# White Paper Presentation

## *Roadmap to a Successful Information Management Program*

*By Randy Bridges*
*CEO, L5 Consulting*

For companies that have grown to a large enterprise business, an effective Information Management (IM) Program has very likely been built and is working well. Most of the larger companies implement ISO/IEC standards or a Capability Maturity Model (CMM) as a framework for managing Information in the workplace. Many of them also mirror "Best of Breed" standards. While these are excellent ways to implement Information systems, they are also costly, and they frequently take upwards of a year to implement and to get certified.

There are two other sizes of business that have a strong need for improved IM Programs: the Small and Medium Business (SMB) or the Small and Medium Enterprise (SME) markets. Outnumbering large businesses 100-to-1, these markets have contact and do business with some of the most critical businesses in the world, and they often store some of the most critical information outside of governments.

However, studies show that both SMBs and SMEs are sorely lacking when it comes to having effective IM Programs. Most of these companies do not incorporate any kind of strong program to protect the interests of the company itself, choosing instead to follow the "Ostrich Principle" – stick your head in the sand and hope the problem goes away. Not only is this ineffective, it also leaves the business vulnerable to severe repercussions, both legally and ethically.

After interviewing hundreds of businesses, it became clear to the author that smaller businesses need a clear implementation model for Information and Information Technology (IT) that can provide a relatively strong degree of structure, as well as can be implemented in stages and implemented as budget dollars become available.

This White Paper looks to provide an effective and affordable roadmap for implementing and maintaining a maturing Information Management Program – one that a). builds on previous stages, b). breaks the stages down into simple and manageable pieces, and c). provides for an expansion program down the road.

First, though, we need to review some presumptions and define some terms.

SMB usually refers to a single company location and 10-500 employees; SME looks at slightly larger businesses (50-1,000 employees) that usually operate with a corporate headquarters and at least one branch office.

These days, remote access from home and from client/customer locations presents a more distributed nature than ever before. In fact, SMEs look and work very much like multi-national companies, but they tend to be spread across state boundaries instead of national boundaries. For SMB and SME businesses, the employee counts and the semi-distributed nature of the business create Information Security risks that go beyond traditional planning to manage.

## Information Overview

Information Management (IM) differs from Information Technology in both scope and impact. IT is generally limited to the impact and scope of what is stored immediately on computers and servers; whereas Information Management covers any kind of information communication source.

The introduction to ISO/IEC 27002 states explicitly: “Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post of using electronic means, shown on films, or spoken in conversation. Whatever form information takes, or means by which it is shared or stored, it should always be appropriately protected.”

In addition, Information Management’s scope is business-wide, so it includes how information is treated in other non-technical ways, like dealing with Operational Security (need to know), excess Discretionary Security (giving too much access), inference information (being able to tell about something from something else), aggregate information (being able to put small bits of information into larger critical pieces of information), and disposal (document shredding, electronic storage destruction, and office waste controls from “dumpster diving”).

Then, there is the “leakage” of Personally Identifiable Information (PII) Management which involves people giving away private and unique information – examples include Social Engineering (people representing others with more authority than they have, frequently by phone); “shoulder surfing”, which involves watching people type login credentials or watching the screen for information as it is being typed; “tailgating”, which involves slipping in behind or with someone who has the access to a protected area; verbal distribution (talking about information); and other forms of simple manipulation of situations to the person’s advantage.

Normally, Information Management is integrated with everyday business security, so management, Information Security, facilities, personnel (HR) and IT often work in concert to provide a comprehensive view of how security is implemented across all areas of the business.

## Setting the Stage

Now that we’ve defined a few items for clarity and presented the scope differences in different types of programs, most people want to start looking at what it takes to fulfill this program. First, though, we have to understand that there is more to an effective IM Program than simply implementing a handful

of steps – there are some prerequisite elements that are necessary before strong and lasting benefits of the IM Program can be seen.

The first critical element of an IM Program is having some aspect of a Risk Management (RM) Program, even if it is nothing more than what is built into the system. Larger companies must integrate the concept of Risk Management Programs into their business in order to be successful; however, most small and medium businesses have neither the expertise nor the staff to support an effective RM Program. That is the reason why some of the early stages of the suggested IM Program have been developed as a semi-substitute for RM, integrating stages like monitoring, Information Flow Mapping and Vulnerability Management; once a firm IM Program has been established, various consultants can continue the process of RM integration until a full program can be devised or supplanted with a substitute RM Program.

The second critical element that is required is a program of metrics – a way to provide measurable results so that the program can address changes in the business, the customers, the economy and the threat/attack landscape. With a program of measurement, your business will be able to quickly find the areas that need to be addressed because variances in solutions will become apparent as fast as the measurements can be made and noted.

