Contracting for Information Security in Commercial Transactions, Volume II:

Model Contract Terms for Certified Information Security Management Services

This publication is for informational purposes and does not contain or convey legal advice. The information in this publication should be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer.

Participation in the development of this publication does not represent an endorsement of the content of this publication on the party of any specific company or corporation.

Additional copies of this publication can be purchased at www.isalliance.org or by calling (703) 907-7799.

Internet Security Alliance Board of Directors

Chairman
Ken Silva
Chief Information Security Officer
Verisign

1st Vice Chair
Ty R. Sagalow, Esq.
President, Product Development.
AIG

2nd Vice Chair
J. Michael Hickey
Vice President Governmental Affairs & Homeland Security
Verizon

Treasurer
Dr. M. Sagar Vidyasagar
Executive Vice President
Tata Consulting Services

Steve Christensen
Ceridian Corporation

Tim McKnight
Chief Information Security Officer,
Vice President Information Security
Northrop Grumman

Jeff Brown
Chief Information Security Officer
Director IT Infrastructure
Raytheon

Pradeep Khosla
Co-Director
Carnegie Mellon University CyLab

Matt Broda
Leader, Strategic Security
Nortel

Paul Smocer
Senior Vice President
Mellon Financial

Dan Akman
Assistant Vice President Business Development
National Association of Manufacturers

Internet Security Alliance
2500 Wilson Boulevard
Arlington, VA 22201-3834
United States of America
(t) 703.907.7799 (f) 703.907.7093
www.isalliance.org

Preface

Contracting for Information Security Standards is a product of the Model Contract Project, a special development effort conducted by the members of the Internet Security Alliance (ISAlliance), a leading voice for providing private sector leadership in improving global information security. For further information, see www.isalliance.org.

This book has been developed through the ongoing collaboration of a team of professionals drawn from inside and outside the membership of the Internet Security Alliance. While drafts of this book have been circulated and reviewed by many ISAlliance members and affiliated organizations, the following individuals deserve special recognition: Sanjay Bahl, Chief Security Officer Tata Consultancy and Karen Worstell, Co-Founder Waters Edge Consulting. In addition, we appreciate the efforts of John DiMaria of BSi Management Systems, Inc. for his review of the text.

The Model Contracts Project has been supported by Waters Edge Consulting, LLC (www.wec-llc.com). Their staff conducted research on the standards and prevailing practices and were responsible for developing the text and coordinating and reconciling comments and contributions from the members and other commentators. Jeffrey Ritter, the founder of Waters Edge, served as the Reporter for this project.

These acknowledgements would not be complete without recognizing the stewardship of Larry Clinton, our executive director, whose continued leadership helped assure the timely completion of this work and Don Morrison, who has staffed the Internet Security Alliance's support of the Model Contracts Project.

Ken Silva,
Chief Information Officer, Verisign
and ISAlliance Chairman

Table of Contents

Part I

Introduction: The Reasons for this Book

On a global basis, companies are doing business by digitally connecting to one another across the Internet. To succeed, the companies must work to protect the integrity and security with which their electronic information is created, processed, communicated and stored. Doing so requires many tools, but perhaps the most important resource to managing information security between companies (and the related risks) is a well-crafted commercial agreement. For many thousands of companies, across tens of thousands of relationships, producing an agreement that properly addresses information security requirements is difficult, expensive, technically overwhelming and often ineffective at doing the job required to be done.

This book enables business executives and their lawyers to be more effective in addressing information security in their commercial agreements with business partners, suppliers and customers. The objective is simple: to provide a uniform contracting structure designed around the prevailing global standard for managing information security. Implementing that uniform contract structure will simplify the due diligence process, enable risk-based analyses to connect more effectively to the governing commercial agreement and lower transaction costs, all while improving the overall, collective execution of effective information security practices.

The model language included here is absolutely unique—for the first time, companies that have developed and implemented information security management systems (ISMS) which are certified to comply with the prevailing global standard for ISMS—ISO/IEC 27001, as published by the International Organization for Standardization—have a means with which to simplify the contracting process in every single relationship. As a result, significant savings can be achieved in the time and resources required to draft and negotiate contract language and implement appropriate management of the information security features of the relationship.

The Challenges of Existing Commercial Practices

In Part I, this book surveys the challenges and difficulties of addressing information security in the current contracting environment. Specifically, the analysis highlights the increasing burden on both service providers and customers to manage the complex array of information security topics in the ordinary course of negotiating and drafting their agreements. Faced with inconsistent due diligence processes, irregular treatment of information security within the agreements and constantly changing risk environments, companies often fail to have in place "win-win" information security arrangements with their external business community. Unfortunately, the adverse consequences of that situation are often realized only as the parties attempt to respond to, or recover from, an information security incident that occurs while the agreement is being performed.

In late 2005, the Internet Security Alliance published Contracting for Information Security in Commercial Agreements: An Introductory Guide. That book includes a portfolio of detailed model terms and conditions addressing many different types of information security risks. The publication assists companies negotiating specific controls relating to those risks, but did not contemplate that one or both of the parties had in place an information security management system (ISMS) through which an organization's security requirements, needs and objectives are systematically defined and appropriate controls, business processes and resources are rigorously acquired and used.

The Publication of ISO 27001

At nearly the same time as the 2005 publication by the Internet Security Alliance, the International Organization for Standardization (ISO) formally published *ISO/IEC 27001: Information technology—Security techniques—Information security management systems—Requirements* ("ISO 27001").[1] This standard is an enormous contribution to improving information security, defining a globally valid methodology for establishing and executing information security management within organizations. ISO 27001 was developed to enable the integration of information security management into broader enterprise management systems, including those built to satisfy other ISO management standards. The standard provides an integrated framework in which individual information security controls can be coherently managed as part of a systematic approach to security that aligns security business objectives more closely to overall business objectives.

One of the most important features of ISO 27001 is that the standard enables accredited third-party certification bodies to evaluate an organization's information security management system ("ISMS") and, if appropriate, certify that the organization's ISMS complies with the requirements of ISO 27001. The resulting certificate is of significant value, confirming that the company's risk management processes, and the related controls, are being managed effectively. Similar to a certificate issued for compliance with ISO 9000 (or related standards), an ISO 27001 certificate confirms the quality of information security is a priority for the certified company and ratifies that management practices are in place to assure that new risks are properly identified, evaluated and addressed with appropriate controls as a part of a continuous improvement process (referred to as "Plan-Do-Check-Act" or "PDCA").

The impact of an ISO 27001 certificate is a function of the quality with which the accredited third-party certification body conducts its evaluation and assessment. To be accredited within the international standards community, a certification body must develop and employ rigorous procedures that assure the integrity and objectivity of their assessments and fully document the quality of their own assessment systems.[2] Those

[1] A complete copy of ISO 27001, as well as other standards referenced in this publication, may be purchased from the American National Standards Institute (ANSI) Standards Bookstore, available online at http://webstore.ansi.org/ansidocstore/default.asp.

[2] The complete accreditation guidelines applicable to certification bodies are published by the European Co-operation for Accreditation in EA Guidelines for the Accreditation of Bodies Operating

evaluating an ISO 27001 certificate (or seeking a certification body to conduct an assessment) should investigate and understand the credentials and experience of the certification body in order to assure the related certificate will be meaningful.

For companies wishing to demonstrate the quality of their information security management, an ISO 27001 certificate can be valuable. The certificate confirms that, in contrast to addressing specific information security risks with specific controls, the organization has embraced PDCA processes into a systemic management approach through which the information security risks are identified, evaluated and addressed with appropriate controls. As a result, an ISO 27001 certificate provides an organization with a short-hand expression and confirmation of the quality of its information security controls. For many companies, the existence of an ISO 27001 certificate will enable improved efficiency in other areas of operations, potentially lower compliance costs and contribute to a stronger integration of information security into the overall enterprise management.

For those addressing information security concerns in commercial agreements, ISO 27001 also delivers a standards-based, globally-recognized framework through which to proceed; the ISO 27001 certificate can provide a measure of assurance around which the contracting language can be constructed. Doing so is mutually beneficial to all of the parties to an agreement, and provides a significant value to their respective stakeholders.

Certification/Registration of Information Security Management Systems (2000). An updated version of these guidelines, aligned to ISO 27001, is expected to be published in 2007.

A Sample Transaction

A retail clothing/catalog company engages a service provider to whom certain retail fulfillment services are outsourced, such as shipping all merchandise to identified individual customers. A commercial agreement is prepared under which the services will be provided.

As part of the agreement, the retailer requires the provider to provide suitable information security (for example, to protect the personal information of the retailer's customers). The provider has previously obtained and maintains an ISO 27001 certificate.

In the agreement, the contract terms provide that the retailer may rely on the existence of the certificate as evidence of the quality of the provider's information security, and the provider agrees to maintain the certificate (and operate its information security consistent with the information security management system to which the certificate relates).

In turn, this enables the retailer to provide assurances to their customers regarding the quality of the retailer's overall information security controls ("Our service provider is certified under ISO 27001").

Similarly, both the service provider and its customer can communicate to regulatory auditors the existence of measurable, transparent and rigorous information security practices.

For customers, an important attribute of certified information security is that ISO 27001 requires a commitment by the certified organization to measure the effectiveness of information security controls on an ongoing basis. Beneath that requirement is an orientation that the controls be capable of measurement in quantitative terms, that the measurements be recorded and documented, and that comprehensive records be maintained. As a result, many of the business needs for a customer to monitor a provider's information security can be satisfied by an ISO 27001-certified organization. Customers often prioritize the need to have transparency into the operation of certain information security controls through reporting mechanisms established in the commercial agreement; effective information security management under ISO 27001 produces the types of reports often required by customers as part of the program. Thus, for the service provider, it becomes much easier to meet customer requirements using 27001-related reporting tools, rather than developing and producing one-off reports (with their added incremental costs).

A second, and perhaps equally important, value arises from the ISO 27001 controls required to manage and respond to adverse information security incidents. As a result of measurement-based controls, an ISO 27001-certified organization must establish ongoing monitoring and incident-response capabilities that identify, and seek to prevent and/or mitigate, any adverse events. This can be extremely useful in creating alternative strategies for resolving one of the most contentious negotiation topics in information security.

Customers will often seek to impose within the commercial agreement a responsibility on the service provider to report to the customer the occurrence of adverse information security events (such as unauthorized access to personal information records). For regulated companies in the United States and other countries, the need for the reports is now generally considered an essential requirement to meet their legal requirements. But the debate in negotiations can be particularly challenging when the customer is requesting information about events that do not directly involve the customer's data or operations, but nevertheless reflect on the overall information security management performed by the service provider.

From the service provider's perspective, it is argued there is no need to disclose those events if the customer has not been directly affected. But, in reality, in the absence of ISO 27001-based systems, the actual reporting, management and remediation controls within many service provider organizations can vary widely. At times, a service provider's objections to reporting obligations are disguising the quality of their internal reporting controls, or the lack of those controls.

Under ISO 27001, however, an organization cannot be certified without the internal reporting controls being in place. Moreover, effective records must be maintained, with suitable escalation and remediation procedures in place for deployment when needed. Thus, the customer can have confidence in the service provider, and the service provider can more readily provide appropriate reports. There are still valid issues to negotiate regarding the level of disclosure (including protecting the identity and interests of other customers), but the tools are now in place for that reporting to be structured as an extension of existing operations within the ISO 27001-certified organization.

Who Can Benefit from this Book

This book provides a useful tool for the following organizations:

Service Organizations (Service Providers/Vendors/Operators)

Companies challenged to demonstrate their information security management practices to prospective new customers can employ the model contract structure presented in this book to:

- Establish a consistent due diligence process that can be affirmatively offered to customers, in substitution for responding to non-standardized "one-off" due diligence questionnaires, checklists and onsite interviews and systems testing. Doing so will:

    - Expedite and simplify due diligence by relying on the ISO/IEC 27001 certificate and related documentation to describe a supplier's information security controls and management procedures.

    - Reduce the time and resource demands on the contract negotiation and drafting process by integrating due diligence procedures and documentation more closely to the contract structure.

- Establish and integrate a consistent contractual model for addressing information security management issues in commercial agreements. Doing so will:

    - Create a more reliable management framework through which information security services can be adapted to meet the specific requirements of specific industries or individual customers.

    - Integrate information security management more effectively into the primary terms and business models around which the principal commercial agreement is developed.

- Create a defensible standard of care for addressing information security that is transparent, demonstrable and consistent with the prevailing international standard for effective information security management practices.

