TOSA

Your skills. Your advantage.

Tosa CyberCitizen

Exam Blueprint

contact@isograd.com

Table of Contents

Introduction

to the Tosa® Exam Blueprint

For Tosa® Assessment and Certification

Tosa® (Test on Software Applications)

Tosa® assessments and certifications are designed to determine a candidate's proficiency level by evaluating their skills in office software and digital tools commonly used in a professional or educational environment.

These tests are specifically developed to validate the professional competencies of candidates looking to enhance their employability (employees, students, job seekers, and individuals undergoing career transitions).

Tosa® assessments and certifications are adaptive tests, developed using scientific methodologies. The scoring is based on Item Response Theory (IRT). The test algorithm adapts to each candidate's response in real time, adjusting the difficulty level of subsequent questions until it precisely determines the candidate's skill level by calculating the upper limit of their competencies. As a result, the tests provide a detailed and unique diagnosis of each candidate's abilities.

The rigor and reliability of Tosa® tests stem from the combination of a mathematical model for analyzing question difficulty and the relevance of the questions selected for each candidate (IRT).

Tosa® Exam Blueprint Objective

This exam blueprint outlines all the skills assessed within the domains and sub-domains of the Tosa® assessment and certification tests for CyberCitizen.

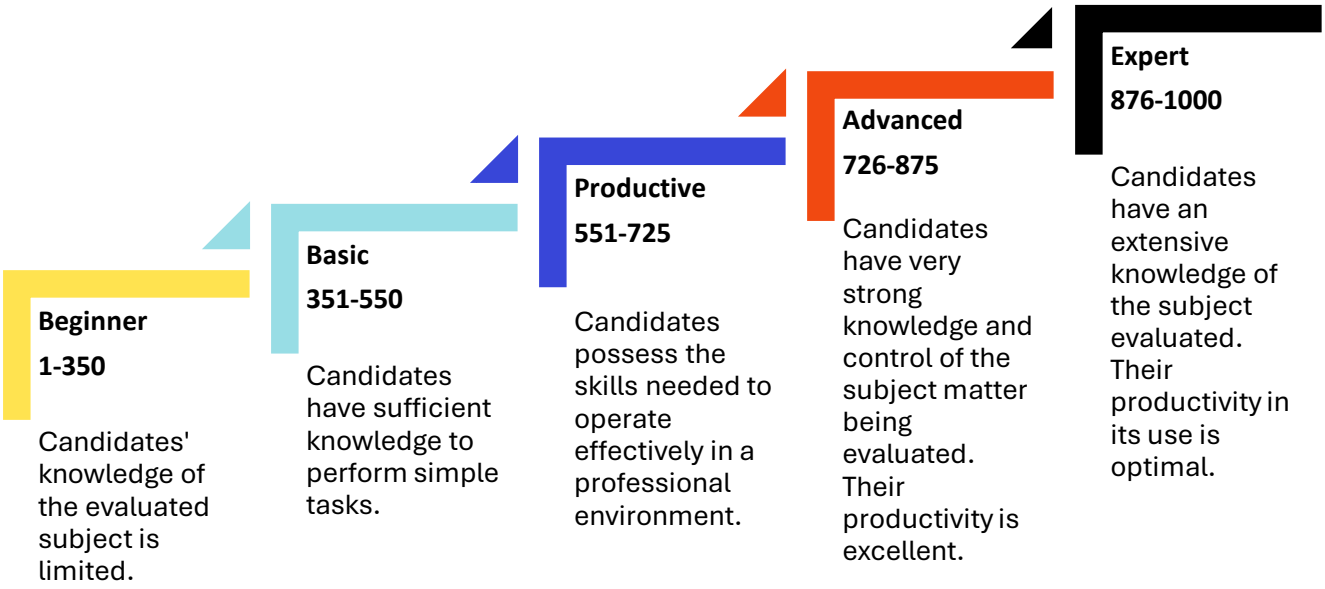
Tosa® assessment and certification solutions are designed to determine learners' proficiency levels using a single scoring scale—ranging from 0 to 1000 for certification—and divided into five levels, from "Beginner" to "Expert," for the assessment.

The purpose of this blueprint is to specify the technical knowledge expected at each level and within each of the four main skill categories of CyberCitizen. It is intended to help identify the most appropriate teaching or training programs to match a learner's target score.

Unique Tosa® Scoring

The Tosa® assessments and certifications are based on a unique score, divided into five levels.