The third critical element is to devise a comprehensive companywide program rather than combining a group of smaller autonomous programs. Without a comprehensive program, the costs will spiral out of control and the effectiveness will be far less.

In addition, make sure the Information Management Program is supported top-to-bottom, meaning Senior Management must be the first group of people onboard. Without them, the Information Program will not carry the backing in the company that is necessary to make the Program successful.

Finally, one should plan to work from a framework in order to be both specific and flexible. Without it, any program tends to stray from its target objectives, mostly because objectives are left too generic and they often don't comprise more than a horse-blinder view of a project or a challenge.

That being said, let's start looking at the parts of the roadmap.

## Building the Roadmap

Implementing a successful IM Program for smaller companies is fairly easy. It should have several success factors built in, including:

- Ability to implement the Program in stages
- Ability to add ad hoc parts according to business need
- Provide an escalation process, where parts can be implemented to address more critical business needs as the program continues
- Ability to re-address Program parts without addressing the entire Program

Now, we get to the actual "Roadmap of an Effective Information Management Program," presented as a Triangle of services. This is part of the full Managed Security Services program as shown below.

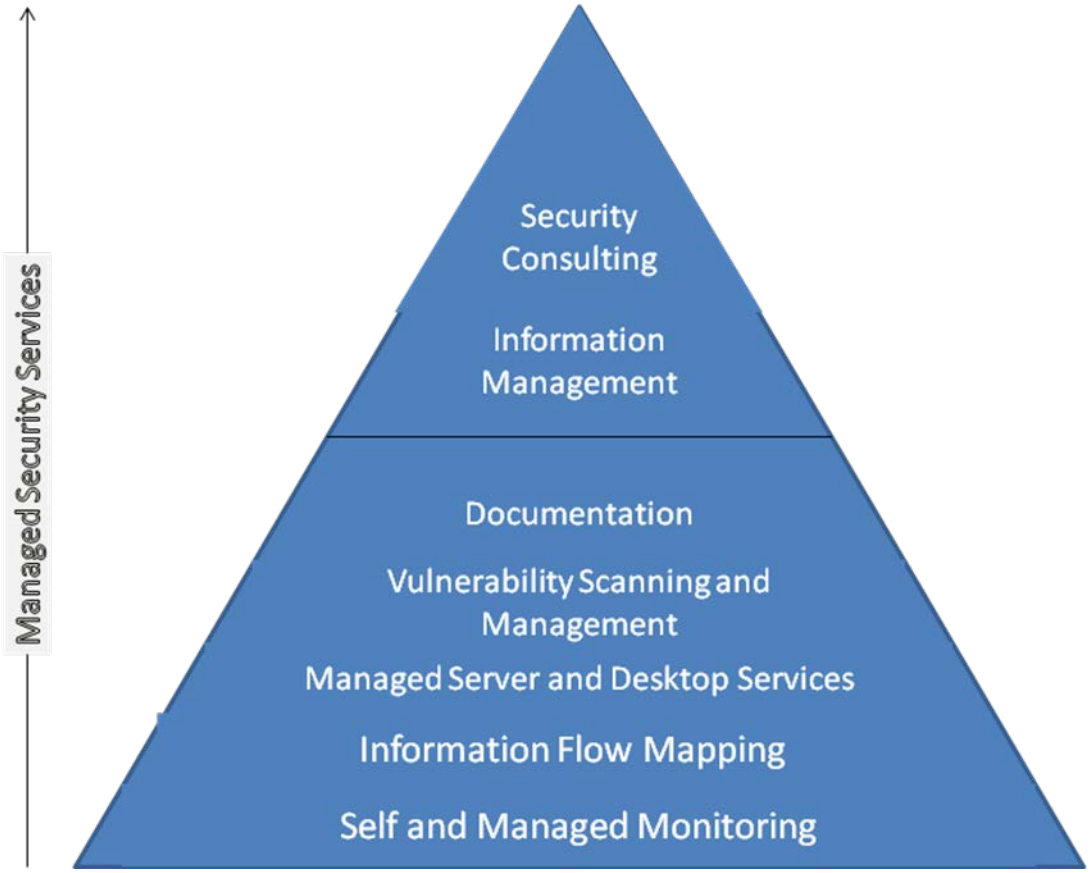


**Figure 1 - Triangle of Managed Security Services for IM Program**

As you can see in Figure 1 above, the Roadmap is a series of stacked parts that focus on individual types of tasks rather than discreet tasks. The parts complete a full Managed Security Services Program, or simply ISM, but we are only interested in the pieces up through Information Management. Let's look at each part and break out how it impacts and improves the program - they include: Monitoring; Information Flow Mapping; Managed Server and Desktop Services; Vulnerability Scanning and Management; and the Information Management section, which includes Employee Awareness.

