

FAQs FOR GOSECURE

General Questions

1. What is GoSecure? What are the objectives?

GoSecure is designed to support ICT SMEs to build up their cybersecurity capabilities and support the adoption of cybersecurity tools and services internally. The programme aims to help ICT SMEs leverage these tools and services, as well as put in place safeguards and Security-by-design practices, to improve the overall security posture of their products and solutions.

2. How can ICT SMEs be supported under GoSecure?

Under GoSecure, ICT SMEs can be supported in the following ways:

- ICT SMEs can conduct a self-assessment of their internal digital capabilities in cybersecurity through a free **Tech Capability Assessment Tool**. The online tool is developed by IMDA to help ICT SMEs assess their capability gaps with recommendations on how they can address these gaps.
- ICT SMEs will also be able to adopt cybersecurity tools and services for use during solution development and deployment from a list of pre-approved vendors published in Business Grants Portal and Tech Depot at SME Portal (under “Infocomm” sector) **(i.e. GoSecure with New Tools and Services)**
- ICT SMEs can receive Security-by-Design consultation and obtain Vulnerability Assessment services from Singapore Institute of Technology at below market rate **(i.e. GoSecure with SIT)**

2. What are the benefits of GoSecure?

Through GoSecure, ICT SMEs will be able to:

- Conduct self-assessment to ascertain current capability gaps in cybersecurity through the free Assessment Capability Tool and receive recommendations on how to address the identified gaps
- Develop cybersecurity capability by incorporating cybersecurity best practices and adopting cybersecurity tools and services in the product and solution development
- Reduce the total cost of development through early identification of vulnerabilities
- Reduce the number of security vulnerabilities in their product, resulting in increased confidence and trust from their customers
- Meet the cybersecurity criteria in the pre-approved solutions under the SMEs Go Digital programme (only for GoSecure with SIT)

Additionally, with the partnership with SIT, GoSecure provides real-life industry exposure and training for students involved in the vulnerability assessment as part of their projects.

Questions Relating to GoSecure with SIT

3. Is this a cybersecurity certification programme for software solutions?

The Vulnerability Assessment (VA) report is not a certification for cybersecurity. However, the VA report can be used for customers' references or to demonstrate compliance to mandatory cybersecurity criteria for pre-approved solution under SMEs Go Digital programme.

4. How many rounds of Vulnerability Assessment Testing will there be?

ICT companies will be required to undergo two rounds of vulnerability assessment testing. The first round will assist company to uncover the vulnerabilities within their solution and second round is validation to ensure that vulnerabilities are resolved.

5. What is required from my company after each Vulnerability Assessment Test?

After the completion of the first round of vulnerability assessment testing, ICT companies are expected to commit their resources to resolve the vulnerabilities uncovered in the testing.

6. Do companies pay less for these services by signing up for GoSecure?

There are different variables, e.g. scope of work, man-day rate that will contribute to the cost of security testing. Comparatively, commercial rates could be up to two times higher than the cost of services rendered through the GoSecure programme.

7. If an ICT company does not meet the criteria for GoSecure with SIT, are there any other commercial service providers that can provide similar services? What is the difference?

For ICT SMEs that do not meet the criteria for GoSecure, they may approach commercial service providers that provide security testing services. However, they might not get access to the one-on-one Security by Design Consultation that is put in place by SIT as part of GoSecure. They will also likely to pay for vulnerability assessment testing services at a higher rate.

8. Who can participate in GoSecure with SIT?

Eligibility criteria include:

- Priority for First-Time Applicant for GoSecure
- Singapore-Owned or Singapore-Based ICT SME
- Owns the IP of the product or solution to undergo vulnerability assessment
- Have positive net equity based on the latest financial statement (optional for start-up companies)

- Have local technical resources to go through capability upskilling and vulnerability assessment testing

9. How to Apply and Participate in GoSecure with SIT?

ICT SMEs that wish to participate in the GoSecure with SIT programme may write in to cybersecurity@Singaporetech.edu.sg.

Participating in SMEs Go Digital

10. Would the companies that have completed GoSecure be automatically pre-approved as vendors with solutions for SMEs under SMEs Go Digital programme?

ICT SMEs that have completed their projects under GoSecure and successfully completed their vulnerability assessment (VA) tests and cleared all the major vulnerabilities highlighted can submit their VA report as third party assessed report to meet the cybersecurity criteria when they submit applications to be a pre-approved vendor with solutions for SMEs. They must still be able to meet the other criteria and requirements of SMEs Go Digital programme for pre-approval.

ICT SMEs may refer to the SMEs Go Digital Programme page (<https://www.imda.gov.sg/smesgodigital>) - "I am ICM Vendor" section for a list of supportable solution categories.

