CSA/ANSI T200:22

National Standard of Canada
American National Standard

Evaluation of software development and cybersecurity programs

Legal Notice for Standards

Canadian Standards Association (operating as "CSA Group") develops standards through a consensus standards development process approved by the Standards Council of Canada. This process brings together volunteers representing varied viewpoints and interests to achieve consensus and develop a standard. Although CSA Group administers the process and establishes rules to promote fairness in achieving consensus, it does not independently test, evaluate, or verify the content of standards.

Disclaimer and exclusion of liability

This document is provided without any representations, warranties, or conditions of any kind, express or implied, including, without limitation, implied warranties or conditions concerning this document's fitness for a particular purpose or use, its merchantability, or its non-infringement of any third party's intellectual property rights. CSA Group does not warrant the accuracy, completeness, or currency of any of the information published in this document. CSA Group makes no representations or warranties regarding this document's compliance with any applicable statute, rule, or regulation.

IN NO EVENT SHALL CSA GROUP, ITS VOLUNTEERS, MEMBERS, SUBSIDIARIES, OR AFFILIATED COMPANIES, OR THEIR EMPLOYEES, DIRECTORS, OR OFFICERS, BE LIABLE FOR ANY DIRECT, INDIRECT, OR INCIDENTAL DAMAGES, INJURY, LOSS, COSTS, OR EXPENSES, HOWSOEVER CAUSED, INCLUDING BUT NOT LIMITED TO SPECIAL OR CONSEQUENTIAL DAMAGES, LOST REVENUE, BUSINESS INTERRUPTION, LOST OR DAMAGED DATA, OR ANY OTHER COMMERCIAL OR ECONOMIC LOSS, WHETHER BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR ANY OTHER THEORY OF LIABILITY, ARISING OUT OF OR RESULTING FROM ACCESS TO OR POSSESSION OR USE OF THIS DOCUMENT, EVEN IF CSA GROUP HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INJURY, LOSS, COSTS, OR EXPENSES.

In publishing and making this document available, CSA Group is not undertaking to render professional or other services for or on behalf of any person or entity or to perform any duty owed by any person or entity to another person or entity. The information in this document is directed to those who have the appropriate degree of experience to use and apply its contents, and CSA Group accepts no responsibility whatsoever arising in any way from any and all use of or reliance on the information contained in this document.

CSA Group is a private not-for-profit company that publishes voluntary standards and related documents. CSA Group has no power, nor does it undertake, to enforce compliance with the contents of the standards or other documents it publishes.

Intellectual property rights and ownership

As between CSA Group and the users of this document (whether it be in printed or electronic form), CSA Group is the owner, or the authorized licensee, of all works contained herein that are protected by copyright, all trade-marks (except as otherwise noted to the contrary), and all inventions and trade secrets that may be contained in this document, whether or not such inventions and trade secrets are protected by patents and applications for patents. Without limitation, the unauthorized use, modification, copying, or disclosure of this document may violate laws that protect CSA Group's and/or others' intellectual property and may give rise to a right in CSA Group and/or others to seek legal redress for such use, modification, copying, or disclosure. To the extent permitted by licence or by law, CSA Group reserves all intellectual property rights in this document.

Patent rights

Attention is drawn to the possibility that some of the elements of this standard may be the subject of patent rights. CSA Group shall not be held responsible for identifying any or all such patent rights. Users of this standard are expressly advised that determination of the validity of any such patent rights is entirely their own responsibility.

Authorized use of this document

This document is being provided by CSA Group for informational and non-commercial use only. The user of this document is authorized to do only the following:

If this document is in electronic form:

- load this document onto a computer for the sole purpose of reviewing it;
- search and browse this document; and
- print this document if it is in PDF format.

Limited copies of this document in printed or paper form may be distributed only to persons who are authorized by CSA Group to have such copies, and only if this Legal Notice appears on each such copy.

In addition, users may not and may not permit others to

- alter this document in any way or remove this Legal Notice from the attached standard;
- sell this document without authorization from CSA Group; or
- make an electronic copy of this document.

If you do not agree with any of the terms and conditions contained in this Legal Notice, you may not load or use this document or make any copies of the contents thereof, and if you do make such copies, you are required to destroy them immediately. Use of this document constitutes your acceptance of the terms and conditions of this Legal Notice.

