Information security guideline for professional services

February 2023

Summary

This generic guideline encourages professional services providers and clients to identify, evaluate and address information risks relating to engagements. It offers information security, privacy, governance and other controls to mitigate unacceptable information risks. Pragmatic guidance and checklists make this guideline worthwhile even for small organisations.

Contents

1 Introduction

'Professional services' involve the provision of advice and guidance by competent and experienced specialists to their business clients or customers. The umbrella term 'consulting' encompasses a broad range of information-centric professional services such as:

- Building and construction services *e.g.* architecture, surveying;
- Business services *e.g.* marketing and sales, strategy and management consulting, auditing, quality consulting;
- Engineering services *e.g.* electrical and electronic design, materials science, measurement and calibration;
- Financial services *e.g.* book-keeping and accounting, plus investment, tax and insurance advice;
- Human resources services *e.g.* recruitment, employment disputes, mentoring and training;
- Information technology and telecommunications services *e.g.* Internet services, cloud computing, technical support, outsourced development, datacentre facilities;
- Legal services *e.g.* commercial and family law, contracting, compliance, forensics, prosecution and defence, intellectual property protection;
- Security services *e.g.* information risk and security consulting, IT auditing, digital forensics, background checking, surveillance;
- Other specialist advice and information processing services.

Through one or more assignments, jobs, projects, activities or tasks within an engagement, professional services clients and providers exchange, generate and utilise valuable and often sensitive information.

Information is the raw material and work product of the engagement.

This guideline takes a risk-based approach, advising both clients and providers to identify, evaluate and treat (address, deal with) information risks relating to or arising from professional services, proactively (meaning systematically, deliberately and explicitly).

It suggests a range of information security, privacy, governance and other controls to mitigate unacceptable information risks using practical, conventional and well-proven measures that are applicable to all types and sizes of organisation. Simple, straightforward guidance and checklists cover three main phases of a professional services engagement, making this guideline eminently pragmatic and worthwhile even for small and medium-sized organisations that do not employ specialists in this area.

2 Scope

This guideline suggests information security controls to mitigate unacceptable information risks associated with the provision of professional services in the business context.

The guideline concerns the information risk-related aspects of the service provision and management, regardless of the information content of the professional services provided. It does not concern the particular legal, financial, IT, medical, engineering or other specialist advice given by professional service providers to their clients, for instance. It concerns the manner in which such advice is sought, provided, managed and used, in order to protect both parties and perhaps others

against unacceptable information risks. It focuses on the information risks and related matters such as information security and privacy controls, governance, compliance and ethics, in the course of a professional services engagement.

This is a generic guideline, applicable to a wide range of organisations and situations. The simple checklists offering straightforward, pragmatic advice (appended) are particularly useful for smaller organisations providing or obtaining professional services *without* the dedicated resources typical of large, mature organisations.

As well as conventional consultancy-type assignments, the guidance has some relevance to:

- Long-term professional services where a distinct organisation is contracted to perform a corporate function on behalf of the client organisation and perhaps others (insourcing and outsourcing);
- Regular/routine and flexible, sporadic, *ad hoc* or supplementary assignments, including call-off arrangements where a specialist person or team is contracted or retained to provide professional services as and when required, often at short notice *e.g.* incident response and forensic services;
- Professional services provided internally by specialists within an organisation or group structure to colleagues *e.g.* IT, HR, Internal Audit, Information Risk and Security;
- Non-commercial arrangements, not-for-profit assignments and informal or voluntary arrangements *e.g.* charity and *pro bono* work such as mentoring.

