
**Kmetijski stroji, traktorji in stroji za zemeljska dela - Kibernetska varnost izdelkov
(ISO/DIS 24882:2025)**

Agricultural machinery, tractors, and earth-moving machinery - Product cybersecurity
(ISO/DIS 24882:2025)

Landwirtschaftliche Maschinen, Traktoren und Erdbewegungsmaschinen -
Cybersicherheit von Produkten (ISO/DIS 24882:2025)

Matériels agricoles, tracteurs et engins de terrassement - Cybersécurité des produits
(ISO/DIS 24882:2025)

Ta slovenski standard je istoveten z: prEN ISO 24882

oSIST prEN ISO 24882:2026

<https://standards.sist.si/catalog/standards/sist/3d7f09b4-4606-4b83-a91d-768ac60746dd/oSIST-prEN-ISO-24882-2026>

ICS:

53.100	Stroji za zemeljska dela	Earth-moving machinery
65.060.01	Kmetijski stroji in oprema na splošno	Agricultural machines and equipment in general

oSIST prEN ISO 24882:2026

en,fr,de



DRAFT International Standard

ISO/DIS 24882

Agricultural machinery, tractors, and earth-moving machinery – Product cybersecurity

ICS: 53.100; 65.060.01

ISO/TC 23/SC 19

Secretariat: DIN

Voting begins on:
2025-12-09

Voting terminates on:
2026-03-03

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[oSIST prEN ISO 24882:2026](https://standards.iteh.ai/catalog/standards/sist/3d7fc9b4-4b0b-4b83-a91d-7b8acb0746dd/osist-pren-iso-24882-2026)

<https://standards.iteh.ai/catalog/standards/sist/3d7fc9b4-4b0b-4b83-a91d-7b8acb0746dd/osist-pren-iso-24882-2026>

Member bodies are requested to consult relevant national interests in ISO/TC 127/SC 3 before casting their ballot to the e-Balloting application.

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 24882:2025(en)

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

© ISO 2025

ISO/DIS 24882:2025(en)

iTeh Standards (<https://standards.iteh.ai>) Document Preview

[oSIST prEN ISO 24882:2026](https://standards.iteh.ai/catalog/standards/sist/3d7fc9b4-4b0b-4b83-a91d-7b8acb0746dd/osist-pren-iso-24882-2026)

<https://standards.iteh.ai/catalog/standards/sist/3d7fc9b4-4b0b-4b83-a91d-7b8acb0746dd/osist-pren-iso-24882-2026>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

ISO/DIS 24882:2025(en)

Contents

Page

Foreword	viii
Introduction	ix
1 Scope	1
2 Normative references	1
3 Terms and Definitions and Abbreviated Terms	1
3.1 Terms and Definitions	1
3.2 Abbreviated Terms	4
4 General considerations	4
5 Risk assessment for the system of interest	8
5.1 Risk assessment introduction	8
5.2 System of interest identification	9
5.2.1 General	9
5.2.2 Prerequisites	9
5.2.3 Requirements	9
5.2.4 Work products	10
5.3 Assets, damage scenario identification	10
5.3.1 General	10
5.3.2 Prerequisites	10
5.3.3 Requirements	10
5.3.4 Work products	11
5.4 Threat identification	11
5.4.1 General	11
5.4.2 Prerequisites	11
5.4.3 Requirements	11
5.4.4 Work products	12
5.5 Impact rating determination	12
5.5.1 General	12
5.5.2 Prerequisites	12
5.5.3 Requirements	12
5.5.4 Work products	13
5.6 Likelihood rating determination	13
5.6.1 General	13
5.6.2 Prerequisites	14
5.6.3 Requirements	14
5.6.4 Work products	17
5.7 Risk rating determination	17
5.7.1 General	17
5.7.2 Prerequisites	17
5.7.3 Requirements	17
5.7.4 Work products	17
5.8 Risk treatment decision	18
5.8.1 General	18
5.8.2 Prerequisites	18
5.8.3 Requirements	18
5.8.4 Work products	18
5.9 Cybersecurity requirements determination	18
5.9.1 General	18
5.9.2 Prerequisites	19
5.9.3 Requirements	19
5.9.4 Work products	19
6 Cybersecurity technical requirements for risk mitigation	19
6.1 Technical requirements introduction	19
6.2 Secure software - update	19

ISO/DIS 24882:2025(en)

