

**Provision of Publicity and Event Management Services for
Energy Efficiency and Conservation Publicity Campaign
Sub-theme 1 - Energy Efficiency Life Style**

Project 1.5 - Online e-Learning Platform for Publicity Works

1 ESSENTIAL REQUIREMENTS

**1.1 Professional Staff Requirements for Website Development Services
("WDS")**

All proposed project team members must be employees of the Contractor or the proposed Sub-Contractor(s).

The composition of the Contractor's project team must include at least the following roles who meet the requirements specified in the table below:

Roles	Quantity (Resident/ Non-resident)	Requirements
Web Manager	1	<ul style="list-style-type: none"> ● At least 8 years of IT experience (Notes 1 & 2) including at least 3 years of experience on IT project management within the past 10 years.
Web Designer	At least 1	<ul style="list-style-type: none"> ● At least 2 years of IT project experience (Notes 1 & 2) in a design role for websites within the past 10 years; and ● At least 2 live-run projects references on the experience in a design role for HKSAR Government websites within the past 5 years.
Web Developer	At least 1	<ul style="list-style-type: none"> ● At least 2 years of IT project experience (Notes 1 & 2) in a development role for websites within the past 10 years; and ● At least 2 live-run projects references on the experience in a development role for websites within the past 5 years.

Notes:

1. IT experience refers to the full-time involvement in IT job positions. The following are not taken as IT experience:
 - a. Time spent on full-time undergraduate or full-time postgraduate studies on IT;
 - b. Time spent on sandwich training in full-time undergraduate or full-time postgraduate studies on IT;
 - c. Sales or marketing of IT related products and services; and
 - d. Teaching of IT related subjects.
2. “Years of IT experience” is counted up to the Proposal Closing Date regardless of whether the date has been extended subsequently. Overlapping periods of experience will only be counted once.

The Contractor shall propose distinct members to meet each role as specified in Clause 1.1 for the project team.

1.2 Professional Staff Requirements for Security Risk Assessment & Audit Services (“SRAA”)

All proposed project team members must be employees of the proposed Sub-Contractor(s).

The composition of the Contractor’s project team must include at least the following roles who meet the requirements specified in the table below:

Roles	Quantity (Resident/ Non-resident)	Requirements
Manager	1	<ul style="list-style-type: none">● Minimum 8 years of IT experience (Notes 1 & 2) with at least 4 years to deliver IT projects on web-based applications / SRAA exercises for the HKSAR Government during past 20 years● At least 4 projects* in IT security risk assessment and audit with role as Manager during past 2 years before the Closing date;● At least ONE of the following recognised qualifications (with valid

		<p>certificates) related to IT security (as of the Closing date):</p> <ul style="list-style-type: none"> ■ Certified Information Security Professional (CISP; 註冊信息安全專業人員) from China Information Technology Security Evaluation Centre (CNITSEC; 中國信息安全測評中心); ■ Certified Information Security Member (CISM; 註冊信息安全員) from CNITSEC. ■ Certified Information Systems Security Professional (CISSP) from International Information System Security Certification Consortium (ISC)²; ■ Certified Information Systems Auditor (CISA) from Information Systems Audit and Control Association (ISACA); ■ Certified Information Security Manager (CISM) from ISACA. <p>* Project(s) shall be completed before the Closing date</p>
Security consultant	1	<ul style="list-style-type: none"> ● At least 4 projects* in IT security risk assessment and audit during past N years before the Closing date; ● Minimum four (4) years of IT experience including at least two (2) years of experience* in IT security risk assessment and audit during past 10 years before the Closing date; and ● At least ONE of the following

		<p>recognised qualifications (with valid certificates) related to IT security (as of the Closing date):</p> <ul style="list-style-type: none"> ➤ Certified Information Security Professional (CISP; 註冊信息安全專業人員) from CNITSEC; ➤ Certified Information Security Member (CISM; 註冊信息安全員) from CNITSEC; ➤ Certified Information Systems Security Professional (CISSP) from (ISC)2; ➤ Certified Information Systems Auditor (CISA) from ISACA; ➤ Certified Information Security Manager (CISM) from ISACA; ➤ ISO/IEC 27001 Lead Auditor from International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC); ➤ Global Information Assurance Certification (GIAC) Security Expert (GSE) from SANS Institute; ➤ Certified Ethical Hacker (CEH) from International Council of Electronic Commerce Consultants (EC-Council). <p>* Project(s) shall be completed before the Closing date</p>
--	--	--

Notes:

1. IT experience refers to the full-time involvement in IT job positions. The following are not taken as IT experience:
 - e. Time spent on full-time undergraduate or full-time postgraduate studies on IT;
 - f. Time spent on sandwich training in full-time undergraduate or full-time postgraduate studies on IT;
 - g. Sales or marketing of IT related products and services; and
 - h. Teaching of IT related subjects.
2. “Years of IT experience” is counted up to the Proposal Closing Date regardless of whether the date has been extended subsequently. Overlapping periods of experience will only be counted once.

The Contractor shall propose distinct members to meet each role as specified in Clause 1.2 for the project team.

