



# Information Security for Small and Medium Sized Businesses

---

*Creating a Business Focused Security Plan for Small and Medium Sized Businesses*

Prepared for

Norwich University, MSIA  
Seminar Six: Management Tools  
Final Essay

*Report prepared by:*

Becki True, CISSP  
[becki@beckitrue.com](mailto:becki@beckitrue.com)

# Table of Contents

---

**INFORMATION SECURITY FOR SMALL AND MEDIUM SIZED BUSINESSES**  
..... 5

**Executive Summary** ..... 5

**Introduction** ..... 6

    Why Information Security is Important ..... 6

    Approach ..... 7

    Organization ..... 8

**PART ONE: CREATE A COMPREHENSIVE SECURITY PROGRAM**..... 8

**Align Security to Support the Business** ..... 9

    The ISM3 Framework ..... 10

    Defining Business Objectives ..... 10

        Example: Acme Sports Memorabilia ..... 11

        Risk Committees and Advisory Boards ..... 13

        A Word About Best Practices ..... 13

    The Unified Compliance Framework ..... 14

    UCF Organization ..... 15

        Using UCF for Compliance ..... 16

        Using the UCF Spreadsheets to Create a Security Controls List ..... 17

    Metrics ..... 19

**Conclusion** ..... 20

**Glossary** ..... 21

**Bibliography** ..... 22

## List of Tables

---

Table 1: ISM3 Relationship between business and security objectives .....10  
Table 2: Mapping Security Targets to Business Objectives.....11  
Table 3: Example of harmonized control list using UCF spreadsheet.....18

## List of Figures

---

Figure 1: How the harmonized control relates to the authority documents and metrics.....15

# Information Security for Small and Medium Sized Businesses

## *Creating a Business Focused Security Plan for Small and Medium Sized Businesses*

The following paper is the first part of a yet-to-be published book on information security (IS) for small and medium sized businesses (SMBs). It is the author's intent that this paper be read from that point of view, even though it is submitted as the Master of Science in Information Assurance (MSIA) final paper. The intended audience for the book is SMB owners, managers, and information technology (IT) practitioners.

**Note:** For the purposes of the MSIA paper, the scope of this paper is limited to the creation of a security plan for SMBs.

---

## Executive Summary

This book will help the SMB owner, manager, or IT professional understand how to create an information assurance (IA) strategy, and the tactics required to implement that strategy. The goal of this book is to help the SMB executive create a cost effective security strategy that supports business objectives and compliance requirements.

According to the Information Security Management Maturity Model (ISM3), "to be secure means to be reliable, in spite of attacks, accidents and errors."<sup>1</sup> This definition is different from what many people may think of as the definition of security, to be invulnerable to attacks. It is impractical for most businesses to spend the amount of money it takes to be invulnerable to attacks, if invulnerability is even possible, so there must be another option.

Security spending has to make good business sense, just as any decision about how and where to spend capital and human resources. To be cost effective, increased revenues, reduced expenses, or both must offset the cost of security. A business should spend enough on security to support the business objectives, and not a penny more.

However, business owners and executives often do not know how much they should spend on security or where they should spend it. The resulting confusion often results in

---

<sup>1</sup> Vicente Aceituno, Information Security Management Maturity Model v2.10, 15.

frustration between the business decision makers and those responsible for information technology (IT) or information security (IS). The business executive management does not understand the benefit of spending money on IS and the IT people think the executives “don’t get it”. The problem is that these two groups do not speak the same language or share the same point of view.

This book will help the SMB executives focus their security efforts where they help the bottom line. SMB executives and IT staff will learn to use concepts from the Information Security Management Maturity Model (ISM3) and the Unified Compliance Framework (UCF) to map their security processes and controls to specific business objectives, including compliance requirements. Once a security strategy is created, both the SMB executives and their IT staff or outsource partner can share the same vision and language. Both groups will know:

- Which business objectives are important
- Why they are important
- Which security objectives map to each business objective
- What is expected – the metrics for each objective
- How each metric is measured
- How often each metric is measured
- How often the results are reported and reviewed

By the end of the book the reader will have the knowledge to create:

- A unified security framework that meets business and compliance requirements
- Measurable security objectives that support business objectives
- A list of security controls that meet the business and compliance requirements
- An actionable security plan

## Introduction

SMBs have many of the same IT and information security challenges as large companies do, but they have far fewer capital and human resources to deal with these challenges. Where a large company almost certainly has a dedicated IT staff, a SMB might not have any IT staff. Consequently, there is often a lack of IT and IS expertise available to the SMB executive. These executives have no trusted advisor for information security related matters. This book aims to be that trusted advisor.

