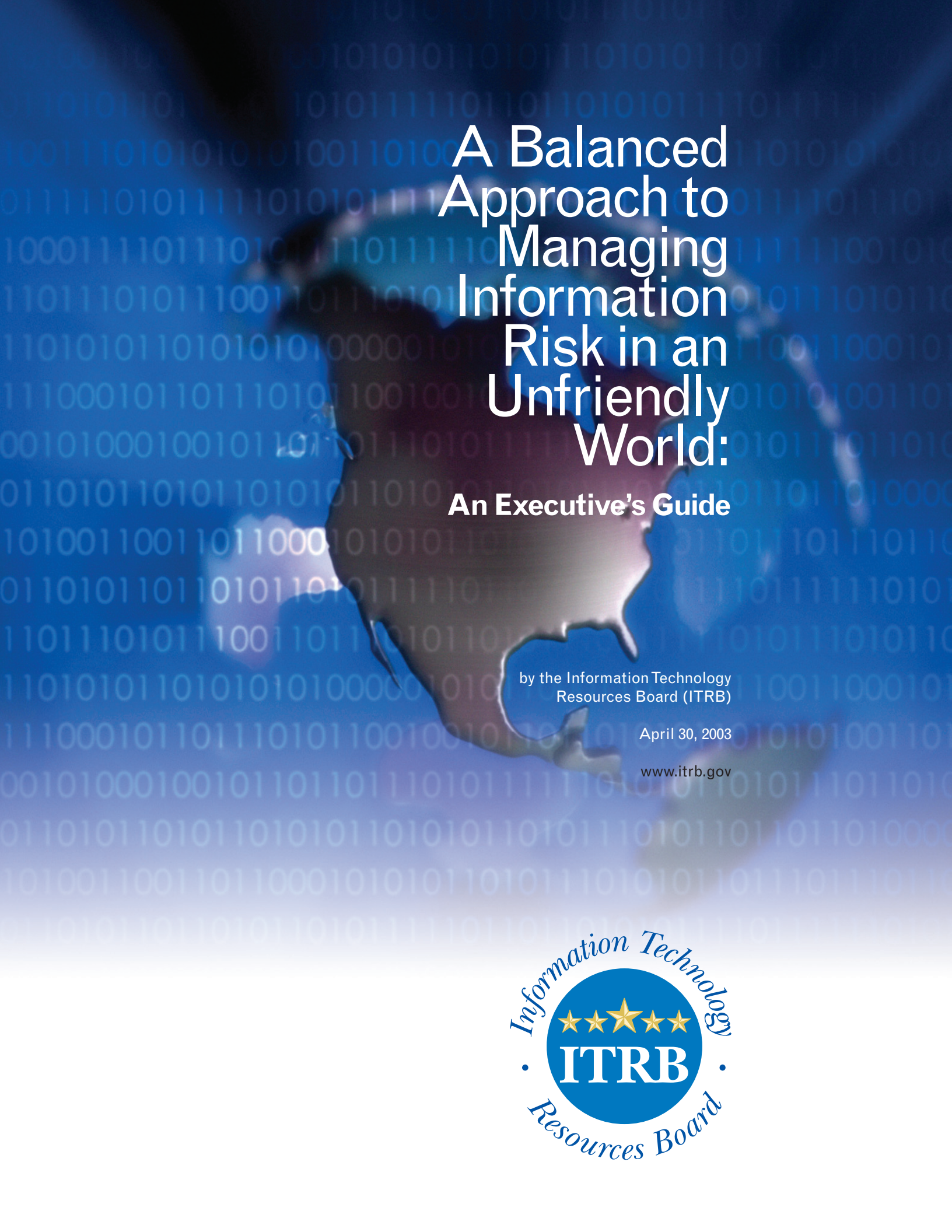

A Balanced Approach to Managing Information Risk in an Unfriendly World:

An Executive's Guide

by the Information Technology Resources Board (ITRB)

April 30, 2003

www.itrb.gov

Information Technology ITRB Resources Board

preface

This Guide is for you, a leader responsible for guiding a federal department, agency, or program to successful achievement of its mission - keeping the promises made to citizens and stakeholders. Information technology, supported by cost-effective information risk management, is now an essential element of your ability to achieve those missions. While you may not be an expert in information technology or information security, you are nonetheless ultimately responsible - and accountable - for managing these increasingly complex and critical functions.