- Ranging from 1 to 1000 for the certification.
- Divided into five levels, from Beginner to Expert, for the assessment.



Certification failed	**Certification earned**	**Certification earned**	**Certification earned**	**Certification earned**
Certificate of completion issued	Diploma issued	Diploma & Credly digital badge issued	Diploma & Credly digital badge issued	Diploma & Credly digital badge issued

About the Tosa® CyberCitizen certification

The Tosa CyberCitizen Certification relies on a database of more than 150 questions. It is composed of 35 questions from the question database and lasts for 1 hour. The algorithm adapts to each of the candidate's answers to adjust the difficulty level of the questions until reaching the candidate's skill limit. This ensures a precise and accurate result.

Since the test is adaptive, the series of questions that a candidate gets is unique for each test. This algorithm allows for a more accurate evaluation of the candidate's level. It also limits cheating and the memorization of questions on different passages.

Our platform allows individuals to take the certification in a classroom setting, an approved testing center, or remotely via our integrated asynchronous online proctoring solutions.

Our remote proctoring solutions provide added flexibility for both the administrator and the candidate, allowing the certification exam to be taken anywhere, at any time. The candidate only needs an internet connection and a computer equipped with a working webcam and microphone.

Candidates receive a numeric score out of 1000 points. This score corresponds to one of five proficiency levels. Candidates who score between 1 and 350 points do not earn the certification. They receive a certificate of completion in lieu of a diploma. Candidates who score 351 points or above earn the certification and will receive a diploma by email within five business days. If a candidate scores 551 points or above, they will also be eligible to receive a digital Credly badge.

There are no prerequisites to be eligible to take the exam, but to ensure a candidate is well prepared on exam day, we suggest they:

- Take at least one Tosa CyberCitizen adaptive assessment to estimate their level and get familiar with the test format
- Use the free practice tests on our website for training
- Follow an e-learning or training course (average duration per level is between 10 and 15 hours per certification, so around 150 hours total)

Tosa certification diplomas are valid for three years from the date of issue. This three-year period has been set to ensure that our certifications are consistently accurate and relevant, taking into account software version updates as well as the natural evolution of a candidate's skills over time. Limiting the certification period also reflects the need for life-long learning and continual professional development.

Tosa certifications can be retaken when they expire. Earners willing to improve their score and proficiency level can retake the exam at any time.

Tosa Sequence for Progressive Skills Development

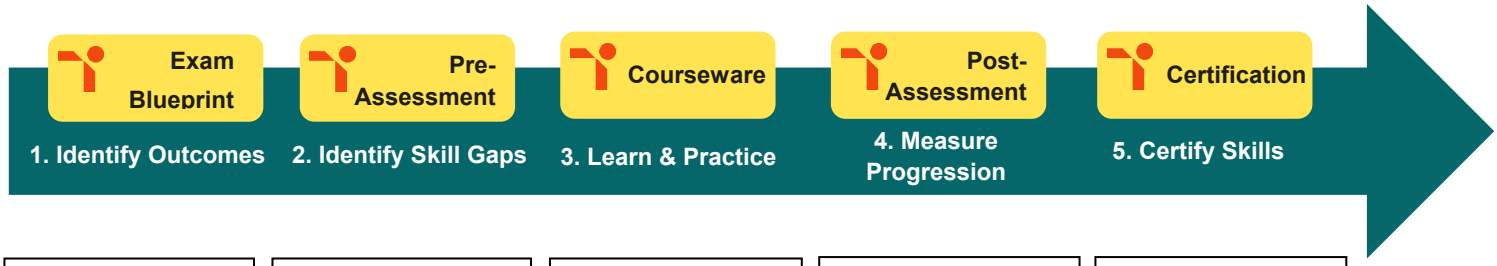
Students and professionals can tailor their certification journey with Tosa through vertical progression, demonstrating increasing proficiency in cybersecurity. Starting at a productive level, users can advance to advanced and expert levels as their skills grow. This clear path encourages continuous improvement and validates each stage of their development. Tosa's structure makes it easy to track progress and showcase evolving expertise.

Isograd Learning Lab

The Isograd Learning Lab is a multifaceted and adaptable courseware solution designed to help learners prepare for Tosa certification exams. It offers personalized, self-paced, and fully interactive learning experiences, equipping candidates with the essential digital skills that employers seek. These skills span a wide and varied range, applicable to learners just starting their career journey to those wishing to advance on their path.