For those service organizations that have invested in, and obtained their certification under, ISO 27001, the model contract terms presented in this book:

- Contribute to satisfying information security control objectives expressly stated in ISO 27001, as well as regulatory duties to address information security management in commercial agreements relating to data services.

- Leverage the 27001 certificate to provide a uniform structure through which specific information security controls that may be required within specific service industries, or to sustain individual customer relationships, may be addressed within a more complete and consistent manner, integrated within their certified ISMS.

Customers/Joint Venture Participants

Companies that require information security assurances from their suppliers or other parties to a commercial agreement can employ the model contract terms in this book to:

- Develop requests for proposals that solicit suppliers or other prospective parties to respond to information security control topics with a demonstration of their status under ISO 27001 and/or a description of their plans to complete an ISO 27001 assessment. In doing so, the company should:

    - Author its information security requirements to align to the control objectives and controls that are the substantive structure within ISO 27001.

    - Produce scoring criteria employed to evaluate proposals that affirmatively favor respondents that have obtained, or are committed to obtaining, an ISO 27001 certificate.

- Evaluate existing contracting requirements for information security and consider whether, in relying upon an ISO 27001 certified service provider, those requirements can be simplified for the mutual benefit of the parties.

- Implement due diligence procedures that anticipate ISO 27001 certified services to be in place, and be prepared to conduct focused, informed evaluations of a provider's environment that mutually benefit the parties and take advantage of the verified quality of that environment.

- Draft and negotiate suitable commercial agreements that incorporate the model contract terms and align to the due diligence processes that are employed. Selected customer-required controls can be clearly expressed within an ISO 27001 context in order to enable their integration into the information security management systems employed by their service providers.

Regulatory Authorities

Officials that are responsible for developing and assuring compliance with regulations that address information security topics should evaluate the possibility of revising current regulations (or the manner in which current regulations are interpreted) in order that ISO 27001 certified organizations are affirmed as responsible and responsive information security practitioners. Affirmative official support for the certified ISO 27001 management of information security would also extend to the concept that commercial agreements based on the model terms presented here are sufficient to meet regulatory rules for information security to be addressed in relevant contracts; this approach (referencing and relying on published contract models) has been successfully implemented in other regulatory contexts.

The Contents of this Book

In addition to this Part I, this book includes the following additional Parts:

Part II The Challenge to Achieve Information Security in Electronic Commercial Relationships

Part II analyzes existing contracting practices regarding information security and identifies the challenges and difficulties commercial parties face in drafting and managing the related terms and conditions.

Part III The Essential Standards for Information Security

Part III describes ISO 27001 in further detail and identifies other published standards and references that are important to defining and managing information security. Part III also briefly explains how certification bodies operate in evaluating information security management systems and the accreditation process under which certification bodies operate.

Part IV Contracting for Information Security Standards

Part IV provides an overview of the structural elements of most commercial agreements and describes two different contracting approaches employed for information security—a *control-specific approach* and a *Certificate-enabled approach.* The model contract terms included in Part V generally reflect the *Certificate-enabled approach*—the distinction helps enable different pre-signing strategies in due diligence and negotiation activities.

Part V Model Schedule for Certificate-Based Information Security

Part V presents the actual model contract terms, presented as a Model Schedule for Information Security Services. The Model Schedule is accompanied by drafting assumptions and notes which alert the reader to issues to be considered, and are footnoted to provide further guidance to anyone using the Model Schedule in commercial practice to draft or negotiate appropriate contract provisions.

In addition, an Annex of Additional Resources is included, which identifies other publications of interest, as well as sources from which standards and those publications may be purchased.

Part II

The Challenge to Achieve Information Security in Electronic Commercial Relationships

In the 21st Century, virtually any commercial relationship between businesses will involve the creation and movement of digital information. Within many industries, and for many different types of relationships, securing digital information is an essential priority within the business, making information security a key feature of the agreements through which a company's commercial relationships are established and governed. Information security is often required by official regulations that govern specific industries, such as pharmaceutical production or financial services, or apply to specific classes of information, such as personal information.

While few disagree about the importance of information security, significant challenges face companies when they attempt to integrate information security into the substantive terms and conditions of the related commercial agreements. The challenges arise in nearly any possible commercial arrangement, including:

- An agreement for services performed by a service provider ("Provider") for a customer ("Customer"). Service arrangements of this nature which require information security to be addressed include, by example:

    - *Retail transaction processing*, in which the Provider collects or receives personal information relating to retail purchasers of Customer's products or services.

    - *Business process outsourcing*, in which the Customer transfers to the Provider substantial operating responsibility for entire business process functions, such as mortgage processing, payroll processing, retail order fulfillment, IT data center management, etc.

    - *Web hosting/application hosting (or ASP) services*, in which the Provider operates or hosts a website for the benefit of the Customer, or the Provider maintains a web-accessible software application employed by the Customer for processing business information in the daily activities of the Customer's business.

    - *Software development services*, in which the Provider is developing software or other high-value intellectual property assets for the Customer or the services often involve transferring or maintaining sensitive or competitively-important digital assets.

- Agreements for services which are mutually performed (or shared) between two (or more) parties, and may include a Provider. Service arrangements frequently focus on information security that protects the proprietary digital assets of each party from inadvertent disclosure or misuse by those working for any other party. Service arrangements of this nature include, by example:

  - *Storage of business records*, in which multiple parties electronically transfer and maintain digital business records in a shared facility, often operated by third parties.

  - *Shared processing facilities*, in which two parties may share or jointly operate the same data center or similar facility to process their respective information or transaction (this type of arrangement will often occur in connection with business mergers or acquisitions where the selling party continues to use the same data center as the buying party).

  - *Shared data assets*, in which multiple parties have shared access to specific data assets, such as patient information records, with the added privileges of being able to edit or revise the specific data assets.

The preceding examples largely illustrate commercial arrangements in which information processing may be the dominant service. However, with digital reporting and performance tracking being indispensable to effective management in any industry, it is important to emphasize that many other types of commercial arrangements can require information security to be addressed, including, by example, sales, transportation, manufacturing, engineering design, and health care service delivery, to name just a few. Indeed, it is the rare commercial relationship in which the parties will be insensitive to the need to consider information security and the movement of digital business information between them.

The Difficulties for Information Security in Commercial Agreements

In drafting commercial agreements, there can be many difficulties experienced when writing the contract terms that express the information security requirements to be satisfied by the parties. These difficulties arise in all of the types of commercial arrangements just described. Information security professionals and experienced lawyers can offer an endless collection of anecdotes, war stories and tales that substantiate the prevalence of the following difficulties:

- *Intentional omission*—Since information security is, by its nature, technology-intensive, many lawyers and business managers with overall responsibility for structuring commercial relationships will avoid even raising information security issues as they structure the transaction. The primary motivation is often, quite simply, the very human quality of avoiding a topic that is not understood. But, from a strictly business perspective, omitting information security issues can enable the parties to maintain the momentum of the negotiations toward a successfully executed agreement ("Just get the deal done").

- *Disruptive impact*—When information security topics are raised, particularly if later in the lifecycle of the negotiation and drafting of the commercial agreements, the topics will often disrupt the balances being achieved between the parties. The disruption can be significant if the information security topics introduce new costs to be imposed on the Provider that were not taken into account in the bidding and proposal process. This problem of unexpected costs is less likely within industries subject to official regulatory supervision (e.g., banking, healthcare, or environmental management) where information security is more likely to be included in original statements of a project's requirements. But, whenever the new information security requirements are raised, a Customer can face extraordinary pressure from the Provider to make changes in the original pricing proposal to adjust to the related operating costs. As a result, the information security can be minimized, diluted, or ignored in the contract language.

- *Boilerplate approaches*—Customers will impose a boilerplate approach on different service providers in an attempt to streamline the contracting process, insisting on uniform language regardless of the "tier" status of service providers. For example, a service provider with two employees doing very specific functions may offer much less exposure than first tier service providers who routinely perform highly sensitive processes or handle sensitive data in large volumes; nevertheless, the information security contract terms are the same. The lack of a risk-based approach can complicate the negotiations, and often disadvantage a Provider who is otherwise a competitive choice for the Customer.

- *Too little (and too late)*—Often as a result of any one or all of the preceding challenges, when information security is addressed within a commercial agreement, the substantive terms fail to provide either party with significant detail regarding the related obligations, duties and liabilities (e.g., ". . . shall employ commercially reasonable information security procedures"). This approach is often an accommodation for the late emergence of the information security topics in the negotiation.

  The situation can be exacerbated by a fairly common practice occurring when the proposed Customer conducts a due diligence review of the information security practices of the Provider and establishes which controls may be required to be maintained by the Provider, but the legally enforceable terms of the commercial agreement are silent regarding the actual controls themselves. This dis-connect between the due diligence and the actual agreement can produce significant legal and business risks for the Customer, since the due diligence placed the Customer on notice of the need for controls to be in place, while the contract remains silent as to those controls.

- *Too much detail*—When information security is fully embraced as an essential business objective within the agreement, the information security controls can be extremely detailed. But that outcome, properly expressed in the commercial agreement and managed within the overall relationship, requires significant resources. Once the contract is signed, the resources needed to properly "inspect what you expect" are often insufficient, since the cost of doing so has not been factored into the Customer's or the Provider's pricing models. As negotiations become more detailed, and the cost burden of effective oversight more clear, parties often begin to mutually move away from the detail that is actually appropriate.

Regardless of how these various challenges arise in a specific transaction, the outcome can be quite comparable—information security does not receive appropriate attention and the commercial agreement fails as a sufficient roadmap with which to navigate the issues which develop. The consequences, when they arise, can be unpleasant and often disruptive of the original business objectives of the parties.

The Consequences of Inadequate Information Security Contract Terms

The difficulty is that inadequate due care in addressing information security issues during negotiations usually becomes apparent only *after* a related adverse information security event; once the event occurs, the parties must scramble to address the consequences of their earlier inattention to information security. This "time-bomb" impact can be significant:

- As a practical matter, regardless of the responsibilities allocated by the contract to the Provider, the Customer is always accountable for any event that jeopardizes the security of a third party's assets (such as retail customer personal information). A failure to address information security adequately in the contracting stage, particularly when there is ample evidence of the need to do so in the popular media, can expose the Customer to legal liability for negligence in the event of an improperly handled incident, in addition to other possible adverse sanctions or consequences.

- The silence of the agreement on information security controls may justify the Provider not notifying the Customer of an information security event, or delaying the notification, even if the Customer's data or services has been directly affected.

- The absence of defined service levels for certain information security controls can result in the Provider avoiding liability for events otherwise within their control to manage and defend (and certainly can create conflicts between the parties in allocating the resulting losses).

- The lack of management processes in place between the Customer and the Provider (for addressing information security events) can result in confusion in responding to, and remediating, an incident (such as improper access, unauthorized disclosure or loss of information, or denial-of-service), with possible delayed disruptions in services or increased legal consequences (such as fines, investigations, etc.).

- The failure for the parties to have discussed risks important to the Customer (for which the Customer requires appropriate controls, including meeting regulatory obligations) can seriously endanger the reputation and integrity of the Customer, as well as trigger other adverse consequences described above.

The Importance--and Difficulties--of Due Diligence

In order to avoid, or at least minimize, any of these adverse consequences, companies seeking information security controls will incorporate into the pre-contract due diligence an increased attention to the quality of the information security controls of the other party(ies). This trend has been somewhat unilateral—Customers tend to make more demands for due diligence upon Providers, but some Providers (largely as a defensive measure) are also inquiring about the controls in place within their Customer's environments. Of course, in other types of commercial arrangements, the due diligence process can be more bi-lateral or multi-lateral.

The objectives of due diligence, of course, are to review—through fact-finding, disclosures by the other commercial parties, referrals and independent testing—whether information security controls are in place that meet a party's business requirements, and their adequacy and effectiveness in addressing the related risks. Focal points within the due diligence process, when properly constructed, are tied to possible controls that will be required, including those to be expressed or referenced by the terms and conditions of the commercial agreement.

During the last several years, ISO 17799 has rapidly become an indispensable reference around which information security due diligence is constructed.[3] ISO 17799 presents a code of practice for information security, identifying specific control objectives and controls to be considered in responding to identified security risks (ISO 17799 is discussed further in Part III). Those parties performing due diligence (e.g., the Customer) create checklists or questionnaires to be submitted to the counterparty(ies) (e.g., the Provider) and require the checklists/questionnaires to be completed and returned in writing. The checklists/questionnaires can be quite detailed (often exceeding 100 topics of inquiry) and require significant internal effort to prepare a useful response.