Cost-effective information risk management can be a powerful enabler to help you safely take advantage of the tremendous promise of the digital world... and avoid unacceptable consequences. Because you are ultimately responsible, your support for information risk management is essential. You must deal with it directly in collaboration with your information security program manager and a senior cross-functional information risk management team. To support your mission appropriately, cost-effective information security requires thoughtful and well-informed trade-offs. The challenge is to invest resources in the right areas and in the right balance, with the greatest impact. This Guide offers principles and practical tips you and your executive team can implement to improve your information risk management program and thus support your mission effectively.

In addition to offering guidance to you, the agency or program executive, in implementing cost-effective information security in support of mission achievement, this Guide can help other leaders who have security roles in your organization. You may choose to read the Introduction and Chapter 1, Practical Advice for Getting Started, along with Chapter 4, Epilogue, which highlights the importance of keeping abreast of emerging trends in information security and risk management. Program Managers, the Chief Information Officer (CIO) and the Information Security Officer (ISO) will want to read the entire Guide, while focusing on Chapter 2, Organizing to Manage Information Risk, and Chapter 3, Implementing Your Information Risk Management Program.

This Guide focuses on durable principles and proven techniques for managing information risk, rather than on detailed rules and concepts that must change frequently to meet each new threat. For this reason, there are deliberately few references to specific statutes, regulations, or procedural guidebooks. Many of the principles and recommendations in this Guide are not only good practices, but also are required by law and policy. As always, agencies must comply with existing statutory requirements and Office of Management and Budget (OMB) policy. Your agency Information Security Officer, CIO, and General Counsel are familiar with current requirements, as well as guidance and recommendations from key sources like the National Institute of Standards and Technology (NIST) and the General Accounting Office (GAO).

As we all now recognize, cyberspace can be a dangerous place; information security is the latest "hot issue" to force itself onto your already crowded agenda.

The requirements for safely doing business in cyberspace are still evolving, but there is much that you can and must do immediately. Reading this Guide is a first step.

This is a publication of the Information Technology Resources Board (ITRB). The ITRB was formalized in July 1996 by Executive Order 13011 to provide peer review assessments of mission critical information systems by: identifying critical issues and findings; framing these in management and/or technical perspectives; and by recommending actions to mitigate risks or

resolve issues. The ITRB's assessments cover initiatives at various stages in their life cycles, from conceptualization to product or service delivery. The lessons the Board learns can contribute to successful outcomes across the government. ITRB members are experienced practitioners from across the federal government who bring broad program, technical, and acquisition management experience to managing and developing major information technology (IT) systems. The ITRB's activities promote measurable improvements in mission performance and service delivery through the strategic application of information technology.

This Guide offers the combined experience of ITRB members in delivering mission critical systems, the Board's unique collective perspective drawn from its assessments of major federal IT projects, and interviews with leaders in the field. The Board gratefully acknowledges input to development of this Guide from current and former federal government executives with key roles in information security policy and management. The Board also received valuable advice and assistance from our GSA Program Manager and the EDS support team. However, the views and recommendations contained in the Guide are those of the ITRB.

table of contents

introduction: navigating the perfect storm

A "perfect storm" of circumstances came together at the beginning of the 21st Century, sounding alarms from Main Street to Wall Street to Pennsylvania Avenue. Private businesses foundered in the storm and the operations of more than one federal agency were seriously impaired.

The storm is about the vulnerability of the automated systems that we depend on in virtually every aspect of our lives for our health, our financial security, our individual and national security, and even our entertainment and personal relationships.

The Internet has revolutionized the way governments govern, the way businesses do business, and the way individuals live their lives. Modern societies now use information technology and the Internet to improve life in almost every area of human endeavor. It is now simply a fact of life that modern societies are critically dependent on information technology systems.