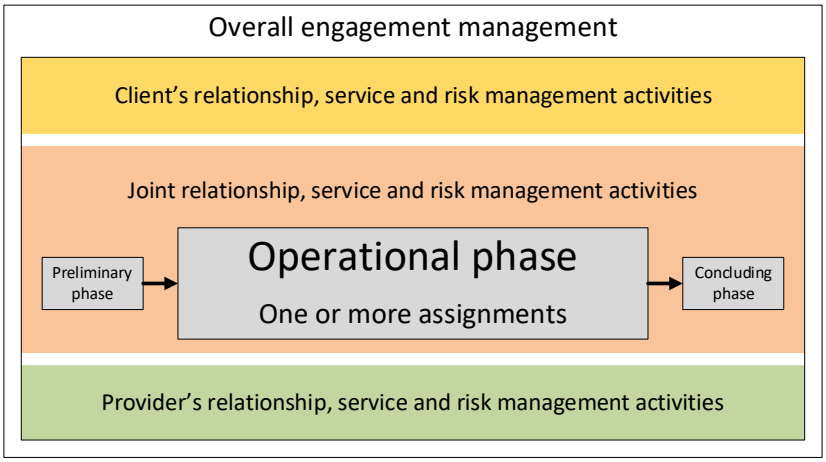
3 Defined terms

Term	Definition
Client and provider	The acquirer of professional services is known as the 'client', and whoever delivers professional services is the 'provider'. Such services may be formal or informal, commercial or non-commercial (*e.g.* voluntary) in nature. Similar terms such as 'acquirer' or 'customer' may be preferred. The client and provider may be employed by distinct organisations, or by different parts of the same or a related organisation (*e.g.* different departments, functions, business units or companies within a group structure). Either party may be acting in a personal or informal capacity rather than working on behalf of, through or representing an organisation.
Assignment	This guideline uses the generic term 'assignment' to mean a discrete item or packet of work within a professional services engagement. Similar terms such as 'job', 'gig', 'project' and (confusingly) 'contract' may be preferred.
Contract	This guideline refers to the agreement between provider and client regarding professional services as the 'contract', implying a legally-binding document. For some business services, engagements or assignments, it may be an 'agreement', perhaps a verbal, informal, casual or implicit 'understanding' between the parties.

4 Background and overview

4.1 Professional services engagement lifecycle

This guideline addresses three key stages in the course of a typical engagement – a business relationship between professional services client and provider – plus the client and provider's management activities throughout the engagement ▶



The simplified professional services engagement model disregards complexities such as:

- Professional services that are provided through mechanisms other than the systematic approach described in this guideline, including diffuse assignments without clearly delineated beginnings and endings, sporadic assignments (*e.g.* individual consultancy assignments or forensic investigations within an overall 'service', 'umbrella' or 'call-off' contract) and informal arrangements (perhaps without contracts or agreements);
- Professional services that are provided or acquired by multiple organisations or people working together (collectively or collaboratively) or independently (*e.g.* professional advisors working on discrete stages or elements of a single client project or initiative);
- Extended engagements - persistent relationships in which individual work assignments overlap or follow-on in succession;
- Engagements, relationships or assignments that fail or are terminated prematurely for some reason, perhaps even before the operational phase;
- Changes to the commercial, operational, risk or other aspects during the course of the engagement, whether driven by the participants or not (*e.g.* new legislation or employees);
- Obligations to, or involvement of, third parties (*e.g.* regulatory authorities, legislation);
- Discrepancies between what should happen in theory and what actually takes place in practice.

Although some such complexities are mentioned below, this guideline deliberately takes a simplistic, generic approach.

4.1.1 Preliminary phase

Section 5 covers the early part of the engagement lifecycle when business relationships are formed, prior to the provision of professional services. The checklist provided in Appendix A is a prompt for both clients and providers to address the key points relating to the preliminary phase, such as:

- Limited information disclosures by both clients and providers in the form of invitations to tender, marketing (branding, advertisements, promotions and offers), opportunistic contacts *etc.*;
- Clarifying and understanding the services required and offered, leading to some form of agreement to proceed (such as a contract);

- Planning and preparing to manage the engagement and undertake one or more assignments in the next phase (*e.g.* governance, reporting and commercial arrangements).

4.1.2 Operational phase

Section 6 concerns the main part of the engagement when professional services are delivered and used. In particular, it draws out the information risk management aspects relating to the maturing relationship and increasing amount and depth of information exchanged, focusing on information security, privacy and incident management. The checklist provided in Appendix B is a prompt for both clients and providers to address the key points relating to the operational phase, such as:

- Exchanging (disclosing or revealing and receiving), generating, interpreting, and using, consuming and exploiting information;
- Managing the assignment, relationship and engagement, handling any concerns, issues, incidents and changes;
- Managing the information risks and security controls, ensuring compliance and effectiveness.

4.1.3 Concluding phase

Section 7 applies at the conclusion of a professional services engagement, both while it draws to a close and thereafter. Again, it focuses on the information risk, security, privacy and related aspects.