## Stage 1 - Monitoring

Obviously, it's important to know what is happening on a network, so it is critical to integrate a thorough plan to review and monitor all parts of the network.

There are many products on the market that simply address a monitoring function of devices, but putting in a simple device that monitors uptime and health does not present a long-term view for the IM Program. We want to monitor both devices and the overall communication itself, so the monitoring program should be robust in order to provide the greatest and most comprehensive view.

When considering a monitoring option, you should also consider outsourcing this aspect to an outside service team. Not only are they more aware of the options, it is likely that they already have a program they are using to provide monitoring services. Compared with buying your own, an outside monitoring service can be quite inexpensive without losing any of the effectiveness.

### Stage 2 - Information Flow Mapping

After monitoring, our next step is measuring what a system's criticality is for doing business. We do that by using Information Flow Mapping.

With Information Flow Mapping, we first measure the criticality of the information flowing through the network; then, we see what systems support and provide all of the pieces for each part of the information. The goal is to clearly see the information flowing to and from systems as part of your view. Obviously, the more critical the information, the more critical the systems it flows through – it is usually a 1-to-1 ratio for small companies, but larger companies can reach 1-to-5 or more.

As an example, some companies might utilize a Customer Relationship Management (CRM) system heavily in order to do business. Often, these comprise a front-end web or application server *plus* a backend database server that might also shared for multiple applications. If all you see is the initial system, you might miss the dual nature of the critical backend system in this example.

For Senior and Department Management, Information Flow Mapping provides a comprehensive view of what information flows are affected during system outages, and it also helps them to easily understand what represents a proper amount of the IT budget for a given system or set of systems. Not only does this provide cost-shifting mechanisms, it also provides critical Risk Management and Business Continuity scenarios in advance of further implementations later on in the IM process. Clearly, having this detailed view provides a much more realistic understanding of the impact to the information and the systems that are being used.

### Stage 3 - Managed Servers and Desktops

Now that we know the critical nature of the information, systems and devices on the network, we can start evaluating and building a support program that matches the information Flow Mapping criticality view. This provides a more cost-effective and impact-related program – one that spends money where it truly needs to be spent and in the proper distribution.

For systems that have low critical natures, we can perhaps implement simple baseline support – for Executive Reporting, we can focus on disk, memory, process, service and uptime evaluation.

For the absolutely critical or multiple duty (more than one critical information flow) servers, we can choose to implement something more in-depth, such as 24-hour monitoring with pager response alerting, clustering of servers to reduce impact from outages, testing for patch management, and other high impact support services. While these are far more expensive, the understanding of the criticality provides a means of evaluating what is an appropriate support expense.

These days, most companies are using Managed Services – a.k.a. "Outsourcing" – to provide parts of the support solution. This involves shifting the normal level, everyday support functions from internal employees to a 3rd-party outside agency. This provides for a lower cost alternative to having expensive internal technicians perform mundane tasks; by using Managed Services, these same expensive technicians can focus on more critical support services.

At the same time, Managed Services allows subject matter experts to provide higher level consulting with management on ways to improve internal IT processes. Since they consistently work with multiple companies and different verticals at the same time, they often can provide a wider view of options and experience, more so than internal employees who might only have experience with one or two companies and perhaps one vertical.

### Stage 4 - Vulnerability Management

With the changing attack vectors from hackers to distributed "command and control" botnets, it is important to understand the ways that your company systems are vulnerable to malicious attack.

Vulnerability Management (VM) programs provide a way to evaluate the effectiveness of your system security and hotfix patching programs. It should also provide you with a 3rd-party evaluation as independent results rather than internal evaluations by System Administrators only.

In addition to vulnerability aspects, VM also helps with the process of managing a baseline of system(s) from a Risk Management perspective. By showing that new vulnerabilities have been released or that a system is potentially at risk, the Risk Management evaluator(s) can make an educated decision based on the priority of one system whether a similar system is probably facing the same vulnerability.

When vulnerabilities cascade across multiple systems, this is generally referred to as aggregate risk, or the accumulation of risk that increases the impact according to the number of affected systems.

Small amounts of risk - or in this case, vulnerabilities - are normal, but in many cases there comes a point when the aggregation of risk across the enterprise grows to an unacceptable point. As with all other stages, VM must have a metrics point to make sure that the aggregate risk does not increase beyond the acceptable threshold and that the trend in managing the vulnerabilities decreases over time. If it does not, then perhaps it is necessary to re-visit Stage 3 and determine where the support cycle does not work properly with the vulnerability management cycle.