## Why Information Security is Important

There are many reasons a SMB owner or manager should pay attention to information security, and they all come down to staying in business. According to ISM3, “to be secure

means to be reliable, in spite of attacks, accidents and errors.”<sup>2</sup> It is fair to say that all businesses want to be reliable in spite of attacks, accidents and errors and few businesses can afford to be shut down for any length of time for any reason.

How long will a SMB survive if it were to lose its data or if it were unavailable for any reason? A recent study by Symantec as reported by eWeek.com found that, “the average SMB has experienced three outages within the past 12 months, with the leading cause being viruses or hacker attacks, power outages, or natural disasters. Affected SMBs estimated the cost of these outages as being about \$15,000 per day.”<sup>3</sup> That amounts to an average yearly loss of \$45,000 plus the cost of any data that may have been lost. That is a large hit to the bottom line in most SMBs. Obviously, outages of a longer duration could cost so much that the business has to close.

Many SMBs are also subject to legal and regulatory compliance requirements. For example, all merchants that accept credit card payments are subject to the Payment Card Industry Data Security Standards (PCI-DSS) requirements. All companies who are in the health care industry and who, “conduct certain financial and administrative transactions electronically” are subject to the Health Insurance Portability and Accountability Act (HIPAA).<sup>4</sup> Many states have their own laws that SMBs must follow too. As an example, companies that do business in Nevada, even online business, must comply with Nevada’s new data privacy law that requires the business to encrypt their customers’ personally identifiable information (PII).<sup>5</sup>

Notice that the reasons a SMB owner should pay attention to information security all have to do with business requirements. There are laws and regulations the SMB owner must follow, and there are real dollar costs associated with service interruptions and data losses. In other words, information security is no longer optional. A SMB owner who ignores this fact is literally gambling with their business future.

## Approach

From the business manager’s point of view, there is little reason to begin with a list of security controls and a discussion on how to implement them. The business owner needs to know how to meet regulatory or compliance requirements, and how IS will improve the bottom line. Therefore, rather than begin with a discussion about security controls and how

---

<sup>2</sup> Vicente Aceituno, Information Security Management Maturity Model v2.10, 15.

<sup>3</sup> eWeek.com, “Survey Indicates Half of SMBs Have no Disaster Recovery Plan”, eWeek.com, <http://www.eweek.com/c/a/Data-Storage/Survey-Indicates-Half-of-SMBs-Have-No-Disaster-Recovery-Plan-687524/>

<sup>4</sup> HHS, “Who must comply with HIPAA privacy standards”, HHS, [http://www.hhs.gov/ocr/privacy/hipaa/faq/covered\\_entities/190.html](http://www.hhs.gov/ocr/privacy/hipaa/faq/covered_entities/190.html)

<sup>5</sup> Ben Worthen, Wall Street Journal, “New Data Privacy Laws Set for Firms”, WSJ, <http://online.wsj.com/article/SB122411532152538495.html>

to implement them, the book begins with creating the security plan using methods from ISM3 and UCF.

Part two of the book shifts its focus to security controls and a technical discussion on how to implement them.

## Organization

The organization of this book is essentially two books in one:

- Part one is a business discussion about why and how to create a comprehensive security plan.
- Part two is a more technical discussion about security controls.

The organization of part two is to introduce a concept or security control and then follow with two sections:

1. **Why this is important:** a discussion on the topic and why it is important for the reader to understand it.
2. **How to do this:** a technical discussion on how to perform this task or implement this control.

# Part One: Create a Comprehensive Security Program

A comprehensive security plan is a requirement for some businesses. For example, a recently passed Massachusetts law requires that, “that every person or business that has the "personal information" of a Massachusetts resident develop, implement and maintain a "comprehensive information security program ("CISP") that is written in one or more readily accessible parts" by March 1, 2010. In practice, this will mean that you will need to review and update your existing privacy and data protection policies to be compliant with the Regulations and adopt in writing a CISP. You also need to train your employees with respect to such policies.”<sup>6</sup>

The approach of this book is to create a comprehensive security plan using the ISM3 and UCF models. The purpose of the security plan is to provide the SMB owner or manager with a roadmap to follow as they create and maintain their security program.

Using the combination of the ISM3 and UCF models to create the SMB security plan results

---

<sup>6</sup> Association of Corporate Counsel, “New Massachusetts data security law and regulations – comprehensive security plan required before March 1, 2010”, ACC, <http://www.lexology.com/library/detail.aspx?g=d7c1e806-6f3f-4cb5-9080-d2ce0d6cc90f>

in a plan that is focused on supporting the business. The processes and controls are targeted to support the business objectives and compliance requirements. This approach is targeted and efficient because there is no expense or effort spent on activities that do not support a business objective.