The checklist provided in Appendix C is a prompt for both clients and providers to address the key points relating to the end of professional services engagements, such as:

- Retrieving information and related assets from the counterparty, and withdrawing access;
- Reminding those involved of their ongoing commitments to information security and privacy;
- Reviewing the engagement, drawing out any opportunities to improve future professional services engagements.

The concluding phase may be required sooner than anticipated if the engagement is terminated prematurely for some reason, such as a significant incident, inadequate performance or other changes. The activities may be conducted in a hurry under adverse or acrimonious conditions, factors that should be borne in mind in the previous phases (*e.g.* the contract may cater for a premature conclusion under specified conditions, and priorities relating to information risks and the professional services may change markedly during and following certain types of incident).

4.2 Collaboration and joint management

In contrast to the trading of generic commodities, information-rich professional services necessarily involve close cooperation between clients and providers, often with joint design and provision or delivery of the services. This guideline emphasises the collaborative aspects with both client and provider sharing common goals and working together for mutual benefit. The depth, intensity and duration of professional services relationships materially affect the quantity and nature of the information exchanged and hence the value generated and the associated information risks, compared to, say, the procurement of stationery supplies, raw materials or fuel.

At the same time, professional services clients and providers also have distinct objectives and pressures relating to the remainder of their business and life activities. They often have other providers and clients, other engagements, and many other concerns aside from the professional

services and each other, competing for resources and management attention. Providers may be guided or constrained by professional standards, codes of practice *etc*. from trade bodies, as well as generic expectations about the nature and quality of their services.

This guideline deliberately takes a pragmatic approach, acknowledging that (with some exceptions) information risk and security are seldom the client or provider's main concerns. The aim is to manage (identify, evaluate control and contain) the risks in an optimal, business-like and cost-effective manner using appropriate controls, rather than attempt to eliminate them completely.

4.3 Governance

Although professional services engagements and assignments clearly vary, there are common factors that may also apply to other business relationships. It may be worthwhile identifying and incorporating relevant requirements from this guideline and other sources into corporate strategies, policies, procedures, checklists, contract templates etc., in general. Reviewing the associated governance, compliance and other management arrangements may suggest changes to ensure that, for instance:

- Necessary preparations are made in advance *e.g.* policies and procedures are written and authorised, people are aware of and if appropriate trained to perform as expected (including information risk assessment and other parts of information risk management such as incident management);
- The appropriate people or corporate functions are informed and engaged in the process, with additional support or specialist assistance available if needed;
- Roles, responsibilities and accountabilities are clearly understood and accepted, including arrangements to monitor and report on activities, risks, issues, incidents *etc*. to the appropriate levels of management, escalating promptly where necessary, and assurance aspects (such as supplier reviews or audits);
- Applicable policies, procedures, checklists, templates *etc*. are used as intended;
- Key activities and controls are not omitted, ignored or short-cut;
- Senior management is aware of and agrees to any exceptions or changes to the established arrangements, treating any associated information risks appropriately.

4.4 Roles, responsibilities and accountabilities

Clarifying and assigning roles, responsibilities and accountabilities to the appropriate individuals, departments or organisations, and ensuring the obligations are met (compliance), is a blend of governance and management. Specifically in relation to information risk and related matters, management should determine who will:

- Take the lead on information risk and security, providing direction and support to others;
- Identify, evaluate and decide how to treat information risks;
- Allocate sufficient, suitable resources for the associated activities;
- Monitor/measure, oversee and participate in various information risk-related activities;
- Liaise and coordinate as necessary with other interested parties;

- Ensure that obligations and reasonable expectations arising from legal, policy, ethical or other considerations are satisfied cost-effectively;
- Act as an escalation route for significant issues and incidents;
- Seek to prevent or avoid incidents if practicable, otherwise reduce their probabilities and impacts using suitable controls;
- Communicate effectively on information risk-related matters *e.g.* providing suitable reports to the client and provider management teams, and potentially other stakeholders.

4.5 Competence

Professional services, by their very nature, clearly depend on the providers' competence, capabilities and suitability to provide high quality services. More subtly, their clients also play a part in the provision of most professional services, for example interpreting and understanding the advice given and acting accordingly.