[3] ISO/IEC 17799: 2005 Information technology—Security techniques—Code of practice for information security management. ISO 17799 ". . . establishes guidelines and general principles for initiating, implementing, maintaining, and improving security management in an organization."

But not every checklist/questionnaire is identical; variations exist for numerous reasons, and in their variations, the checklists/questionnaires can become quite burdensome. For a Provider seeking consistency in both the information they disclose, as well as uniformity in the services offered, the variations quickly place a strain on the Provider's business model (including their internal projected estimates of the level of effort required to negotiate and finalize each agreement).

Beyond the checklists/questionnaires, further due diligence activity may involve on-site interviews, inspection of information security control records (such as incident reports, audit findings, or management review reports) and testing of the effectiveness of selected controls. All of these activities require the cooperation and response of the Provider, and are often preceded by detailed non-disclosure agreements to protect the confidentiality of the information disclosed to the Customer.

For the Provider, the due diligence process strains one of the most essential principles of information security: the actual risk analysis, control objectives and controls that are the building blocks of an organization's information security management program should, themselves, be kept confidential and secure against improper abuse. As a result, due diligence on information security is inherently an insecure process and, as a result of the tension, often frustrating for both sides of the dialogue. While a non-disclosure agreement may provide some sense of assurance, it is difficult to convince a good information security professional that such a "control" is sufficient to fully protect the disclosures required to be made to the other party during a vigorous due diligence.

A further vexing aspect of information security due diligence is the irregularity of what occurs after the due diligence is completed. For many companies, due diligence is successful solely to the extent it does not produce a basis to withdraw from the transaction. Once negotiations continue, the information gathered through due diligence can often be disregarded, as discussed earlier in Part I: (a) the agreement will not address information security; (b) the agreement will address information security but does so without taking account of the due diligence (e.g., using generic form language that often requires modification because it is inappropriate); or (c) the agreement addresses information security with full coverage of the topics raised in due diligence, but without adjustment to reflect the due diligence output (creating obvious tension and pressure on the negotiation process).

Ironically, when the due diligence is properly considered, the commercial agreement (and the relationship of the parties) can still be vigorously stressed. The problem is a transitive one: when the due diligence questions are non-uniform, the resulting information provided by the Provider can be unique, which causes the substantive contract language to also be unique and non-uniform, both for the Customer and the Provider. This creates a difficult tension that is not easily reconciled:

- For the Provider that has developed its service offering around certain uniform structures, recurring instances of "one-off" contract language that establishes unique terms for each Customer are expensive, difficult to govern and ultimately a source of increased legal risk. Customer demands for tailored, specific information security controls are often distinguished by:

- Different requirements for the disclosure of, and adherence to, specific security controls.

- Varying procedures for notices of information security incidents (notice of incidents not directly affecting a Customer's data or services are particularly difficult items to negotiate).

- Service level standards and performance metrics that require sharing production data with customers generally considered proprietary and confidential.

- For the Customer, there is pressure to establish uniform treatment of information security in contractual arrangements, without regard to a Provider's "standard" service offering. The pressure can originate from different policy sources:

    - An internal corporate policy that service providers be considered as part of the "extended enterprise" and subject to the information security policies and controls of the Customer.

    - Public companies (or their suppliers) are required to institute information security controls that further the reliability of their financial reporting under the Sarbanes-Oxley legislation (as well as similar laws in other nations) and, as a result, must assure that information processed outside the company is comparably protected.

    - Regulations governing specific industries or specific classes of information (such as personal information) require companies to institute information security controls within the related commercial agreements.

For any of the parties experiencing these tensions, there are direct and indirect economic consequences. Any service provider that must develop "one-off" solutions will incur higher expenses, which in turn must be absorbed into the pricing of the services themselves to be paid by the customer. Transaction-related costs (such as legal fees and the fees for experts conducting onsite audits) will be higher as well, adversely impacting all sides of the transaction. Should an information security incident occur, both parties also absorb the costs of investigation and remediation, as well as the added expenses of legal or business conflict resolution procedures regarding the incident itself (and the allocation of the direct costs).

The Model Schedule in Part V presents to businesses and their legal counsel an effective option to the challenges, risks and expenses described in the preceding analysis. The objective is simple: to provide a uniform contracting structure designed around prevailing global standards for managing information security. Using that structure simplifies the due diligence process, enables risk-based analysis to connect more effectively to the governing commercial agreement and lowers transaction costs, all while improving the overall, collective execution of effective information security practices.

Part III

Understanding the Essential Standards for Information Security

Until 2005, no international standard existed that defined a benchmark against which companies could implement a *comprehensive* and *integrated* approach to information security. These are important qualities to be combined together--the *comprehensive* criterion defines the breadth of the risks, control objectives and information security controls to be implemented, while the *integration* criterion defines the need for system-based processes to be employed in any implementation. The publication of ISO 27001 in October, 2005 provided to the global business community a responsive standard.

But ISO 27001 arrived at a time when various other published authoritative works were being relied upon by those that manage information security. This Part of the book provides a brief overview of ISO 27001 and describes in some detail key features of the standard and the related certification process under which an organization can obtain an independent assessment of the compliance of its ISMS with ISO 27001. In addition, this Part summarizes, and provides some perspective regarding, other standards relating to information security. However, a more complete discussion of these topics is outside the scope of this work; the Annex of Additional Resources identifies some useful materials that can be reviewed in greater detail.

ISO/IEC 27001

The formal title of this standard is ISO/IEC 27001:2005 Information technology—Security techniques—Information security management systems—Requirements. ISO 27001 was developed "to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS").[4] It adopts a "process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's ISMS".[5] In doing so, ISO 27001 aligns information security management with other ISO standards for quality business management, including ISO/IEC 9001:2000 and ISO 14001:2004, in order to support consistent and integrated implementation and operation of related management systems. This creates the opportunity within an organization for one unified management system to satisfy the requirements of all of these standards.[6]

[4] ISO 27001, §0.1 General.

[5] Id., § 0.2.

[6] Id., § 0.3. ISO 27001 includes as Table C.1 an illustration of the relationships among the clauses of these various standards.

Integrated Management of Information Security Controls

A significant feature of ISO 27001 is the relationship between the standard and its predecessor, ISO 17799.[7] As briefly discussed in Part II, the latter publication is a code of practice for information security, presenting a robust list of control objectives and controls to be employed for information security; in essence, ISO 17799 is an extremely comprehensive checklist.[8]

Information security pursuant to these standards has a common framework:

- First, a *risk assessment* is conducted, through which the threats and information security risks an organization confronts can be identified and analyzed.

- Second, in response, for each risk, a *control objective* is defined and suitable *controls* are selected. The result is to align the controls to the risks in order to properly deliver an appropriate level of information security.

But ISO 17799 lacked a management process framework through which the separate controls could be developed and executed on an integrated basis. That is the significant contribution that ISO 27001 provides.

ISO 27001 extends from ISO 17799 to describe and require a management process ("Plan-Do-Check-Act" or "PDCA") in which, following the identification and assessment of information security risks, an organization must select and implement control objectives and controls that meet the requirements of the risk assessment. Indeed, ISO 27001 includes a list of the ISO 17799 control objectives and controls (Annex A to ISO 27001) and instructs that an organization shall select from that list those controls which are suitable to cover the identified requirements.

However, ISO 27001 also makes clear that the Annex A list of control objectives and controls is not exhaustive and that additional control objectives and controls may also be selected. Thus, while the combined ISO 17799 and 27001 provide an invaluable toolset, no organization necessarily should rely exclusively on the two standards to define all possible control objectives and controls.[9] In practice, information security professionals will consider other resources and publications, particularly when information security is being coordinated, as ISO 27001 contemplates, with other management systems (see *Other Related References*, below in this Part III).

[7] ISO/IEC 17799: 2005 Information technology—Security techniques—Code of practice for information security management may be purchased online from ANSI at the ANSI eStandards Store; see Part I, note 1, *supra*.

[8] The content of ISO 17799 is regularly updated, most recently in 2005. The revised version adds 17 additional controls and reorganizes the structure in which they are organized, as well as enhance the "user-friendliness" of the standard. *See* http://www.iso27001certificates.com (at ISMS FAQs).

[9] In December, 2006 it was anticipated ISO will republish ISO/IEC 17799 as a code of practice extension of 27001 (see the discussion of ISO/IEC 20000 infra., below).

Certified Information Security Management Systems

The introduction of a management framework within ISO 27001 enables another important outcome: an organization that develops an ISMS pursuant to ISO 27001 can have its compliance with the standard certified by an independent, rigorous assessment process conducted by an accredited certification body (“Certification Body”). If the Certification Body determines that an organization’s ISMS meets the requirements of ISO 27001, a Certificate is issued and registered by the Certification Body into a public database.

The Value of a Certified ISMS

An ISO 27001 Certificate is intended to be relied upon by organizations and third parties. As discussed more fully below, a Certificate exists only after a rigorous process has been completed within the organization and in the assessment. An ISO 27001 Certificate for an organization’s ISMS has many attributes and benefits, including confirming that:

- The information security risks arising within an organization’s operations and services have been considered in a comprehensive and integrated manner, and that the need for appropriate controls responding to those risks has been evaluated.

  - The certificate process requires that, if any risks/controls are not addressed in the organization’s management process, those exclusions must be specifically identified and justified.

- Controls have been developed, installed and operated that enable measurable performance analysis in order to assure that the identified risks are, in fact, being effectively managed.

  - The certificate process requires that, if the responsibility for any risks is being transferred to a third party, such as an insurer or subcontractor or the customer, those transfers must be specifically identified and explained.

- Records and reporting functions are established which assure detailed documentation is maintained and available to support ongoing management and evaluations.

- Management processes are in place to enable continuing improvements as well as to adapt to dynamic and changing requirements.

The existence of an ISO 27001 Certificate provides the basis for reliance by third parties regarding the quality of an ISMS; however, the reasonableness of that reliance, and the degree to which a third party chooses to forego independent audit, testing and reporting of an ISMS in reliance on the ISO 27001 Certificate, can be influenced by the experience and credentials of the Certification Body which has issued the Certificate.

Accredited Certification Bodies

Accreditation for a certification body is conducted pursuant to a publication entitled “EA Guidelines for the Accreditation of Bodies operation Certification/Registration of Information Security Management Systems” (also known as EA-7/03).[10] Originally published to support accreditation activity within the EU, EA-7/03 is relied on by others around the world to accredit Certification Bodies.

Meeting the accreditation standards requires a Certification Body to conduct itself as a disciplined, well-managed audit organization. EA-7/03 focuses on the personnel experience and qualifications[11], certification requirements, and methods for dispute and appeals from certification decisions. The documentation to be maintained by a Certification Body with respect to each reviewed ISMS is described, as well as the procedures to control all documents and data relating to certification/registration functions.

Accreditation is actually managed by national standards bodies, the organizations (both private sector and public sector) which participate on behalf of their country in the International Organization for Standardization. Public directories are maintained that identifies accredited certification bodies, as well as the organizations that have received ISO 27001 certificates.[12]

One of the key factors to be considered by commercial parties implementing a *certificate-enabled approach* (*see* discussion of this approach in Part IV, *infra.*) is to have confidence in the quality and experience of the Certification Body which has issued a Certificate for an organization’s ISMS. For example, a Customer asked to rely on a Certificate should be entitled to have a Provider confirm that the Certification Body is accredited (and that the accreditation has not been revoked, suspended or limited since the date of the Certificate) and that the Certification Body has acted within the scope of the accreditation which has been issued. Customers may also be interested to know the degree of experience a Certification Body may have working within a specific industry or region in order to evaluate their potential skill at investigating possible weaknesses in an ISMS being assessed.

Requirements for Certification

To obtain a Certificate, both the organization and the Certification Body must comply with rigorous requirements described in EA-7/03. The fact these requirements exist and must be satisfied as a pre-condition to a Certificate can be relied upon by a third party,

[10] A copy of EA-7/03 may be obtained at http://www.european-accreditation.org, which also contains additional information about the accreditation process.

[11] Separate training and certification programs exist for those employees who perform ISMS audits for a Certification Body.

[12] The database listing organizations accredited as certification bodies can be found at www.xisec.com. Those organizations with active ISO 27001 certificates can be found at http://www.iso27001certificates.com.

such as a Customer, to confirm extensive due diligence has been conducted and that compliance with ISO 27001 has been audited. Among the requirements to be satisfied by an organization are the following:

- An official application, in which the applicant agrees to comply with the requirements for certification.

