Cybersecurity in M&A:
A Checklist for Evaluating M&A Platform Security

Formal Audits and Certifications

Vendors should comply with all required certifications and undergo routine audits to ensure compliance at every level.

- □ Does the vendor have their own ISO 27701 Information Security Management System certification?
- □ Did a trusted and reputable auditor provide the ISO certification?
- □ Has the vendor already secured ISO certificates? (As opposed to 'working on' securing them – this may be detrimental to your program's overall security systems.)
- □ Is the vendor using its own certifications (rather than a hosting provider's e.g., AWS, Azure) to ensure compliance?
- □ Can the vendor provide comprehensive audit reports upon request?

Technical Audits

Technical audits are essential in protecting against external threats.

- □ Does the vendor use third-party (OWASP or similar) firms to conduct regular penetration tests?
- □ Does the vendor comply with GDPR and similar regulations in the United States (e.g., CCPA)?
- □ Does the vendor use third-party (OWASP or similar) firms to conduct regular penetration tests?
- □ Does the vendor provide unredacted penetration tests for your review?*
- □ Does the vendor allow you to conduct your own penetration tests?

**Note that printouts from some online analysis tools (e.g., Qualys) may be indicative but provide only a superficial (and sometimes misleading) picture of the vendor's level of information security.*

Application Security

Questions to discern the vendor's competence and reliability in the marketplace.

- □ Does the vendor allow you to conduct your own audit?
- □ Can the vendor verify its key claims with artifacts?
- □ In the absence of a complete security review and/or audit, can you speak to the vendor's CICO to ascertain the organization's level of competence?
- □ In lieu or in support of your own security audit, can the vendor provide its publicly available security information? (e.g., Cloud Security Alliance (CSA) Star database, Privacy Shield.)
- □ Does the vendor have military contractors, financial service institutions, or security software vendors as current customers?*

** Customers in these industries typically perform in-depth security reviews. Organizations like these can benchmark the competence and quality of the vendor's security programs.*

Software Development Practices

Review the vendor's coding practices to ensure security and compliance with best practices.

□ Does the vendor have documented SDLC processes that take security into account?

□ Does the vendor follow OWASP secure coding practices?

□ Did the vendor utilize vulnerability scanners and SAST tooling during development?

□ Does the vendor perform both manual and automated testing in their software development?

Operational Security

Review operational security measures to determine how securely the vendor develops their software.

□ Does the vendor require employee background checks?

□ Are internal employees developing the vendor's software, rather than an outsourced development team?

□ Is the development team located in a country with strict legal infrastructure, governance, and low corruption?

□ Does the vendor have a robust development team to ensure expertise, resiliency, and availability of support?

Midaxo