2 GOVERNMENT STANDARDS, METHODOLOGIES AND QUALITY REQUIREMENTS

- 2.1 The Contractor shall comply with the following Government regulations, policies, standards, guidelines, methodologies and quality requirements:
 - a. Baseline IT Security Policy
 - b. IT Security Guidelines
 - c. Practice Guide for Security Risk Assessment & Audit
 - d. Practice Guide for Information Security Incident Handling
 - e. Practice Guide for IT Outsourcing
 - f. Practice Guide for Data Loss Prevention
 - g. Practice Guide for Destruction and Disposal of Storage Media
 - h. Practice Guide for Mobile Security
 - i. Practice Guide for Internet Gateway Security
 - j. Practice Guide for Website and Web Application Security
 - k. Practice Guide for Penetration Testing
 - l. The HKSARG Interoperability Framework
 - m. Web Content Accessibility Guidelines (WCAG) 2.2
 - n. Web Accessibility Handbook
 - o. W3C WCAG 2.2 Level AA in web accessibility standards
 - p. Common Look and Feel Guidelines and Design Specifications
 - q. CIS Web Hosting Services Usage Guidelines

- r. Technical Notes on Website Development and Maintenance
- s. Security Risk Assessment and Audit Guidelines
- t. Best Practices for Business Analyst
- u. Effective Systems Analysis and Design Guide
- v. The Government Technology and System Architectures (GTSA) Framework
- w. EMSD Departmental IT Security Documents

For Government websites, the Contractor needs to adopt mobile friendly design to provide good user experience with different devices (including desktop, notebook computers, tablets & smartphones) in accordance to the "Common Look and Feel Guidelines and Design Specifications".

- 2.2 Where necessary, the Contractor has to adopt adaptations to the methodologies and quality management system specified in Clause 2.1. The Contractor shall seek agreement from EMSD on any adaptations of the methodologies and quality management system that will be adopted for delivering the required services/products of this project. For all agreed adaptations, the Contractor has to document the reason why such adaptations are adopted in relevant quality records.

3 PROJECT DELIVERABLES, MILESTONES & IMPLEMENTATION SCHEDULE

The Contractor shall provide the project deliverables ("Deliverables") in Clause 2.1 which are based on the prevailing Government standards and methodologies that can be found at DPO's website:

https://www.digitalpolicy.gov.hk/en/our_work/digital_infrastructure/methodology/

3.1 Project Deliverables

- a. The Contractor shall provide a complete set of WDS Deliverables for this project. The major deliverables are listed below:
 - i. Management Products
 - Project Initiation Document ("PID") with detailed Project Plan;
 - Minutes of Project Steering Committee ("PSC") and Project Assurance Team Meetings; and
 - Highlight Reports if required by EMSD.
 - ii. Technical Products

- Webpage design options;
 - Implemented Webpages and Website;
 - Web Accessibility Assessment Report with successful compliance result; and
 - Source codes, original editable graphic, pictures, programs of the Website, and media files.
 - Handover list
- iii. Unless waived by EMSD, formal and informal reviews of the above products shall be conducted on a need basis throughout the course of the project; management presentations to EMSD shall also be conducted at the commencement of the project and for the user acceptance of the Webpage design options.
- iv. The Contractor is required to provide one softcopy for each product.
- b. The Contractor shall provide a complete set of SRAA Deliverables for this project. The major deliverables are listed below:
- Detailed project plan
 - General control checklists
 - Fallback/recovery procedures
 - A list of identified and valuated assets in the agreed scope
 - Security Risk Assessment Report
 - Completed general control checklist for Security Risk Assessment Report
 - Security Audit Report
 - Completed general control checklist for Security Audit Report
 - Presentation on security risk assessment and security audit
 - Follow-up plan
 - Verification report
 - Presentation on verification
- i. Unless waived by EMSD, formal and informal reviews of the above products shall be conducted on a need basis throughout the course of the project; management presentations to EMSD shall also be conducted at the commencement of the project and for the user acceptance of the Webpage design options.
- ii. The Contractor is required to provide one softcopy for each product.

3.2 Milestones and Implementation Schedule

- a. Upon receiving the Letter of Acceptance, the Contractor is required to commence the project on the date as specified in the Letter of Acceptance
- b. The WDS will tentatively be conducted for a period of 10 months. The Contractor shall propose a detailed timetable for the project and ensure that they are able to deliver the website and work closely with EMSD in accordance with the timetable.
- c. A high level timetable of the WDS is as follows.

Milestone / Major Task	Key Deliverable	End of Date
Stage 1 – Project Initiation		
● Project Initiation Meeting	● Project Initiation Document	End of 1 st month
Stage 2 – Website Design		
● Website Design Proposals	● Submission of three designs of visual mock-up of the website (including graphics, icons, user interface and screen flow) for EMSD's review	End of 2 nd month
Stage 3 – Website Development		
<ul style="list-style-type: none"> ● Website Development ● Document Conversion 	<ul style="list-style-type: none"> ● Website with full functions ready for UAT 	End of 5 th month
Stage 4 – User Acceptance & Cutover		
<ul style="list-style-type: none"> ● Security Compliance ● User Acceptance Test ● W3C WCAG compliance 	<ul style="list-style-type: none"> ● Implemented safeguards according to SRAA reports ● Web Accessibility Assessment Report ● Test plan, test cases, 	End of 9 th month

● Bug Fixing	test results and follow-up on the reported problems	
● Migration and Production Launch of Website	● Production Launch of W3C compliant website	
Stage 5 – Nursing and Tuning		
● System Nursing and Tuning (for 2-months)	● Issue log and fix plan	End of 10 th month
● Documentation on Setup or Installation	● Security incident handling procedures of the website.	End of 10 th month

- d. The SRAA will tentatively be conducted for a period of 12 weeks. The Contractor shall propose a detailed timetable for the project and ensure that they are able to deliver the website and work closely with EMSD in accordance with the timetable.

e. A high level timetable of the SRAA is as follows.