The pace of change in technology, and our adoption of it, outstrips our ability to ensure the safety and continuity of our information technology infrastructures. With each advance in technology, new vulnerabilities are introduced that can be exploited by individuals, groups, or nations. The sophistication and proliferation of attack methods are alarming. Governments, businesses, and individuals have been ill-prepared to deal with the vulnerabilities resulting from this whirlwind of change.

There is a silver lining to the crisis of information security. Some of the same technologies needed for flexible and effective security also offer enhancements to systems, services, and the ability to support the mission. Technologies required for establishing the identity and access rights of authorized system users also can be used to offer clients self-service and personalized services. Management processes that make sure information security is built into new or enhanced systems also can be used to implement other policies reliably, like accessibility or quality standards.

Whatever the challenges, one thing is certain. There is no turning back. The benefits of technology are too compelling to abandon and isolating our systems is not an option. As the events of September 11, 2001 taught us, the dangers of not being able to share information effectively are as great as the danger of having it compromised. federal managers must continue to take advantage of the benefits of the digital age, but safely through implementation of cost-effective information security. That means adopting and using smarter methods of managing information risk.

The pace of change in technology outstrips our ability to ensure the safety and continuity of IT infrastructures.

Integrating Information Risk Management

Cost-effective information security means balance. Too much security is cost-prohibitive and impedes operations; too little security endangers mission accomplishment. Some risk must be accepted. A dollar of loss from poor information security is equivalent to a dollar of loss from poor workforce management or poor inventory control. It makes little sense to spend more to eliminate one type of loss than the other.

Implementation of information risk management should result in cost-effective

information security to support mission objectives. This Guide provides practical information on implementing information risk management in your organization.

Information Risk Management and Information Security

This Guide places paramount emphasis on the concept of information risk management as a business issue, not a technical issue, which is ultimately the responsibility of senior management. For the purposes of this Guide, information risk management includes "information security," the technical means of protecting IT systems, and encompasses the total business process that balances the cost and potential gains of protective measures against the risks.

"(A)t this point, there is no evidence that poor security is a result of lack of money."

- Office of Management and Budget: FY 2001 Report to Congress on Federal Government Information Security Reform

Cost-effective information security means balance.

Overview to this Guide

The rest of the Guide provides advice to agency and program executives on how to establish an information risk management process that can help you survive today's tempests and improve agency results tomorrow.

Chapter 1: Practical Advice for Getting Started. As an executive you can't and won't be dealing with implementation details. Here are some "stars to steer by" and high-level criteria you can use to evaluate your agency's current and target information risk management program. There's a lot to do, so setting priorities is essential. Included are some tips on what to do first and some common mistakes to avoid.

Chapter 2: Organizing to Manage Information Risk. Getting the right people involved, giving them training, and providing the right incentives are the keys to success in any program. Information risk management is no exception.

Chapter 3: Implementing Your Information Risk Management Program. This Guide offers you practices from organizations that have had success in implementing information risk management. This chapter will provide particular value to program managers.

Chapter 4: Epilogue. A look at some of the new and urgent information risk management issues facing federal agencies.

chapter 1: practical advice for getting started

Your responsibility is to lead the agency to mission success. Until recently, information security was viewed as a particularly arcane technology issue, managed "down in the IT department." With intense focus on e-government, and increased reliance on technology, information security suddenly became a critical element in the operation of the entire enterprise. Computer viruses make headlines. Hacker exploits shut down entire agencies. Searing events like September 11, 2001, dramatized some vulnerabilities created by our dependence on technology. As an agency executive, you must make sure the information risk management program can keep the systems that support the agency mission available and operating safely.

Information security suddenly became critical in the operation of the entire enterprise.

There are many technical publications on information security. But as a non-technical executive, you can't and won't be dealing with implementation details and security jargon. You need to get comfortable with managing information risk and to find a rational path through the minefield of security issues. The following section provides some strategic principles to help you.