- A detailed submission to the Certification Body of information and documentation in advance of the assessment, which is to be reviewed before an assessment team is assigned.

- A complete assessment of the ISMS against all applicable certification requirements, including the full content of ISO 27001; procedures are outlined for assessing complex operations, such as multi-site organizations.

- An assessment report prepared by the Certification Body, which is subject to a review, comment and discussion process between the Certification Body and the organization.

A final informed decision to certify an organization's ISMS is made by others not actually participating in the audit assessment process itself. The Certificate must present information regarding the Certification Body, the scope of the assessment and the resulting decision. These requirements are supplemented by restrictions against any misuse or misrepresentation of a Certificate by the organization. Of course, all of these rules are intended to substantiate the reliance by a third party on the Certificate itself.

Documents and Records

Pursuant to ISO 27001 and EA-7/03, a certified organization must maintain detailed documents and records relating to the ISMS operations. The documents include internal reports on the measurable effectiveness of the controls and records relating to any information security incidents or events. In addition, the organization must maintain and make available for review by the Certification Body records of any complaints received relating to failures of the ISMS to perform as intended.

A Statement of Applicability is an important record within an organization's ISMS. The Statement of Applicability is the documented statement describing both the control objectives and controls that have been adopted in response to an integrated risk assessment. The Statement of Applicability is important to the certification; the existence of a Certificate confirms that the Statement of Applicability is accurate and that the described controls have been implemented consistent with their description. An organization is responsible to maintain the accuracy of its Statement of Applicability and, on an annual and tri-annual basis, the Certification Body reviews the ISMS to re-affirm the continued validity of the Certificate (and the accuracy of the Statement of Applicability).

Thus, the Statement of Applicability should always reflect the controls that are in place for a certified ISMS. When a Customer requires due diligence regarding a Provider's operations, the Statement of Applicability is an appropriate record to be presented by a Provider for review, in substitution for a Customer's one-off due diligence questionnaire, in order to demonstrate the scope and integration the Provider has established. This can be very beneficial to both parties, enabling a more consistent and reliable structure through which due diligence can proceed.

The Statement of Applicability will also allow the Customer to evaluate whether the existing controls must be supplemented with any additional or different controls required to meet the Customer's specific needs. Those needs may arise from different sources (such as regulations, contractual obligations or established trade practices); however, employing the Statement of Applicability allows both parties to more efficiently align the existing controls to the Customer's requirements; if there are changes made by the Provider to meet the Customer's needs, an amended Statement of Applicability can be prepared to reflect the related additional or revised controls.

Surveillance and Reassessment

Once a Certificate is issued, an organization must enter into written agreements to permit the Certification Body to conduct periodic surveillance (generally, not less frequently than at least once per year) and reassessments (once every three years) of the ISMS. Those reviews are intended to verify that the certified ISMS continues to be implemented by the organization consistent with its terms.

For the third party relying upon a Certificate (such as a Customer), the surveillance and reassessment process can help assure that oversight for information security is being provided, perhaps at a comfort level that allows the third party to perform less direct oversight. For the certified ISMS, the surveillance and reassessment process offers a consistent, uniform and objective review that can perhaps displace the need for individual, one-off audits from different customers and third parties. Of course, the regulatory duties imposed on some third parties may limit the ability to completely discharge the oversight function, but even in those cases, the documentation required to enable surveillance and reassessment by a Certification Body can help make any third party oversight significantly easier to support.

Related Standards and References

The following are additional widely recognized standards and publications which provide guidance to professionals structuring the overall controls and management frameworks through which information security is managed; there is significant literature available on the strengths, weaknesses and features of each of these resources and the manner in which any one organization may elect to draw from them to support their own IT and information security management efforts:

> *ISO 20000* is an international standard for IT service management. ISO 20000 is composed of two parts. ISO 20000:1 is a specification for a service management system; ISO 20000:2 is a code of practice.[13] Together, the two parts provide a complete framework through which IT assets can be integrated to overall business strategy, including information security objectives. While ISO 20000 and ISO 27001 were separately developed, there are significant benefits to developing and implementing management systems that comply with both standards on an integrated basis.[14]
>
> *ISO 15489* is an international standard for records management practices. ISO 15489 is composed of two parts: ISO 15489:1 is a standard for records management; ISO 15489:2 provides guidelines for the related practices (a table included in ISO 15489:1 aligns their individual elements). Records management is increasingly important to information security practices, particularly since ISO 27001 gives such emphasis to creating and managing the records of information security management as a component of an effective ISMS. In addition, particularly when an information security incident occurs, the related records can be important to the resolution of legal claims or investigations regarding the incidents.[15]
>
> *ITIL® (the IT Infrastructure Library)* is a cohesive set of best practices in IT service management, consisting of a series of books giving guidance on delivering quality IT services and the facilities needed to do so. ITIL® supports a systematic and professional approach to IT management, covering applications, infrastructure, security, software asset management and service delivery and support.[16]
>
> *CobiT® 4.0, Control Objectives for Information and Related Technology* is a publication of the IT Governance Institute® (ITGI). CobiT provides an IT control and governance framework that allows business managers to develop coherent policies and practices; the most recent version emphasizes regulatory compliance. Those employing CobiT can access various tools which enable them to harmonize

[13] ISO/IEC 20000-1:2005 Information technology—Service management—Part 1: Specification and ISO/IEC 20000-2:2005 Information technology—Service management—Part 2: Code of practice may be purchased at the ANSI eStandards Store; see Part I, note 1, *supra*.

[14] For further information, see www.bsi-global.com, included in the resources listed in the Annex of Additional Resources.

[15] ISO/IEC 15489-1:2001 Information and documentation—Records management—General and ISO/IEC 15489-1:2001 Information and documentation—Records management—General may be purchased at the ANSI eStandards Store; see Part I, note 1, *supra*.

[16] Additional information on ITIL®, and the means to purchase the included books, can be found at http://www.itil.co.uk (last visited on January 12, 2007).

the elements of CobiT with other standards, notably ISO 17799.[17] As with ISO 20000, many organizations pursue integrating their reliance on CobiT and ISO 27001.

In addition, other standards can influence how an ISMS is designed and implemented, including those relating to incident handling, disaster recovery and response and network management. [18]

Working with the Standards

Standards are inherently normative, but managing information security requires scaled and variable approaches which take account of a large range of factors, as discussed elsewhere in this book and in related professional literature, some of which is included in the *Annex of Additional Resources*. As a result, there is no "perfect" or "ideal" structure to an ISMS—the dynamic and changing nature of web-based commerce actually demand a great deal of agility and adaptability to new risks. In information security, the ISO 27001 and ISO 17799 standards are important for the order they bring to the analytical process; when an organization undertakes to put into place any business process or system that finds its inspiration from published standards, the organization is committing to a structured analysis and documentation effort that is enormously important to assuring the overall quality of the result.

In the field of information security, ISO 27001 is considered an indispensable and increasingly influential reference for defining a business management process that assures that the related risks to be managed are suitably defined, control objectives articulated and controls implemented with discipline and accountability. The additional standards, when relied upon (including, for example, to identify additional control objectives or controls to be included in an ISMS), enrich the integrity of the process and empower the organization to better adapt its ISMS to the overall demands and services associated with its operations.

New information security standards enhancing and extending ISO 27001 are in the development process. In addition to a re-alignment of ISO 17799 as a code of practice directly related to ISO 27001, additional standards providing ISMS implementation guidelines and addressing the metrics for measuring performance of information security controls are under development.[19] Taken as a whole, this portfolio will deliver a robust, uniform, comprehensive and integrated expression of quality and best practices for the management of an ISMS.

[17] Additional information on CobiT® and ITGI, and the means to download the publication, can be found at http://www.isaca.org (last visited on January 12, 2007).

[18] A more complete list of these associated standards is available at www.iso27001certificates.com (at ISMS FAQs).

[19] See www.iso27001certificates.com (at ISMS FAQs).

Part IV

Contracting for Information Security Standards

This Part IV begins with an overview of the structural elements that distinguish most commercial agreements. The overview illustrates the purposes each general section of an agreement serves and, therefore, provides a framework in which to understand how any treatment of information security fits into the broader structure. The discussion also highlights the different elements of an agreement that must be considered in addressing any major topic, including information security, in order to achieve a good "meeting of the minds" between the parties.

The second portion of this Part IV introduces two different contracting approaches for information security—a *control-specific* approach, currently the prevailing method for addressing information security, and a *Certificate-enabled* approach, which leverages the existence and importance of an ISMS for which a Certificate has been issued by an accredited certification body. Generally, the Model Schedule presented in Part V reflects the *Certificate-enabled* approach, while still allowing for certain key topics to be addressed through *control-specific* terms and conditions.

Contract Structure Overview

Commercial agreements are dynamic instruments that provide the structure and governance for a commercial relationship. Examples of the many different types of commercial agreements that address information security are listed in Part II.

For each type of transaction, the contract expresses many of the rules that will govern the relationship, including the duties to be performed, the obligations (including negative covenants prohibiting certain conduct), the liabilities for things going wrong and various administrative items. Here is a more complete description of the key elements in commercial agreements, many of which are regularly relied upon in addressing information security control and management.

Defined Terms

Commercial agreements benefit from the use of terms that have uniform meanings between the parties; many legal disputes arise, in fact, when there is disagreement on the specific meaning to be assigned to the words of the agreement. As a result, those drafting the agreements often employ capitalized terms to which specific meanings are assigned as a part of the contract.

Frequently, the defined terms are set forth at the beginning, in order to assure that the intention of the parties is understood in considering later provisions.

Technical topics, such as information security, often require defined terms, particularly if "terms of art" exist within the related field that have alternative meanings. The defined terms assure the parties have selected the same meaning for the actions or services to which a topic relates. The use of defined terms within the agreement also provides a foundation for the remaining governing provisions, in which the defined terms are the building blocks from which other substantive provisions are formulated. As a result, the definitions themselves can often be vigorously negotiated. An investment in achieving consensus on the meanings of the defined terms produces benefits later in the relationship by minimizing or avoiding disputes regarding the intentions of the parties.

Representations and Warranties

The representations and warranties within an agreement serve two purposes:

- Representations are affirmative statements of fact offered by one party to the other party(ies). Representations are used to express important facts, the truth of which is considered influential to the decision to enter into the agreement. Lawyers crafting commercial agreements will employ the representations to establish the factual foundation on which specific aspects of the agreement depend.

- Warranties are promises that a fact is true; when a party warrants certain facts, the party is generally considered to indemnify the other party against losses that arise if the fact is not true. The value of a warranty is that it relieves the party relying on the warranty to independently determine the truthfulness of the related fact.

Most commercial agreements will combine the representations and the warranties into one substantive provision; doing so assures the reliant party of the strongest legal recourse in the event the statements of fact are not accurate, whether as a result of willful deception, innocent error or negligence.[20]

Duties and Obligations

The essential substance of an agreement, of course, are the substantive duties and obligations to be performed by the parties. In drafting the actual provisions, lawyers (and their clients) engage in a risk-based analysis to determine the level of precision, specificity and direction to be expressed by the language of the

[20] A recent analysis of the distinctions between representations and warranties, and the different legal remedies available to the reliant party may be found at http://www.abanet.org/buslaw/blt/2006-01-02/nonbindingopinion.html (last visited December 19, 2006).

agreement. For those areas in which the absence of precision can introduce significant risk, the provisions can become quite substantive. As discussed in Part I, there are various drafting approaches employed for information security which often fail to reflect good risk-based analysis.

The obligations of the parties are generally expressed in covenants; affirmative covenants describe conduct parties must demonstrate to be in compliance ("Provider shall . . . ") and negative covenants prescribe conduct from which parties must abstain to be in compliance ("Provider shall not . . . ").   In any agreement, performance obligations, whether affirmative or negative, can be dependent on various conditions described in the terms of the contract themselves.

Enforcement

Many commercial agreements contemplate that disagreements may arise between the parties that will require resolution. Disputes can be considered through different contract mechanisms, whether at the administrative level of managing the relationship, through the application of financial incentives or penalties to compensate for performance failures or credits, or with reliance on increasingly adversarial proceedings (such as mediation, arbitration or commercial litigation).

Contemporary business practices, particularly those that are heavily based on technology or networked services, are not easily terminated—to create and operate the related services or transactions, the parties invest heavily in systems, data transfer protocols and other interdependent features, establishing an investment that can be substantial. As a result, when disagreements arise, parties favor resolving the matter without terminating the overall agreement.

