



PROFILE SHEET WSP-G3-016

“WEB SECURITY EXPERT”

G3 Web Skills Profiles - version 2.0

Generation 3 European ICT Professional Profiles

Appendix to the official specification of 30 June 2014

Current version: <http://www.skillprofiles.eu/stable/g3/en/v2/profiles/WSP-G3-016.pdf>

Previous version: <http://www.skillprofiles.eu/stable/g3/en/v1/profiles/WSP-G3-016.pdf>

Latest version: <http://www.skillprofiles.eu/stable/g3/en/profiles/WSP-G3-016.pdf>

-
- Editor:**
- Pasquale Popolizio (Group coordinator [IWA Italy - Web Skills Profiles](#))
 - Roberto Scano (President [IWA Italy](#))
 - Simone Onofri
 - Claudia Spagnuolo

Copyright

The contents of this document are protected by a Creative Commons license [CC-01] “Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).

The names, marks, and logos mentioned in this document such as, for example, CEN, the name and mark of the IWA Italy association and the Certified Web Professional (CWP) mark are protected by current applicable laws. Therefore, all marks reported below belong to their legitimate owners; third party marks, product names, trade names, corporate and company names mentioned may be the marks of their respective owners or registered marks of other companies and are used purely for explanatory purposes and for the benefit of the owner, without any intent to violate current copyright laws.

Table of Contents

| | |
|--|---|
| Copyright | 1 |
| Table of Contents | 2 |
| Profile WSP-G3-016. Web Security Expert..... | 3 |
| Appendices..... | 6 |
| Appendix A. Glossary..... | 6 |
| Annex B. Profile sheet structure | 6 |
| Annex C. References..... | 7 |

Profile WSP-G3-016. Web Security Expert

This section is normative.

The profile sheet, listed below and described in appendix B, is an integral part of the document, "G3 Web Skills Profiles - version 2.0 - Generation 3 European ICT Professional Profiles", official specification of 30 June 2014" [WSPG3-03].

| Profile WSP-G3-016 | Web Security Expert |
|---------------------------|--|
| Summary statement | Professional position that analyses the reference IT context, evaluates, and proposes a suitable security policy to match corporate policies and the specific context. He or she is responsible for periodically verifying the security of the system and for conducting appropriate tests (e.g. Penetration Test). Additionally, he or she is in charge of education and awareness about security topics. |
| Mission | The Web Security Expert analyses the reference context, evaluates and proposes an appropriate security policy to be implemented in compliance with the corporate policies to protect applications, Web servers, data, and related processes. He or she analyses potential attack scenarios and defines the technical security requirements. He or she is responsible for verifying security during the various phases of developing a Web project and/or for various periodic verifications after release. He or she may personally implement the Security strategies by executing direct actions in various areas requiring protection such as architectures, networks, systems, or applications. |
| Deliverables | Accountable (A) <ul style="list-style-type: none">• Periodic reports of security test results. Responsible (R) <ul style="list-style-type: none">• Proposes user-driven maintenance and Change Requests that require the integration of new security controls. Contributor (C) <ul style="list-style-type: none">• Writing of the Security Risk Management Policy.• Writing of the Risk Management Policy.• Writing of the Disaster Recovery Plan.• Writing of the Digital Information Security Policy. |
| Main tasks | <ul style="list-style-type: none">• Periodically analyze the occurrence of potential security risks for the IT infrastructure and data: evaluate technical vulnerabilities, analyze the impact, and where necessary propose solutions. |

| | |
|-----------------------------------|---|
| | <ul style="list-style-type: none"> • Define the Recovery Plan to manage technical vulnerabilities and security risks, plan, support and approve recovery activities. • Help write the technical security section of the Disaster Recovery plan, so as to ensure security and operational continuity in the event of a disaster. • Monitor the security of the IT infrastructure and data: supervise the security team (if present), periodically conduct security tests (e.g. through Penetration Tests or denial of service attacks) and write the related Reports. • Train / educate / update the members of the organization about security issues. |
| E-CF competences | <ul style="list-style-type: none"> • C.2. Change Support: Level e-3. • C.3. Service Delivery: Level e-3. • D.1. Information Security Strategy Development: Level e-4. • D.9. Personnel Development: Level e-3. • D.10. Information and Knowledge Management: Level e-4. • E.8. Information Security Management: Level e-4. |
| Skills / Knowledge | <p>Technical</p> <ul style="list-style-type: none"> • Knowledge of international security standards (e.g. ISO 27001, ISO 22301). • Knowledge of national data protection standards (e.g. Italian Legislative Decree 196/2003) and sector regulations governing the application context (e.g. PCI-DSS). • Knowledge of security issues concerning IT networks (e.g. antivirus software and firewalls). • Knowledge of secrecy, encryption, authentication, non-repudiation, and data integrity issues (e.g. use of applications for secure authentication, secure password selection policies). • Knowledge of Vulnerability Assessment methods (e.g. ISECOM OSSTMM, OWASP). <p>Informatics</p> <ul style="list-style-type: none"> • Ability to harden processes, architectures, networks, systems, and applications. • Ability to use Techniques and tools for Vulnerability Assessment and Penetration Tests. <p>Strengthening</p> <ul style="list-style-type: none"> • Team Management. • Training. |
| Key Performance Indicators (KPIs) | <ul style="list-style-type: none"> • Security Policy Effectiveness. • Cost/risk Analysis. |