Standards Update Service

CSA/ANSI T200:22
April 2022

Title: *Evaluation of software development and cybersecurity programs*

To register for e-mail notification about any updates to this publication
- go to **www.csagroup.org/store/**
- click on **Product Updates**

The **List ID** that you will need to register for updates to this publication is **24296.3**

If you require assistance, please e-mail **techsupport@csagroup.org** or call 416-747-2233.

Visit CSA Group's policy on privacy at **www.csagroup.org/legal** to find out how we protect your personal information.

Canadian Standards Association (operating as "CSA Group"), under whose auspices this National Standard has been produced, was chartered in 1919 and accredited by the Standards Council of Canada to the National Standards system in 1973. It is a not-for-profit, nonstatutory, voluntary membership association engaged in standards development and certification activities.

CSA Group standards reflect a national consensus of producers and users — including manufacturers, consumers, retailers, unions and professional organizations, and governmental agencies. The standards are used widely by industry and commerce and often adopted by municipal, provincial, and federal governments in their regulations, particularly in the fields of health, safety, building and construction, and the environment.

More than 10 000 members indicate their support for CSA Group's standards development by volunteering their time and skills to Committee work.

CSA Group offers certification and testing services in support of and as an extension to its standards development activities. To ensure the integrity of its certification process, CSA Group regularly and continually audits and inspects products that bear the CSA Group Mark.

In addition to its head office and laboratory complex in Toronto, CSA Group has regional branch offices in major centres across Canada and inspection and testing agencies in fourteen countries. Since 1919, CSA Group has developed the necessary expertise to meet its corporate mission: CSA Group is an independent service organization whose mission is to provide an open and effective forum for activities facilitating the exchange of goods and services through the use of standards, certification and related services to meet national and international needs.

For further information on CSA Group services, write to
CSA Group
178 Rexdale Boulevard
Toronto, Ontario, M9W 1R3
Canada

A National Standard of Canada is a standard developed by a Standards Council of Canada (SCC) accredited Standards Development Organization, in compliance with requirements and guidance set out by SCC. More information on National Standards of Canada can be found at www.scc.ca.

SCC is a Crown corporation within the portfolio of Innovation, Science and Economic Development (ISED) Canada. With the goal of enhancing Canada's economic competitiveness and social well-being, SCC leads and facilitates the development and use of national and international standards. SCC also coordinates Canadian participation in standards development, and identifies strategies to advance Canadian standardization efforts.

Accreditation services are provided by SCC to various customers, including product certifiers, testing laboratories, and standards development organizations. A list of SCC programs and accredited bodies is publicly available at www.scc.ca.

Standards Council of Canada
600-55 Metcalfe Street
Ottawa, Ontario, K1P 6L5
Canada

Cette Norme Nationale du Canada n'est disponible qu'en anglais.

Although the intended primary application of this Standard is stated in its Scope, it is important to note that it remains the responsibility of the users to judge its suitability for their particular purpose.

CSA Group

The Canadian Standards Association (operating as "CSA Group"), under whose auspices this National Standard has been produced, was chartered in 1919 and accredited by the Standards Council of Canada to the National Standards system in 1973. It is a not-for-profit, nonstatutory, voluntary membership association engaged in standards development and certification activities.

CSA Group standards reflect a national consensus of producers and users including manufacturers, consumers, retailers, unions and professional organizations, and governmental agencies. The standards are used widely by industry and commerce and often adopted by municipal, provincial, and federal governments in their regulations, particularly in the fields of health, safety, building and construction, and the environment.

More than 10 000 members indicate their support for CSA Group's standards development by volunteering their time and skills to Committee work.

CSA Group offers certification and testing services in support of and as an extension to its standards development activities. To ensure the integrity of its certification process, CSA Group regularly and continually audits and inspects products that bear the CSA Group Mark.

In addition to its head office and laboratory complex in Toronto, CSA Group has regional branch offices in major centres across Canada and inspection and testing agencies in fourteen countries. Since 1919, CSA Group has developed the necessary expertise to meet its corporate mission: CSA Group is an independent service organization whose mission is to provide an open and effective forum for activities facilitating the exchange of goods and services through the use of standards, certification and related services to meet national and international needs.

For further information on CSA Group services, write to
CSA Group
178 Rexdale Boulevard, Toronto, Ontario,
Canada M9W 1R3

American National Standards Institute

The American National Standards Institute (ANSI), Inc. is the nationally recognized coordinator of voluntary standards development in the United States through which voluntary organizations, representing virtually every technical discipline and every facet of trade and commerce, organized labor and consumer interests, establish and improve the some 10 000 national consensus standards currently approved as American National Standards.