In drafting the enforcement and dispute resolution provisions of an agreement, lawyers and their clients will develop mechanisms that assure, if a service issue arises, there is a protocol through which the issue or disagreement can be addressed. For information security issues, this is particularly useful, since the technology-intensive nature of the issues can often collide with more general mechanisms employed within the agreement.   If these mechanisms are not in place, one of the most important qualities of good information security can be placed at risk—the ability to mutually collaborate and restore operations following an adverse incident.

Annexes

Modern contracting practices increasingly rely on annexes or schedules attached to the primary agreement for many purposes, including to express the detailed defined terms, representations/warranties, duties and obligations, and enforcement mechanisms relating to specific services or obligations. The annexes are still considered part of the entire agreement and specific language is generally employed to assure that result.

> Annexes permit the parties to assemble all of the related materials in one location within the agreement; doing so can also simplify the management of the ongoing services. Specific annexes, rather than the full agreement, can be distributed to the particular managers or business units responsible for the described services, thereby improving the likelihood the substantive terms will be understood and properly executed.[21]

Contracting for information security, done well, will include terms within each of the preceding major sections of an agreement. Information security requires a shared vocabulary (defined terms), truthful statements regarding existing systems and controls (representations and warranties), clearly described actions and responsibilities which all parties must exercise (duties and obligations), and extensive provisions for addressing what happens when things go wrong (enforcement). However the technically-intensive nature of information security can challenge contract drafters—the difficulty is that the overall utility of the agreement can be overwhelmed by the complex terms required to address information security. The result can be an agreement in which the primary functions of the agreement becomes almost subordinate to the topic of security, and the overall relationship is more difficult to administer.

Drafting Models

As a result, there are generally two structural models through which information security topics may be addressed: an *integrated model*, in which the information security terms are presented within the primary text of the agreement, and a *schedule-based model*, in which nearly all of the information security terms are separately presented and integrated into one schedule or annex that is attached at the back of the primary agreement. Both models have their advantages and disadvantages.

For a specific transaction, the most suitable structure will be influenced by different factors, including the type of transaction, the importance of information security, the relative sophistication of the parties, the governing law, and the degree to which the primary agreement may be required to be disclosed at some point in the future.

An *integrated model* permits the drafter to place the various terms relating to information security throughout each major component of the agreement (defined terms, representations and warranties, etc.). To manage and track the parties' respective duties, one must navigate across the entire text of the agreement. While an *integrated model* may be suitable for contracts in which information security is treated lightly, the approach is more difficult to apply in more complex agreements as the overall volume of applicable terms increases. Moreover, it is difficult to protect the confidentiality of the information security requirements, particularly if the entire agreement must be distributed

[21] This approach can also protect the confidentiality of certain terms within the agreement from others who do not have a "need to know" those terms—examples include pricing, dispute resolution mechanisms and, of course, information security controls and standards.

across an organization in order to support the ongoing management of the underlying commercial relationship or transactions.

There are no reliable means to determine whether, for information security, there is a specific trend, but it is very common for the *schedule-based model* to be used. The primary agreement will include a very general commitment of the parties to provide information security pursuant to an attached schedule (or annex) which is incorporated as a part of the agreement. The schedule fully presents the terms addressing information security, largely on an integrated and stand-alone basis; in many cases, the schedule will reflect the overall contract structure, including its own definitions, representations and warranties, duties and obligations, and enforcement provisions.

As presented in this book (see Part V), the *schedule-based model* approach has been employed for the model terms and conditions (the "Model Schedule"). As described in the Drafting Notes and Assumptions that accompany the Model Schedule, there are still terms that must be included in the primary agreement in order for the Model Schedule to work in the larger context. The *schedule-based model* is also slightly more adaptable to the different approaches employed to address information security, as more fully described in the next section.

Two Approaches to Information Security

Within the general framework for a contract's structure, two possible approaches can be employed to address information security: a *control specific approach* or a *certificate-enabled approach (which relies on the existence of an ISO 27001 Certificate).* With both approaches, there are drafting considerations that cannot be overlooked. In any treatment of information security, the vocabulary, requirements and consequences of non-performance must be carefully balanced and integrated with the overall commercial agreement and the related and unrelated terms and provisions.

The Control-Specific Approach

Information security management has been historically approached with a specific attention to identifying and implementing specific information security controls. In commercial relationships, the negotiations will generally focus on the controls that a Customer requires to be in place. Deciding which controls to include is a function of different influences, including external legal or regulatory requirements, trade practices, internal corporate business policies, and requirements under operations or cyber-insurance coverages.

As suggested throughout earlier portions of this book, the comprehensive expression of a full suite of information security controls can be a very detailed process. Under ISO 17799, nearly 130 different control functions are identified for consideration, a list which is also largely incorporated as the components of a strong ISMS. In 2005, the Internet

Security Alliance published Contracting for Information Security in Commercial Transactions: An Introductory Guide (the “2005 Guide”) to provide model contract language for many of the individual controls that are often included in commercial agreements.

The 2005 Guide serves to support a *control-specific* contracting approach. For each topic included, specific language illustrates how the related obligations can be expressed in a commercial agreement. The 2005 Guide is not a complete inventory of all of the topics addressed in ISO 17799, but the scope is extensive, including:

Change Control Policies
Device Security
Encryption
Equipment Disposal
Incident Reporting and Response
Network Architecture
Reporting Malicious Software
Password Management
Patch Management
Personal Information
Records Retention
Systems Integration

The 2005 Guide did not include model language for other additional controls that are often addressed, particularly in major commercial agreements. As discussed earlier, in many transactions, ongoing measurement and reporting relating to specific controls is required by a Customer, for which detailed enabling terms and conditions are required in the agreement. Those types of contractual terms are not easily reflected by model language.

A *control-specific* approach frequently confronts many of the risks and adverse consequences identified in Part I. The resulting language, done well, can be voluminous and complex; done poorly, the contract can present parties with additional “time-bombs” when future information security incidents arise (*see* the related discussion in Part II).

A Certificate-enabled Approach

The Model Schedule employs a C*ertificate-enabled* approach as an alternative to the *control-specific* approach. Under a *Certificate-enabled* approach, the parties generally replace the exercise of negotiating and managing specific controls between themselves by substituting their mutual reliance on the existence of a trusted Certificate from an accredited third party which verifies the quality and integrity of an information security management system.

For a Customer, a *Certificate-enabled* approach assures that the Provider has in place a focused, and comprehensive, management process around information security. At the beginning, rather than rely on its own due diligence, the Customer may rely upon the due diligence and review which the Certification Body performs as a pre-condition to the issuance of the Certificate to provide the Customer with assurance regarding the adequacy of the Provider’s controls. Under the contract, the Customer may also rely on the continued validity and effectiveness of a Certificate (and the ongoing audits conducted by a Certification Body) to assure that the ISMS remains functioning and consistent with the original expectations; in return, the Provider should commit to report to the Customer any deficiencies or other circumstances which would make the Customer's reliance on the Certificate inappropriate.

The existence of a Certificate does not eliminate the need for a Customer to understand more fully a Provider's information security environment when appropriate (for example, when required by regulations), and to evaluate the adequacy of specific controls for addressing risks associated with the Customer's business or electronic information. For that, a Customer and Provider can employ the Provider's Statement of Applicability (described in detail in Part III). A Customer may also have regulatory obligations to document due diligence of a Provider's ISMS, for which the Customer may require access to certain records and reports of the Provider. The existence of a Certificate assures to a Customer that those records and reports exist and, with appropriate confidentiality, can be reviewed for those purposes.

For the Provider, a *certificate-enabled approach* provides the potential to achieve consistent and substantially uniform treatment of information security controls within its commercial agreements, as well as throughout the contract lifecycle. Reliance on the Certificate enables the Provider to deliver consistent information to its customers, including the content of reports and assessments by the Certification Body. In the information security field, this approach is not new; third party service providers, particularly in the United States, have become accustomed to sharing audit reports regarding selected security controls generated pursuant to SAS 70.[22] By contrast, an ISO 27001 Certificate, and the related assessment report, can generally provide a more intensive level of assurance and, of course, is aligned to a global, rather than national standard.

[22] SAS 70 is Statement on Auditing Standards (SAS) No. 70, Service Organizations, an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). An audit or examination under SAS 70 "... represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes." *See* www.sas70.com (last visited January 12, 2007).

Part V--

Model Schedule for Certificate-based Information Security Services

This Part V presents a Model Schedule for Information Security Services to be employed when the parties are relying on the existence of an ISO 27001 Certificate in connection with the performance of information security services. In reviewing or relying on any model terms and conditions to be employed in commercial agreements, it is important to understand the general assumptions and additional considerations that shape the possible use of the model language—those are set forth below in the first section of this Part. The Model Schedule is the remaining section. The Model Schedule includes footnotes providing additional comments and drafting tips that are best presented in the context of the actual language that is included.

Drafting Assumptions and Notes

The Model Schedule is intended to be employed in a commercial agreement in which the information security management systems and information security controls of one or more parties to the agreement are addressed. In order to improve the utility of the Model Schedule for those drafting actual commercial agreements, here is a framework of the key assumptions relied upon in its development:

- The Model Schedule is structured to be incorporated into a commercial agreement ("Agreement") in which a service provider ("Provider") is contracting with a customer ("Customer") to provide commercial services, such as outsourcing, data processing, or transaction processing ("Services"), under the Agreement. The Services include information security services ("Information Security Services") in which information security controls ("Controls") are employed.

  Comment: The Model Schedule terms can be modified to support two alternative structures:

  - First, the parties can elect to use an *integrated model,* as an alternative to the *schedule-based model*; as discussed in Part IV, this approach incorporates the substantive information security provisions, including specific Controls, into the primary terms of the Agreement.

  - Second, the parties may wish to make mutual commitments to maintain Controls, where the commercial relationship requires reciprocal commitments to Controls (for example, between two financial institutions exchanging transaction data in both directions between the institutions); in that case the Model Schedule provisions can be prepared as bilateral provisions applicable to both parties.

- The Provider (a) has already completed, for the Provider's information security management system ("ISMS"), the ISO 27001 certification process employing a properly accredited Certification Body,[23] (b) has obtained from that Certification Body a Certificate reflecting accreditation of its ISMS under ISO 27001, and otherwise created and maintained the necessary records required under ISO 27001, and (c) intends to maintain the Certificate during the term of the Agreement.

  Comment: In the event a Provider has not yet obtained a Certificate, the Model Schedule terms can be modified to include a timetable against which the Certificate will be obtained, as well as contingency provisions for the consequences of a Certificate not being obtained. Of course, in the absence of a Certificate, a Customer may require a non-ISO 27001 approach to information security to be in effect until a Certificate is in place. For model terms and conditions applicable in that situation, *see* Contracting for Information Security in Commercial Transactions: An Introductory Guide (Internet Security Alliance, 2005).[24]

  Comment: The Model Schedule does not require that a Customer have obtained a Certificate prior to contracting with the Provider; in some cases, a Provider may wish to require the Customer also be certified, in order to better address operating risks that may arise when a Customer does not itself have commercially reasonable information security management in place.

- The Model Schedule assumes that the Agreement will contain additional substantive terms and conditions, including defined terms, which address related topics important to the overall commercial relationship. For the purposes of brevity, actual language for those additional terms and conditions, many of which have well-established structures, has not been included with the Model Schedule.

  Here is a representative list of topics to be addressed in the Agreement that can provide support to the effectiveness of the Model Schedule as part of a complete Agreement (note: this list is certainly not exhaustive of all possible related topics):

  - Defined Terms, including:
    - "Applicable Law"

[23] A more complete discussion of how certification for an ISMS is obtained under ISO 27001 is set forth in Part III of this book.

[24] The option of including required contract terms addressing individual Controls is also a part of the proposed Model Schedule; see Section 4.1 of the Model Schedule (relating to the mandatory use of "Selected Controls").

        - "Customer Data"
        - "Effective Date"
        - "Person"
        - "Services"
        - "Subcontractor"
        - "Term"
    - Services Management/Relationship
    - Transaction Records
    - General Representations and Warranties
    - Confidentiality
    - Governing Law
    - Limitations of Liability
    - Exclusions of Damages
    - Insurance Coverage; Claims
    - Dispute Resolution (Arbitration or Mediation)
    - Survival of Selected Provisions

- The Agreement into which the Model Schedule is to be incorporated is assumed to be developed under, and governed by, the commercial contract law of the United States (as designated by the parties in standard governing law provisions).

