SSPA INDEPENDENT ASSESSMENTS FOR MICROSOFT SUPPLIERS

In today's digital age, strong privacy and security practices are paramount for businesses.

Without the right safeguards in place, businesses may be exposing themselves and their customers to significant risks that can result in severe financial and reputational consequences.

To address these risks, Microsoft has developed a set of requirements and practices, Supplier Security and Privacy Assurance (SSPA), which all vendors of their information supply chain are required to comply with. As such, any supplier who wishes to conduct business with Microsoft needs to have a deep understanding of SSPA and how it applies to their business.

To assist, we've answered several key questions regarding SSPA requirements and as Microsoft's Preferred Assessor, how BDO can help and guide you through this process.

WHO MUST COMPLY WITH SSPA?

Any supplier that processes what Microsoft defines as Microsoft Personal Data or Microsoft Confidential Data must fulfil specific compliance requirements within SSPA. The level of those requirements, however, depends on the type of data the supplier processes while providing services to Microsoft and how that data is processed.

According to Microsoft, "processing" is any operation or set of operations that are performed on any Microsoft Personal Data or Microsoft Confidential Data. This can include collecting or altering data, transmitting it to a third party, erasing or storing it, and several other uses.

WHAT IS 'MICROSOFT PERSONAL DATA' UNDER SSPA?

Microsoft Personal Data is any personal data that is processed by, or on behalf of Microsoft. Data is considered personal if it is linked or linkable to the individual, meaning that the data can be used directly or indirectly to identify someone.

WHAT IS 'MICROSOFT CONFIDENTIAL DATA' UNDER SSPA?

Microsoft Confidential Data can be defined broadly as any information about Microsoft that a supplier knows because of its business relationship with Microsoft and that the general public would not know. This includes items that are obviously sensitive, such as corporate financial data and trade secrets shared under a non-disclosure agreement.

HOW CAN BDO HELP?

As a Microsoft Preferred Assessor, BDO helps current and prospective Microsoft suppliers meet Supplier Security and Privacy Assurance (SSPA) program requirements as they seek to initiate or renew contracts. Our team of experienced data privacy and security professionals is equipped and trusted by Microsoft to counsel clients throughout each stage of the SSPA compliance process.

By leveraging BDO's full suite of cyber security and data privacy services, we can help you understand the evolving SSPA program, educate and coach on security and privacy gaps, and maximise your Independent Assessment engagement to support ongoing data protection efforts beyond SSPA.

We have worked with companies of all sizes to help them comply with SSPA and strengthen their security practices. We understand that the steps a supplier takes to meet the SSPA requirements are not a one-size-fits-all proposition. Based on a detailed assessment of each supplier's current practices and business objectives, we identify any gaps that need remediation and recommend

WHAT IS AN SSPA PREFERRED ASSESSOR?

A Preferred Assessor is a company that has been vetted by Microsoft's procurement department to perform an independent assessment against Microsoft's Data Protection Requirements. These companies understand the Microsoft SSPA program, will provide competitive pricing, and are qualified to perform an SSPA assessment.

OUR PROCESS FOR SSPA INDEPENDENT ASSESSMENTS

Four to eight week timeline.

1. BDO collaborates with Supplier to determine scoping, pricing, and timing of Independent Assessment
2. BDO schedules Independent Assessment inquiry and artifact inspection dates
3. BDO provides Supplier with BDO's SSPA Client Collaboration Tool, a preliminary artifact request list, and an inquiry request list
4. BDO performs Independent Assessment inquiries and artifact inspections (can typically be performed remotely)
5. BDO provides a list of identified compliance gaps for Supplier's remediation (as needed) and an updated list of artifacts needed to complete the Independent Assessment
6. BDO completes Independent Assessment artifact inspections
7. BDO performs final follow-up inquiries based on completed artifact inspections (as needed)
8. BDO provides Supplier with Independent Assessment Letter
9. Supplier provides Independent Assessment Letter to Microsoft
10. BDO is available throughout the year for ongoing support and questions regarding SSPA compliance

ASSESSMENT SCOPING AND PRICING

Accurately scoping your SSPA Independent Assessment is critical for a successful engagement. Additionally, engagement pricing is heavily dependent on the scale and scope of services you supply to Microsoft.

Key considerations for scoping include:

- Breadth of requirements applicable per Microsoft-approved DPR self-attestation
- Number of Microsoft Supplier IDs requiring an Independent Assessment
- Number of current SOWs that involve the Processing of Personal and/or Microsoft Confidential data
- Complexity of services performed for Microsoft
- Complexity of information systems involved with the Processing of Personal and/or Microsoft Confidential data
- Maturity of data privacy and security posture.

"…Often times, SSPA Independent Assessments and the DPR are intimidating, especially for a smaller company like ours, but BDO made us feel informed, comfortable, and confident. We truly could not be more grateful for BDO's experience, friendliness, and organization and we highly recommend them to anyone looking for a company to complete their independent assessment."

HEATHER ZINDEL,
CEO, Bloom Consulting Group
CORISSA CRUZEN,
Project Manager Intern, Bloom Consulting Group

MARK GRIFFITHS
Partner,
Risk Advisory Services

MORE INFORMATION

1300 138 991 www.bdo.com.au

NEW SOUTH WALES • NORTHERN TERRITORY • QUEENSLAND • SOUTH AUSTRALIA • TASMANIA • VICTORIA • WESTERN AUSTRALIA