ISM3 is a process-oriented security maturity model. “Process management is the core discipline of ISM3. It is through well-defined processes that information security is improved, risk is reduced and maturity is measured. Clear responsibilities are essential to process management and for corporate governance. Security aims must be appropriate to the business needs of the organization and the security in context model helps to achieve this.”<sup>7</sup>

UCF is a controls-oriented model that allows the business to implement a set of security controls that enables the organization to meet all of their business and compliance requirements. “The Unified Compliance Framework (UCF) is the first and largest independent initiative to map IT controls across international regulations, standards, and best practices.”<sup>8</sup> UCF has a database of “authority documents” from hundreds of laws and compliance standards. The user specifies the authority documents with which they are subject and the UCF tools produce a single normalized list of security controls.

For example, SMBs that are required to comply with both PCI-DSS and HIPAA would select those authority documents using the UCF tools and the list of controls would include all the controls common to both PCI-DSS and HIPAA plus those controls that are unique to each. An example of a control that is common to both is the requirement for individual logins to critical computing systems.

In the opinion of the author, using the UCF is much easier for a SMB because the work of compiling, maintaining and learning about new laws and regulations has essentially been outsourced. Trying to make sense of all of the laws, regulations, and dozens of security frameworks can be a full time job for one or more people depending on the business. UCF is a great alternative considering that UCF compiles hundreds of US federal, state, international and industry laws, regulations and compliance requirements as well as security frameworks into a single tool. UCF also sends out updates four times a year.<sup>9</sup> This is a fantastic service for a very reasonable price (\$1000 per year).<sup>10</sup>

## Align Security to Support the Business

The mantra of this book is to spend enough on security to meet business objectives, but not a penny more. How does the SMB owner know how much to spend on security? The SMB

---

<sup>7</sup> Vicente Aceituno, Information Security Management Maturity Model v2.10, 9.

<sup>8</sup> UCF, “IT UCF: What is the UCF”, UCF,  
[http://www.unifiedcompliance.com/what\\_is\\_ucf/](http://www.unifiedcompliance.com/what_is_ucf/)

<sup>9</sup>[http://www.unifiedcompliance.com/it\\_impact\\_zones/faqs\\_1/will\\_we\\_get\\_updates\\_for\\_the\\_ma.html](http://www.unifiedcompliance.com/it_impact_zones/faqs_1/will_we_get_updates_for_the_ma.html)

<sup>10</sup> <http://www.unifiedcompliance.com/buynow.html>

owner must first understand his business and its objectives. How often can he afford his customer database to be unavailable and for how long? With which regulatory and legal requirements is the SMB required to comply? What controls are required to meet the compliance requirements? What percentage of lost revenue due to missing or bad invoicing is acceptable? The answers to these questions determine where and how much to spend on IS.

The SMB owner will suffer one of three fates if she does not know the answers to these questions:

1. The SMB owner will overspend on security
2. The SMB owner will under-spend on security
3. The SMB owner will spend time and money on the wrong activities

Each of these situations places the business at risk of failure.

## The ISM3 Framework

ISM3 is a process-centric maturity model that views security in the context of business. In other words, the ISM3 philosophy is that what is an acceptable level of security in one business may be unacceptable in another.

The table below demonstrates the relationship between the business objectives and the security objectives and controls.<sup>11</sup>

Goals, objectives, needs and limitations	Depend total or partially on...
Business goals	Business objectives
Security objectives	Compliance needs and limitations Technical needs and limitations Business needs and limitations
Compliance needs and limitations	(UCF)
Technical needs and limitations	Environment patching, hardening Malware protection, etc. (UCF)
Business needs and limitations	Access control objectives (UCF)

**Table 1: ISM3 Relationship between business and security objectives**

All of the security objectives will ultimately depend on the controls listed in the UCF using the approach proposed in this book. ISM3 does not promote one framework over any other.

## Defining Business Objectives

<sup>11</sup> Vicente Aceituno, Information Security Management Maturity Model v2.10, 21.

The first step is to start with the business goals to define the business objectives. The exact objectives will be different for each business, but there is a set of goals that is typically common to all businesses, and those will be used for illustrative purposes here.

Common business goals include<sup>12</sup>:

- Making a profit or staying in business
- Provide a product or service
- Attract and grow talent
- Build and grow brand image
- Comply with regulations and contracts
- Act ethically

Remember, our definition of what it means to be secure: to be reliable, in spite of attacks, accidents and errors. Therefore, the security efforts must support these objectives in such a way as to make them reliable in spite of attacks, accidents and errors. For each business objective, we will map a security objective that supports it.