    Comment: While the Model Schedule is very suitable for adaptation and use in commercial agreements governed by other national laws based on common law principles similar to those of the United States (e.g., Canada, India, United Kingdom, and Australia), no due diligence has been performed to specifically assure that legal issues do not arise under those legal systems in connection with the use of the Model Schedule. Similarly, the enforceability of the Model Schedule under other national laws has not been considered and drafters are encouraged to be familiar with the challenges of adapting contractual language intended for agreements governed by common law principles to agreements subject to other legal systems.

    Comment: Drafters should consider whether the Model Schedule is consistent with any regulations directly applicable to the Services, including regulations that establish specific standards for information security controls applicable to particular industries, transactions or processes. For example, privacy regulations governing the protection of personally identifiable information may impose specific requirements for information security services with which the Provider and the Customer must comply. That type of due diligence is also required to be part of the certification review conducted by a Certification Body.

    Comment: Companies complying with ISO 27001 are required to keep extensive records regarding their ISMS, including records relating to Information Security Events and Information Security Incidents (as such terms are defined in the Model Schedule), which records are often reviewed and/or held in the files of the Certification Body (subject to non-disclosure arrangements). Drafters should be aware those records may become available to official regulatory authorities under certain circumstances, including routine examinations and audits as well as in connection with specific investigations or subpoenas.

Excluded Content

In relying on the Model Schedule for Information Security Services, users should note that the following topics, often associated with information security, are *not* addressed in the Model Schedule. Model terms for many of these topics are difficult to develop, since the dynamics of the specific relationship will often influence the structure and terms with which these topics are addressed:

- The timelines, responsibilities and validation mechanisms that govern how the Services are to be established and tested, including the Information Security Services. These management topics vary widely from transaction to transaction and are not suitably presented in a model format.

- The allocation of responsibility for the liabilities and costs related to delivering notices of information security incidents involving the disclosure of personal information. The obligation to deliver those notices arises under various state and federal laws and regulations within the United States, as well as the national laws and regulations of other countries.

- The structure and criteria for employee or contractor background checks on specific individuals. Many companies are subject to specific privacy laws, as well as duties to conduct background checks due to the nature of their business or the class of data that is involved; these requirements require careful attention and are not easily addressed with model language.

- The rules for specific types of controls that may be required under certain laws or regulations are not identified nor specifically addressed; users of the Model Schedule must assure that compliance with these types of rules, if applicable, can be achieved.

- Specific amounts or types of insurance coverage required to be obtained by those operating an ISMS.

Model Schedule on Certificate-based Information Security Services

Consistent with the preceding Drafting Notes and Assumptions, the following Model Schedule, beginning on the next page, is intended for use as an annex to a primary commercial agreement between a Customer and a Provider:

Schedule on Information Security Services

This Schedule on Information Security Services is incorporated into, and considered a part of, that certain Services Agreement between Provider and Customer described below:

Provider: ________________________________
Customer: ________________________________
Agreement Number: ________________________________
Effective Date: _________________ ___, 20__

---

1. General. This Schedule describes those Information Security Services to be performed by Provider which serve to protect Customer Data, Provider Systems and related resources against improper access, abuse, loss, destruction, alteration or other information security risks. This Schedule is supplemental to the terms and conditions of the Agreement; in the event of any conflict or ambiguity between the terms of this Schedule or any other terms or conditions set forth in the Agreement, the terms of this Schedule shall be deemed controlling between the parties.

2. Additional Capitalized Terms. This Schedule uses certain capitalized terms that have the specific defined meanings set forth below. This Schedule uses certain additional capitalized terms, for which the meanings are provided in the remaining terms and conditions of the Agreement.

   "Certificate" means the written certificate delivered to Provider by a Certification Body which certifies the ISMS of Provider, as more fully described in Annex A to this Schedule.

   "Certificate Date" means the date on which the Certificate was issued by the Certification Body.

   "Certification Body" means the third party that (a) has been accredited by [insert name of the accreditation body for the Certification Body] to assess and certify information security management systems of organizations with respect to ISO 27001 and any required supplementary documents, and (b) has issued the Certificate for the ISMS. The Certification Body is more fully described in Annex A to this Schedule.

   "Controls" means those controls performed by Provider pursuant to, and in furtherance of, the ISMS, together with any additional Selected Controls which Provider is required to perform, for (a) the purposes of verifying that an electronic communication, signature or performance is that of a specific Person, (b) detecting changes or errors in Data contained in an electronic record or (c) otherwise protecting any Systems or records against improper access, alteration, destruction or loss. "Controls" may include, without limitation, adopted procedures that require the use of algorithms or other codes, identifying words or numbers, encryption, sum digit calculations, callback or other acknowledgment or verification procedures, access management tools, monitoring and reporting functions as well as other devices or procedures contemplated by ISO 27001 or ISO/IEC 17799 or its successors.

"Information Security Event" means an identified occurrence involving any Provider System indicating a possible breach of information security policy or a failure of any Controls, whether occurring currently or at a previous time (at which time the occurrence was not discovered[25]).

"Information Security Incident" means a single or a series of information security events that have a significant probability of compromising the security of the Services or any Customer Data or the effective performance of the ISMS (including Selected Controls).

"Information Security Management System" (or "ISMS") means those information security management systems through which Provider performs and manages the Information Security Services, including all Provider Systems and Controls employed pursuant to, and as a part of, the ISMS. The ISMS includes all policies, procedures or protocols that relate to the manner in which the management systems and relating Information Security Procedures are performed.

"Information Security Services" means those Services to be performed pursuant to this Schedule through which Provider performs activities that serve to secure the Customer Data, including all Controls.

"ISMS Records" means and includes those records relating to the Information Security Services, including those relating to the ISMS, and all records required to be retained pursuant to ISO 27001 (including without limitation, records relating to Information Security Incidents and Information Security Events) maintained by Provider in an electronic or other medium, which are retrievable in perceivable form by Provider. The ISMS Records also include the Statement of Applicability.

"ISO 27001" means the international standard published by the International Organization for Standardisation (ISO) entitled "27001: Information technology—Security techniques—Information security management systems—

[25] The parties may wish to include in a separate Annex a description of specific occurrences which will constitute Information Security Events (or Information Security Incidents, which are separately defined), in order to assure that Provider delivers notice of such occurrences pursuant to Section 4.4 of this Schedule. By example, this might be appropriate if Customer is subject to disclosure or notice obligations arising from Information Security Events (or Information Security Incidents) that relate to unauthorized access to Customer Data that is personally identifiable information; another example might be a virus attack on either Customer or Provider that impacts the overall Services.

Requirements", the most recent published version of which is dated [October 15, 2005][26], together with any and all additional standards identified within ISO 27001 that are relevant to implementing ISO 27001.[27]

["Exclusions" means those Controls that have not been implemented by Provider as part of the ISMS, as described in the ISMS Records, the exclusion of which has been reviewed and approved by the Certification Body as part of the process through which the Certificate was issued.[28]]

"Nonconformities" means any features or operations of the Information Security Services (including, without limitation, any Controls) that fail to conform to the requirements of the ISMS or relevant Applicable Law, whether identified in connection with any Information Security Event, Information Security Incident, as the result of internal ISMS audits by Provider or following any surveillance or reassessment conducted by the Certification Body.[29]

"Provider Systems" means those information systems, computers, networks, applications, operating documentation and personnel employed by Provider to perform the Services, including the Information Security Services.[30]

"Reports" means those reports included in the ISMS Records, whether prepared by Provider, the Certification Body or any other Person, which (a) evaluate the performance of the ISMS and all Controls, including any surveillance or reassessment reports produced by the Certification Body during the term of the Agreement, (b) report on Information Security Incidents or Information Security Events, including without limitation, any remediation or corrective actions taken in response to such items, or (c) otherwise inform Provider of the ongoing

[26] ISO will update various standards or issue supplemental standards from time to time; it is important to be sure all parties are in agreement as to which version of each applicable standard is being relied upon by them. Parties may wish to consider including supplemental standards if applicable—for example, ISO is currently planning (as of January, 2007) to re-issue ISO/IEC 17799 as a supplemental standard under ISO 27001.

[27] ISO 27001 was published in order to harmonize information security management with other business management standards within the ISO business management library. Some ISO 27001 criteria anticipate compliance with those other standards will also be occurring; if that is not the case, it is appropriate for the Provider to identify the exceptions as Exclusions, to be described on Annex C.

[28] See ISO 27001, Sec. 2. "Any exclusion of controls must be justified and evidence needs to be provided that the associated risks have been accepted by accountable persons." The purpose of identifying Exclusions, to be disclosed on Annex C, is to assure that Customer does not misplace its reliance on a Certificate; requiring Provider to identify Exclusions helps Customer assure that Provider's ISMS is, in fact, suitable for the Customer Data and related transactions.

[29] See 27001, Secs 6, 8.1. Nonconformities are important to transparency; if they exist, the value of a Certificate to a Customer is greatly diminished unless the Nonconformities are remedied or otherwise addressed within the ISMS in order that the associated risks are controlled or transferred.

[30] This definition may not be required if the Agreement otherwise provides an equivalent defined term; the objective is to describe all of the materials employed by Provider to perform the Services. The definition is inclusive of operating documentation and procedures, since the polices and rules by which the remaining assets are administered are important to their overall functionality and are often important components within Controls.

effectiveness of the ISMS or the Information Security Services performed under this Agreement.[31]

"Selected Controls" means those Controls described on Annex B to this Schedule that Provider is required to perform, and for which Provider is to provide related reporting to Customer, as more fully provided in Section 4.3 of this Schedule.[32]

"Statement of Applicability" means the Statement of Applicability relating to the ISMS prepared by Provider, describing the control objectives and Controls that have been implemented by Provider as part of the ISMS.[33]

3. Representations and Warranties.

3.1. Representations and Warranties. Provider hereby represents and warrants to Customer the following with respect to the ISMS, the Provider Systems and related matters:

3.1.1. Use of ISMS for the Services. In performing the Services (including all Information Security Services), Provider shall have full access to, and use of, the ISMS, together with all related Controls, described in the Certificate and the Statement of Applicability.[34]

3.1.2. ISMS Properly Certified. The ISMS has been properly certified by the Certification Body and Supplier has obtained a Certificate for the ISMS from the Certification Body prior to the Effective Date.[35]

[31] ISO 27001 establishes various requirements for an organization to establish and maintain the types of reports described within this definition; as a result, this definition does not impose any additional obligation on Provider but only serves to support the inspection rights of Customer under Section 4.9 of this Schedule.

[32] While a Customer is expected to rely on a Certificate to assure the existence of an ISMS, the specific needs of a specific transaction may justify Customer requiring that specific Controls be described in further detail and that the measurement of their effectiveness be disclosed to Customer as part of the Services. Specific controls may also be required in order for Customer to assure that Provider complies with legal regulations applicable to Customer. In non-ISO 27001 parlance, these types of requirements are referred to as "service level agreements" or "SLAs". This definition, and related terms set forth in Sections 4.1, 4.2.1, and 4.9 of this Schedule permit Customer and Provider to designate specific Controls and the responsibility of Provider to report to Customer on the effectiveness of those Controls.

[33] The Statement of Applicability provides a summary of decisions concerning risk treatments and the decisions regarding Exclusions. Review of the Statement of Applicability by Customer permits Customer to confirm the suitability of Provider's analysis of the various risks and the responsive objectives and Controls, without requiring an exhaustive evaluation of all of the Controls. If Customer is aware of specific risks unique to Customer's requirements, a review of the Statement of Applicability will enable Customer to assure those risks are considered and possibly addressed in defining the overall Information Security Services.

[34] It is essential to a 27001 approach that the ISMS described in the Certificate on which Customer is to rely is available to Provider, together with all related Controls, and that Provider will not employ other resources to provide the Information Security Services.

[35] This term places the responsibility on Provider that the certification process has been properly performed and that a Certificate has been obtained prior to the Effective Date. The requirements for a proper certification review are detailed in EA-7/03, EA Guidelines for the Accreditation of Bodies Operation Certification/Registration of Information Security Management Systems ("EA-7/03"). As of January 2007, that publication was scheduled to be issued in a revised format to more fully reference ISO 27001.

