Official statement of certification for Fox-IT

This document certifies that the Security Operations Center (SOC) of **Fox-IT**, located in Delft, The Netherlands, has successfully passed the *SOC-CMM* certification audit at the risk-driven level. The audit was conducted by **LRQA** in May 2024.

Certification
An organisation that has passed the *SOC-CMM* certification audit has a verified and mature implementation and operation of the *SOC-CMM*, and their SOC services are delivered in a standardized and mature fashion. Note that this does not guarantee that **Fox-IT** SOC customers cannot be hacked or that the **Fox-IT** SOC will detect any and all breaches in SOC customers.

Risk-driven certification
A certification at the risk-driven level means that the **Fox-IT** SOC has implemented and operationalised all elements in the *SOC-CMM* that allow for SOC service delivery in a way that ties into customer risk and is informed by risks and threats gathered in a threat intelligence capability.

Statement of applicability
Fox-IT has passed the certification audit at the risk-driven level. This is the highest level of *the SOC-CMM* audit framework (see annex A), that also includes all control objectives at the lower certification levels. **Fox-IT** has included all elements into the certification audit scope. Annex B contains a full overview of all SOC elements that were subjected to auditing.

Validity and audit cycle
The *SOC-CMM* certification is valid for a period of 3 years. SOC-CMM certification has an annual cycle, in which **LRQA** and the **Fox-IT** SOC discuss the progress of the minor findings and any changes and improvements made to the SOC to ensure continued adherence to the evolving SOC-CMM standard.

Issuing date: 14.06.2024
Valid until: 14.06.2027

On behalf of SOC-CMM,

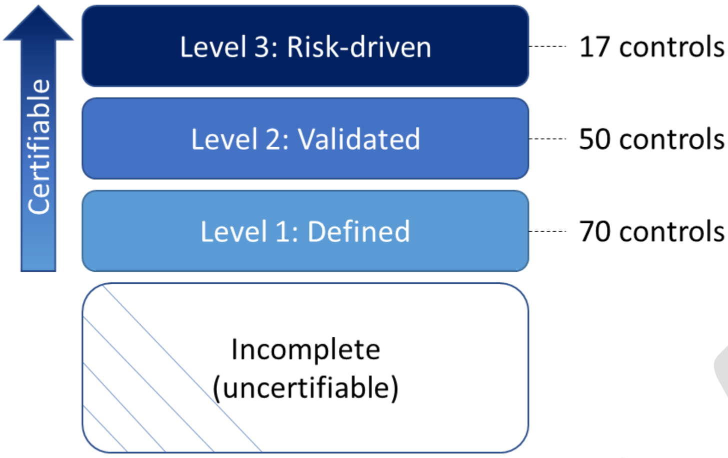
Rob van Os
CEO and founder

SOC CMM
CERTIFIED
RISK DRIVEN

CERTIFICATION ID
2OI2-OFKL-EI0S-98ES

Annex A: SOC-CMM audit framework

The audit framework is designed to evaluate SOCs at one of three certifiable levels:



The certification levels are stacked. This means that in order to achieve a higher certification level, all controls at the lower level must also be satisfied. The SOC-CMM certification control framework has a total of 136 controls, distributed as outlined in the figure.

Annex B: Statement of applicability

The following elements of the SOC-CMM were audited and verified for implementation and operating effectiveness.

SOC-CMM domain	SOC-CMM element in scope
Business	Business drivers
	Customers
	Charter
	Governance
	Privacy & policy
People	Employees
	Roles & hierarchy
	People management
	Knowledge management
	Training & certification
Process	SOC management
	Operations & Facilities
	Reporting
	Use case management
	Detection engineering
Technology	Security monitoring tooling
Services	Security monitoring
	Security incident management
	Threat intelligence
	Threat hunting