Strategic Principles

Here are 10 principles to guide an effective top-down approach to information risk management.

1. It's about the business! - The only purpose of an information risk management program is to support the agency's mission. As a leader, focus relentlessly on this principle. It's not about technology. It's not just about compliance. It's about achieving the right balance of information risk management to achieve your mission and goals.

2. The goal is balance. - The idea that information risk can be eliminated is impractical. Even if it were possible, the cost and operational restrictions would compromise more important business goals. Buying too much security is as foolish as having too little. It is just as bad to over-restrict access to information as to under-restrict it. Look also for balance among different types of risk.

3. Engage agency business executives. - Ensure business or program executives, not just your technology or security managers, take ownership of and responsibility for information risk management. They are responsible for the agency's assets and strategic goals. They also are the ones who must make the critical judgments about the business impact of potential security lapses, threat motivations, and non-technical alternatives for absorbing the risk. Managers will routinely evaluate all sorts of risks to their programs; information risk is not fundamentally different. Include the functional executives from finance, legal, and stakeholder relations in an information risk management team led by the CIO or ISO. Leverage their authoritative insight into liability issues and risk mitigation alternatives that may not be apparent to program managers or technology staff. Give the members of the information risk management team responsibility for this function and hold them accountable.

"You can't protect everything."

- Pat Schambach, Assistant Administrator for Information Technology & Chief Information Officer, Transportation Security Administration

4. Do first things first. - Separate short-term issues from long-term issues. Prioritize and track both. This Guide provides a manageable list of immediate steps to reduce risk that probably won't

require new funding. Don't stop there. Sophisticated cyber-crime and ambitious e-government projects require more robust protection that takes longer to plan and implement. To build security into systems from the start-which is cheaper and more effective than adding it after a failure or an audit-you'll need to upgrade your IT planning and management processes. Build skills and an agency management culture that deals effectively with information risk.

5. Know where you're going. - Develop a blueprint of your target information security posture and a roadmap to get there. This is amazingly effective for coordinating efforts throughout a large organization. Projects that don't fit the plan, or are duplicative, become easier to spot. It does wonders for explaining to funding authorities what the money is for and it builds confidence that you know what you're doing.

6. Consider non-technical options first. - Use your business savvy to identify the most cost-effective solutions. It's often both less expensive and more effective to eliminate or absorb risk without relying on technology. For example, an agreement to limit liability could be negotiated with a business partner. This is where engaging a non-technical executive in information risk management pays off.

7. Manage for results. - Set goals for the outcomes of security efforts rather than the outputs. Measure work time lost because of computer virus infections, not the number of viruses stopped. This approach is consistent with performance-based management. You must still comply with process-oriented audits, but completing a checklist never guarantees you'll meet your mission goals.

Top 10 Things Not To Do!

No executive guide is complete without a "Top 10" list. So here are ten common misconceptions about information security:

1. A firewall protects our systems –Wrong! A firewall is important, but only if it is correctly configured, continually updated, and continuously monitored.
2. Antivirus software protects our systems against viruses –Wrong! Antivirus software only offers protection if it is properly installed and kept current.
3. Our data is on backup tapes and so we're protected against disasters – Wrong! Stored data is useless if you don't have a workable plan for putting everything back in order after a disaster or an attack.
4. We did background investigations on all our employees, so they don't pose a security risk –Wrong! Someone who was not a security risk last year may have become a risk last week.
5. We have a public key infrastructure (PKI), so everything is secure – Wrong! Public key technology can provide several security services, including encryption, but a single technology is never the whole answer.
6. We have an Information Security Officer assigned and he/she will take care of our security problems –Wrong! Security is everyone's business. An ISO can help organize the effort, but can never do the job alone.
7. All our contractors operate under clauses that make them responsible for security on agency systems –Wrong! If a system crashes and the public can't access your agency, it is scant comfort that the contractor must pay a penalty.
8. Computer security is one thing, but physical security is another –Wrong! Information security requires a comprehensive set of protections, including physical security, employee security, security technology, and security policies and procedures.
9. We use the same software as the private sector, so we have limited risk – Wrong! Government and private sector organizations both face risks from commercial software and both have to take precautions.
10. We have protected ourselves against our biggest vulnerability: attacks from hackers and other outsiders –Wrong again! Insiders cause eighty percent of system compromises through intentional or accidental acts.