3.1.3. ISMS Authorization by Management. The ISMS has been authorized for implementation and operation by the Board of Directors of Provider, or by any committee of the Board or officer to which the authority to provide such approval has been delegated by such Board, and such authorization has not been withdrawn or modified since such authorization was obtained.[36]

3.1.4. ISMS Fully Implemented. [Except as provided on Annex C (Statement of Exclusions)], (a) Provider has fully implemented and operates the ISMS consistently with the description and requirements set forth in the ISMS Records maintained by Provider, and (b) since the Certificate Date, Provider has not suspended, withdrawn or made any material changes to the ISMS or any of the Controls in effect on the Certificate Date.[37]

3.1.5. Statement of Applicability. Provider has developed and accurately maintains the Statement of Applicability relating to the ISMS as part of the ISMS Records. Prior to the Effective Date, Provider has reviewed the Statement of Applicability and confirmed that all of the Provider Systems and Controls to be implemented pursuant to the Agreement, including any Selected Controls, have been accurately described in the Statement of Applicability and that the Services, including the Information Security Services, require no changes in the Statement of Applicability in order for the Statement of Applicability to correctly describe the overall operating environment of Provider in which the Information Security Services will be performed.[38]

3.1.6. Compliance with Applicable Law. The Information Security Services comply with all Applicable Law relating to Provider and, to Provider's knowledge, none of the Information Security Services fail to comply with

The term anticipates that Provider has already successfully completed the ISO 27001 certification process prior to the Effective Date; this provides assurance to Customer that the information security services are well-defined and in place to support the overall Services.

[36] ISO 27001, Sec. 4.2.1 (i) requires "management authorization" but does not specify the level of authorization required. Consistent with several United States regulations that require Board of Directors involvement in such matters (*see*, e.g., 17 CFR 248.30, the SEC Privacy Rule), this term contemplates that the Board has directly or indirectly authorized the ISMS; since this is a factual representation, if necessary, the language should be modified to accurately describe the level of management authorization that has been obtained.

[37] This warranty reaffirms the reasonableness of relying on the Certificate, representing Provider's assurance that the ISMS is implemented and operated consistently with the Certificate.

[38] This warranty similarly reaffirms the reasonableness of relying on the Statement of Applicability; Provider's warranties assure that no changes are required in order for the Information Security Services to be performed. If changes are required, the Statement of Applicability can be modified or the parties can address the changes by amending the text and indicating with a separate annex the Information Security Services that are not addressed by the Statement of Applicability.

any Applicable Law to which Customer is subject relating to the Services being performed.[39]

3.1.7. No Transferred Risks or Residual Risks. Except as set forth on Annex C (Statement of Exclusions), (a) Provider has not transferred to any other Person, including any Subcontractor, insurance carrier or Customer, any risks (as such term is described in ISO 27001) relating to the Provider Systems or the Services (including the Information Security Services) and (b) Provider has not identified any residual risks (as such term is described in ISO 27001) remaining after the ISMS has been implemented that relate to the Provider Systems or the Services (including the Information Security Services).[40]

3.1.8. ISMS Certification.[41] With respect to the Certificate that Provider has obtained with respect to the ISMS:

3.1.8.1. Annex A properly and accurately describes (a) the Certificate (including the Certificate Date, the term during which the Certificate is in effect, and the ISMS to which the Certificate relates), and (b) the information available to Provider with respect to the Certification Body. Provider has delivered to Customer a true and accurate copy of the Certificate.

3.1.8.2. The Certificate has not been suspended, withdrawn or revoked in any manner, nor has the Certification Body taken any action to modify the description of the ISMS to which the Certificate relates. Provider has received no notice from the Certification Body that the Certification Body is considering any such suspension, withdrawal, revocation or modification, whether as a result of any surveillance, reassessment or other action by the Certification Body.

3.1.8.3. Provider has received the Certificate from a Certification Body properly accredited for such purposes by an accreditation body authorized to provide such accreditation with respect to ISO

[39] This warranty is intentionally included, in addition to a similar warranty on legal compliance that may be included in the Agreement; the separate treatment of the topic is intended to assure full attention has been given to Applicable Laws that impact both Provider and Customer with respect to information security. Since many services to which this Schedule may apply will be offered by Providers with special experience in certain industries, it is not unreasonable for Provider to have knowledge of what activities will or will not comply with Applicable Law relating to an industry in which Customer operates.

[40] This warranty helps assure Customer that reliance on the Certificate does not inadvertently expose Customer to any undisclosed Exclusions which Provider has knowingly not addressed within the ISMS (as a result of unaddressed residual risks or transferred risks).

[41] This warranty helps assure Customer of the quality of the Certificate itself, the identity (and accreditation) of the Certification Body and related factual matters important to the continuing utility of the Certificate during the Agreement.

27001 and related information security management systems. To Provider's knowledge, the accreditation for such Certification Body has not been revoked, suspended or otherwise limited since the Certificate Date.

3.1.8.4. Prior to the Effective Date, Provider has reviewed the accreditation under which the Certification Body has acted and confirmed that the issuance and delivery of the Certificate, as well as the performance of related services which the Certification Body has performed, are within the scope of the accreditation received by the Certification Body.

3.1.8.5. Provider has entered into binding agreements with the Certification Body (or another certification body capable of satisfying the accuracy of Sections 3.1.8.1 through 3.1.8.3 above) to require (a) the surveillance of the ISMS and related Provider Systems not less than once during each calendar year of the Term, and (b) the reassessment of the ISMS within three years of the Certificate Date. Provider has no knowledge of any reason why either Provider or the Certification Body will not proceed with and complete the performance of all surveillance and reassessment services contemplated under the applicable agreements. Annex A accurately describes the date(s) on which the surveillance and reassessment services are currently scheduled.

3.2. Relationship to Other Terms. The representations and warranties made in this Section 3 are supplemental to any additional representations and warranties made elsewhere in the Agreement. In the event of any conflict or ambiguity between the terms of this Section 3 or any other terms or conditions set forth in the Agreement, the representations and warranties set forth in this Section 3 shall be deemed controlling.

4 Provider Duties.

4.1. Implement and Maintain ISMS. Provider shall employ the ISMS to perform the Information Security Services and, at all times, shall maintain the ISMS pursuant to the Statement of Applicability and the Certificate. Except as described on Annex A, Provider shall manage and execute all of the Information Security Services pursuant to the ISMS and employ the Controls described within the ISMS Records (including the Statement of Applicability), and, if not so described, all Selected Controls, if any.[42]

[42] Provider's obligation to employ the Controls described within the ISMS Records obligates Provider to employ Controls the details of which may not be fully disclosed to Customer, but which are summarized in the Statement of Applicability. This result balances Customer's interest in having assurances the ISMS is

4.2. Changes in Controls.[43]

4.2.1. In the event that Provider wishes to make [material] changes in any of the Controls, Provider shall notify Customer pursuant to Section ___ of the Agreement.[44] Provider shall include in Provider's notice to Customer (a) a description of the Controls affected by the proposed changes, including a specific identification of any Selected Controls that are affected, (b) the scheduled effective date for the proposed changes, and (c) whether (i) Provider has any reason to believe that the proposed changes will adversely impact the applicability of the Certificate after installing the related changes or (ii) as a result of the proposed changes, any risks relating to the Controls are being transferred to any other Person or any residual risk (including relating to risks not previously identified and considered as of the Certificate Date) is remaining unaddressed.[45]

4.2.2. Provider shall attempt to notify Customer sufficiently in advance of the effective date of the proposed changes in order to provide Customer and Provider a mutual opportunity, acting in good faith, to review whether the proposed changes, when implemented, will adversely impact the performance of any of the Services, including any Selected Controls, or the continued applicability of the Certificate to the ISMS; the parties mutually acknowledge that certain changes may require immediate action by Provider for which prior notice will not be commercially feasible and, in such event, Provider shall provide the required notice to Customer following the installation of the changes as soon as it is commercially feasible to do so.

being fully implemented against Provider's desire to not fully disclose sensitive details regarding the information security controls.

[43] The parties should consider the overall value of this Section carefully. One benefit of the ISO 27001 process is that an organization can create various solutions for the Controls that fulfill recognized objectives stated within the ISMS and thereby address the related risks. As a result, Customers should restrain from imposing restrictions on a Provider that limit the Provider's ability to make changes within the ISMS, provided the Certificate is not invalidated by the changes. In some circumstances where information security services are vital, stronger restrictions (as set forth in this section) may be appropriate. While parties may wish to define what constitutes a "material change" in greater detail, without further definition, "material changes" are likely those that would (a) invalidate the Certificate or (b) compromise the effectiveness of any Selected Controls in a manner adverse to a Customer's interests.

[44] The cross-reference is intended to identify the term or terms within the Agreement that describe relationship administration, notices, etc.

[45] This section serves to provide a mechanism by which Provider can operate with some level of flexibility in managing the ISMS, while still assuring Customer that changes will not impact the quality of the Information Security Services. Whether notice is given only of material changes, versus notice of all changes, is a topic of negotiation; however, the purpose of an ISMS and Certificate-based approach is to provide Customer with the assurances that ongoing changes will not adversely impact the quality of the Information Security Services. A further option is to eliminate this section, on the basis that Customer has sufficient assurances in place provided the continuing validity of the Certificate is not placed at risk.

4.2.3. Following receipt of any prior notice from Provider under this Section 4.2, Customer shall cooperate in good faith with Provider to review whether the proposed changes will adversely impact the performance of the Services, including any Selected Controls, or the continued validity of the Certificate. In the event Customer determines the proposed changes will have an adverse impact on any of the preceding, Customer shall so notify Provider and Provider shall subsequently cooperate with Customer to review the proposed change and consider alternative changes will eliminate or minimize the perceived adverse impact. Customer and Provider mutually acknowledge that[, except as provided in Section 4.2.4,] Customer's right to receive notice and to cooperate with Provider under this Section 4.2.3 does not grant Customer any right to prevent or interfere with the implementation of any proposed changes.[46]

4.2.4. [In the event either a) Provider's notice under Section 4.2.1 indicates that Selected Controls will be affected by the proposed changes, or b) Customer determines pursuant to Section 4.2.3 that the proposed changes will cause any of the Selected Controls to be ineffective in controlling the risks identified with any of such Selected Controls, Provider shall not install the proposed changes without first securing Customer's written approval, which shall not unreasonably withheld or delayed, of the proposed changes or alternatives to the proposed changes.][47]

4.3. Reporting on Controls; Effectiveness.

4.3.1. Provider shall produce and maintain (a) all Reports required pursuant to the ISMS and (b) all Reports relating to the performance or effectiveness of the Selected Controls required by Annex B. Provider shall maintain all such Reports during the Term, and for a period of [three] years following the end of the Term.[48] Provider shall make all such Reports available to Customer pursuant to any inspections performed pursuant to Section 4.9.

4.3.2. Not less than [once each calendar month/quarter/year], Provider shall deliver to Customer a written statement, in the form attached as Annex D, certifying that, during the time period since the Effective Date (or the date of the prior written statement), all of the Controls, including all of the Selected Controls have been performed as required by the ISMS and that

[46] Note: Customer otherwise would have recourse under normal Agreement provisions if the proposed changes do prevent the Services from being performed or result in a breach of the related warranties.

[47] This section is optional; as an alternative, Customer's prior approval would not be necessary unless Provider knows the changes will make it impossible to comply with Selected Controls.

[48] The duration of the retention period will be influenced by any requirements on Customer to retain specific records for the purposes of fulfilling audit or compliance obligations. For example, if the Services and Controls relate to business records subject to a public company's Sarbanes-Oxley compliance program, a seven year retention period may be appropriate. See Rule 2-06 of Regulation S-X. Drafters are encouraged to consider the survival clause in the Agreement with respect to retention obligations that are intended to be binding following the expiration or termination of the Agreement.

no Information Security Incidents or Information Security Events have occurred (except as otherwise reported, if at all, pursuant to Section 4.4 below).[49]

4.4. <u>Monitoring; Information Security Events and Information Security Incidents</u>.

4.4.1. Provider shall perform on a timely basis all monitoring and review procedures that are required pursuant to the ISMS, including, without limitation, those procedures employed to detect processing errors, identify any attempted or successful security breaches (whether from external or internal sources), and measure the effectiveness of the Controls implemented pursuant to the ISMS. [Without limiting the preceding, Provider shall conduct internal audits of the ISMS at planned intervals [Alternate: not less than once every ___ month(s)/calendar quarter] to determine the Controls and other procedures described by the ISMS conform to the requirements of Applicable Law and identified information security requirements, perform as expected and are effectively implemented and maintained.][50]

4.4.2. Provider shall immediately notify Customer when any Information Security Event or Information Security Incident occurs that involves either of the following:

(a) any Provider Systems which are identified in the ISMS, whether or not those Provider Systems are directly employed for the Services [alternate A: any Provider Systems directly employed for the Services][alternate B: any Customer Data stored or processed on any Provider Systems directly employed for the Services]; or

(b) the performance (or the failure to perform) of any of the Selected Controls.

