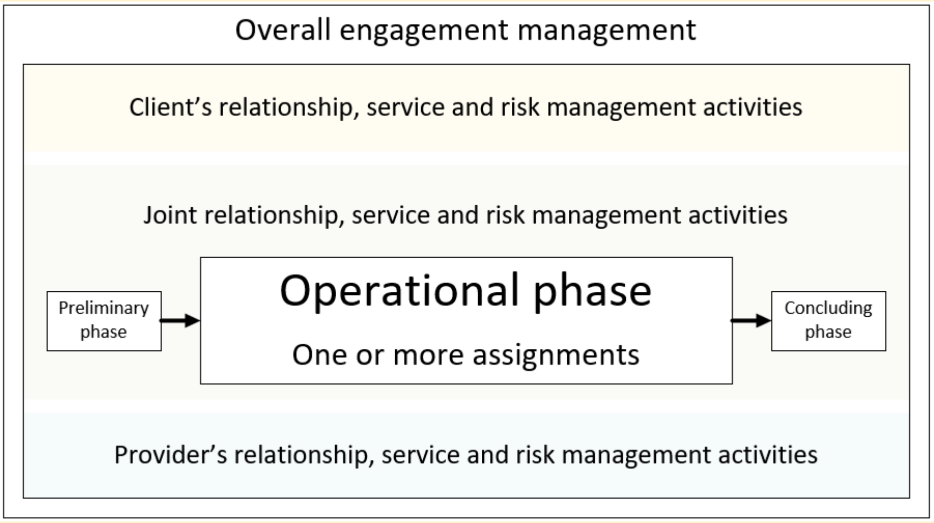
Information security checklists for professional services

May 2022

These checklists are designed to help clients and providers address information risks at each phase of a typical professional services engagement.


Overall engagement management
Client's relationship, service and risk management activities
Joint relationship, service and risk management activities
Preliminary phase
Operational phase
One or more assignments
Concluding phase
Provider's relationship, service and risk management activities

Further guidance is available in the SecAware [Information security guideline for professional services]

Preliminary phase checklist

Professional services clients and providers can use this checklist as a prompt to identify, consider and address relevant information risk, security and privacy aspects at the commencement of a professional service relationship, determining and agreeing the commercial/working arrangements prior to the operational service provision phase.

- □ Use applicable policies, procedures, checklists etc. (including this one!)
- □ Clarify roles and responsibilities for whoever should be involved in the present and subsequent phases (e.g. sales and procurement, information risk and security, management, legal), and inform or engage them
- □ Identify, consider and evaluate any significant information risks relating to the proposed professional service, alongside commercial, compliance and other risks
    - ○ Focus on potentially significant, damaging incidents, and the associated threats, vulnerabilities and impacts
    - ○ Consider obligations to third parties e.g. the principals or data subjects for any personal information, and the stakeholders or owners of valuable or sensitive information in general
    - ○ Specify key controls as appropriate
    - ○ Ensure that the associated costs are factored into any commercial arrangements (e.g. time required to prepare and review progress reports, hold relationship or risk management meetings, and deal with concerns, issues or incidents)
- □ Specify whatever information security, privacy, compliance or other controls are required to mitigate key risks at the appropriate level of detail, covering key elements explicitly if appropriate
- □ Consider the risks arising from the need to disclose details such as service requirements or features, if appropriate pre-qualifying potential counterparties, entering into preliminary nondisclosure agreements, seeking assurances or limiting or delaying the information provided until there is sufficient trust between the parties (e.g. talking in generalities, expressing certain aspects discreetly and verbally rather than in writing)
- □ Clarify relationship and assignment management arrangements (e.g. regular client-provider meetings, progress reports, periodic invoicing, escalation paths to raise and resolve service issues)
- □ Discuss relevant risks and controls both internally and with counterparties, clarifying and completing any actions arising
- □ Conduct due diligence checks e.g. provide and take-up references, validate claimed qualifications, certifications, solvency etc.
- □ Ensure that relevant aspects are incorporated appropriately into the contract, including the information risk, security and privacy elements of performing, measuring/monitoring and managing the relationship, handling changes, notification and dealing with incidents, and requirements at the conclusion of the assignment or relationship (e.g. persistent obligations towards confidentiality and privacy)
- □ Prepare financial estimates, quotations, budgets etc. and if necessary seek management authorization
- □ Execute (sign) the contract and archive a definitive copy

Operational phase checklist

This checklist covers information risk, security and privacy-related activities during the main operational phase of a professional services engagement when the services are being delivered and used/consumed.

During an extended engagement, possibly involving a succession of assignments, it may be worth revisiting this checklist periodically (e.g. once a year or once per assignment), reviewing the information risks and associated management arrangements and controls.

- □ Comply with contractual and other applicable obligations such as laws, policies, standards and professional codes of conduct
- □ Operate, manage, maintain and monitor appropriate information security and privacy controls, particularly any key controls specified in the contract or agreement
- □ Maintain vigilance and awareness towards information risk, security, privacy, compliance and related matters
- □ When appropriate (e.g. after several months or if there are concerns, issues or incidents), review information risks associated with the engagement and assignment/s, if appropriate updating the controls
- □ Report and be prepared to respond promptly and appropriately to potential concerns, issues or incidents, such as ignorance, carelessness, accidental or inappropriate disclosures, incompetence, non-compliance or fraud
- □ Escalate anything significant to your senior management, and if authorized also to the counterparty’s management or to relevant third parties
- □ Maintain the focus on information risk and related matters, perhaps gently or more forcibly reminding participants of their responsibilities as appropriate
- □ Participate willingly in reviews, audits and re-assessments of information risk-related matters, changing priorities etc.
- □ Look for opportunities to maximise the value derived from or generated by the relationship and assignment, such as avoiding or cost-effectively mitigating unacceptable information risks

Concluding phase checklist

This checklist concerns information risk-related activities at the conclusion of a professional services assignment or relationship, and thereafter.

□ Recover tangible information assets (IT equipment, storage media and documentation) from the counterparty if possible, seeking adequate assurance that remaining information assets have been securely destroyed

□ Recover or disable site access passes, passwords etc. from the counterparty

□ Remind everyone involved of their persistent professional, contractual and ethical obligations, plus any licensing or similar arrangements protecting information generated or exchanged during the assignment

□ Organise a post-relationship review to draw out lessons for the future, embodying them into strategies, policies, procedures, training and awareness materials

□ Maintain contact with the counterparty in case of issues, incidents or opportunities for further business, if applicable