

SAP Security Assessment G-Cloud 15





TABLE OF CONTENTS

1	Service Overview	3
2	Business Need	3
3	Our Approach	3
4	Buyer Responsibilities	4
5	Service Management	5
6	Protection of Data	5
7	On-boarding and Off-boarding	6
8	Skills and Knowledge Transfer	6
9	Partnerships/Alliances	6
10	Vendor Accreditations/Awards	6
11	Sub-contractors	6
12	Business Continuity and Disaster Recovery	7
13	Pricing	7
14	Ordering and Invoicing	7
15	Termination Terms	7
16	Further Information	7



1 Service Overview

Online threats are increasing in numbers, diversity, and impacts. Organizations across all industries are implementing various applications and systems to drive mission-critical processes and becoming targets to opportunistic attacks. Likewise, ERP application vulnerabilities are also on the target lists of attackers. Citing the sensitivity of data stored and processed by these systems, exploitation of these vulnerabilities can lead to severe financial and reputational damages.

Many organisations experienced at least one ERP breach in the last 24 months. These organisations either lacked patching cadence, effective security operations, or a proper SAP risk management solution.

Securing SAP platforms demands a proactive approach. An effective Security Assessment and Security Management program helps to identify new threats, weaknesses in security configurations, and prioritizes SAP vulnerability remediations for mission critical SAP systems.

2 Business Need

SAP has become an integral part of intelligent enterprises where SAP applications are providing businesses a way to manage their various departments effortlessly. At the same time, the complex SAP systems need continuous monitoring to identify threats and vulnerabilities.

Key challenges faced by customers in maintaining an effective cybersecurity posture in the SAP landscape include:

- Gaining insight of vulnerabilities and threats in SAP application and database, including security (and compliant state)
- Preventing attackers from bypassing the segregation of duties (SoD) and authorization controls
- Handling risk of unsecure code or configuration and setting up continuous reporting on SAP cybersecurity posture
- Maintaining controls in a compliant state of SAP landscape and enforcing security baselines for SAP
- SAP ECC or SAP S/4HANA(r) landscapes

3 Our Approach

Capgemini provides a holistic solution to shield your systems from data breaches and potential losses through the following solution offerings for the SAP landscape:

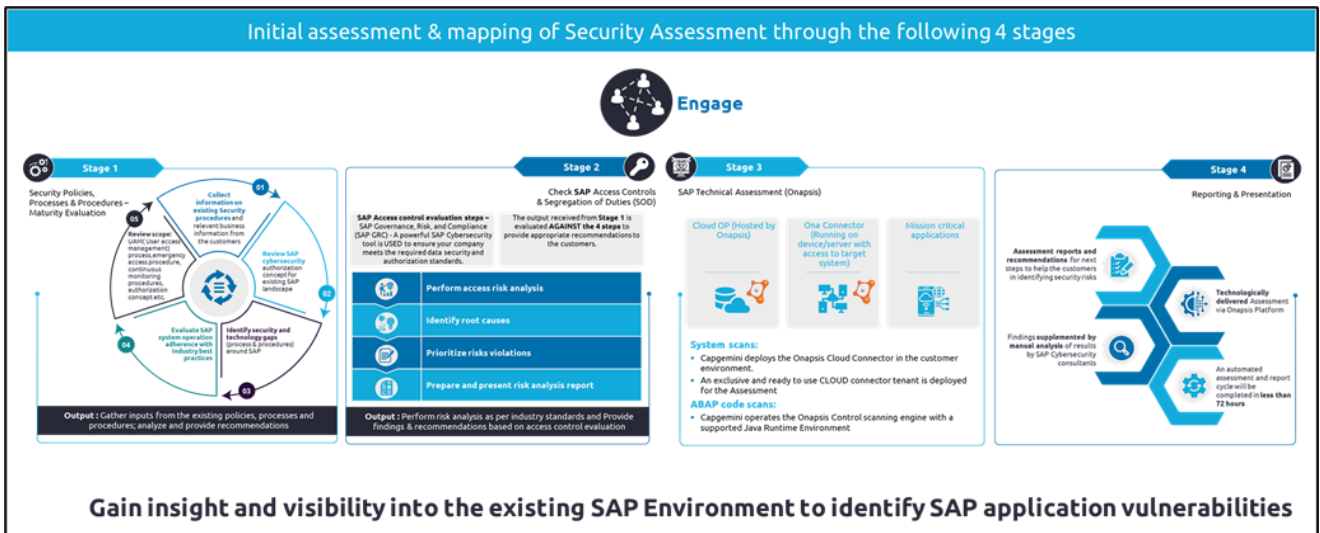
SAP Security Assessment

With Capgemini's SAP Security Assessment, we provide you with an assurance of safety. Our solution enables quick and real time insights with visibility into an existing SAP environment to identify system and application vulnerabilities by:

- Reviewing SAP cybersecurity process and procedures
- Evaluating SAP access control
- Identifying unpatched SAP applications
- Identifying weaknesses in application-specific security configurations and security gaps inherited within the existing custom ABAP codes
- Providing recommendations on changes required to secure systems



■ Reporting and presentation



SAP Security Management

Capgemini's SAP Security Management solution enables continuous monitoring and identification of new vulnerabilities in the SAP environment, laying the foundation to achieve patching cadence.

Our Security Management solution comprises of following key activities:

- Identifying new threats to the SAP environment
- Identifying weaknesses in application-specific security configurations on a continuous basis including Vulnerability Management in SOC/SIEM
- Analysing and prioritizing SAP vulnerability remediation
- SAP GRC access control risk analysis and remediation/mitigation
- Ensuring timely patching of SAP applications, verifying remediation, and producing executive reports
- Identifying security gaps in newly developed custom ABAP codes

4 Buyer Responsibilities

Please refer to the Supplier Terms listed with this service on the Platform. These may contain additional Buyer obligations/costs the Buyer is subject to that are not identified anywhere else in the Supplier's Application or on the Platform.

The Buyer responsibilities as part of this service are as follows:

- Buyer shall promptly notify Capgemini of an Incident.
- Buyer shall provide a concise description of the commands and procedures that reveal the Error and the operating environment, the specification of release and version of the applicable Product, a short description of the Error; examples of input, resulting output, expected output and any special circumstances surrounding the discovery of the Error.
- Buyer shall back up all data, files and information prior to Capgemini providing the Support Services.
- Buyer shall assume sole responsibility for any lost or altered data, files or information.
- Buyer shall ensure its Authorized Representatives have the requisite organizational authority, skill, experience and other qualifications to perform their obligations hereunder.



- Buyer shall run only the current release level of the Software made available by Capgemini (in case Capgemini is selling the Vulnerability Assessment, Vulnerability Management software, hereafter referred to as VA VM software).
- Buyer shall install all Maintenance Releases as soon as reasonably possible from the date they are made available by Capgemini (in case Capgemini is selling the VA VM software).
- Buyer shall provide Capgemini with all such cooperation and assistance as Capgemini may reasonably request, or otherwise as may reasonably be required, to enable Capgemini to perform the Support Services including, but not limited to reasonable, uninterrupted virtual access to Product(s); reasonable access to appropriate Customer personnel, including network, systems, operations and applications personnel; and all necessary authorizations and consents, whether from third parties or otherwise, in connection with any of the foregoing.
- Buyer shall certify that a Product is no longer in service no less than thirty (30) days prior to submitting a request to remove such Product from Support Services (in which event, all such licenses for the decommissioned Product shall be deemed null and void) (in case Capgemini is selling the VA VM software).
- Buyer shall ensure that its Customer Representatives are in completion of the applicable Capgemini training courses or equivalent training and experience. Customer shall not assign or transfer this Policy or any of the rights and obligations hereunder without Capgemini's prior written consent.

If these responsibilities do not match your expectations, then please contact us in order that we can explore options to vary our approach.

5 Service Management

Capgemini's service can be consumed in the following deployment and delivery models, all fully managed by Capgemini. Please contact us to discuss which of these fits your requirements. These are:

- **Offshore resources:** Our consultants work from our offshore locations. This provides a very cost-effective solution with access to a large pool of related skills.
- **Onshore resources:** Our consultants work from our UK offices. This provides a cost-effective solution for buyers that require UK delivery.
- **Dedicated resources:** Our consultants work on your sites, embedded as part of your team. This provides a solution for buyers that require skills augmentation and a high degree of control over the work.