While clients are responsible for ensuring that their chosen providers can satisfy their requirements, and providers are accountable for providing the agreed services, the information risk and security aspects may deserve special consideration, particularly in the case of professional services revolving around security, privacy and related matters. Potential controls include:

- Checking or validating suppliers' claims regarding their suitability, competence, qualifications, references etc.;
- Specifying, monitoring and proactively managing the competence and suitability of individuals providing and receiving the services;
- Providing information in a manner that optimises the value of the assignment, responding if appropriate to issues or improvement opportunities (*e.g.* supplementing written deliverables with presentations, discussions and explanatory notes);
- Handling incompetence in a professional manner (*e.g.* with additional training and support, or substituting individuals).

4.6 Compliance

Many professions are supported, guided and to some extent regulated by trade bodies to which professionals may belong. Their prime focus is on supporting and enabling members to provide valuable, high-quality services, incidentally enhancing the reputation and trustworthiness of the profession as a whole. Membership typically involves applicants formally agreeing to uphold and comply with the trade body's standards, rules, requirements or expectations concerning both the professional services provided and the manner in which they are provided and managed. Trade bodies provide guidance and training, and in some cases formally certify or accredit members. They may offer additional benefits such as insurance and arbitration services in case of incidents between members and their clients.

Some professions are further regulated by legislation, and may be overseen by regulatory authorities with varying powers. Organisations and individual practitioners may, for instance, need to be formally qualified and licensed in order to practice legitimately.

Contracts between professional services clients and providers generally have a formal, legal basis, and once executed are to some extent binding on both parties. Agreements and informal

arrangements may not be binding in a legal sense, but may achieve similar aims provided the participants have integrity *i.e.* they are honest, trustworthy, diligent and behave ethically and professionally.

This guideline complements and does not challenge, overrule or supersede any such obligations or expectations. However, professional services clients and providers may further wish to monitor, assess and manage both their own and the counterparty's compliance with their respective obligations to each other and to third parties, such as trade bodies and authorities. Poor performance, conflicting requirements or various forms of noncompliance may be handled routinely in the course of assignment and relationship management, and may lead to or constitute incidents that threaten the overall engagement. As a general rule, clients and providers are well advised to communicate openly and honestly, promptly raising and dealing with such situations fairly and realistically among themselves. Ideally, significant incidents (such as breaches of compliance obligations) should be forestalled, avoided or prevented, if not minimised, contained and resolved. It may be appropriate or necessary to escalate serious concerns to higher levels of management, to independent, mutually-accepted arbitrators, or to authorities and other third parties.

In addition to sanctions, incentives may encourage compliance and performance, for example:

- Bonuses or discounts for exceeding expectations;
- Recommendations, references, positive reviews, referrals, awards nominations *etc*. plus the prospect of further business;
- Professional introductions, case studies, promotions and networking opportunities;
- Personal recognition, citations, thanks and encouragement to the individuals involved, as well as their organisations.

4.7 Ethics

As mutual understanding, respect and trust grow stronger through the intensive, tightly-integrated nature of many professional services, each party inevitably becomes more vulnerable to exploitation by the other party. Incidents may be deliberate or accidental *e.g.*:

- Failing to communicate openly, fully and honestly (*e.g.* neglecting to disclose issues relating to capabilities, resources, timescales or quality; deliberately concealing or delaying the release of material facts for some reason);
- Misusing confidential information obtained from or about the other party (*e.g.* valuable intellectual property such as strategic initiatives, products in development, customer lists, competitive positioning, pricing, costs and profitability), whether or not it relates to the assignment;
- Misleading or manipulating the other party (*e.g.* to secure additional business or more favourable rates);
- Defrauding the other party (*e.g.* submitting false timesheets or expenses);
- Errors and omissions in the information provided, advice given *etc*.

At a wider level, professional services relationships may be affected and perhaps exploited by third parties, including clients and providers of other professional or business services, business partners and others (*e.g.* hackers that infiltrate either organisation's networks). Disclosing such incidents to

clients or providers can be embarrassing and commercially damaging, as can withholding or delaying release of the information. There are ethical as well as legal and practical aspects to consider.

On rare occasions, clients and providers may collude to mislead, defraud or otherwise exploit third parties.

