business objectives while maintaining safe and uninterrupted operations. The assessment is non-invasive and does not require system downtime to conduct.
- By implementing a prevention-first methodology that removes the noise in environments and allows IT security professionals to focus on the activities that can be truly harmful, you can focus on what's most meaningful and avoid areas of limited impact.
- Create remediation strategies while balancing risk and benefit to get the best available return on your investment.

Deliverables

The Security Assessment helps you identify weaknesses and develop actionable recommendations to mitigate the risks in your ICS environment. The information obtained from the assessment is used to provide the organization with:

- A risk profile that addresses impact, threat, vulnerability, probability, and countermeasures
- A prioritized road map for remediating security concerns

ICS Risk Assessment

The ICS Risk Assessment provides a high-level evaluation of the security practices of your system environments to determine the risk profile of these systems. It gives you a better understanding of how these security practices are implemented across various business units and how these practices can impact their overall susceptibility to a cyber attack. The assessment's goal is to determine a high-level benchmark of an organization's security posture to help with an efficient risk-reduction program covering both IT and OT. Our ICS experts will recommend where you can get the most risk reduction with the money and time that they have.

The engagement's methodical analysis process involves a detailed questionnaire, interviews with key management and leadership, and calculated performance measurement across 15 assessment categories. The results are then compiled and analyzed to generate a risk profile score for each category:

- Network Architecture
- Defensive Technology
- Mobile Devices
- Removable Media
- Risk Assessment
- Patch Management
- Personnel
- Account Management
- Physical Security
- Configuration Management
- Business Continuity
- Network Security Policy
- Security Standard
- Asset Management
- Incident Response Readiness

Value

- Get a broad understanding of your organization's security posture to help accelerate your cyber security solution/program development.
- Avoid potential business interruptions or theft of data by proactively identifying and addressing potential areas of risk and opportunities to improve.
- Establish a baseline that can be used to track risk reduction and progress among multiple facilities through the use of a measured approach via peer comparison analysis, then maximize your resources to efficiently and objectively address high-priority areas of concern.

Deliverables

With the ICS Risk Assessment, you get a comprehensive report that includes:

- The top three areas of improvement sorted by order of impact
- Strategic recommendations on how to mitigate vulnerabilities
- A summary of notable security strengths that surpass the industry norm and best practices
- Overall individual risk score
- A gap score by category

Where applicable, we can also conduct a peer comparison analysis to understand the security posture of each individual facility in your organization. A peer report on all business units or environments includes, but is not limited to:

- An overall risk score ranked against organizational risk imposed by each business unit or environment
- A compiled list of individual risk scores from each business unit or environment
- An overall summary of notable and common security strengths across the organization
- A list of top areas of improvement across the organization

Partners – AVEVA and BlackBerry Cylance

AVEVA creates industrial software that inspires people to shape the future. Our comprehensive software portfolio makes manufacturing more productive, and assets and operations safer and more effective and sustainable. From water and energy to food and infrastructure, our solutions drive meaningful results and turn opportunities into business value.

For our ICS cyber security projects, we work in partnership with BlackBerry Cylance to enable heightened levels of security for customers leveraging our software across their industrial and infrastructure operations. This partnership means that for each project, you get the knowledge and experience of AVEVA pertaining to your AVEVA software and unique operations, as well as the ICS cyber security expertise of BlackBerry Cylance. This collaborative approach is an important differentiator and ensures you get highly relevant and targeted information about your ICS environment and how to efficiently and effectively secure it.

POWERED BY BlackBerry | CYLANCE

About BlackBerry Cylance

- Global experts work synergistically across practice areas to deliver consistent, fast, and effective services.
- ICS experts that have a wide range of expertise covering both IT and OT capabilities, allowing them to balance the concerns of both sides and ensure that they are aligned, integrated, and consistent.
- Incorporates artificial intelligence into tools and processes to more efficiently and effectively secure the environment to prevent attacks from happening.
- Utilizes multiple techniques to collect information, assess data, provide a risk profile, recommend actions, and highlight notable strengths for an organisation.
- Techniques are designed to not impact operations in any way.

The AVEVA Customer FIRST Program – Accelerating Your Success!

Customer FIRST is AVEVA's comprehensive, fee-based software maintenance and technical support program that helps you achieve maximum benefit from your investment in AVEVA software. It includes access to our award-winning technical support and services team to quickly resolve issues, software version upgrades and updates, and valuable services and software utilities.

In addition to the base program, we also offer a range of optional success accelerators designed to help you throughout the lifecycle stages of your application.

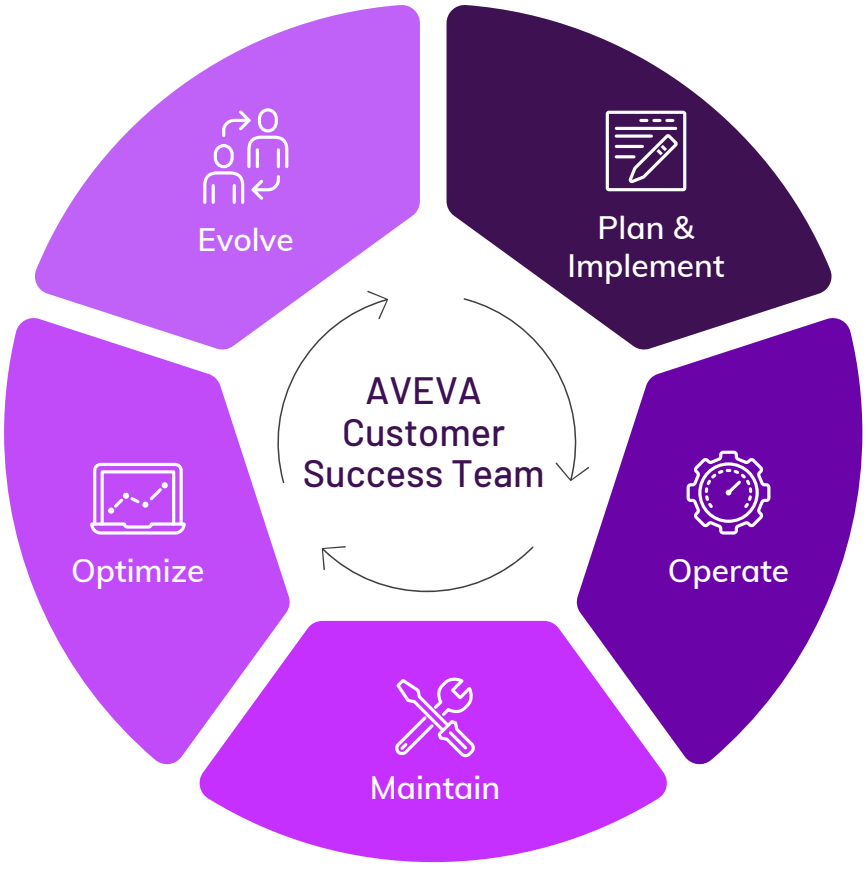
Plan & Implement –Engineer best practices and application architecture and improve time to value

Operate – Effectively run your software with expert training and drive increased engagement and adoption

Maintain – Efficiently maintain your software, including updates, patches, and license management

Optimize – Improve software performance and reliability and drive changes to address new market requirements

Evolve – Drive innovation through the deployment of major version upgrades, adopt new technology, and future-proof your application



To learn more, please contact your AVEVA representative or visit us online. sw.aveva.com