Milestone / Major Task	Key Deliverable	End of Date
Stage 1 – Project Initiation and Implementation		
<ul style="list-style-type: none"> ● Project Initiation Meeting ● Formation of project organisation ● Prepare detailed project plan 	<ul style="list-style-type: none"> ● Detailed project plan 	End of week 1
<ul style="list-style-type: none"> ● Prepare general control checklists and have them agreed upon by the concerned B/D ● Prepare fallback/recovery procedures before vulnerability tests ● Perform Asset Identification and Valuation 	<ul style="list-style-type: none"> ● General control checklists ● Fallback/recovery procedures ● A list of identified and valued assets in the agreed scope 	End of week 2
Stage 3 –Security Risk Assessment and Security Audit Common Tasks		
<ul style="list-style-type: none"> ● Conduct site visits and multi-level interviews, group discussion and surveys ● Perform general control review ● Perform vulnerability scanning ● Perform web penetration testing ● 		End of week 3

Stage 4 –Security Risk Assessment		
● Perform security risk assessment		End of week 4
● Compile Security Risk Assessment Report	<ul style="list-style-type: none"> ● Security Risk Assessment Report (includes: vulnerability scanning report; penetration testing report; and application source code review report) ● Completed general control checklist 	End of week 5
Stage 5 –Security Audit		
● Conduct compliance checking against S17 and Departmental Security Policy or policies that are relevant and within the scope of security audit		End of week 6
● Compile Security Audit Report	<ul style="list-style-type: none"> ● Security Audit Report (includes: vulnerability scanning report; penetration testing report; and application source code review report) ● Completed general control checklist 	End of week 7

Stage 5 –Follow-up Plan for Security Risk Assessment and Security Audit		
● Conduct presentation to report the findings of the security risk assessment and security audit	● Presentation on security risk assessment and security audit	End of week 8
● Develop a follow-up plan on recommendations with implementation schedule	● Follow-up plan	End of week 9
Stage 6 –Verification for Security Risk Assessment and Security Audit		
● Review the security status after implementation of safeguards		End of week 1 after implementation of safeguards
● Compile verification report	● Verification report	End of week 2 after implementation of safeguards
● Conduct presentation to report the findings of the verification	● Presentation on verification	End of week 3 after implementation of safeguards

4 ACCEPTANCE CRITERIA

4.1 The Government Representative will accept the WDS only if:

- a. the Contractor produces all agreed Deliverables for the services required, which have adhered to Government standards, methodologies and quality requirements stipulated in Clauses 3 hereof and to the satisfaction of EMSD; and
- b. the Contractor fulfils the acceptance criteria for the major project Deliverables as follows:

Milestone / Major Task	Key Deliverable	Acceptance Criteria
Stage 1 – Project Initiation		
● Project Initiation Meeting	● Project Initiation Document (“PID”)	PID accepted by EMSD
Stage 2 – Website Design		
● Website Design Proposals	● Submission of three designs of visual mock-up of the website (including graphics, icons, user interface and screen flow) for EMSD’s review	Design accepted by EMSD
Stage 3 – Website Development		
<ul style="list-style-type: none"> ● Website Development ● Document Conversion 	● Website with full functions ready for UAT	Website ready for UAT by EMSD
Stage 4 – User Acceptance & Cutover		
● Security Compliance	● Implemented safeguards according to SRAA reports	All security findings are effectively addressed and the safeguards are accepted by EMSD

<ul style="list-style-type: none"> ● User Acceptance Test ● W3C WCAG compliance ● Bug Fixing 	<ul style="list-style-type: none"> ● Web Accessibility Assessment Report ● Test plan, test cases, test results and follow-up on the reported problems 	<ul style="list-style-type: none"> ● The web accessibility conforms to W3C WCAG 2.2 ● All tests passed and EMSD users accept the testing result
<ul style="list-style-type: none"> ● Migration and Production Launch of Website 	<ul style="list-style-type: none"> ● Production Launch of W3C compliant website 	<ul style="list-style-type: none"> ● The website in production
Stage 5 – Nursing and Tuning		
<ul style="list-style-type: none"> ● System Nursing and Tuning (for 2-months) 	<ul style="list-style-type: none"> ● Issue log and fix plan 	<ul style="list-style-type: none"> ● System performance at a pre-defined acceptable level; all issues are logged with follow-up plan
<ul style="list-style-type: none"> ● Documentation on Setup or Installation 	<ul style="list-style-type: none"> ● Security incident handling procedures of the website. 	<ul style="list-style-type: none"> ● Documentation and security incident handling procedures accepted by EMSD

- 4.2 The Government Representative will accept the SRAA only if:
- the Contractor produces all agreed Deliverables for the services required, which have adhered to Government standards, methodologies and quality requirements stipulated in Clauses 3 hereof and to the satisfaction of EMSD; and
 - the Contractor fulfils the acceptance criteria for the major project Deliverables as follows:

Milestone / Major Task	Key Deliverable	Acceptance Criteria
Stage 1 – Project Initiation		
● Project Initiation	● Detailed Project Plan	Detailed Project Plan accepted by EMSD
Stage 2 –Security Risk Assessment and Security Audit Common Tasks		
● Security Risk Assessment and Security Audit Common Tasks	<ul style="list-style-type: none"> ● General control checklists ● Fallback/recovery procedures 	<ul style="list-style-type: none"> ● General control checklists accepted by EMSD ● Fallback/recovery procedures accepted by EMSD
Stage 3 –Security Risk Assessment		
● Security Risk Assessment	<ul style="list-style-type: none"> ● Security Risk Assessment Report ● Completed general control checklist 	<ul style="list-style-type: none"> ● Security Risk Assessment Report accepted by EMSD ● Completed general control checklist accepted by EMSD
Stage 4 –Security Audit		
● Security Audit	<ul style="list-style-type: none"> ● Security Audit Report ● Completed general control checklist 	<ul style="list-style-type: none"> ● Security Audit Report accepted by EMSD ● Completed general control checklist accepted by EMSD

Stage 5 –Follow-up Plan		
● Follow-up Plan	<ul style="list-style-type: none"> ● Presentation on security risk assessment and security audit ● Follow-up plan 	<ul style="list-style-type: none"> ● Presentation on security risk assessment and security audit accepted by EMSD ● Follow-up plan accepted by EMSD
Stage 6 –Verification		
● Verification	<ul style="list-style-type: none"> ● Verification report ● Presentation on verification 	<ul style="list-style-type: none"> ● Verification report accepted by EMSD ● Presentation on verification accepted by EMSD

- 4.3 The Government Representative will require in general up to ten (10) working days to consider each required Deliverable and, if it deems appropriate, to confirm the acceptance of the Deliverables. Allowance should be made in the proposed project plan for such activities.