Mitigating controls in the ethics domain include:

- Ethical guidance in the form of corporate policies, procedures, standards, guidelines *etc.*;
- Personal and corporate integrity, trustworthiness, honour and professionalism;
- Reciprocal expectations and mutual respect;
- Supervision and oversight;
- Agreements and contractual sections *e.g.* non-disclosure agreements, plus laws and regulations concerning trade secrets, intellectual property, fraud *etc.*;
- Awareness, training and guidance from management;
- Mechanisms to facilitate and encourage disclosure of suspected or actual wrongdoing *e.g.* management's 'open door policy', confidential reporting hotline.

5 Prior to the provision of professional services (preliminary phase)

5.1 Introduction

Before professional services are delivered, the client and provider discover each other and form a business relationship, negotiating and establishing the ground rules and clarifying their expectations and requirements of each other, particularly regarding the professional service at the core of the relationship and key terms (such as deliverables, costs and timescales).

Clients and providers may have done business together in the past (either through their current organisations or personally), or this may be the first time. Their brands and reputations may precede them, partly as a result of their marketing and promotional activities, partly due to general understandings and perhaps prejudices (*e.g.* the common perception that professional services are 'costly' as opposed to 'valuable'). They may have been introduced by a third party or attracted by advertisements and promotions (*e.g.* websites and social media). Assignments may be pre-planned, or may yet emerge in the course of business.

In addition to the services required, the *manner* in which they are to be provided, and how the assignment/s and engagement are to be managed, can usefully be determined, discussed and agreed between the parties during the preliminary phase.

Depending on the nature of the professional services and relationship, suitable sections may be incorporated into the contract or agreement specifying particular ('key') controls to address unacceptable information risks, such as:

- Identification, authentication and access controls including cryptography to protect the confidentiality and integrity of information exchanged;
- Other cybersecurity controls such as Virtual Private Networking, antivirus and security patching;
- Privacy controls such as those required by applicable laws and regulations;

- Supply chain aspects such as information security and privacy requirements applicable to any upstream suppliers and downstream customers;
- Availability and business continuity arrangements such as resilience, fallback, recovery and contingency arrangements;
- Assurance controls such as: honest, regular and *ad hoc* communications between the parties (*e.g.* relationship management meetings); mechanisms to raise and if necessary escalate more serious or urgent matters; maintenance of necessary professional qualifications, licenses, certifications, permits etc.; and the right to review or commission independent audits of the security and privacy arrangements under and within certain conditions;
- Physical security controls to protect tangible information assets, including health and safety measures for workers;
- Procedural and general controls such as security awareness and training, visitor procedures, change and configuration management procedures;
- Controls relating to invoicing and payment (*e.g.* arrangements to prevent fraudulent invoicing, identity theft or redirection of payments);
- Other controls required by relevant policies and good practices (*e.g.* documentation relating to any deliverables; cyberinsurance).

The preliminary phase typically involves drafting, discussing, negotiating and eventually agreeing formally to the contractual arrangements, an important control in its own right. As with any business relationship, particularly those bound by contract, due diligence requires all parties – before committing – to consider their intentions and abilities to meet their own obligations if they proceed, and likewise determine the capability, suitability and trustworthiness of the other parties.

Assurance may be appropriate in this regard, such as:

- Exploring competencies, capabilities, resources *etc*.;
- Validating claimed qualifications, licenses, permits, authorities, intellectual property ownership *etc*.;
- Taking-up references, considering feedback and review comments from third parties.

Potentially significant information and commercial risks may be associated with the contract. It may for instance:

- Be inappropriate for the relationship and service *e.g.* too narrowly-scoped or precisely-defined to allow for legitimate variations, creativity and innovation, or too vague or inaccurate to cover important points appropriately;
- Be too onerous and costly for one or both parties to achieve sufficient value from the contract to engage fully with the service provision (both parties should carefully consider the risks, opportunities, value and controls relating to the contract before executing it and entering into the commitment);
- Be technically/legally invalid *e.g.* ineptly drafted, not in compliance with applicable laws, incomplete or incorrectly executed;
- Bypass or shortcut due process, committing either or both organisations without proper consideration, review and authority to proceed;
- Lead to real problems later on, for instance if the assignment fails or the relationship turns sour.