ANSI provides that the interests of the public may have appropriate participation and representation in standardization activity, and cooperates with departments and agencies of U.S. Federal, state and local governments in achieving compatibility between government codes and standards and the voluntary standards of industry and commerce.

ANSI represents the interests of the United States in international nontreaty organizations such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The Institute maintains close ties with regional organizations such as the Pacific Area Standards Congress (PASC) and the Pan American Standards Commission (COPANT). As such, ANSI coordinates the activities involved in the U.S. participation in these groups.

ANSI approval of standards is intended to verify that the principles of openness and due process have been followed in the approval procedure and that a consensus of those directly and materially affected by the standards has been achieved. ANSI coordination is intended to assist the voluntary system to ensure that national standards needs are identified and met with a set of standards that are without conflict or unnecessary duplication in their requirements.

Responsibility of approving American standards rests with the
American National Standards Institute, Inc.
25 West 43rd Street, Fourth floor
New York, NY 10036

National Standard of Canada
American National Standard

CSA/ANSI T200:22

Evaluation of software development and cybersecurity programs

American National Standards Institute, Inc.

Approved on March 10, 2022 by ANSI
Published in April 2022 by CSA Group
A not-for-profit private sector organization
178 Rexdale Boulevard, Toronto, Ontario, Canada M9W 1R3

To purchase standards and related publications, visit our Online Store at www.csagroup.org/store/
or call toll-free 1-800-463-6727 or 416-747-4044.

ICS 35.030
ISBN 978-1-4883-3958-5

Contents

Technical Committee on Operational Security

I. Verhappen	Willowglen Systems, Calgary, Alberta, Canada *Category: Producer Interest*	*Chair*
F. A. Khan	TwelveDot Inc., Ottawa, Ontario, Canada *Category: General Interest*	*Vice-Chair*
T. Capel	Comgate Engineering Ltd., Ottawa, Ontario, Canada *Category: General Interest*	*Vice-Chair*
G. Chopra	Electro Federation Canada, Toronto, Ontario, Canada *Category: Producer Interest*	
F. Coallier	École de technologie Supérieure (Université du Québec) (ÉTS), Montréal, Québec, Canada	*Non-voting*
J. Fitchett	Innovation Science and Economic Development Canada, Ottawa, Ontario, Canada *Category: Government and/or Regulatory Authority*	
S. Griffith	NEMA, Arlington, Virginia, USA	*Non-voting*
V. A. Hailey	The VHG Corporation, Stouffville, Ontario, Canada *Category: General Interest*	
R. Kaun	Verve Industrial Protection, Heritage Pointe, Alberta, Canada *Category: Producer Interest*	
S. Kozma	SIL4 Solutions Inc., Calgary, Alberta, Canada	*Non-voting*

J. MacFie	Microsoft Canada, Ottawa, Ontario, Canada *Category: Producer Interest*	
W. R. MacGowan	CISCO, Toronto, Ontario, Canada *Category: Producer Interest*	
G. Nasby	City of Guelph, Guelph, Ontario, Canada *Category: User Interest*	
O. Ogundare	Canadian Centre for Cyber Security, Ottawa, Ontario, Canada	*Non-voting*
J. Palmer	Canadian Centre for Cyber Security, Ottawa, Ontario, Canada *Category: Government and/or Regulatory Authority*	
R. Roberts	Calgary, Alberta, Canada *Category: General Interest*	
D. Rogers	BC Hydro, Vancouver, British Columbia, Canada *Category: User Interest*	
F. St-Hilaire	Hydro-Québec Transénergie, Montréal, Quebec, Canada *Category: User Interest*	
J. Taylor	Schneider Electric Government & Industry Alliances, Georgetown, Texas, USA *Category: General Interest*	
R. Nehru	CSA Group, Toronto, Ontario, Canada	*Project Manager*

