IACS High-Level Risk Assessment for Cloud Products and Services

The introduction of a cloud service into an industrial / automation control environment requires a Cyber Security Management System (CSMS)[i] to manage risk by creating policies and procedures, assignment of organization responsibilities, planning and implementation of awareness training, and selection of countermeasures to be implemented by the owner / operator. The CSMS initial high-level risk assessment requires gathering information about the cloud service, some of which must be provided by the product / service provider. This information will allow the owner / operator to confirm the Capability Security Level (SL-C) components that are implemented and maintained by the product / service provider. This information will initiate the CSMS process and provide the starting point for a detailed risk assessment using the Cloud Security Maturity Model[ii].

Initial High-Level Risk Assessment

Information gathering is a team effort between the owner / operator and product / service provider. Here is a breakdown of responsibilities for providing information during the initial high-level risk assessment. Overall, the owner / operator is responsible for ensuring all the information collected is complete. The owner / operator's project owner should review the data and ask clarifying questions until each section is completed.

Project Overview – Owner / Operator
Cloud Service Description – Product / Service Provider
Product / Service Foundational Requirements – Product / Service Provider
Zone and Conduit Characteristics – Owner / Operator

Project Overview

Description of the project and cloud components	
Project Executive Sponsor	
Dates of implementation phases (initiation, phases, production)	
IACS Integration Service Provider Lead	
IACS Maintenance Service Provider Lead	
IACS Cloud Lead (Owner / Operator)	
IT Cloud Lead (Owner / Operator)	
IT Security Cloud Lead (Owner / Operator)	
Description of the project and cloud components	

IACS High-Level Risk Assessment for Cloud Products and Services

Cloud Service Description

Which cloud service provider?	AWS Azure Google Digital Ocean Other:
Type of cloud model	Private Public Hybrid Community
Type of cloud service	Platform-as-a-Service (PaaS) Infrastructure-as-a-Service (IaaS) Software-as-a-Service (SaaS) Other:
Cloud Region(s)	
Which contain services are used?	Docker Kubernetes Virtual Machines Other None
Basic description of countermeasures to protect communications and access from the cloud to the control environment provided as a part of the implementation of the product / service?	
Capability Security Level (SL-C) with description	
State of product / service compliance and certifications (i.e., ISASecure and/or SOC2 certification)	

Product / Service Foundational Requirements

Describe the product / solution's capabilities for Identity and Access Control (IAC)	
Describe the product / solution's capabilities for Use Control (UC)	
Describe the product / solution's capabilities for Data Integrity (DI)	
Describe the product / solution's capabilities for Data Confidentiality (DC)	
Describe the product / solution's capabilities for Restricting Data Flow (RDF)	
Describe the product / solution's capabilities for Timely Response to Events (TRE)	
Describe the product / solution's capabilities for Resource Availability (RA)	

Zone and Conduit Characteristics

Name / Unique Identifier	
Accountable Organization / Business Unit	
Definition of logical boundary	
Definition of physical boundary	
Safety designation	
Connected zones and conduits	
Targeted Security Level (SL-T)	
Applicable security requirements	
Applicable security policies	
Assumptions and external dependencies	
List of logical access points	

List of physical access points	
List of data flows	
List of assets	

[i] ANSI/ISA–62443-2-1 Annex A (informative): https://www.isa.org/products/isa-62443-2-1-2009-security-for-industrial-automat
[ii] Cloud Security Maturity Model (CSMM) Diagnostic: https://www.iansresearch.com/resources/cloud-security-maturity-model