

Tosa Skills Framework

CyberCitizen

Overview

Introduction to Tosa Skills Framework2

TOSA® (TEST ON SOFTWARE APPLICATIONS).....	3
TOSA SKILLS FRAMEWORK OBJECTIVE	3
UNIQUE TOSA SCORING	3
CYBERCITIZEN DOMAINS AND SUBDOMAINS	4
ABOUT THE CYBERCITIZEN CERTIFICATION	4

Level 1 – Beginner User.....6

OVERVIEW	7
----------------	---

Level 2 – Basic User8

THE CYBERSECURITY WORLD	9
SECURITY IN THE WORKPLACE	9
SECURITY ON THE MOVE	9
SECURITY AT HOME.....	9
OVERVIEW	10

Level 3 – Productive User.....11

THE CYBERSECURITY WORLD	12
SECURITY IN THE WORKPLACE	12
SECURITY ON THE MOVE	12
SECURITY AT HOME.....	13
OVERVIEW	14

Level 4 - Advanced User.....15

THE CYBERSECURITY WORLD	16
SECURITY IN THE WORKPLACE	16
SECURITY ON THE MOVE	16
SECURITY AT HOME.....	17
OVERVIEW	18

Level 5 – Expert User19

THE CYBERSECURITY WORLD	20
SECURITY IN THE WORKPLACE	20
SECURITY ON THE MOVE	20
SECURITY AT HOME.....	21
OVERVIEW	22

Introduction to Tosa Skills Framework

For Tosa Assessment and Certification

Tosa® (Test on Software Applications)

The Tosa assessments and certifications will determine and validate a candidate's proficiency and skill level in software applications used in a professional environment. The Tosa assessments are designed to validate the professional CyberCitizen software skills of individuals (students, trainees, employees, or jobseekers) in supporting their employment, professional or academic objectives.

Tosa assessments employ the Adaptive Testing methodology, which creates a personalized testing experience adapted to a candidate's skill level for a selected software application. The score is based on the Item Response Theory using a 3-parameter logistic model, similar to the GMAT scoring method. Adaptive-based testing selects questions that challenge candidates to the limit of their knowledge and abilities.

Tosa Skills Framework Objective

This Tosa framework provides an overview of the subject areas being assessed during the Tosa Assessment and Certification exams. The Tosa CyberCitizen validates candidate awareness and knowledge of cybersecurity using a score on a scale from 1-1000 for the Certification Assessment, and a score divided into five levels from "Beginner" to "Expert" for the Diagnostic Assessment.

The objective of this document is to present an overview of the technical skills associated with each of the four main cybersecurity domains within each proficiency level. This information will also support educators and trainers in tailoring their training program to achieve desired proficiency levels.

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 assessment.

Tosa® levels	Corresponding Tosa® score
Expert	876 - 1000
Advanced	726 – 875
Productive	551 – 725
Basic	351 – 550
Beginner	1 – 350

CyberCitizen domains and subdomains

The cybersecurity world	<ul style="list-style-type: none"> ■ Cybersecurity people and institutions ■ Targets and impacts of an attack ■ Reacting in case of an attack ■ Digital identity and authentication
Security in the workplace	<ul style="list-style-type: none"> ■ Workstation security ■ Social engineering ■ Removable devices ■ Software versions and updates
Security on the move	<ul style="list-style-type: none"> ■ Physical security of terminals ■ Smartphones and security ■ Wireless networks ■ Data overexposure
Security at home	<ul style="list-style-type: none"> ■ Phishing ■ Cloud and file backup ■ External files ■ Privacy and personal protection

About the CyberCitizen certification

The Tosa CyberCitizen certification relies on a database of around 140 questions. It is composed of 35 questions and lasts one hour. The algorithm adapts to each answer of the candidates to adjust the difficulty level of the questions until they reach the exact definition of the candidates' level by calculating the limit of their skills.

Since the test is adaptive, the series of questions that each candidate gets is unique for each test. This uniqueness 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 class, in 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.

The Tosa CyberCitizen certification is delivered with a score (between 1 and 1000), corresponding to a level (Beginner, Basic, Productive, Advanced, or Expert). There is no requirement to be eligible to take the exam, but our recommendations to be well prepared on exam day are:

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

Tosa certification diplomas are valid for three years from the date of issue as skill levels evolve or decline over time, depending on the use of the software. New software and software versions are released every year, and skills must be updated. We cannot legitimately certify a digital skills level for more than three years. Limiting the certification validity reinforces the need for life-long learning and professional development.

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

Level 1 – Beginner User

Between 1 and 350 points

The Beginner Proficiency is set for a score from 1 to 350, which is the lowest Tosa score category. Attaining the Beginner level means that the candidate has little to no knowledge of even simple aspects of cybersecurity and cannot apply them in a professional environment.