| | |
|---|--|
| | <ul style="list-style-type: none"> • Final impact of security incidents. |
| <p>Qualification / Certifications <i>(this section is informative)</i></p> | <ul style="list-style-type: none"> • European ICT Professional Profiles “ICT Security Specialist”. • ISECOM OPST/OPSA/OPSE. • OSCP. • eCCPT. • “CIW (Certified Internet Web Professional) - Security Specialist” Certification. • “CIW (Certified Internet Web Professional) - Security Professional” Certification. |
| <p>Attitudes (non ICT) <i>(this section is informative)</i></p> | <p>Interpersonal and Organizational</p> <ul style="list-style-type: none"> • Problem Solving. • Working to meet objectives. • Effective communication. • Team Leading. <p>Linguistic</p> <ul style="list-style-type: none"> • Good knowledge of the national language or the language used by the working group - minimum level: C1 QCER. • Good knowledge of the English language - minimum level: A2 QCER. |
| <p>Relationships / Reporting line <i>(this section is informative)</i></p> | <p>Interacts with:</p> <ul style="list-style-type: none"> • Web Business Analyst • Web DB Administrator • Frontend Web Developer • Server Side Web Developer • Web Server Administrator • Mobile Application Developer <p>Reports to:</p> <ul style="list-style-type: none"> • Web Project Manager |

Appendices

Appendix A. Glossary

Informational (informative)

for the purposes of information and not required for compliance.

Note: The content required for compliance is referred to as "normative".

normative

Required for obtaining compliance.

Note: Content listed as "informative" or "non-normative" is never necessary for compliance.

Annex B. Profile sheet structure

The Web skills profiles are identified by an unambiguous code and are structured in reference to paragraph 4.2 of the CWA CEN document, "European ICT Professional Profiles" [CWA-01] updated upon European e-Competence Framework 3.0 [CWA-02].

- **Profile Title.** Name - including the identification code - of the Web skill profile according to the unambiguous international catalogue from the IWA/HWG.
- **Summary statement.** Lists the primary purpose of the profile. The purpose is to give all stakeholders and users a brief, concise description of the specified Web skill profile, written in a form understandable by ICT professionals, managers, and Human Resources staff.
- **Mission.** Describes the basic assignment of the profile. The purpose is to specify the working role defined in the Web Skill Profile.
- **Deliverables.** Describes the documents produced by the job description as accountable (guarantee), responsible (support), and contributor (contribution).
- **Main tasks.** Provides a list of typical tasks carried out by the profile. A task is an action undertaken to achieve a result in a broadly defined context and contributing to the definition of the profile.
- **E-CF competences.** Provides a list of the skills necessary (taken from the e-CF references) to carry out the assignment. A skill is the outcome of the previous definition of the Profile and helps to differentiate profiles.
- **Skills / knowledge.** A list of abilities and knowledge necessary for the definition of the profile, subdivided into technical, informatics, and strengthening (improving abilities for the profile).
- **Key Performance Indicators (KPIs).** Based on KPI (Key Performance Indicators), the area of application of the KPI is a more generic indicator, consistent with the grade level of the overall profile. It applies for adding depth to the assignment.

- **Qualification / Certifications.** These are the recommended, but not essential, qualifications and certifications for carrying out the activities in the profile. However, these qualifications and certifications may be used for developing knowledge of specific skills within the profile. This section is for informational purposes.
- **Attitudes (non ICT).** A list of aptitudes supporting the abilities and knowledge, subdivided into interpersonal/organizational and linguistic. This section reports references to the QCER [CE-01], which promotes the understanding of specific language certifications. This section is for informational purposes.
- **Relationships / Reporting line.** A list of Web skills profiles and not with whom the profile discusses (relationships) or reports (reporting lines). This section is for informational purposes.

Annex C. References

| | |
|------------|---|
| [CC-01] | Creative Commons <i>Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)</i> http://creativecommons.org/licenses/by-sa/4.0/deed |
| [CE-01] | Council of Europe <i>Common European Framework of Reference for Languages: Learning, Teaching, Assessment (CEFR) (January 2002)</i> http://www.coe.int/t/dg4/linguistic/CADRE_EN.asp |
| [CWA-01] | CEN (European Committee for Standardization) <i>CWA 16458:2012 European ICT Professional Profiles updated by e -CF version 3.0 competences (March 2014)</i> http://relaunch.ecompetences.eu/wp-content/uploads/2013/12/EU_ICT_Professional_Profiles_CWA_updated_by_e_CF_3.0.pdf |
| [CWA-02] | CEN (European Committee for Standardization) <i>CWA 16234:2014 Part 1. European e-Competence Framework 3.0. A common European Framework for ICT Professionals in all industry sectors (March 2014)</i> http://ecompetences.eu/wp-content/uploads/2014/02/European-e-Competence-Framework-3.0_CEN_CWA_16234-1_2014.pdf |
| [WSPG3-01] | IWA (International Webmasters Association) <i>G3 Web Skills Profiles - version 2.0 Generation 3 European ICT Professional Profiles Official specification of 30 June 2014 (English version)</i> http://www.skillprofiles.eu/stable/g3/en/2013-06-30.pdf |