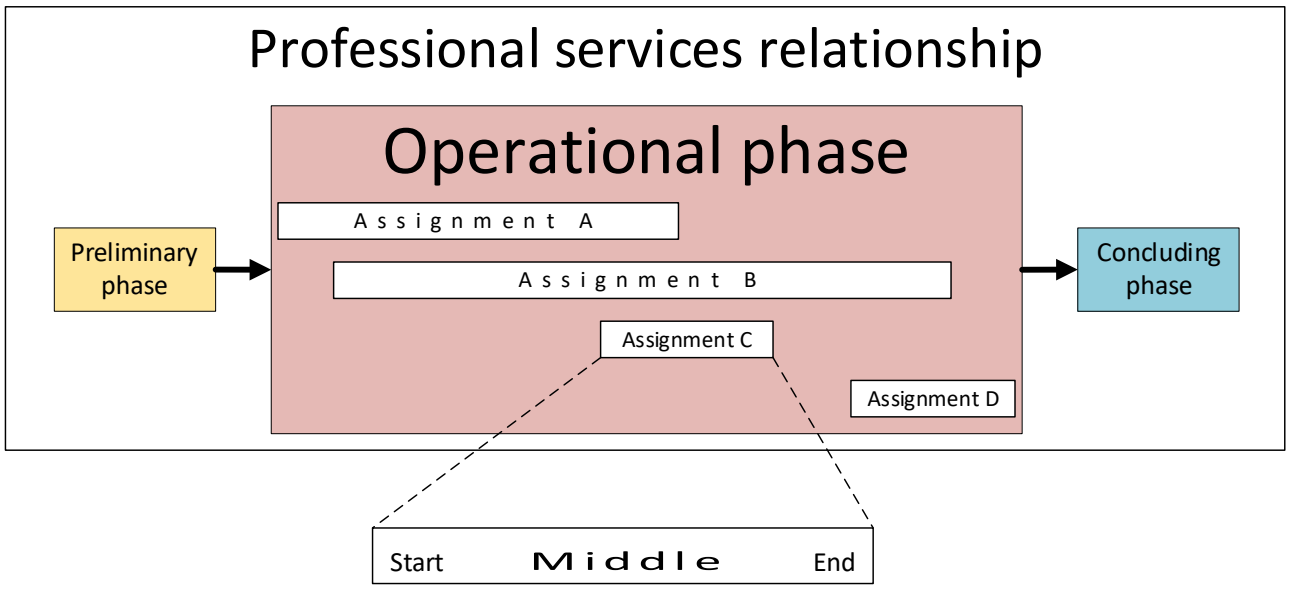
Rows in the tables that follow either distinguish the client and provider activities or perspectives in separate columns, or describe joint activities and shared interests. Either way, the intent is to encourage each party to respect and take account of the other's perspective, not just their own.

5.2 Information risk management during the preliminary phase

Client	Provider
Identify someone appropriate to manage and lead the assignment, and perhaps other team members	Identify someone appropriate to manage and lead the assignment, and perhaps other team members
Identify, assess, evaluate and decide how to treat any significant information risks associated with the relationship, assignment/s and engagement, from the client perspective	Identify, assess, evaluate and decide how to treat any significant information risks associated with the relationship, assignment/s and engagement, from the provider perspective
Conduct due diligence, covering information risk-related aspects as well as commercial and other aspects	Participate in due diligence, providing information requested such as references, qualifications and certificates
Clarify and discuss any confidentiality aspects of the services required	Clarify and discuss any confidentiality aspects of the services provided
Clarify and discuss any integrity aspects of the services required	Clarify and discuss any integrity aspects of the services provided
Clarify and discuss any availability aspects of the services required	Clarify and discuss any availability aspects of the services provided
Clarify, discuss and agree any terms and conditions relating to information risk, security, privacy, compliance or related matters (such as information ownership and any specific security or privacy controls required), preferably in writing	
Check that the provider is committing to provide the necessary/required security and privacy controls	Check that the security and privacy controls required by the client, or by applicable laws and regulations, are in fact part of the professional services being offered
Clarify, discuss and agree how information risk, security, privacy, compliance and related matters are to be managed and governed (directed, controlled, monitored/measured, reported and adjusted if necessary)	
Gain proper authority or permission to acquire the professional services and enter into a contract	Gain proper authority or permission to provide the professional services and enter into a contract
Enter into a binding contract for the professional services, including suitable information risk-related sections for subsequent phases and eventualities	
Execute the contract, planning and initiating the joint management arrangements	

6 During the provision of professional services (operational phase)

6.1 Introduction



The provision (service delivery) and consumption (receipt and use) of professional services is usually the longest phase in the lifecycle. Once the contract is executed and an assignment commences, both parties communicate information to each other, processing, enhancing and using the information in various ways and generating value from the engagement (one or several). Advice may be sought, given, considered and taken, modified or rejected. Documentation may be drafted, reviewed and finalised. Matters are discussed, sometimes with third parties.