### Example: Acme Sports Memorabilia

Let us examine an example to illustrate this concept. Acme Sports Memorabilia is a SMB that buys and sells sports memorabilia such as baseball cards, sports jerseys, and items autographed by famous sports figures. Acme has their own web site and also uses eBay to buy and sell their products. Customers may also place orders using email, telephone, or fax.

What security objectives would Acme require to support their business goal of providing a product or service? The table below illustrates the linkage of the security objectives to business objectives related to reliably, in spite of attacks, accidents and errors, while providing a product or service.<sup>13</sup>

Business Objective	Security Target
Web server availability to customers	Fewer than five incidents a year lasting less than 30 minutes each
Product database availability	Fewer than five incidents a year lasting less than 30 minutes each
Customer database availability	Fewer than three incidents a year lasting less than 30 minutes each
Customer confidentiality	Fewer than three incidents a year
Customer address precision	Fewer than two incidents per year

<sup>12</sup> Vicente Aceituno, Information Security Management Maturity Model v2.10, 15.

<sup>13</sup> Vicente Aceituno, Information Security Management Maturity Model v2.10, 16.

	<p>where more than 1% of customer addresses are wrong or outdated any working day.</p> <p>Loss is less than 0.1% of accounting value of company</p>
Deliver all products and services ordered	<p>Fewer than 10 incidents a year</p> <p>Loss of less than 0.1% of total revenue</p>
Invoice all products and services delivered	<p>Fewer than 10 incidents a year</p> <p>Loss of less than 0.1% of total revenue</p>
Tax information retention	<p>No more than one incident every year where more than 1% of data with a 7-year retention requirement is lost.</p> <p>Loss is less than 0.1% of accounting value of company</p>

**Table 2: Mapping Security Targets to Business Objectives**

Acme's executive leadership team set the security targets. They decided how many incidents they were willing to accept as well as the scope and cost of each incident. For example, Acme decided they could afford to have four incidents of 30 minutes or less where their product database is unavailable. More incidents or incidents of a longer duration are not acceptable.

Acme's leadership made this decision based on the costs associated with the incident. In this case, Acme will probably lose revenue if their product database is unavailable. The website will not be able to display the merchandise consequently, customers cannot place orders using the website. 85% of all Acme sales are made through the website, so Acme cannot afford to have this sales channel unavailable for an extended period of time.

Acme's leadership can establish a budget for their business objectives based on their defined security targets. Continuing with the product database example, let us say that Acme determined they were willing to accept an annual loss of \$20,000 due to incidents with their product database. They also estimate the cost to their brand image will be \$5000 or less if they meet their security targets. Therefore, they should be willing to spend up to \$25,000 on security controls to meet this security target.

Of course, this is a rather simplistic cost estimate, but serves as a good example of the process. Other direct and indirect costs should be considered to make a more realistic estimate. However, it is impossible to make exact estimates, and the SMB management should keep that in mind. For example, the number of sales that happen between 2 AM and 6 AM might average \$47.65 per sale, while sales between 6 PM and 9 PM average \$128.92 per sale, but on holidays... The author's advice is to ballpark the estimate and move on.

Management can always change their security targets if they find that they are either too strict or too loose.

## Risk Committees and Advisory Boards

Ideally, Acme's owners would have a risk committee or advisory board helping them make these decisions. The knowledge required to make even a good ballpark estimate in our example requires business, legal, financial, technology, and information security skills. The SMB owner probably does not have all of those skills, so it would be in their best interest to find trusted advisors to assist with this exercise and to act as an advisory board for other issues.

Most small businesses have a lawyer and accountant, but might not have a trusted IT or IS professional on their board. SMB owners should consider contacting their local information security chapters from groups such as the International Information Systems Security Certification Consortium ([ISC2](http://www.isc2.org/))<sup>14</sup>, the Information Security Audit and Control Association ([ISACA](http://www.isaca.org/))<sup>15</sup>, or the Information Systems Security Association ([ISSA](http://www.issa.org/))<sup>16</sup> to find someone qualified to perform the duties of information security advisor.

The SMB owner should assemble his or her advisory board at least once a year to review new requirements and update the security plan.

## A Word About Best Practices

Some readers may be asking themselves, "Can't I just follow best practices and be done with it?" That is an option of course, but how does that support the business objectives? For example, the SANS organization published a list of 20 Critical Security Controls<sup>17</sup> that can be considered "best practices". Each of these security controls is very good, but does every business need to perform account monitoring and control? If there is no business objective that requires it, then the answer is no. Does that control make the business more secure? Again, if there is no business objective requiring it, then the answer is no. In other words, a generic list of "best practices" is out of context with the business. A best practice security control that is in context for one business will be out of context for another.