Subcommittee on Cybersecurity Verification

F. A. Khan	TwelveDot Inc., Ottawa, Ontario, Canada	*Chair*
H. Banavara	S&C Electric Company, Burlington, Massachusetts, USA	
R. Brash	Verve Industrial Protection, Montréal, Québec, Canada	
T. Capel	Comgate Engineering Ltd, Ottawa, Ontario, Canada	
V. Chiew	Calgary, Alberta, Canada	
V. A. Hailey	The VHG Corporation, Stouffville, Ontario, Canada	
D. Lenasi	Signify Canada Ltd, Langley, British Columbia, Canada	
T. Macaulay	Intel Security, Markham, Ontario, Canada	
J. Pollard	PCSS, Oro-Medonte, Ontario, Canada	
D. Rogers	BC Hydro, Vancouver, British Columbia, Canada	
F. St-Hilaire	Hydro-Québec TransÉnergie, Montréal, Québec, Canada	
J. Taylor	Schneider Electric Government & Industry Alliances, Georgetown, Texas, USA	
R. Nehru	CSA Group, Toronto, Ontario, Canada	*Project Manager*

Preface

This is the first edition of CSA/ANSI T200, *Evaluation of software development and cybersecurity programs*.

This Standard was prepared by the Subcommittee on Cybersecurity Verification, under the jurisdiction of the Technical Committee on Operational Security and the Strategic Steering Committee on Information and Communication Technology, and has been formally approved by the Technical Committee.

This Standard has been developed in compliance with Standards Council of Canada requirements for National Standards of Canada. It has been published as a National Standard of Canada by CSA Group.

This Standard has been approved by the American National Standards Institute (ANSI) as an American National Standard.

Notes:

1) *Use of the singular does not exclude the plural (and vice versa) when the sense allows.*
2) *Although the intended primary application of this Standard is stated in its Scope, it is important to note that it remains the responsibility of the users of the Standard to judge its suitability for their particular purpose.*
3) *This Standard was developed by consensus, which is defined by* CSA Policy governing standardization — Code of good practice for standardization *as "substantial agreement. Consensus implies much more than a simple majority, but not necessarily unanimity". It is consistent with this definition that a member may be included in the Technical Committee list and yet not be in full agreement with all clauses of this Standard.*
4) *To submit a request for interpretation of this Standard, please send the following information to inquiries@csagroup.org and include "Request for interpretation" in the subject line:*
   a) *define the problem, making reference to the specific clause, and, where appropriate, include an illustrative sketch;*
   b) *provide an explanation of circumstances surrounding the actual field condition; and*
   c) *where possible, phrase the request in such a way that a specific "yes" or "no" answer will address the issue.*

   Committee interpretations are processed in accordance with the CSA Directives and guidelines governing standardization *and are available on the* Current Standards Activities *page at standardsactivities.csa.ca.*
5) *This Standard is subject to review within five years from the date of publication. Suggestions for its improvement will be referred to the appropriate committee. To submit a proposal for change, please send the following information to inquiries@csagroup.org and include "Proposal for change" in the subject line:*
   a) *Standard designation (number);*
   b) *relevant clause, table, and/or figure number;*
   c) *wording of the proposed change; and*
   d) *rationale for the change.*

CSA/ANSI T200:22
Evaluation of software development and cybersecurity programs

0 Introduction

The purpose of this Standard is to provide requirements and guidance on the development of a method to evaluate the software development and the related cybersecurity practices of an organization that is producing software or product connected to a network, including

a) Internet of Things (IoT);
b) operational technology (OT);
c) connected devices; and
d) embedded devices.

Governments, businesses, and consumers are looking to the rapid adoption of connected products and services to automate tasks and provide efficiencies in many market areas. While these technologies can dramatically advance the capabilities of those users and businesses, they pose a potential cyber and privacy risk to the end user. The end user is typically under the assumption that these products have undergone some level of security testing and evaluation, including the assumption that products pose no direct risk to them or their businesses. However, given the significant increase in purpose-built malware for IoT and related products, including the sizable increase of botnet activity of affected devices, the assumption that products have been designed and tested for security can hold untrue or be applied inconsistently across similar products. Therefore, a method to evaluate organizations on their cybersecurity practices can assist in identifying products designed with security considerations to reduce the overall risk of deploying these technologies. Organizations that implement this approach will typically start at the baseline and then proceed to include additional controls to increase their control maturity over a period for each of the domains defined.

1 Scope

1.1

This Standard describes a methodology for assessing the product software and cybersecurity control maturity of an organization.

This Standard provides the evaluators and vendors a method to determine the control maturity of the organization and products/solutions being developed regardless of solution vertical. It covers the entire product system life cycle from conception to full commissioning and until the end of life. It supports effective executive business decisions that establish a comprehensive maturity model approach to cybersecurity.

1.2

This Standard is applicable to all IoT and related products/solutions.