6 Protection of Data

All data is handled in compliance with ISO 27001 and client-specific requirements. Sensitive information is encrypted in transit and at rest. Capgemini consultants are subject to rigorous background checks and confidentiality agreements.

Protection of Data - for Lot 1 and 2

If your service processes data and needs to consider protection of data you must retain the following paragraph (Delete if not applicable):

This service is based on a security classification of 'Official', however should you have a requirement for a different security classification that you would like us to consider, please contact us to discuss. Additional requirements this may be subject to additional Charges in accordance with the SFIA Rate Card.

Protection of Data - for Lot 3

If your service processes data and needs to consider protection of data you must retain the following paragraph (Delete if not applicable):



This service is based on a security classification of 'Official', however should you have a requirement for a different security classification that you would like us to consider, please contact us to discuss.

7 On-boarding and Off-boarding

Use the following wording (if you feel that this does not fit with your offer please contact the G-Cloud Team for advice):

Capgemini shall undertake on-boarding and off-boarding activities agreed within the Order Form (including as a minimum an exit plan in line with the Call-Off Contract terms) which will be charged for in accordance with the Pricing section for this service.

8 Skills and Knowledge Transfer

Capgemini recognises that skills and knowledge transfer is a critical element in the provision of G-Cloud services to public sector clients. Where possible and applicable, this forms part of the delivery plan for the service agreed at the start of the engagement. Our consultants and engineers are experienced in providing skills and knowledge transfer for major private and public sector clients.

Where appropriate, we may use a standard approach, tailored to topic, skills-gap and individual, to ensure consistency and effectiveness. The approach, Capgemini's Assess-Plan-Implement framework, has been used repeatedly by our teams to structure the work involved in transferring skills and creating new teams capable of driving and sustaining change long after the end of the formal programme. The framework can be applied throughout a project to understand knowledge transfer objectives, plan training delivery methods and materials, and deliver and evaluate success.

9 Partnerships/Alliances

We have partnered with industry leaders such as SAP, Onapsis, Security Bridge, Google Cloud, Microsoft Azure and AWS. We will leverage our partner relationships to provide you with a high level of service.

10 Vendor Accreditations/Awards



For the 13th year in a row, Capgemini has been recognised as one of the World's Most Ethical Companies® by the Ethisphere® Institute. This is an acknowledgement of our ethical culture that makes us an employer of choice and responsible player in the eyes of our clients, shareholders, and the wider community.

Our team holds certifications including SAP Security, ISO 27001, CISSP, and CISM. Capgemini is recognised globally for ethical business practices and technical excellence.

11 Sub-contractors

Capgemini UK may use the following subcontractors to deliver this service:

- Capgemini Technology Services India Limited.

Only include other, non-India sub-contractors that this service cannot be delivered without - if we do include them we must complete onerous documentation for those sub-contractors as part of our Tender for a place on the G-



Cloud framework. If there are none, please remove this purple guidance note and the section. **Note:** we can agree to use other sub-contractors at any time by declaring them in a proposal and including them in our Call-Off Contract.

12 Business Continuity and Disaster Recovery

No disaster recovery plan is provided as part of these Services.

13 Pricing

This service is priced in accordance with the Rate Card attached. Capgemini can also provide offshore resources at reduced rates where appropriate. Projects can be priced either on a Time & Materials or Fixed Price basis.

14 Ordering and Invoicing

Please refer to the Supplier Terms for this service.

We would be pleased to arrange a call or meeting to discuss your requirements of our service in more detail.

15 Termination Terms

Please refer to the Supplier Terms for this service.

16 Further Information

For more information about this or any of our G-Cloud services, please contact our Public Sector Team.

Phone: 0370 904 4858

Email: publicsector.opps.uk@capgemini.com including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.



About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

Make it real. | www.capgemini.com



This presentation contains information that may be privileged or confidential and is the property of the Capgemini Group.

Copyright © 2026 Capgemini. All rights reserved.