Security is making the business reliable in spite of attacks, accidents and errors. If the business can be reliable without account monitoring, and if there is no contractual or compliance requirement to implement that control, then by definition, the control will not make the business more secure.

---

<sup>14</sup> <http://www.isc2.org/>

<sup>15</sup> <http://www.isaca.org/>

<sup>16</sup> <https://www.issa.org/>

<sup>17</sup> <http://www.sans.org/critical-security-controls/>

## The Unified Compliance Framework

As stated earlier, the author chose to promote the use of UCF as the best security framework for SMBs because it greatly simplifies the regulatory and compliance process. UCF supports the philosophy of contextual security that supports the business, and “eliminates redundant, conflicting, and underperforming IT policies and procedures.”<sup>18</sup> Paul Roberts from Techtarger.com wrote this about UCF, “Presumably, if companies can identify which regulations they're bound by and then areas that overlap, they can reduce their compliance costs by taking a "fix once, comply many" approach that will streamline internal audits and reduce capital expenditures.”<sup>19</sup>

Other frameworks such as ISO 27001 may have specific requirements for security controls that do not meet any business objective for a particular business. Unless there is a specific business reason to be compliant with ISO 27001, a business can waste time, money and effort on security controls that are completely out of context for that business. On the other hand, if a SMB does have a business reason to be certified as compliant with ISO 27001, UCF works in that case too.

UCF might not be the best framework if a SMB has no compliance requirements, but that likelihood is becoming less and less as states pass information security laws such as those recently passed by Massachusetts and Nevada.

The value of UCF increases with the number of laws, compliance and contractual requirements to which a SMB is subject. So UCF greatly simplifies the creation of a security controls list for a business that accepts credit card payments, has customers in Nevada and Massachusetts, and is required by a customer to be ISO 9000 certified.

The alternative to using UCF or something like it is to attempt to comply with each framework individually, but these frameworks were written at different times for different purposes. To further complicate matters, these frameworks were neither designed nor written to work with each other, so there is a significant amount of overlap and redundancy. UCF on the other hand is “... a database that distills 450 regulatory and legal authority documents (U.S. and international) into a set of 30,000 unique citations and 2,500 distinct controls, each with a unique and persistent ID.”<sup>20</sup>

---

<sup>18</sup> UCF, “IT UCF: Say what you do toolkit”, UCF, [http://www.unifiedcompliance.com/it\\_compliance/say\\_what\\_you\\_do/say\\_what\\_you\\_do\\_toolkit.html](http://www.unifiedcompliance.com/it_compliance/say_what_you_do/say_what_you_do_toolkit.html)

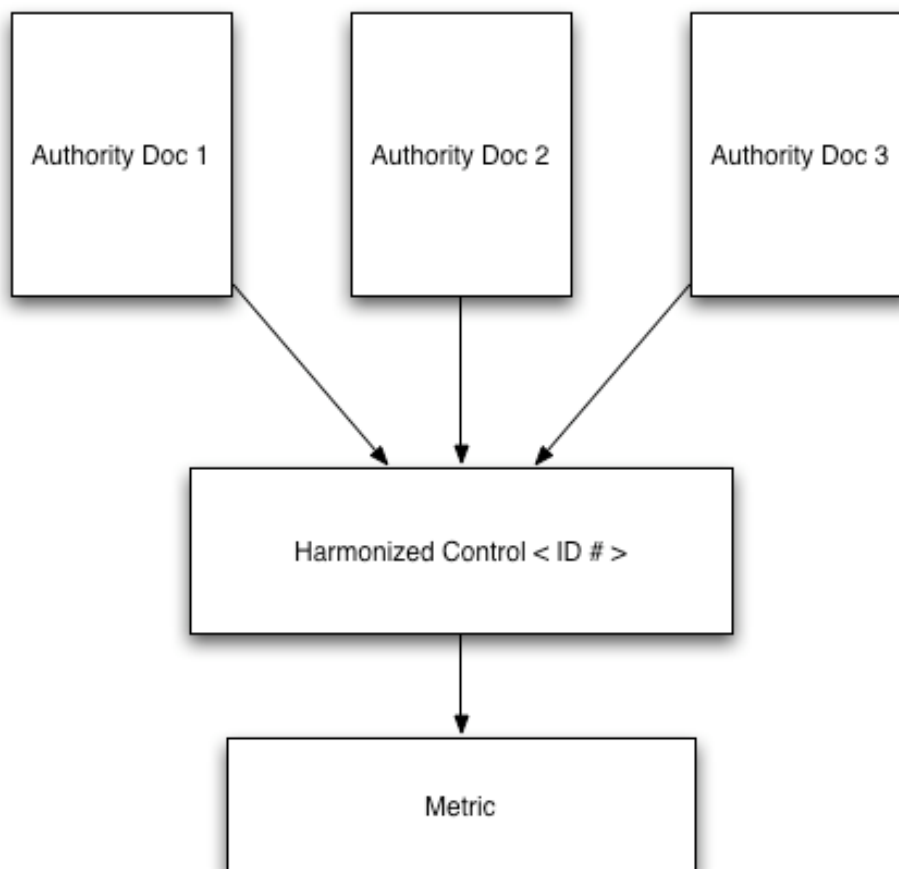
<sup>19</sup> Paul Roberts, Techtarger.com, “Unified Compliance Framework unties overlapping compliance standards” Techtarger.com, [http://searchcompliance.techtarget.com/tip/0,289483,sid195\\_gci1377669\\_mem1,00.html](http://searchcompliance.techtarget.com/tip/0,289483,sid195_gci1377669_mem1,00.html)