Overview

Domains	Skills Assessed
The cybersecurity world	<ul style="list-style-type: none">Understand the purpose of a passwordDefine a cyber attack
Security in the workplace	<ul style="list-style-type: none">Know the importance of updates
Security on the move	<ul style="list-style-type: none">Name the risks exposed to by travel (theft, data exposure)Recognize a connection via HTTPS
Security at home	<ul style="list-style-type: none">Know the use of a cookieRecognize a captcha

Level 2 – Basic User

Between 351 and 550 points

Prior to the acquisition of the skills of the Basic level, the candidate will have mastered the skills of the Beginner level.

The Cybersecurity World

Passwords

Create strong passwords and know the characteristics of a strong password.

Business application: create secure access to all business services as soon as one joins the company.

Cybersecurity people and institutions

Identify the main cybersecurity contacts, private or public, internal or external to the company.

Business application: quickly know who to turn to or where to look for information when needed on cybersecurity issues, to speed up the transmission of information.

Security in the Workplace

Computer access

Secure physical and electronic access to computers.

Business application: guarantee the security of data and access to computers in case of absence from the workstation, whatever the duration.

Security on the Move

Theft of a computer while on the move

Limit the risk of theft of a computer, smartphone, or data during transport.

Business application: to be able to leave on a business trip while reducing the risk of theft of the computer, or too obvious exposure of the data.

Security at Home

Email phishing

Verify the absence of phishing elements when opening an email.

Business application: be able to process emails without exposing one's company to the risks of a phishing attack.

Electronic document management

Use electronic document management tools.

Business application: guarantee the backup of all work files, even in case of loss or change of workstation.

Overview

Domains	Skills Assessed
The cybersecurity world	<ul style="list-style-type: none"> Create strong passwords Identify the key roles within a company (CISO, SOC, pentesters) Name the fields of action of a SOC
Security in the workplace	<ul style="list-style-type: none"> Secure one's workstation while away Transfer public data securely
Security on the move	<ul style="list-style-type: none"> Identify the increase in cybersecurity risks when traveling Know the risks of a connection on a public Wi-Fi (airport or train station for example) Use the airplane mode to secure devices containing sensitive data
Security at home	<ul style="list-style-type: none"> Name the elements to check to ensure the trustworthiness of an email Recognize a potential email phishing attempt Store professional files on the cloud

Level 3 – Productive User

Between 551 and 725 points

Prior to the acquisition of the skills of the Productive level, the candidate will have mastered the skills of the Basic level.

The Cybersecurity World

Attacker profiles

Name different attacker profiles, both groups and individuals, and recognize examples for each profile.

Business application: facilitate awareness and identification of risk by recognizing different attacker targets.

Password managers

Use a password manager (Keepass is used as an example in the test).

Business application: guarantee a high level of security on all its accesses to business services

Security in the Workplace

Social engineering

Recognize a potential manipulation attempt.

Business application: avoid the intrusion of a malicious person or the leakage of information due to the presence of an intruder in the office.

Software updates

Update software and operating system.

Business application: guarantee the installation of the latest versions of software and OS to ensure the application of security patches as soon as they are published.

Security on the Move

Wireless networks

Recognize and use a secure wireless network (Wi-Fi, Bluetooth).

Business application: to be able to continue working on the Internet even when travelling in a public place or from another company's office.

Smartphone security

Secure access to data and services on a smartphone.

Business application: to be able to use one's business smartphone on the move without exposing oneself to data leaks.

Security at Home

Unsafe files

Apply the required precautions with unknown files and recognize a potentially dangerous file.

Business application: limit the risk when opening files sent as attachments.

Phishing

Detect phishing attempts on different channels (email, SMS, call)

Business application: be able to use all professional communication channels for sensitive documents or data, limiting their exposure to a risk of leakage or attack.

Overview

Domains	Skills Assessed
The cybersecurity world	<ul style="list-style-type: none"> Know the usefulness of a password manager Add a password in a password manager (Keepass) Secure one's digital identity with various passwords Identify the privileged targets of potential attacks Name the usual motivations of attackers
Security in the workplace	<ul style="list-style-type: none"> Apply automatic software updates Apply automatic operating system updates Detect tampering by an external agent React appropriately to the presence of unknown persons in the office
Security on the move	<ul style="list-style-type: none"> Classify the security of the different Wi-Fi security protocols Add an access code on one's phone Recognize an SSL certificate Find the certification authority of an SSL certificate
Security at home	<ul style="list-style-type: none"> React to suspected phishing Check the extension of an external file Handle files sent as attachments Digitally send large public files

Level 4 - Advanced User

Between 726 and 875 points

Prior to the acquisition of the skills of the Advanced level, the candidate will have mastered the skills of the Productive level.