5 HIGH-LEVEL WEBSITE REQUIREMENT SPECIFICATIONS

Title of the Website:

EnergyLand (能源資訊園地) or other name to be confirmed with ECC/EMSD

Language Selection Page:

Major supported languages for each webpage are Traditional Chinese, Simplified Chinese, and English. Additional supported languages on some webpages include Bahasa Indonesia, Tagalog, Urdu, Hindi, Punjabi, Nepali, Thai and Vietnamese, or other EM languages, if necessary. No more than 10 webpages each with their EM language versions would be required.

Style:

- Government's Common Look and Feel Standard
- Web Content Accessibility Guidelines 2.2 Level AA Standard
- Responsive web design

Font Size:

All text resizable up to 200% without the loss of content or functionality

Appearance: Professional, modern, visually engaging with interactive elements

Current Website Index for the EnergyLand thematic website:

- Energy Principles
 - What is Energy?
 - Forms of Energy
 - Energy Source
 - Use of Energy
 - Measuring Energy
- Energy and Environment
 - Limited Reserve
 - Pollutants
 - Global Warming
 - Greenhouse Gases
 - Energy Conservation
- Energy Use in Hong Kong, China

- The Energy Scene of Hong Kong, China
- Hong Kong Energy End-use Data
- Transportation and LPG Consumption
- Energy Consumption Indicators and Benchmarks
- Application of Renewable Energy in Hong Kong, China

- Energy Efficiency in Transport
 - Vehicle and the environment
 - Greener Fuel Vehicles
 - Electric Vehicles

- New and Renewable Energy
 - Solar Energy
 - Solar Thermal Energy
 - Solar Photovoltaic
 - Wind Energy
 - Biomass Energy
 - Energy from Waste
 - Hydro Energy
 - Tidal Energy
 - Wave Energy
 - Marine Current Energy
 - Ocean Thermal Energy Conversion (OTEC)
 - Geothermal Energy
 - Hydrogen
 - Hydrogen Economy
 - Fuel Cells
 - Fusion Energy

- Appliances and Energy Efficiency Equipment
 - Appliances
 - Energy Efficiency Labelling Schemes
 - Voluntary Energy Efficiency Labelling Scheme (VEELS)
 - Mandatory Energy Efficiency Labelling Scheme (MEELS)
 - Energy Efficient Equipment
 - Air-conditioning
 - Lighting
 - Lifts and Escalators

- Heat Pump
- Building
 - Energy Use in a Building
 - Water-cooled Air-conditioning System
 - District Cooling System
 - Conventional Air-conditioning System
 - District Cooling System (DCS)
 - Benefits of DCS
 - DCS in Other Countries
 - DCS in Hong Kong, China
 - Combined Heat and Power
 - Building Energy Codes
- Education
 - Energy Education Kits
 - Energy Saving Tips
 - Energy Efficiency & Conservation Outreach Programmes
 - Energy Audit and Carbon Audit
- Frequently Ask Questions
- Fun Zone
 - Games
- Useful Information
- Disclaimer
- Copyright
- Contact Us
- Sitemap

Note: The new structure of the new website is subject to discussion and confirmation with ECC/EMSD.

6 SERVICE REQUIREMENTS FOR SRAA

- i. The scope of services of SRAA are:
 - To evaluate the security risks of new online e-Learning Platform, the Contractor shall identify and recommend safeguards with the aim of strengthening the security protection of the system and the related data to an acceptable level.
 - A security audit will be carried out to determine the state of the existing protection and to verify whether the existing protection has been implemented effectively.
 - A verification process will be carried out to review the security status of the system(s) and data to ensure that all risks identified in the security risk assessment and security audit have been mitigated or reduced to an acceptable level.
- ii. The scope of the services shall cover the security areas and controls specified in Baseline IT Security Policy (S17), in particular the 14 areas listed in section 2.1 of S17.
- iii. The Contractor shall reference the documents listed in Clause 2 of Annex F-2 when performing security risk assessment and security audit.
- iv. Gather all relevant information such as security requirements and objectives, system and network architecture and infrastructure, evidence or supporting documents indicating that the physical environment of computer rooms meets the physical security requirements according to the classification of data resided, applications and servers information, access controls, identification and authentication mechanisms, policies and guidelines, operational processes, key generation and management procedure, etc. of the new website and/or the shared and common information systems by conducting site visits to user sites at EMSD Headquarter, Kai Shing Street, Kowloon, Hong Kong or any locations in Hong Kong specified by EMSD and perform multi-level interviews, group discussions, surveys, equipment and configuration checking etc.