As the relationship matures, clients and suppliers learn of and increasingly appreciate each other's requirements and capabilities in some depth. Mutual respect and trust increase, subtly changing the nature of the information exchanges: the formalities may be relaxed as both parties align their processes and timing, perhaps even anticipating future needs and enhancing the services offered and provided. At the same time, client and provider may become increasingly reliant on each other, particularly if the relationship proves effective and valuable. They grow closer together, perhaps more interdependent.

Professional services revolve around valuable information hence the associated information risks are of concern. Managing information risks is therefore an important activity in the operational phase, an integral part of the business relationship.

Related aspects that also deserve management attention include:

- Operating, managing and maintaining the required/necessary security and privacy controls in accordance with obligations, requirements and expectations, including any specified in the contract, professional standards, codes of practice, laws and regulations *etc*.;
- Changes to the engagement, whether sharply defined (*e.g.* different consultants or client contacts) or gradual (*e.g.* while working together, people get to know and appreciate each other's strengths and weaknesses, interests, capabilities, knowledge, prejudices *etc*.), planned and intentional or unplanned and imposed. There are dynamic and potentially complex aspects to this, juggling finite resources and competing priorities;

- Changes to the information risks such as new or different threats, vulnerabilities or impacts, including changes made within the client or provider organisations partly as a result of the professional services (*e.g.* the introduction of new policies and procedures)
- Incidents, plus issues, concerns, problems, complaints, events and near-misses, particularly those which involve or concern the valuable information at the core of the assignment, the professional services, the business relationship, the commercial arrangements and the individuals directly involved. Information risks may involve threats, vulnerabilities and impacts affecting either or both parties, potentially leading to events or incidents directly or indirectly associated with the service provision. Preparing for, identifying, communicating and dealing effectively with, actual or potential incidents may be an important part of the relationship management;
- Performance and quality of service (*e.g.* the nature, volume, timeliness and utility of advice provided; client feedback, comments, suggestions and engagement generally; competence and diligence);
- Assurance, gaining confidence in the suitability, adequacy and effectiveness of the information risk and security-related controls, management activities, oversight and supervision *etc*.;
- Value (benefits less costs), a motivational factor for both client and provider, even in voluntary, *pro bono* and similar arrangements.

6.2 Information risk management during the operational phase

Once an assignment commences and information is exchanged between client and provider, the associated information risks have to be treated. Various information security controls are typically required. Exactly what those controls are depend on the nature of the risks and the context, for example:

- Identification, authentication and access controls may be needed to permit legitimate, authorised access while preventing illegitimate, unauthorised access to the information;
- Physical security and safety controls may be needed to protect physical information assets such as hardcopy documents, disk drives, USB memory sticks, IT equipment and workers engaged on the assignment;
- Workers are required to follow appropriate procedures in accordance with contract clauses, policies and laws. Processes cover information security management and operational activities such as backups, configuration management, version control, security monitoring, incident management *etc*.
- Since the information risks may vary dynamically during the engagement, client and provider should continue monitoring, evaluating and responding to the changes – particularly in the case of protracted or repeated assignments. For example, if it has been determined or is 'obvious' that there are significant information risks associated with an assignment, it is important to maintain a state of alertness and readiness to respond promptly and appropriately to concerns, issues and incidents arising as the assignment proceeds. Without management attention, the information risk management aspects may be subsumed or overtaken by other concerns and activities, perhaps even neglected and forgotten as the relationship matures and participants settle into the routine.

Retaining the focus on information risk and security may be as simple as:

- Opportunistically pointing out information risk-related concerns, issues with controls, compliance obligations, improvement opportunities *etc*.;
- Incorporating appropriate information risk and security metrics into regular reporting;
- A standing agenda item for relationship management, coordination and progress meetings;
- Emphasising the mutual interest in *proactively* minimising incidents, which implies working together on avoidance, prevention and other controls;
- Conducting *ad hoc* or planned reviews or audits to confirm and gain assurance of the effectiveness of key controls.