6.2.1	Applicability	19
6.2.2	Requirement	19
6.2.3	Rationale	20
6.2.4	Guidance	20
6.2.5	Verification criteria	20
6.3	Secure software - update notification	20
6.3.1	Applicability	20
6.3.2	Requirement	21
6.3.3	Rationale	21
6.3.4	Guidance	21
6.3.5	Verification criteria	21
6.4	Secure software - integrity and authenticity check	21
6.4.1	Applicability	21
6.4.2	Requirement	21
6.4.3	Rationale	21
6.4.4	Guidance	21
6.4.5	Verification criteria	22
6.5	Hardening - secure configuration	22
6.5.1	Applicability	22
6.5.2	Requirement	22
6.5.3	Rationale	22
6.5.4	Guidance	22
6.5.5	Verification criteria	22
6.6	Hardening - production mode	22
6.6.1	Applicability	22
6.6.2	Requirement	23
6.6.3	Rationale	23
6.6.4	Guidance	23
6.6.5	Verification criteria	23
6.7	Secure logging and reporting - access control monitoring (authorized and unauthorized)	23
6.7.1	Applicability	23
6.7.2	Requirement	23
6.7.3	Rationale	23
6.7.4	Guidance	23
6.7.5	Verification criteria	24
6.8	Secure logging and reporting - anomaly detection	24
6.8.1	Applicability	24
6.8.2	Requirement	24
6.8.3	Rationale	24
6.8.4	Guidance	24
6.8.5	Verification criteria	24
6.9	Secure logging and reporting - detection of integrity violations	25
6.9.1	Applicability	25
6.9.2	Requirement	25
6.9.3	Rationale	25
6.9.4	Guidance	25
6.9.5	Verification criteria	25
6.10	Secure logging and reporting - secure logging mechanisms	25
6.10.1	Applicability	25
6.10.2	Requirement	25
6.10.3	Rationale	25
6.10.4	Guidance	25
6.10.5	Verification criteria	26
6.11	Secure logging and reporting - report logs & events	26
6.11.1	Applicability	26
6.11.2	Requirement	26
6.11.3	Rationale	26
6.11.4	Guidance	26
6.11.5	Verification criteria	26

ISO/DIS 24882:2025(en)

6.12	User access management - authentication authorization	26
6.12.1	Applicability	26
6.12.2	Requirement	27
6.12.3	Rationale	27
6.12.4	Guidance	27
6.12.5	Verification criteria	27
6.13	User access management - role-based access control (RBAC)	27
6.13.1	Applicability	27
6.13.2	Requirement	27
6.13.3	Rationale	27
6.13.4	Guidance	28
6.13.5	Verification criteria	28
6.14	Diagnostics access management - authentication authorization	28
6.14.1	Applicability	28
6.14.2	Requirement	28
6.14.3	Rationale	28
6.14.4	Guidance	28
6.14.5	Verification criteria	29
6.15	Diagnostics access management - role-based access control	29
6.15.1	Applicability	29
6.15.2	Requirement	29
6.15.3	Rationale	29
6.15.4	Guidance	29
6.15.5	Verification criteria	29
6.16	Data confidentiality - secure data at rest	30
6.16.1	Applicability	30
6.16.2	Requirement	30
6.16.3	Rationale	30
6.16.4	Guidance	30
6.16.5	Verification criteria	30
6.17	Data confidentiality - secure data in transit	30
6.17.1	Applicability	30
6.17.2	Requirement	30
6.17.3	Rationale	30
6.17.4	Guidance	31
6.17.5	Verification criteria	31
6.18	Data integrity - secure data at rest	31
6.18.1	Applicability	31
6.18.2	Requirement	31
6.18.3	Rationale	31
6.18.4	Guidance	31
6.18.5	Verification criteria	31
6.19	Data integrity - secure data in transit	32
6.19.1	Applicability	32
6.19.2	Requirement	32
6.19.3	Rationale	32
6.19.4	Guidance	32
6.19.5	Verification criteria	32
6.20	Data minimisation	32
6.20.1	Applicability	32
6.20.2	Requirement	32
6.20.3	Rationale	32
6.20.4	Guidance	33
6.20.5	Verification criteria	33
6.21	Cybersecurity resilience - availability	33
6.21.1	Applicability	33
6.21.2	Requirement	33
6.21.3	Rationale	33
6.21.4	Guidance	33