The browser-based platform supports all learning styles with a wide array of features, including in-application exercises. These in-application capabilities allow learners to experience real-world examples of specific tasks within a given software environment. The lab includes inclusive learning resources, along with extension activities and project-based learning challenges that foster creativity and critical thinking.

All course content on the Isograd Learning Lab is aligned to a Tosa exam blueprint, which is the foundation of any Tosa certification exam. By aligning course content to an exam blueprint, learners will be prepared to take the exam once they complete the courseware.



1. Identify Outcomes	2. Identify Skill Gaps	3. Learn & Practice	4. Measure Progression	5. Certify Skills
Using a Tosa® exam blueprint, instructors integrate Tosa® certifications into their existing content or curriculum and set define outcomes.	Students begin with a formative pre-course assessment to identify their current skills level. Instructors gather data and adjust lesson plans based on students' results.	Instructors match courseware in the Isograd Learning Lab to student's proficiency levels and intended course objectives.	Once the courseware is completed, students take a summative assessment to verify their skills match the intended proficiency level. If skill gaps still exist, instructors can assign additional course content.	When instructors are satisfied with students' progress, certification exams are given.

Tosa® CyberCitizen Level Descriptions

At each level, candidates can:

Beginner

- Understand the basic concepts related to cybersecurity and common threats.
- Identify the function of passwords and recognize a secure connection (HTTPS).
- Spot software updates without necessarily knowing how to apply them.
- Distinguish a few obvious risks when using devices while on the move or at home.

Basic

- Create strong passwords to secure access.
- Identify the appropriate cybersecurity contacts in an organization (CISO, DPO, etc.).
- Physically and digitally secure a workstation when absent.
- Detect a simple fraudulent message (phishing, spam) and back up files.
- Limit the exposure of data while traveling.

Productive

- Use a password manager to store and protect credentials.
- Recognize and report social engineering attempts.
- Regularly update systems and software to fix security vulnerabilities.
- Configure and use secure network connections, including on mobile devices.
- Analyze suspicious files or messages before opening them.

Advanced

- Identify vulnerabilities and alert security teams in case of risk.
- Select and install software from trusted sources.
- Safely manage devices and sensitive data while traveling.
- Configure and use a VPN to secure remote connections.
- Analyze incoming documents with specialized tools such as antivirus software.
- Separate and protect personal and professional uses on the same device.

Expert

- Assess the impact and criticality of attacks on an organization.
- Collect and document intrusion evidence according to established procedures.
- Deploy and manage encrypted storage and transfer solutions.
- Organize secure work environments, on-site or remote.
- Administer large-scale security systems (e.g., MDM) and train employees.
- Ensure business continuity and data protection in the event of a major incident.

Business Applications

Achievement of a Beginner score indicates little or limited knowledge of cybersecurity concepts and tools, including basic security functions and principles, highlighting the candidate's inability to operate effectively in a professional security environment.	*Junior IT technician, help desk assistant, customer support representative, or any position requiring occasional use of cybersecurity practices such as managing passwords, identifying phishing attempts, or following basic data protection procedures.*	*Operations assistant, network coordinator, junior security analyst, IT support technician, or any role requiring the regular use of cybersecurity tools for monitoring systems, managing access controls, and applying routine security measures to support daily business operations.*	*Security analyst, systems administrator, IT project manager, risk consultant, or any position requiring advanced use of cybersecurity tools for monitoring and analyzing threats, implementing secure network architectures, and developing automated defense workflows to support strategic organizational security.*	*Senior security analyst, cybersecurity manager, chief information security officer (CISO), or security consultant, or any role requiring expert-level proficiency in cybersecurity for designing and deploying scalable security solutions, conducting advanced threat analysis, and supporting high-level decision-making through strategic risk management and automation.*

TOSA
Your skills. Your advantage.

Domain 1: The Cybersecurity World

Sub-domain 1: Roles in cybersecurity

Covers the major roles around cybersecurity within a work organization as well as the standards, tests, and protocols associated with those roles and how they help organizations to manage sensitive data and best practices in security.

Beginner

- Understand the need for specific roles within a cybersecurity context.
- Demonstrate initial understanding of how cybersecurity is organized within the workplace.

Basic

- Identify specific key roles within an organization (CISO, DPO, SOC).
- Recognize public and industry cybersecurity authorities (such as national cybersecurity agencies or CERTs).
- Describe the primary functions and areas of action of a SOC.