<sup>20</sup> Paul Roberts, Techtarger.com, “Unified Compliance Framework unties overlapping compliance standards” Techtarger.com, [http://searchcompliance.techtarget.com/tip/0,289483,sid195\\_gci1377669\\_mem1,00.html](http://searchcompliance.techtarget.com/tip/0,289483,sid195_gci1377669_mem1,00.html)

## UCF Organization

Network Frontiers assembled a team of lawyers and compliance experts to create the UCF. They reviewed each of the 450 - 500 authority documents and pulled out controls to create a list of harmonized, or normalized, controls (see Figure 1 below). Each control has a unique ID and database record. The UCF spreadsheets include a link from each control ID to a web page that displays the database information associated with that control. Each control web page lists:

- Control status: active or not
- The control name
- Supporting and supported controls (one of the 13 impact zones listed below)
- Authority documents with which it complies
- A general guidance section that explains the control
- Metrics associated with the control: how is it measured



**Figure 1: How the harmonized control relates to the authority documents and metrics**

UCF then groups the controls into 13 “impact zones” with a unique spreadsheet for each<sup>21</sup>:

- Acquisition of technology and services
- Audits and risk management
- Configuration management
- Design and implementation
- Human resources management
- Leadership and high level objectives
- Monitoring and measurement
- Operational management
- Physical and environmental protection
- Privacy protection for information and data
- Records management
- Systems continuity
- Technical security

## Using UCF for Compliance

The first step in using UCF for compliance is to know with which authority documents the SMB must comply. The UCF includes a spreadsheet with more than 400 compliance records for reference, with hyperlinks from the spreadsheet to the authority’s official site.

After the SMB generates their list of compliance authority documents, they will need to create a list of security controls. UCF provides spreadsheets that for that purpose. A discussion of that process can be found in the section below.

At this point, the SMB knows which authority documents they are going to comply with, and they know the controls they could implement. They do not necessarily know the risk levels associated with their systems and data. Therefore, the SMB must perform a risk assessment to ascertain the risk levels of their systems and data.

After the risk assessment and controls list are completed, the SMB can remove controls for systems that have low or possibly medium risk levels. This goes back to mapping the security objectives to the business objectives. The SMB must document why they chose to accept the risk and drop the control. This is an important step for auditing purposes.

After completing all of these steps, the SMB will have a custom matrix of controls complete with corresponding metrics, and they will know to which authority documents they map. This control matrix is context specific to the business. There should not be any duplication of controls nor should the matrix include unnecessary controls. Therefore, because it is

---

<sup>21</sup> UCF, “IT UCF: UCF Spreadsheets”, UCF, [“http://www.unifiedcompliance.com/it-impact-zones/unified-compliance-framework.shtml”](http://www.unifiedcompliance.com/it-impact-zones/unified-compliance-framework.shtml)

targeted and specific to the business, it is cost effective. The business will spend the right amount on implementing their controls.

The SMB can now start creating or modifying policies and procedures to support the controls listed in the matrix, and feed this back into the ISM3 maturity model. The SMB will move up in maturity levels as their processes improve, and more importantly, their ability to remain reliable in spite of attacks, accidents, and errors will also improve.