- v. Identify and recommend the security requirements applicable to the new website. The Contractor shall make reference to the previous SRAA reports and related documents, prevailing Government security standards and industry practices whichever applicable and should provide explanation and justification for any recommendations that deviate from the references;
- vi. Perform general control review to identify any inadequacies in general controls being put in place for the current environment by examining the systems manually for their control and procedures which may include, but not be limited to, the following:
 - Departmental IT security organisation, in particular staff roles and responsibilities;
 - Management responsibilities;
 - IT security policies;
 - Human resource security, including security awareness training;
 - Asset management;
 - Access control, such as access privileges;
 - Cryptography;
 - Physical and environmental security;
 - Operations security;
 - Communications security;
 - System acquisition, development and maintenance;
 - Outsourcing security;
 - Security incident management;
 - IT security aspects of business continuity management; and
 - Compliance

A checklist to conduct the general control review should be prepared and be agreed upon by EMSD before the assessment or audit commence. The checklist must include tasks to check against departmental IT security policy and S17 policy Clauses that are relevant to and are within the scope of the assessment or audit. After assessment or audit, result of the checklist should be submitted to the concerned B/D. Reasons for not performing any tasks in the checklist must be provided. An example of the checklist can be found in Annex D of Practice Guide for Security Risk Assessment & Audit. This checklist is not intended to cover all aspects, but rather acts as a preliminary reference.

- vii. Perform vulnerability scanning at network, hosts, systems and applications which should at least cover the following where appropriate:
- Network level probing/scanning and discovery;
 - Host vulnerability tests and discovery;
 - System/application (including web system/application and mobile application) scanning;
 - Use Dynamic Application Security Testing (DAST) tool(s) for application vulnerability scanning to detect and identify conditions indicative of security vulnerabilities in their running state;

and prepare a vulnerability scanning report detailing the tests conducted and the test results upon completion of the tests. The system/application scanning shall also cover scanning of web systems and applications via the Hyper Text Transfer Protocol (HTTP), including HTTP Secure (HTTPS).

The Contractor shall also review whether patches or adequate compensating measures have been applied for all applicable known vulnerabilities including but not limited to all relevant security alerts issued by the Government Computer Emergency Response Team Hong Kong (GovCERT.HK).

- viii. Perform website/web application/mobile application penetration testing which should at least cover the following:
- Conduct manual penetration testing on IT Systems which covers the latest version of the top ten most critical web application security risks of the Open Web Application Security Project (OWASP) and SysAdmin, Audit, Network, Security Institute (SANS) (i.e. CWE/SANS Top 25; OWASP Top 10; OWASP Mobile Top 10 and etc.), logical flaws, error handling and system information leakage, file uploading and execution and input validation issues, and other areas as deemed necessary.
 - Perform application source code review with reference to at least the latest version of all most critical vulnerabilities of the OWASP and SANS(i.e. CWE/SANS Top 25; OWASP Top 10; OWASP Mobile Top 10 and etc.);
 - The penetration testing shall also cover all of the major application functions.
 - The penetration tests shall be carried out in external network from the position of a potential attacker, and can involve active exploitation of possible vulnerabilities. They should include, but not limited to, the

following security areas:

- Network Security;
 - System Software Security;
 - Client-side Application Security;
 - Server-side Application Security;
 - Physical Security;
 - Intrusion Detection; and
 - Incident Response
- Bring in all tools for the use of the testing and ensure that all hardware/firmware/software used in the testing is legal and properly licensed;
 - Log the actions taken with evidence (such as screen capture, generated network traffic or program logs), clean up and restore any changes that are made during the testing;
 - Explain and analyse the identified vulnerabilities for its likelihood and impact to the website/web application/mobile application as well as with a viable proposal for mitigation and a sound technical solution. Subject to the necessity, a proof of concept (POC) may be required to illustrate the effectiveness of mitigation measures for the identified risks; and
 - Prepare the penetration testing report detailing the test progress, the test results, and recommendation upon completion of the tests. Refer to Clause 7 and 8 for the required report content.

Before conducting the vulnerability scanning and/or web penetration testing, the Contractor should agree with EMSD on the scope, possible impact and fallback/recovery procedure. This should be based on the Business Continuity Plan and Disaster Recovery Plan if mission critical systems are involved.

- ix. Perform application source code review which should at least cover the following:
- Identify potential exploit and vulnerability in source code level;
 - Use Static Application Security Testing (SAST) tool(s) for identifying semantic and language security bugs and optimise the search for vulnerabilities and attack methods, including those identified by OWASP, SANS, and National Institute of Standards and Technology (NIST). The Contractor shall ensure that the tool(s) used for application source code review shall cover all the programming

languages as specified in Annex 6.

- Prepare application source code review report detailing the tests conducted and the test results with recommended rectification measures upon completion of application source code review;
- x. Perform risk analysis on every aspect which shall include, but is not limited to, the following:
- Human resource security;
 - Asset management;
 - Access control;
 - Cryptography;
 - Physical and environmental security;
 - Operations security;
 - Communications security;
 - System acquisition, development and maintenance;
 - Outsourcing security; and
 - IT security aspects of business continuity management
- to determine the value of the assets and their associated risks through the following processes:
- Asset identification and valuation;
 - Threat analysis;
 - Vulnerability analysis;
 - Asset/threat/vulnerability mapping;
 - Impact and likelihood assessment;
 - Risk results analysis;
- xi. Identify and recommend vendor neutral safeguards based on the results of risk analysis in order to reduce the likelihood and impact of identified threats and vulnerabilities to an acceptable level;
- xii. Provide technical advice for the implementation of the safeguards and elaborate clearly how the recommended safeguards can be implemented in EMSD's environment;
- xiii. Document the findings and results of the security risk assessment and vulnerability tests in a report ("Security Risk Assessment Report");
- xiv. Review and revise the relevant IT security policies, standards, guidelines and

procedures;