[In the event the attention required to respond to an Information Security Event or Information Security Incident does not permit Provider to immediately so notify Customer, Provider shall deliver such notice to

[49] Both the form and the frequency of the written statement may be influenced by external compliance obligations imposed on Customer, as well as internal control practices Customer may maintain. For example, as of January, 2007 a public company in the United States must possess this statement within a specific period (generally six months) prior to the date the company provides the attestations required by the Sarbanes-Oxley regulations.

[50] See ISO 27001, Sections 6-8. Internal audits are required under ISO 27001 as a part of an ISMS, but no specific frequency is required. This optional sentence provides Customer greater assurance of that frequency; a Customer may also wish to specify criteria or requirements describing the independence of Provider’s staff conducting the internal audits from the operations of the ISMS.

Customer as soon as reasonably practicable.][51] Following the delivery of any such notice, Customer and Provider shall cooperate in investigating the circumstances relating to the reported Information Security Event or Information Security Incident in order to enable appropriate responsive or corrective actions to be taken.

4.5. Reporting on Surveillances/Reassessments.[52] Provider shall cooperate with the Certification Body in the performance of all surveillances and reassessments of the ISMS which the Certification Body is to perform during the Term. Provider shall deliver to Customer reasonable prior notice (not less than __ days) if any surveillance or reassessment activity requires Customer participation or involvement. Provider shall include any related evaluations or reports delivered by the Certification Body in the ISMS Records. Following the receipt of each such evaluation or report, Provider shall deliver to Customer written notice of such fact within 10 days following receipt and shall include in such notice a written confirmation indicating whether or not the Certificate remains valid following the related surveillance or reassessment. If the evaluation or report requires Provider, as a condition to retaining the validity of the Certificate (a) to eliminate any Nonconformities or (b) to amend any of the Selected Controls, Provider's written notice shall summarize those conditions and indicate whether taking any related actions will affect in any manner adverse to Customer's interests the ability of Provider to perform the Services and comply with Provider's obligations, including those under this Schedule.

4.6. Eliminating Nonconformities, etc.. The following provisions apply in the event (a) Provider knowingly fails to complete any of the monitoring and review procedures identified in Section 4.4.1[, including, without limitation, any internal audits], (b) Provider notifies Customer of an Information Security Event or Information Security Incident pursuant to Section 4.4.2, or (c) any evaluation or report from the Certification Body pursuant to Section 4.5 requires Provider, as a condition to retaining the validity of the Certificate (i) to eliminate any Nonconformities or (ii) to amend any of the Selected Controls:

4.6.1. Provider shall immediately undertake, and continue until completed, all necessary actions required to eliminate any related Nonconformities, or otherwise remedy the related circumstances in order that the risks associated with the Nonconformities (or identified in connection with the

[51] In the absence of ISO 27001, Provider's obligation to notify Customer of information security events or incidents can be one of the most difficult terms to negotiate. However, a certified ISMS must establish and maintain suitable monitoring processes and must create and maintain the related records; as a result, many of a Provider's historic objections do not continue to be applicable. The alternatives are not the exclusive choices by which to describe the trigger events for notice to Customer but illustrate the most likely options in an ISO 27001 environment. It is contemplated the requirement to provide notice relating to Selected Controls will line up with any specific regulatory obligations imposed on Customer to monitor the security relating to those Selected Controls (e.g., protection against improper access to identifiable personal information).

[52] *See* ISO 27001, Sec. 2.1.16.4.

Information Security Event or Information Security Incident) have been addressed and that the responsive Controls have been incorporated into the ISMS. As appropriate, Provider shall conduct any testing or verification required to demonstrate that (i) the related Nonconformities have been remedied and (ii) the related Controls are performing in an effective manner; upon Customer's reasonable request, Provider shall make available for inspection all ISMS Records applicable to the preceding activities.

4.6.2. Provider shall communicate with Customer on a regular basis to inform Customer of the status of Provider's activities under Section 4.6.1 and shall confirm in writing to Customer when the related activities have been completed to Provider's satisfaction. In the event of (a) any Information Security Event or Information Security Incident pursuant to Section 4.4.2, or (b) any evaluation or report from the Certification Body pursuant to Section 4.5 requires Provider to amend any of the Selected Controls, Provider shall cooperate with Customer, at Provider's cost, in making available any ISMS Records to confirm the related Controls are performing in an effective manner after Provider's activities under Section 4.6.1 have been completed.

4.6.3. Notwithstanding any other provision of this Schedule, in the event a Selected Control must be amended in order to eliminate a Nonconformity, to respond to additional risks required to be managed within the ISMS, or otherwise to assure that the Certificate remains valid, Provider shall be entitled to take the necessary action as Provider sees fit without the prior approval of Customer if Provider reasonably determines, acting in good faith, that the effectiveness of the related Selected Controls will not be adversely impacted and that Customer's operations will otherwise not be adversely affected (which determinations Provider shall document in the ISMS Records as part of the related change process). In all other events, Customer's prior approval of an amendment to Annex B will be required before the Selected Controls are modified.

4.6.4. Notwithstanding any other provision of this Schedule, in the event Customer wishes to make modifications in Customer's operations which could impact the operation or effectiveness of any Controls, including Selected Controls, operated by Provider, Customer shall notify Provider in advance and obtain Provider's approval of any such changes prior to their implementation. Provider shall not be responsible for any Information Security Incidents, Information Security Events or any failures of any Controls to perform as expected if such Incidents, Events or failures result from modifications in Customer's operations to which Provider had not provided prior approval.

4.7. Customer Complaints on Information Security Services.[53] Provider shall provide as part of the Information Security Services a separate mechanism through which Customer shall be able to notify Provider of any possible Information Security Event or Information Security Incident occurring with respect to any aspect of the Services to be performed under the Agreement. Provider's mechanisms shall include both telephonic and electronic means of communication and shall support an escalation of priority based on the severity of the impact on the ongoing performance of the Services.

4.8. Staffing; Subcontractors. Provider shall perform all of the Information Security Services employing full-time or part-time employees. Provider shall not rely on any Subcontractors to perform any of the Information Security Services (unless the use of such Subcontractors, and the scope of the Information Security Services they perform) have been specified in Annex B (Selected Controls).[54]

4.9. Inspection of ISMS Records. Provider shall maintain all ISMS Records relating to the ISMS and the Information Security Services during the Term and for a period of [___] years following the expiration or termination of the Agreement.[55] Customer shall be entitled to inspect the ISMS Records (a) on an annual basis, to occur not more than once during each calendar year, to confirm that all of the Selected Controls are performing in an effective manner and as required by this Agreement; (b) following any Information Security Event, Information Security Incident or change in Selected Controls reported to Customer, to the extent required to confirm that the related Nonconformities have been eliminated or that

[53] Customers may wish for this to be detailed as a separate Selected Control. Providers may wish to eliminate this provision and merely rely on normal relationship management services; however, there is significant potential value to assuring that information security complaints (which may or may not be related to possible Information Security Events or Information Security Incidents) can be communicated directly between the security organizations of Customer and Provider. This term provides the mechanisms for that direct communication channel to be structured.

The parties may also wish to include in the primary Agreement's terms addressing dispute resolution additional provisions that specifically describe how to resolve information security complaints arising under the Schedule—security-related incidents often require priority attention, collaboration among multiple stakeholders and, in the final analysis, are rarely considered as a sufficient basis to otherwise terminate the primary commercial relationship.

[54] This section does not address the qualifications or criteria any employee or subcontractor must meet, including the results of appropriate background checks. This section is a function of ISO 27001 terms that treat subcontractors as entities to whom risk is transferred; thus, the language helps assure Customer that the ISMS is being properly executed by Provider's employees and not being subcontracted or outsourced without suitable notice (and possible approval). Annex B provides the ability for Provider to specify the use of Subcontractors and for the parties to establish any Controls (such as background checks and criteria) that should be performed in connection with the use of those Subcontractors.

[55] ISO 27001, Sec. 4.3.3 requires Provider to establish, maintain, protect and control records that provide evidence of conformity to the requirements of ISO 27001 and the effective operation of the ISMS, and establishes the criteria the records must remain legible, readily identifiable and retrievable. The duration of the time period is likely a function of Applicable Law with which Customer must comply or any reservation of rights between the parties provided in the Agreement. *See also* notes accompanying Section 4.3 supra.

related Controls are performing in an effective manner and as otherwise required by the ISMS; or (c) when any inspection of the ISMS Records is required by legal process or regulatory inquiry to which Customer is subject. Provider shall make the ISMS Records available for any such inspection at Provider's principal location from which the Services are performed, during normal business hours, in the media and format in which the ISMS Records are maintained; in connection with any inspection, Provider shall provide the necessary computer equipment and applications to access the ISMS Records and personnel to assist in the inspection process. [Provider shall be entitled to charge Customer an inspection fee, as set forth in the Agreement, in connection with any inspections conducted under this section.[56]] All ISMS Records shall be considered as Provider's Confidential Information.

[56] Provider may wish to specify an inspection fee to compensate for the time and resources required to support Customer's inspection rights; any such fee should be set forth in the terms of the Agreement which express all applicable fees and expenses.

Annex A

Description of Certificate and Certification Body

Description of the Certificate:

Certificate Number:
Name of ISMS Operator:
Scope of Certified Activities:
Original Date of Issue:
Latest Issue:
Expiration Date:

Certification Body:

Name:
Address:
Contact information:
Accreditation by:

Annex B
Selected Controls

Description of Selected Controls

Reporting Requirements for Selected Controls

Annex C
Statement of Exclusions

Exclusions

Transferred Risks

Annex D

Form of Periodic Certification

[to be negotiated between the parties]

Annex of Selected Information Security Resources

This Annex presents a selection of resources that can be relied upon in connection with studying or using this Book. There are many different resources that could be included in this selection—the topic of information security and its relationship to various corporate functions and business topics is robust. For those resources that are included, no endorsement is intended by the fact the listed materials have been included, nor is the exclusion of any specific materials meant to diminish their possible utility.

The Internet Security Alliance joins with many other organizations in valuing the importance of standards and best practices as strong resources to be employed for improving information security. In addition, considerable work has been done by government agencies which provide invaluable guidance to private companies. These materials are intended to highlight the organizations, standards, and publications often recognized as those on which many companies and industries rely.

This Annex was prepared in January 2007; readers are reminded that additional useful publications may become available after that date and that publications referenced here may be subsequently updated or revised.

Organizations

The following organizations maintain Internet-accessible resources addressing information security management:

Internet Security Alliance	www.isalliance.org
Information Systems Security Association	www.issa.org
Information Systems Audit and Control Association	www.isaca.org
International Chamber of Commerce	www.iccwbo.org
International Organization for Standardization	www.iso.org
Organization for Economic Cooperation and Development	www.oecd.org
World Bank	www.worldbank.org
Carnegie Mellon University Software Engineering Inst.	www.sei.cmu.edu
Japanese Computer Security Association	www.jcsa.or.jp
British Standards Institute	www.bsi-global.com

For some industries, specific organizations also exist that make information security a primary focus:

Financial Services Roundtable: BITS (Banking Information Technology Secretariat)	www.bitsinfo.org
American Chemistry Council	www.americanchemistry.com

Standards

The following standards organizations have published standards addressing information security management:

International Organization for Standardisation	www.iso.org
British Standards Institute	www.bsi.org.uk
American National Standards Institute	www.ansi.org
Bundesamt fur Sicherheit in der Informationstechnik	www.bsi.bund.de

Publications

The following publications may be useful in providing greater in-depth discussion of the management issues relating to information security.

<u>Management Guides</u>

Internet Security Alliance Common Sense Guide for Senior Managers (2002)	www.isalliance.org
Contracting for Information Security in Commercial Transactions: An Introductory Guide (2005)	www.isalliance.org
Building Security in the Digital Resource: An Executive Resource—Business Roundtable (2002)	www.businessroundtable.org
ICC Handbook on Information Security	

Policy for Small to Medium Enterprises (2003)	www.iccwbo.org
BITS Framework for Managing Technology Risk in IT Service Provider Relationships	www.bitsinfo.org
IT Baseline Protection Manual- P BSI 7152 E1, BSI—Bundesamt fur Sicherheit in der Informationstechnik	www.bsi.bund.de

Governance Guides

Information Security Oversight: Essential Board Practices (National Association of Corporate Directors)	www.nacdonline.org
IT Governance Implementation Guide	www.isaca.org
Turnbull Report—Internal Control Guidance for Directors on the Combined Code	www.icaew.co.uk