Productive

- Identify the specific tasks of individual cybersecurity roles within the workplace.
- Demonstrate understanding of the chain of command within cybersecurity and the importance of escalation.

Advanced

- Know when to perform a penetration test.
- Explain how and why penetration tests are used.
- Recognize specific threats identified by a penetration test.

Expert

- Name the ISO 27001 standard.
- Explain how the standard helps organizations manage sensitive data.
- Train others on the ISO 27001 standard and communicate effectively about implementation.

Sub-domain 2: Targets and impacts of a cyberattack

Covers the various types of cyberattacks that an organization may face and which security protocols are best suited to protect against these attacks.

Beginner

- Define a cyberattack.

Basic

- Differentiate the threat levels of different cyberattacks.
- Identify the main goals of cyberattacks.

Productive

- Identify the preferred targets of potential attacks within an organization.
- Name the common motivations of attackers.

Advanced

- Independently identify major cyberattack methodologies and their consequences.
- Explain the organizational and individual protocols that are best practices in maintaining data security.

Expert

- Assess the criticality of potential attacks for different companies.
- Identify the risks of various types of attacks (phishing, ransomware, DDoS) within a given company or institution.

Sub-domain 3: Responding to a cyberattack

Covers responding to cyberattacks within an organization, particularly at the early stages of detection and threat management.

Beginner

- Demonstrate initial understanding of how to react when aware of a potential cyberattack.

Basic

- Identify first steps in responding to potential cyberattacks.
- Identify the primary roles in an organization responsible for data security and available communication channels with these roles.

Productive

- Apply security procedures at the workstation in the event of an attack (especially disconnecting from the network).

Advanced

- Explain procedures for ensuring that cyberattacks have not compromised data beyond the initial target.

Expert

- Train others on the implementation of security protocols in the initial stages of a cyberattack.
- Explain and clarify best practices for identifying cyberattacks.

Sub-domain 4: Digital identity and authentication

Covers authentication, particularly around the use of passwords and the various tools that exist to ensure data privacy and security around password-protected services and systems.

Beginner

- Understand the purpose of a password.
- Identify services and tools that necessitate a password.

Basic

- Create strong passwords.
- Identify potential weaknesses in passwords.

Productive

- Understand the purpose of a password manager.
- Add a password to a manager.
- Secure digital identity by using varied passwords.

Advanced

- Authenticate for a service using multi-factor authentication.
- Change a password in a manager.
- Explain potential security failure situations as they relate to passwords and authentication.

Expert

- Train others on the creation of strong passwords.
- Explain best practices in using password managers for large organizations or across varied teams.

Domain 2: Security in the Workplace

Sub-domain 1: Workstation security

Covers best practices in cybersecurity for individuals and private workstations within an organization, as well as the possible motivations of cyberattacks that may affect individuals or teams.

Beginner

- Identify initial security protocols for your workstation during an absence.

Basic

- Explain potential security risks to an individual workstation within the larger network of an organization.
- Transfer public data securely from your workstation.

Productive

- Respond appropriately to the presence of unfamiliar individuals in the workplace.
- Identify roles responsible for authenticating users and visitors within the workplace.

Advanced

- Explain the possible motivations of external cyberattacks on an individual or team within an organization.
- Identify potential financial or social reasons behind various kinds of cyberattacks.

Expert

- Handle paper documents securely.
- Disable a Windows process.
- Train others on best practices in workstation security.

Sub-domain 2: Removable or external devices

Covers the use of peripheral devices and the security threats they may present to an organization.

Beginner

- Identify the risks of removable devices, such as USB flash drives or external hard drives.

Basic

- Demonstrate initial understanding of the safe use of external devices.
- Explain the importance of password protection in relation to external devices.

Productive

- Password protect a removable or external device.
- Identify suspicious removable or external devices.

Advanced

- Handle sensitive data on an external or removable device, following best practices in data security and authentication measures.

Expert

- Train others on the responsible use of external or removable devices.
- Run tests to determine if data contained on an external or removable device is compromised.

Sub-domain 3: Software versions and updates

Covers software versions and the importance of consistent updating protocols to ensure data integrity.

Beginner

- Demonstrate initial understanding of the importance of software updates.

Basic

- Identify changes across software versions.
- Identify the current version of a given software.

Productive

- Name the risks of installing cracked software or software from an unknown source.
- Find a trusted source to download software.
- Perform an antivirus scan before downloading software.

Advanced

- Identify the version of an operating system.
- Troubleshoot software update issues.