8. Secure the whole business process, not just the automated parts. -Some risk analysis tools focus narrowly on computer systems and overlook significant non-automated portions of a business process. An enterprise architecture perspective directs attention to the high-level blueprint of the end-to-end business process, so threats to all (automated and non-automated) components of the process are considered. This approach also leads to development of a risk baseline, incorporating risks accepted in the business process as it operates today. This encourages establishment of realistic security goals.

9. Producing security documents will not manage your risks. - Manage information risk for effectiveness, not just for compliance. Establish an information risk management program, integrate security requirements into your business management processes, and take responsibility for information risk management to ensure cost-effective support of your mission and thereby achieve compliance. And let your Inspector General (IG) know you're serious about information risk management. Seek agreement on how the audit approach can accelerate your plans, not delay them. You should reach out to the IG, as you are more likely to gain IG flexibility and cooperation than your staff.

10. Get involved. -A word from the boss draws attention to an issue. Make a brief progress report on the information security blueprint milestones a regular item in senior staff meetings. Sit in the front row at annual security-awareness training and ask a question. Celebrate and reward successes in information risk management. A few well-focused hours of your time each year can make a huge difference.

Immediate-Action Tasks

Do first things first. Immediate-action tasks usually can be done with available resources. In most situations, these steps could be implemented within six months:

Manage information risk for effectiveness, not just for compliance.

- ***Stop the bleeding*** - A surprisingly large number of organizations still fail to implement basic, widely recommended security measures to defend against the tidal wave of cyber-attacks originating from the Internet. Make sure you're not one of them. There are several well-known lists of common security vulnerabilities endorsed by a consensus of security authorities, like the FBI/SANS Top 20 list. Confirm that your technical staff uses one or more of these lists. Make sure your technical staff receives alerts from the federal incident response organization. Provide and require basic training on password protection, virus control, and social-engineering awareness for everyone as a pre-condition for access to your network and systems. Establish an incident response team for security emergencies like a major virus infection or defaced Web site. There is no excuse for not taking these basic precautions immediately!

- ***Form an Information Risk Management Team and Establish Accountability*** - Appoint an enterprise

"You really can't focus on securing the system. You need to focus on securing the process."

- Mary Mitchell, Deputy Associate Administrator, Office of Electronic Government & Technology, GSA

ISO who reports to the CIO. Make that executive responsible for program management and coordination of a team approach. Make sure every major IT system has a document that formally assigns information risk management responsibility to the business process manager. Establish an Information Risk Management Team from a cross-section of the organization with high-level program and functional participation to guide and support the ISO. Information Risk Management Teams may be established at the enterprise level and at the program and project level.

" We have systems that have never been patched for vulnerabilities that have been out there and exploited for years."

- Marianne Swanson, Senior Advisor for IT Security Management, NIST

- ***Add security into your investment review process*** - Include in your investment review a firm requirement for assignment of a named manager responsible for business process continuity, including system security. Also require that business cases for new systems include a summary of principal security issues raised by the proposed system and the sponsor's strategy for addressing them. Go beyond the requisite statement of conformance with the agency enterprise architecture and compare the proposed system's security approach to the agency's information security target blueprint. Learn to ask about "CIA and A" - Confidentiality, Integrity, Availability and Accountability. Figure 1, Four Principles of Information Security, provides definitions for each.