## Using the UCF Spreadsheets to Create a Security Controls List

UCF has created a unique spreadsheet for each impact zone. The information in the spreadsheet includes:

- The harmonized (normalized) control title
- The unique control ID
- Parent category columns. The parent categories contain the authority documents. For example, the “US Federal Security Guidance” parent category would include authority documents such as the CAN-SPAM Act of 2003<sup>22</sup> and the Cable Communications Privacy Act<sup>23</sup>.
- The parent category column lists a count of the number of authority documents that apply to each control. For example, the risk analysis and decision approval control (UCF control ID 01135) has four authority documents in the US Federal Security Guidance parent category. In this case, the documents are:<sup>24</sup>
  - Clinger-Cohen Act
  - Federal Information Security Management Act of 2002 (FISMA)
  - Federal Information System Controls Audit Manual (FISCAM)
  - GAO/PCIE Financial Audit Manual (FAM)
- The “Internal Guidance” column is used to list only those controls that apply to the business. The spreadsheet user sets up a filter to list the controls that apply to them.

A sample spreadsheet is shown below. This is a harmonized list of controls that are common to Banking and Finance Guidance, Sarbanes Oxley Guidance, and the US Federal Security Guidance as listed in the acquisition of technology and services impact zone, or spreadsheet.

This list contains 18 controls versus the 25 it would have if it were not normalized. In addition this business will be working from one list of controls rather than three. Also note that the reader can link to the specific control from the hyperlink in the control ID column.

---

<sup>22</sup> <http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm>

<sup>23</sup> [http://epic.org/privacy/cable\\_tv/ctpa.html](http://epic.org/privacy/cable_tv/ctpa.html)

<sup>24</sup> UCF, “Risk Analysis report and decision approval”, UCF, <http://www.unifiedcompliance.com//matrices/live/01135.html>

Harmonized Control Title	Control ID	Banking and Finance Guidance	Sarbanes Oxley Guidance	US Federal Security Guidance	Internal Guidance
Acquisition of, facilities, technology, and services	<a href="#">01123</a>	5	2	1	x
Allocation of resources	<a href="#">01444</a>			1	x
Definition of information and security requirements	<a href="#">01124</a>	1		3	x
Define operational requirements and Service Levels	<a href="#">00825</a>			1	x
Define cost-effective security controls	<a href="#">01125</a>	1		2	x
Systems documentation is provided	<a href="#">01445</a>	1	1	1	x
Configuration management plan is provided	<a href="#">01446</a>			1	x
Developer security testing plan is provided	<a href="#">01447</a>			1	x
Conduct an acquisition feasibility study	<a href="#">01129</a>	1			x
Formulation of acquisition strategy	<a href="#">01133</a>	2			x
Third-party service requirements	<a href="#">01134</a>	2	1	1	x
Risk Analysis report and decision approval.	<a href="#">01135</a>	3		3	x
Procurement Control	<a href="#">01136</a>	1		1	x
Document the software product acquisition methodology	<a href="#">01138</a>	1			x
Contract for and manage escrowed documentation	<a href="#">01139</a>	1			x
Software licensing	<a href="#">01140</a>	1		1	x
Establish third-party software maintenance agreements	<a href="#">01143</a>	1			x
Examine received software for vulnerabilities	<a href="#">01898</a>	1		1	x

**Table 3: Example of harmonized control list using UCF spreadsheet**

The UCF spreadsheets are separated into three worksheets:

- US: US related authority documents
- International: international authority documents
- Systems Configuration: controls related to systems configuration in the context of the impact zone.

An example of controls in the systems configuration tab on the acquisition of technology and services impact zone spreadsheet is, “The use of personal devices will be approved only

in extreme cases and only if the owner signs a forfeiture statement in case of a security incident (UCF control ID 04599).<sup>25</sup>

This control complies with the Defense Information Systems Agency (DISA) and is a prime example of a control that a SMB might choose to leave off of their control matrix. Their documentation could show that they are not subject to DISA or Department of Defense (DoD) compliance, and therefore, have no reason to implement the control.

## Metrics

ISM3 and UCF are both metrics driven. Metrics are defined for both the processes (ISM3) and the controls (UCF). The SMB management can, and should use these metrics to evaluate the success and effectiveness of both their processes and controls.

“ISM3 specifies four basic types of process metric:

- Activity: The number of Outputs produced in a time period
- Scope: The proportion of the environment or system that is protected by the process. For example, anti-virus could be installed in only 50% of user PCs
- Update: The time since the last update or refresh of process Outputs and related information systems
- Availability: The time since a process has performed as expected upon demand (uptime), the frequency and duration of interruptions, and the interval between interruptions.”<sup>26</sup>

Each metric should be defined. The definition should include:<sup>27</sup>

- The name
- The threshold
- How it is measured including listing the measurement device and procedure
- How often it is measured
- Unit of measure

Management should review the metrics on a consistent basis and investigate results that miss the target. Some type of incident review or root cause analysis should be conducted resulting in specific recommendations to correct the problem.