Expert

- Train various teams across an organization in maintaining consistent updates.
- Lead teams or individuals in proper software usage and version identification.

Domain 3: Security on the Move

Sub-domain 1: Security while traveling or in new environments

Covers the possible security threats of working in a new environment or working while traveling, including the appropriate responses to these threats.

Beginner

- Identify the risks associated with travel (theft, data exposure).
- Identify the risks associated with working in new and unknown environments.

Basic

- Use airplane mode to secure devices containing sensitive data.

Productive

- Add a passcode to a phone.
- Explain the need for added device security while traveling.
- Identify security measures for devices being used in unknown environments.

Advanced

- Secure access cards (e.g., transportation or hotel key cards).
- Limit the data left behind by a team after working in a new environment: paper documents, written notes, and digital traces.

Expert

- Assess a new environment for possible security threats.
- Lead a team or individuals in setting up devices in a new environment or while traveling to ensure data security.

Sub-domain 2: Wireless networks

Covers wireless networks and the security protocols necessary to ensure safe data transmission and secure internet usage.

Beginner

- Recognize an HTTPS connection.

Basic

- Demonstrate initial understanding of the risks of connecting to public Wi-Fi (for example, in an airport or train station).

Productive

- Rank the security levels of different Wi-Fi security protocols.
- Recognize an SSL certificate.
- Identify the certification authority of an SSL certificate.

Advanced

- Know when to use a VPN.
- Explain the security benefits of using a VPN.

Expert

- Identify the security benefits of using a proxy.
- Explain the benefits of using a proxy to others across teams or organizations.

Sub-domain 3: Data overexposure

Covers the risks and mitigation systems around data privacy.

Beginner

- Identify the risks associated with data overexposure.
- Demonstrate initial understanding of what constitutes data overexposure.

Basic

- Explain why data privacy is important.
- Describe ways data and privacy can be compromised.

Productive

- Identify possible entry points for bad actors in data management systems.
- Identify a variety of ways data may be compromised during data entry, management, and communication.

Advanced

- Use a privacy filter.

Expert

- Identify the advantages and limitations of a professional Mobile Device Management (MDM) service.
- Explain how organizations can ensure data privacy across diverse teams and individual actors.

Domain 4: Security at Home

Sub-domain 1: Phishing, email, and messaging security

Covers protecting oneself during email communication and messaging as well as identifying and responding to phishing attempts and related attempted cyberattacks.

Beginner

- Demonstrate initial understanding of email security protocols.
- Identify the reasons why bad actors instigate phishing attempts.

Basic

- List the elements to check to ensure an email's trustworthiness.
- Recognize a potential phishing attempt by email.

Productive

- React to a suspected phishing situation.

Advanced

- List the elements to check to ensure the trustworthiness of a call or text message.

Expert

- Lead others in detecting and responding to phishing attempts.
- Design and implement protocols for email and messaging security across diverse teams.

Sub-domain 2: The cloud and file management both internal and external

Covers safe and responsible file management, including cloud storage and interacting with external files in cybersecurity-aware ways.

Beginner

- Demonstrate initial understanding of risks associated with cloud storage.
- Identify possible cybersecurity risks associated with working with external files and downloads.

Basic

- Store professional files on the cloud securely.
- Download an external document or an email attachment safely.

Productive

- Digitally send large public files.
- Check the extension of an external file.
- Handle files sent as email attachments safely.

Advanced

- Explain the security features of an attached file.

Expert

- Separate the storage of personal and professional documents.
- Digitally send sensitive files with encryption or other cybersecurity measures.
- Extract a file's metadata.

Sub-domain 3: Privacy and personal data protection

Covers a broad understanding of personal data protection and maintaining desired levels of privacy during online interactions and personal data management.

Beginner

- Explain the purpose of cookies.
- Recognize a CAPTCHA.

Basic

- Demonstrate understanding of personal data protection in online spaces that require the entry or maintenance of personal data.
- Explain basic security features present on sites and applications that ask for personal data.

Productive

- Explain the risks associated with personal data usage in social media networks.
- Describe ways to ensure data privacy across a broad range of websites and applications.
- Identify legal rights that users have in regards to their private data.

Advanced

- Exercise rights over personal data (correction, deletion).
- Explain and apply personal data security features on social networks.

Expert

- Prevent the leakage of professional data on personal or professional social networks.

TOSA

Your skills. Your advantage.

contact@isograd.com

www.tosa.org