Certificate of approval

This is to certify that the Security Operations Center (SOC) of

DTX B.V.

Wezelkoog 11, 1822 BL, Alkmaar, The Netherlands

Has been assessed and found to meet the requirements of

SOC-CMM®:RISK-DRIVEN

This certificate is valid for the following scope (statement of applicability)
Full scope of SOC operations

Issuing date: **25 August 2026**
Valid until: **25 August 2029**

Recertification audit before 25 July 2029
This certificate is property of SOC-CMM foundation and remains valid
subject to satisfactory mandatory annual surveillance audits

Authorised by

Rob van Os
Director, SOC-CMM® foundation

CERTIFICATION ID
MAI3-QGWT-3J5O-6JP8

SOC-CMM® Foundation
Vijfhuizenbaan 8
5133NH, Riel,
The Netherlands
certification@soc-cmm.com
https://certification.soc-cmm.com/
company number: 94151911

Official statement of certification for DTX B.V.

This document certifies that the Security Operations Center (SOC) of **DTX B.V.**, located in **Alkmaar**, **The Netherlands**, has successfully passed the *SOC-CMM®* certification audit at the risk-driven level. The audit was conducted on-site by **LRQA** in **August 2026**.

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 **DTX B.V.** SOC customers cannot be hacked or that the **DTX B.V.** SOC will detect any and all breaches in SOC customers.

Certification process
The certification audit was conducted by **LRQA**, an official *SOC-CMM®* certification partner, meeting the highest standards in certification. The results from the audit were subjected to independent review and verified by the *SOC-CMM® foundation*, providing further assurance on the correctness of the results.

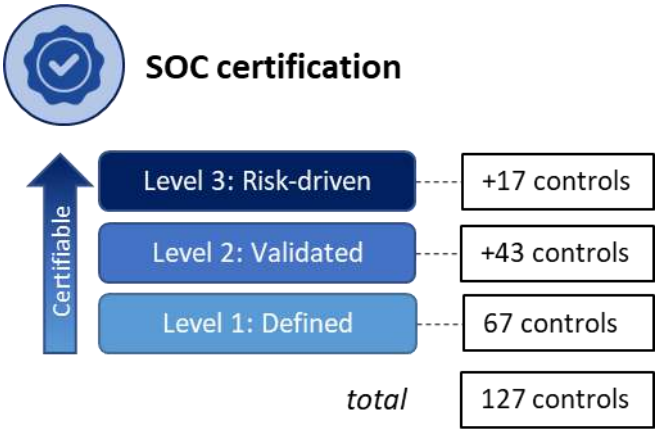
Risk-driven certification
A certification at the risk-driven level means that the **DTX B.V.** SOC has implemented and operationalised all elements in the *SOC-CMM®* that allow for SOC service delivery in a way that ties into customer risk and is informed by risks and threats gathered in a mature threat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

Statement of applicability
DTX B.V. 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 defined and validated certification levels. **DTX B.V.** 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 the period of 3 years. *SOC-CMM®* certification has an annual cycle, in which the auditor and the **DTX B.V.** 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.

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 127 controls, distributed as outlined in the figure.

Annex B: SOC-CMM elements audited

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

SOC-CMM domain	SOC-CMM element in scope	SOC-CMM element out of 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 hunting	
	Threat intelligence	