- xv. Conduct a presentation to EMSD to report the findings of the security risk assessment;
- xvi. Identify the inadequacies of existing IT security policies, standards, guidelines and procedures, and examine the effectiveness and completeness of the security controls being implemented;
- xvii. Identify and review relevant statutory, regulatory and contractual requirements;
- xviii. Check for conformance to existing security policies, standards, guidelines and procedures;
- xix. Document the findings and results of the security audit in a report (“Security Audit Report”);
- xx. Conduct a presentation to EMSD to report the findings of the security audit;
- xxi. Verify the security status after implementation of safeguards to ensure that all risks identified have been mitigated or reduced to an acceptable level with regard to the recommendations provided in the Security Risk Assessment Report and Security Audit Report;
- xxii. Ensure that the services provided have minimum impacts on the daily operation of EMSD and related parties;
- xxiii. Carefully schedule all activities (in particular for vulnerability tests) to avoid/minimise service interruption and agree with user on the schedule, possible impact and fallback/recovery procedure;
- xxiv. Provide the software and equipment, if necessary, for carrying out the tasks free of charge to the Government;

- xxv. Ensure that the security level of the system and network is not affected due to the installation and configuration of any necessary software and equipment. Remove those software and equipment and restore any necessary system and network configuration upon termination or completion of the work assignment such that the security level and the operation of the system and network is not affected; and
- xxvi. Ensure that no malicious software (e.g. computer virus, worm, Trojan horse program), backdoor or anything which would disrupt the operation or lead to compromise of any system is embedded in either the information or its storage media (e.g. in the form of data file, database, document, program code, e-mail, floppy diskette, hard disk, CD-ROM, Internet web page) when they are disseminated and/or exchanged with the Government.

7 CONTENT OUTLINE OF SECURITY RISK ASSESSMENT REPORT

The proposed outline and sample content of the Security Risk Assessment (SRA) report is shown below. The number inside the square bracket refers to the section number of this document.

Item	Section	Contents should include the followings, but not limited to:
1.	Introduction/ Background information	This is to describe the information regarding the events and user environment that has led to this assessment. Reference could be made to the Background section of Project 1.5 in Annex F.
2.	Executive summary	This is to provide executive summary of SRA exercise with identified vulnerabilities and recommended solutions worth-noting by senior management.
3.	Assessment scope	<p>This is to describe the purpose and nature of the assessment. The assessment scope should follow the Scope of the Services defined in the Clause 6.</p> <p><u>Specific requirements</u></p> <ul style="list-style-type: none"> For departmental SRAs which are often quoted as “all-encompassing”, the “Assessment scope” section should indicate a list of applications actually covered during the assessment, plus a list of shared and common information systems. [Clause 6 (i)]
4.	Assessment objective	This is to state the objectives for the assessment. The objective should follow the Project Objectives defined in Project Objectives section of Project 1.5 in Annex F.
5.	Assessment methodology	<p>This is to describe the methodology or approach adopted by the Contractor with an aim to meet the assessment objective.</p> <p><u>Specific requirements</u></p> <ul style="list-style-type: none"> The methodology should address the SRA related Service Requirements defined in the Clause 6. Typically, this will involve use of following techniques: site visits, general controls review, vulnerability scanning, web penetration

Item	Section	Contents should include the followings, but not limited to:
		<p>testing, application source code review etc.</p> <ul style="list-style-type: none"> For vulnerability scanning and web/mobile application penetration testing, a brief description of the testing process, tools, environment, date/ time, tester IP address, testing accounts, test data, should be included.
6.	Assessment time frame	<p>This is to describe the major activities, events and milestones for the assessment in chronological order.</p> <p><u>Specific requirements</u></p> <ul style="list-style-type: none"> Highlights on significant slippage or changes in project schedule compared to the Clause 4.2 should be provided with explanation.
7.	Assessment assumptions and limitations	<p>This is to describe any limitation or assumptions that are deemed relevant and reasonable to the assessment. The Contractor is expected to elaborate on the implication of each limitation or assumption.</p> <p><u>Specific requirements</u></p> <ul style="list-style-type: none"> The Contractor should include a list of applications or components of shared and common information systems deliberately <u>excluded</u> from the assessment. Any issues that might affect the validity of the results and any other unknowns or anomalies identified during vulnerability scanning and web penetration testing should be included.
8.	Current environment description	<p>This is to describe the system and data which has undergone security risk assessment such as its purpose, functions, services, constituent components, host systems and networking equipment, locations, external connections and interfaces etc. Reference could be made to the Current Environment Description section in the Project 1.5 in Annex F.</p>
9.	Security	<p>This is to specify any relevant Government IT security policy,</p>

Item	Section	Contents should include the followings, but not limited to:
	requirements	standards, guidelines and procedures referenced by the Contractor during the assessment. Reference could be made to the Clause 6.
10.	Risk assessment team	This is to describe the composition of the risk assessment team showing names, title, role and qualification. The Contractor should declare whether they meet the Professional Staff Requirements stated in Clause 1.2.
11.	Summary of risk assessment results	<p>This is to give a summary on the key findings or observations, their numbers, distribution, etc., covering all SRA related Service Requirements stated in the Clause 6</p> <p><u>Specific requirements</u></p> <ul style="list-style-type: none"> • Highlights of the Asset Identification and Valuation results. Detailed information for each identified asset should be listed under Annex D. • Highlights of the review of the relevant IT security policies, standards, guidelines and procedures • Overview of the risk assessment results, including highlights of key findings or statistical analysis of findings grouped by security domain or assessment method (e.g. general controls review and technical vulnerability testing).
12.	Risk analysis results & Recommended safeguards	<p>This is to provide a detailed account of the findings, risk analysis result and put forward recommendations on the root cause and the short term as well as long term solutions for each finding.</p> <p>Technical vulnerability testing (such as vulnerability scanning, web penetration testing and application source code review, etc.) results are consolidated and summarized here as “technical vulnerability findings” with risk analysis and recommended safeguards. The technical details are left to Annex B to Annex C of the SRA report.</p>