### Stage 5 - Employee Awareness Training

This is the area where IT Information Management and Human Resources must come together. Awareness Training provides a platform for Senior Management to focus on delivering Policies and Standards for dealing with issues in many environments. From a Security perspective, this includes enforcing "Information Assurance" such that Confidentiality, Integrity and Availability are maintained at all times.

Awareness Training can also be used to expand knowledge by all employees of how to use the information classification that was noted above.

Combining Training with Documentation is a powerful way to keep information under control and reduce the chance that your company will become a victim of privacy issues or accidental information disclosure.

From here, we branch into the Information Security Management (ISM) realm, but that is a different topic.

## Where to Now?

Now that we have the roadmap, the questions come: "What do we do with it?" and "How do we implement it?" Obviously, there is more to an effective IM Program than simply implementing a handful of steps – there are some prerequisite elements that are necessary before strong and lasting benefits of the IM Program can be seen.

The **first critical element** of an IM Program is having some aspect of a Risk Management (RM) Program. While larger companies are easily built to integrate the concept of Risk Management, most small and medium businesses have neither the expertise nor the staff to support an effective RM Program. That is the reason why some of the early stages of the IM Program have been developed as a semi-substitute for RM – stages like monitoring, Information Flow Mapping and Vulnerability Management; once a firm program has been established through stage 5, Security Consulting can continue the process of RM integration until a full program can be devised or supplanted with a substitute RM Program.

The **second critical element** that is required is a program of metrics – a way to provide measurable results so that the program can address changes in the business, the customers, the economy and the threat/attack landscape. With a program of measurement, your business will be able to quickly find the areas that need to be addressed because variances in solutions will become apparent as fast as the measurements can be made and noted.

That being said, let's look at the ways that the different sizes of business can address the Roadmap for improving the IM environment, as well as some of the challenges that they face in the implementation.

### SMB Businesses

The Roadmap here is fairly easy to implement. Most SMB companies can simply work with their team or their IT provider to implement each stage according to need. Again, an effective RM Program is probably not available, so it is important that the company has a complete focus and mastery in each area before moving into the next area of concentration. While the benefits are greater if the business implements them in order according to a schedule, it is not a necessary plan.

Most business owners will be surprised at the change of perception they achieve by simply implementing Monitoring and Information Flow Mapping services in an effective and measurable manner - the overall effectiveness of the IM Program is dramatically increased by the simple awareness factor of what the company has and how critical it is.

The primary challenge here is that Senior Management must support this program in the face of other small business challenges – some of those challenges might include: mediating between the customers

and the employees when policies conflicts with customer expectations; autonomous employees who do not respect the changes that are forced on them; making sure that support by top management is highly visible, both in words and in actions; training for executives and management; commitment to employee awareness programs; etc.

For the SMB, the real benefits begin to show when the company implements Managed Services of any kind. The impact to businesses that implement maintenance programs dramatically increases when the money is not being spent on a "Break-Fix" basis, which is the trademark of traditional IT services.

### SME Businesses

For the SME, the Roadmap is a bit more difficult to implement than the SMB, but the direct returns are increased. SME businesses tend to have usually one or two people to support their IT needs, and following the Roadmap allows the IT individual or team to focus more effectively on strategic support issues across the enterprise.

However, the primary challenges are often related to ineffective communication channels, as communication of directives, changes and expectations are delayed to the branch offices or to the larger workforce. In addition, security measures in branch offices or in discreet work segments are harder to enforce because of the reduced impact by senior management personnel. Like the SMB, there will be necessary adjustments as management also has to provide highly visible support for the IM Program.

By the time a SME business implements Managed Services, the process improvements will most likely grow to the point where they cascade to other areas of the business, creating a cumulative improvement of service across the enterprise. Once they implement Vulnerability Management, they can pretty much presume that most of the effectiveness of low-cost implementations has been served.

## And then …?

When either class of business brings the upper levels of an IM Program into play (stage 5 or 6), the returns on secondary benefits begins to show – benefits like advanced marketing in support of the security measures; sales advantages to answer the 'why should I choose you' question; and the ability to address compliance initiatives like ISO, FDA, HIPAA, SOX, or even the ability to implement a "Best of Class" solution.

Another consideration is to bring Security Consultants into the program earlier than just at the Security Consulting stage. This provides several benefits, including the ability to:

- learn how best to work together before it is absolutely necessary
- find Subject Matter Experts in more than one area
- integrate Security into your regular support program earlier in the process
- integrate the Consultants into a pseudo-management position, giving further evidence of Program commitment to employees

## Finally …

Once you have reached this point, you should have developed a full and complete program, one that provides strong Information Management practices as part of your everyday activities. It should also provide your company with long-term returns as challenges and changes in the Information Management realm make their presence known, yet your company is prepared to address them in a strategic and effective manner.