In many cases, metrics are also necessary to prove compliance. As stated earlier, UCF lists the metrics for each control where applicable. These metrics must be measured and reported. The process for correcting outliers is the same as that described for process.

---

<sup>25</sup> UCF, “UCF acquisition of technology and services.xls”

<sup>26</sup> Vicente Aceituno, Information Security Management Maturity Model v2.10, 13.

<sup>27</sup> Vicente Aceituno, Information Security Management Maturity Model v2.10, 12.

## Conclusion

This section has focused on creating a business specific, cost effective security program for SMBs. Rather than define security as designing and building invulnerable systems; we have defined security to be reliable in spite of attacks, accidents, and errors. Consequently, what is considered secure for one business will not be secure for another. In other words, the business defines security, instead of trying to apply some generic best practice list to the business.

ISM3 and UCF were used in combination to help create the business specific security plan. ISM3 maps security objectives to business objectives, and UCF maps security controls to compliance documents. The SMB executive can use the combination of both models to create a solid, cost effective security plan that meets the business' needs.

Perhaps the biggest benefit of using the approach outlined in this section of the book is the knowledge that security decisions were made in the context of the business, and the security framework is designed to keep security supporting the business objectives into the future.

## Glossary

---

**Authority document:** Document written by a government body or agency or institution. These are the documents that spell out the compliance requirements.

**Business Objective:** Activities that must be carried out to support the business goals.

**Harmonized control:** UCF term, generic name for the security control rather than the name given by each authority document.

**Harmonized list:** UCF term, de-duplicated list of controls.

**Maturity Model:** A tool for objectively rating an organization's ability to reliably execute processes

**Metric:** Qualitative measurement. Used to measure effectiveness of a security control or objective

**Parent Category:** UCF term, broad category name (such as Banking and Finance) found in column headings of the UCF spreadsheet.

**Security Objective:** Also know as security target, threshold that if not met means that there is a failure to meet a business objective.

**Security Control:** method used to protect information

**Security Framework:** high-level description of how people, processes, and technology combine to deliver information security

## Bibliography

---

*Photo on cover page used with the gracious permission of Thom Gould.*

"Who Must Comply with HIPAA Privacy Standards". HHS. 2/27/2010

[http://www.hhs.gov/ocr/privacy/hipaa/faq/covered\\_entities/190.html](http://www.hhs.gov/ocr/privacy/hipaa/faq/covered_entities/190.html).

"New Massachusetts data security law and regulations – comprehensive security plan required before March 1, 2010". Association of Corporate Counsel. 2/27/2010

<http://www.lexology.com/library/detail.aspx?g=d7c1e806-6f3f-4cb5-9080-d2ce0d6cc90f>.

"IT UCF: Say what you do toolkit". UCF. 2/27/2010

[http://www.unifiedcompliance.com/it\\_compliance/say\\_what\\_you\\_do/say\\_what\\_you\\_do\\_toolkit.html](http://www.unifiedcompliance.com/it_compliance/say_what_you_do/say_what_you_do_toolkit.html).

"IT UCF: UCF Spreadsheets", UCF. 2/27/2010

[http://www.unifiedcompliance.com/it\\_impact\\_zones/unified\\_compliance\\_framework\\_s.html](http://www.unifiedcompliance.com/it_impact_zones/unified_compliance_framework_s.html).

"Risk Analysis report and decision approval", UCF. 2/27/2010

<http://www.unifiedcompliance.com/matrices/live/01135.html>.

Aceituno, Vicente. *Information Security Management Maturity Model v2.10*,

Preimesberger, Chris. "Survey Indicates Half of SMBs Have no Disaster Recovery Plan".

eWeek.com. 2/27/2010 <http://www.eweek.com/c/a/Data-Storage/Survey-Indicates-Half-of-SMBs-Have-No-Disaster-Recovery-Plan-687524/>.

Roberts, Paul. "Unified Compliance Framework unties overlapping compliance standards" Techtarget.com. 2/27/2010

[http://searchcompliance.techtarget.com/tip/0,289483,sid195\\_gci1377669\\_mem1,00.html](http://searchcompliance.techtarget.com/tip/0,289483,sid195_gci1377669_mem1,00.html).

Worthen, Ben. "New Data Privacy Laws Set for Firms". Wall Street Journal. 2/27/2010

<http://online.wsj.com/article/SB122411532152538495.html>.

UCF, UCF acquisition of technology and services.xls