Item	Section	Contents should include the followings, but not limited to:
		<p><u>Specific requirements</u></p> <ul style="list-style-type: none"> • Risk analysis results should be documented with sufficient details, consultants are expected to indicate clearly: <ul style="list-style-type: none"> ♦ Asset (ID) affected; ♦ Asset value; ♦ Vulnerability; ♦ Threat; ♦ Impact; ♦ Likelihood; ♦ Risk rating; ♦ Recommended safeguards; and ♦ Management responses, if any <p>for each finding.</p> <ul style="list-style-type: none"> • The question list used to gather information during the course of the SRA should be attached under Annex A and cross-referenced to the general control findings documented above. • Cross-reference to the security requirements listed under Section 9 of the SRA report should be provided where appropriate for each finding. • For technical vulnerability findings, reference to Common Vulnerabilities & Exposures (CVE) database or vendor's security alert or patch alert should be provided if applicable. A Common Vulnerability Scoring System (CVSS) score should be assigned to each finding.
13.	Conclusions	<p>Overall conclusion for the SRA with regard to the project objectives, and the way forward.</p> <p><u>Specific requirements</u></p> <ul style="list-style-type: none"> • The Contractor should indicate a tentative date for the verification check on the SRA findings and the results

Item	Section	Contents should include the followings, but not limited to:
		will be documented in a separate Verification Report (The verification report should document the status of reported findings after the implementation of recommended safeguards, and if any further recommendation should be taken).
14.	Annex A	<p>Completed list of questions for SRA</p> <p>The question list used to gather information during the course of SRA should be attached in Annex A of the SRA report. A sample list of questions could be found under Annex A of the Practice Guide for Security Risk Assessment and Audit. The sample list of questions is not intended to cover all aspects, but rather acts as a preliminary reference. Contractor should tailor-made their question list if necessary.</p>
15.	Annex B	<p>Vulnerability scanning reports</p> <p><u>Specific requirements</u></p> <ul style="list-style-type: none"> • The scanning results must indicate a complete list of targets (e.g. network, hosts, systems, applications, devices, etc.) actually scanned/attempted, and the sampling criteria, where applicable, not just the ones with findings. • A verification checklist to ensure security patches / compensating measures have been applied for all applicable known vulnerabilities including but not limited to all relevant security alerts issued by GovCERT.HK.
16.	Annex C	<p>Penetration testing reports</p> <p><u>Specific requirements</u></p> <ul style="list-style-type: none"> • Executive summary of identified vulnerabilities and recommended solutions understandable by senior management;

Item	Section	Contents should include the followings, but not limited to:
		<ul style="list-style-type: none"> Website and web application description and its background information; Information about the test, including the date and time, tester IP address, if testing accounts are provided, any test data used; Scope of the test, including web pages and/or application functions covered and not covered, and the types of testing; Methodology, environment, tools, assumptions and limitations; Testing process highlighting any issues affecting the validity of the results and any other unknowns or anomalies in the test; Every finding with evidence, steps, risk level and Common Vulnerability Scoring System (CVSS) score; Recommendations on the root cause and the short term and long term solutions for each finding; and Name, role and qualifications of the testers.
17.	Annex D	Asset identification and valuation results
18.	Annex E	<p>Application source code review reports</p> <p><u>Specific requirements</u></p> <ul style="list-style-type: none"> Executive summary of identified vulnerabilities and recommended solutions understandable by senior management; Code base summary of scanned application source code; Rules signature used in the scanning; Every finding of issues found with category, detailed analysis results and affected source code snippets; and

Item	Section	Contents should include the followings, but not limited to:
		<ul style="list-style-type: none"> Recommendations on the fix for each finding.

8 CONTENT OUTLINE OF SECURITY RISK ASSESSMENT REPORT

The proposed outline and sample content of Security Audit (SA) report is shown below. The number inside the square bracket refers to the section number of this document.

Item	Section	Contents should include the followings, but not limited to:
1.	Introduction/ Background information	This is to describe the information regarding the events and user environment that has led to this security audit. Reference could be made to the Background section of Project 1.5 in Annex F.
2.	Executive summary	This is to provide executive summary of the SA exercise with identified deficiencies and recommended solutions worth-noting by senior management.
3.	Audit scope	This is to describe the purpose and nature of the audit. The audit scope should follow the Scope of The Services defined in the Clause 6. <u>Specific requirements</u> <ul style="list-style-type: none"> For departmental SAs which are often quoted as “all-encompassing”, the “Audit scope” section should indicate a list of applications actually covered during the audit, plus a list of shared and common information systems. [Clause 6 (i)]
4.	Audit objective	This is to state the objectives for the audit. The objective should follow the Project Objectives defined in Project Objectives section of Project 1.5 in Annex F.
5.	Audit methodology	This is to describe the methodology or approach adopted by the Contractor with an aim to meet the audit objective. <u>Specific requirements</u> <ul style="list-style-type: none"> The methodology should address the SA related Service Requirements defined in the Clause 6. Typically, this will involve use of following techniques: site visits, general controls review, vulnerability scanning, web penetration testing, application source code review etc.