It helps if such activities were specified, discussed and agreed up-front in the preliminary phase, perhaps being noted in the contract and incorporated into policies and procedures.

As the relationship deepens, additional information risks and opportunities may come to light and, at any point, information risks may eventuate, causing incidents that should be managed. Ideally they should be communicated and addressed jointly by the client and provider for mutual benefit, although that is not necessarily the best approach (*e.g.* if either party is suspected of incompetence, carelessness, negligence or fraud).

'Trust' is generally a critical but fragile control within professional services engagements, hence incident management arrangements on both sides should account for the possibility and the consequences if trust breaks down *e.g.*:

- Monitoring for and responding appropriately to early signs of deteriorating relations or inappropriate activities (such as misrepresentation and fraud);
- Clarifying the nature of any issues, using illustrative examples to substantiate the concerns;
- Bringing client and provider representatives together to discuss and hopefully resolve issues;
- Supporting and encouraging those involved to find mutually satisfactory solutions;
- Providing clear escalation paths in case those directly involved cannot reach a satisfactory resolution, or if corrective actions do not occur as and when promised;
- Threatening and ultimately invoking contractual sections concerning disputes (*e.g.* arbitration or termination of the assignment/s or engagement for due cause).

Client	Provider
Utilise the services effectively and efficiently	Provide the services effectively and efficiently
Manage the services including the information risk, security and privacy aspects *e.g.* measuring/monitoring service provision, updating information risk perspectives and priorities, gaining assurance as to the effectiveness of information security and privacy controls, identifying and responding appropriately to concerns, issues, incidents and changes, and reporting to the respective managers	
Maintain records of valuable information assets exchanged during the assignment, ensuring proper custodianship, control and security arrangements are in place	
Maintain vigilance for early signs of potential incidents, communicating and responding appropriately	
Equitably maximise the value of the assignment/s and the overall engagement	

7 After the provision of professional services (concluding phase)

7.1 Introduction

Eventually, all relationships draw to a conclusion. Clients and providers generally go their separate ways, hopefully parting on good terms unless there were unresolved disagreements, issues or incidents.

Information that was exchanged in the course of assignments persists until it is destroyed, decays or lost, hence information risks and business opportunities may outlast the engagement.

This section focuses on the information risk and security aspects that should be addressed at the conclusion and termination of professional services relationships. As well as the formalities such as secure deletion of sensitive information, ethical aspects such as appropriate versus inappropriate use of information gained or generated in the course of the assignment should also be addressed.

7.2 Information risk management during the concluding phase

<table>
<tr><th>Client</th><th>Provider</th></tr>
<tr><td colspan="2">If possible, retrieve the organisation’s valuable or sensitive information and related assets from the counterparty, or ensure that they are properly disposed of (e.g. data securely deleted)</td></tr>
<tr><td colspan="2">Retrieve or disable any passes, password and other access rights made available to the counterparty</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2">Publicly acknowledge and thank those who performed exceptionally well
and, if necessary, privately inform, coach or warn those who did not</td></tr>
<tr><td>Consider the value of a post-assignment review or case study to draw out improvement opportunities for the future, embodying them into strategies, policies, procedures, training and awareness materials and applying them to other assignments and relationships</td><td>Consider the value of a post-assignment review or case study to draw out improvement opportunities for the future, embodying them into strategies, policies, procedures, training and awareness materials and applying them to other assignments and relationships</td></tr>
<tr><td colspan="2">Maintain contact with the counterparty in case of issues, incidents
or opportunities for further business, if applicable</td></tr>
</table>

Appendix A: preliminary phase checklist[1]

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*.

[1] The three checklists appended to this guideline are succinct generic supplements for the main body sections. It may be appropriate to refine the checklists, elaborating on pertinent details for particular professional services, business situations etc. Conversely, they may be condensed to the bare minimum reminders for the benefit of more experienced users handling low-risk professional services.

- ☐ 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 authorisation
- ☐ Execute (sign) the contract and archive a definitive copy

Appendix B: 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 authorised 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

Appendix C: 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