The Cybersecurity World

Vulnerabilities

Distinguish the main types of vulnerabilities.

Business application: effectively identify potential exposures to cybersecurity risks as soon as one takes up their position, to mitigate their potential impacts.

Cybersecurity contacts

Identify the contact and the channel to alert in case of a proven attack.

Business application: be a strong element in the transmission of information in case of an attack on the company.

Security in the Workplace

External storage

Securely handle external storage devices.

Business application: to be able to securely use or transmit documents from another member of the company or an external partner stored on a USB key or hard drive.

Software installation

Distinguish between trusted software sources.

Business application: securely install software that is necessary for the job but not provided by the company.

Security on the Move

Data overexposure

Limit the exposure of sensitive data in writing, orally or on screen outside.

Business application: to be able to work on sensitive documents from while on public transportation or in public places. Organize meetings outside the company's premises dealing with sensitive subjects.

VPN

Know the usefulness and use of a VPN.

Business application: guarantee a secure connection to the company's services and applications wherever the employee is.

Security at Home

External documents

Securely handle any type of external document, and know how to perform an antivirus analysis on a file (Virus Total is used in the test)

Business application: to be able to safely use a document sent by a partner or an unknown person.

Personal and professional spheres

Separate personal and professional digital uses on terminals and applications (social networks in particular)

Business application: limit the exposure of professional data through the personal use of terminals, tools, or professional social networks of the employee.

Overview

Domains	Skills Assessed
The cybersecurity world	<ul style="list-style-type: none"> Authenticate to a service via multi-factor authentication Know when and why to perform an intrusion test Apply security procedures on one's workstation in case of an attack (disconnection in particular) Modify a password in a password manager (Keepass)
Security in the workplace	<ul style="list-style-type: none"> Name the risks of installing cracked software or software from an unknown source Find a trusted source to download software Perform an antivirus scan (with VirusTotal for example) Find the version of a given software Handle unknown storage devices
Security on the move	<ul style="list-style-type: none"> Use a privacy filter Secure one's access cards (transport, hotel access card for example) Know when to use a VPN Name the benefits of using a VPN for security Limit the data left behind by a team after moving to a new environment: paper documents, writings, electronic traces
Security at home	<ul style="list-style-type: none"> Name the elements to check to ensure the trustworthiness of a call or an SMS Know the security characteristics of an attached file Know and apply the security features of personal data on social networks

Level 5 – Expert User

Between 876 and 1000 points

Prior to the acquisition of the skills of the Expert level, the candidate will have mastered the skills of the Advanced level.

The Cybersecurity World

Attack criticality

Evaluate the different potential impacts of an attack on a company.

Business application: prioritize actions and awareness within a team or a company. At this level, the candidate can train on cybersecurity awareness.

Evidence collection

Reproduce an intrusion evidence collection procedure.

Business application: be an active support to any employee of the company in order to facilitate the mitigation and investigation work of the expert teams.

Security in the Workplace

Exposure of sensitive data

Limit the exposure of sensitive documents or information.

Business application: Guarantee a low level of exposure of the company's data within the premises, to limit its distribution to external or internal personnel who are not authorized to have access.

Encrypted external storage

Secure information on all removable devices.

Business application: be able to transfer any type of document, from public to classified, using the right medium, encrypted or not.

Security on the Move

Securing a new environment

Secure terminals in a new environment (hotel, meeting room).

Business application: to be able to prepare a secure environment for a team, for the organization of a meeting or a long stay in a hotel for example.

Mobile Device Management

Know the principles and usefulness of a professional mobile device management service (MDM).

Business application: be a strong link in the security coverage of the company's mobile fleet, by being the referent on the applications and data controlled by the MDM.

Security at Home

Business continuity

Master the principles of data backup and business stability.

Business application: guarantee a level of business continuity even in the event of a proven attack thanks to the availability of the team's files.

Team teleworking

Protect personal information and privacy while at home or working remotely.

Business application: limit the exposure of professional data through the personal use of terminals, tools, or professional social networks of the team.

Overview

Domains	Skills Assessed
The cybersecurity world	<ul style="list-style-type: none"> Assess the criticality of potential attacks for different companies Name the ISO27001 standard Identify the risks of different types of attacks (phishing, ransomware, DDoS) within a given company or institution
Security in the workplace	<ul style="list-style-type: none"> Transfer sensitive data securely Track the version of the operating system Securely process paper documents Disable a Windows process
Security on the move	<ul style="list-style-type: none"> Identify potential risks in a new environment Distinguish the benefits and limitations of a professional mobile device management (MDM) service Distinguish the benefits of using a proxy for security
Security at home	<ul style="list-style-type: none"> Separate storage of personal and professional documents Prevent leakage of professional data on personal or professional social networks Extract metadata from a file Digitally send sensitive files