Questions Relating to GoSecure with Tools and Services

11. What are the subsidised tools and services that I can use to develop and deploy a cyber-secured solution?

Currently, the following categories of cybersecurity tools and services are available and supported for ICT SMEs' adoption and deployment: Source Code Review Tool, Security Advisory Services and Security Assessment Services.

These categories will be increased when more tools and services are available.

S/N	Categories	Type	What is it for?
1	Source Code Review	Tool	For analysing source codes to identify security flaws, bugs and defects

2	Security Assessment Services for Solutions	Services	For assessing applications, networks and system for vulnerabilities and security issues
3	Security Controls and Operations Advisory Services	Services	To receive expert advice on security issues resulting from insecure development practices in designing, coding and deploying solutions

12. How much grant subsidies can I get from using the pre-approved tools and services?

For eligible ICT SMEs, IMDA will provide a subsidy up to 80% of the costs of the pre-approved tools and services (or a cap of \$5,700 per application whichever is lower).

13. If I want to adopt more than one tool or service, can I submit multiple applications and receive multiple grant subsidies?

Yes, eligible ICT SMEs can submit multiple applications but the total maximum grant cap per ICT SMEs is \$30,000.

14. What is the process to apply for the grant?

To apply for the grant, interested ICT SMEs should:

- i. visit SME Portal's Tech Depot and view the list of pre-approved vendors under the [Productivity Solutions Grant \(PSG\) section \(under "Infocomm" sector\)](#)
- ii. contact the pre-approved vendors and obtain an official quotation
- iii. apply for PSG grant through the Business Grant Portal (BGP) at www.businessgrants.gov.sg

Upon submission of the grant application via the BGP, the application will be routed to IMDA for processing. Upon approval, grant applicant will receive a Letter of Offer informing them of the approved subsidy amount via the BGP.

Upon completion of the installation of tools or services rendered by vendors, ICT SMEs can proceed to submit requests for claim disbursement through BGP.

Questions Relating to Tech Capability Self-Assessment Tool

15. What is this Tech Capability Assessment Tool about? What are the objectives?

The Tech Capability Assessment Tool is developed by IMDA to help ICT SMEs raise their digital capabilities so that they can be more competitive in a Digital Economy. It is a self-assessment tool that allows you to:

- a) Understand your organisation's digital capabilities and uncover digital capability gaps
- b) Receive recommendations on how your organisation can bridge these capability gaps

The Tool was launched on 17 Oct 2019 for self-assessment on Cloud Native. We are launching the Tool to enable ICT SMEs to conduct self-assessment in the area of Cybersecurity with effect from 01 Jun 2020.

16. How long does it take to complete the assessment? Do I need to register to use the tool?

It would take about 10 – 20 minutes to complete the assessment for each capability area. You do not need to register to use the tool and IMDA does not collect any information from companies' usage of the tool. Please note that you would not be able to save the assessment if you exit the tool before completion.

17. Who is the most appropriate person to take this assessment?

This person should preferably be a Chief Technology Officer (CTO)/ Chief Information Technology Officer (CIO) or a Senior Management Executive with knowledge of your company or business in the following areas:

- Technical Architecture and Environment
- Technologies Applied or adopted
- Processes for Software Design, Maintenance & Deployment
- Culture and team, especially knowledge of your development team's technical skill sets and certifications

18. I am not an ICT SME (e.g. MNC, LLE), am I still able to take this assessment?

Yes, you may still use the tool to assess your organisation's digital capabilities. However, the results and recommendations may not be fully applicable.

19. What are the next steps after completing the assessment for Cybersecurity capability?

A self-explanatory assessment report will be available for immediate download upon completion. The report will provide an overall organisation-level capability proficiency level, broken down by the specific cyber security domains, and recommendations on the actions that your company can take to bridge the capability gaps (if any).

If you are interested to address the identified capability gaps in cyber security, you may:

- Visit [Tech Depot](#) website and check on the cybersecurity solution and service providers appointed under IMDA's GoSecure and SMEs Go Digital initiative to secure your products/services
- Consider sending your employees to relevant courses to expand their capabilities. These endorsed courses under CITREP+ programme can be found in [IMDA's SG:DIIM Talent portal](#)
- Follow the recommendations provided within the assessment report, which is specific to each company.

20. Will my organisation information be captured?

The assessment collects Personal Data in connection with the performance of the tool and the Personal Data provided will be processed in accordance with applicable laws. You will be asked to share information on your business or business activities such as business processes, methodologies, marketing, partnerships, strategies and revenue.

Respondents' identities and individual responses will not be collected within the assessment and the responses provided shall be used to create qualitative and insightful reports for respondents' use. Confidential information gathered will be aggregated, with other information known to us to perform industry analysis and comparison and will not be used for participation in any other IMDA or government related programmes and initiatives.