Item	Section	Contents should include the followings, but not limited to:
		<ul style="list-style-type: none"> For vulnerability scanning and web penetration testing, a brief description of the testing process, tools, environment, date/ time, tester IP address, testing accounts, test data, should be included.
6.	Audit time frame	<p>This is to describe the major activities, events and milestones for the audit in chronological order.</p> <p><u>Specific requirements</u></p> <ul style="list-style-type: none"> Highlights on significant slippage or changes in project schedule compared to the Clause 4.2 should be provided with explanation.
7.	Audit assumptions and limitations	<p>This is to describe any limitation or assumptions that are deemed relevant and reasonable to the security audit. The Contractor is expected to elaborate on the implication of each limitation or assumption.</p> <p><u>Specific requirements</u></p> <ul style="list-style-type: none"> The Contractor should include a list of applications or components of shared and common information systems deliberately <u>excluded</u> from the audit. Any issues that might affect the validity of the results and any other unknowns or anomalies identified during vulnerability scanning and web penetration testing should be included.
8.	Description of Current environment	<p>This is to describe the system and data which has undergone security audit such as its purpose, functions, services, constituent components, host systems and networking equipment, locations, external connections and interfaces etc. Reference could be made to the Current Environment Description section in the Project 1.5 in Annex F.</p>
9.	Security requirements	<p>This is to specify any relevant Government IT security policies, standards, guidelines and procedures referenced by the Contractor during the audit. Reference could be made to the Clause 6.</p>

Item	Section	Contents should include the followings, but not limited to:
10.	Audit team	This is to describe the composition of the audit team showing names, title, role and qualification. Contractor should declare whether they meet the Professional Staff Requirements stated in Clause 1.2.
11.	Declaration of security auditor's independence	This is to declare that the security auditor was an independent and trusted party which was supposed to give a true, fair and objective view in an impartiality manner. Auditors did not audit their own work.
12.	Summary of audit results	<p>This is to give a summary on the key findings or observations, their numbers, distribution, etc., covering all SA related Service Requirements stated in Clause 6.</p> <p><u>Specific requirements</u></p> <ul style="list-style-type: none"> • Highlights of inadequacies and effectiveness of the existing policies, standards, guidelines and procedures. • Highlights of review results to the relevant statutory, regulatory and contractual requirements. [Section • Overview of the audit results, including conformance status or statistical analysis of findings grouped by security domain or audit method (e.g. general controls review and technical vulnerability testing).
13.	Detailed findings and recommendations	<p>This is to provide a detailed account of the findings, their conformance status and put forward recommendations on the root cause and the short term as well as long term solutions for each finding.</p> <p>Technical vulnerability testing (such as vulnerability scanning, web penetration testing, etc.) results are consolidated and summarized here as “technical vulnerability findings” with conformance status and recommended remedial actions. The technical details are left to Annex B to Annex C of the SA report.</p> <p><u>Specific requirements</u></p>

Item	Section	Contents should include the followings, but not limited to:
		<ul style="list-style-type: none"> Detailed findings should be documented with sufficient details, auditors are expected to indicate clearly: <ul style="list-style-type: none"> Relevant Clause(s) in the security document listed under section 9 of the SA report; Conformance status: partial, failed, or AOI; Detailed description of the finding; Recommended remedial actions; and Management responses, if any for each finding. Completed audit checklists should be attached under Annex A of the SA report and cross-referenced to the general control findings documented above. Cross-reference to the security requirements listed under Section 9 of the SA report should be provided where appropriate for each finding which breaches or conflicts with one of the policies or guidelines.
14.	Conclusion	<p>Overall conclusion for the SA with regard to the project objectives, and the way forward.</p> <p><u>Specific requirements</u></p> <ul style="list-style-type: none"> The Contractor should indicate a tentative date for the verification check on the SA findings and the results will be documented in a separate Verification Report. The Contractor should give an opinion on the overall compliance status against all security requirements listed under section 9 of the audit report.
15.	Annex A	<p>Completed audit checklist</p> <p>A sample audit checklist could be found under Annex D of Practice Guide for Security Risk Assessment & Audit. This sample checklist is not intended to cover all aspects, but rather acts as a preliminary reference.</p>

Item	Section	Contents should include the followings, but not limited to:
16.	Annex B	<p>Vulnerability scanning reports</p> <p><u>Specific requirements</u></p> <ul style="list-style-type: none"> • The scanning results must indicate a complete list of targets (e.g. network, hosts, systems, applications, devices, etc.) actually scanned/attempted, and the sampling criteria, where applicable, not just the ones with findings. • A verification checklist to ensure security patches / compensating measures have been applied for all applicable known vulnerabilities including but not limited to all relevant security alerts issued by GovCERT.HK.
17.	Annex C	<p>Penetration testing reports</p> <p><u>Specific requirements</u></p> <ul style="list-style-type: none"> • Executive summary of identified vulnerabilities and recommended solutions understandable by senior management; • Website and web application description and its background information; • Information about the test, including the date and time, tester IP address, if testing accounts are provided, any test data used; • Scope of the test, including web pages and/or application functions covered and not covered, and the types of testing; • Methodology, environment, tools, assumptions and limitations; • Testing process highlighting any issues affecting the validity of the results and any other unknowns or anomalies in the test; • Every finding with evidence, steps, risk level and

Item	Section	Contents should include the followings, but not limited to:
		<p>Common Vulnerability Scoring System (CVSS) score;</p> <ul style="list-style-type: none"> • Recommendations on the root cause and the short term and long term solutions for each finding; and • Name, role and qualifications of the testers.
18.	Annex D	<p>Application source code review reports</p> <p>Specific requirements</p> <ul style="list-style-type: none"> • Executive summary of identified vulnerabilities and recommended solutions understandable by senior management; • Code base summary of scanned application source code; • Rules signature used in the scanning; • Every finding of issues found with category, detailed analysis results and affected source code snippets; and • Recommendations on the fix for each finding.