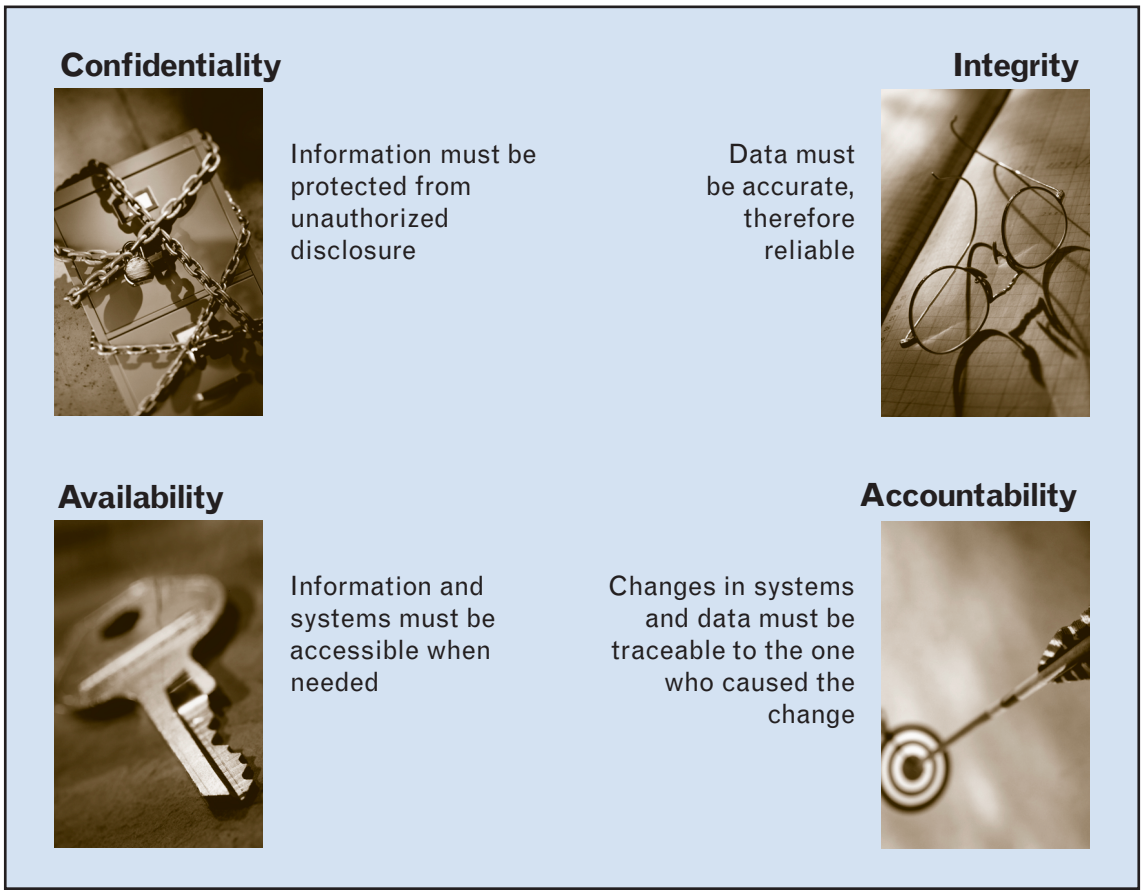

Figure 1, Four Principles of Information Security

- ***Communicate*** **-** Announce the risk management program and explain your goals personally. Identify the Information Risk Management Team and ISO. Brief the IG and oversight entities.

- ***Insist on action to achieve long-term goals*** **-** Have the ISO and Information Risk Management Team prepare project plans with goals, tasks, resourcing, and schedule of milestones for longer-term actions (articulated below). Include these goals in the agency Strategic and Performance Plans, and in the Budget Request.

Longer-term Goals with Lasting Effects

Longer-term elements of your overall information risk management program deliver lasting benefits in terms of protection from more sophisticated attacks, better data quality, and even lower costs. Don't lose sight of them because you've put out the short-term fires. Aim to complete or reach a significant milestone on these items within a year.

- ***Add security touch-points into the way you build systems*** **-** By building security into new system requirements from the start, you'll avoid expensive software changes later to plug security holes. Aim to lower your operating costs by building in as many of the routine security-related, system-administration activities and reports as you can foresee. Figure 2, Building Security into the SDLC, shows an example of security/privacy steps in the phases of a generalized systems development lifecycle (SDLC).

- ***Publish version 1.0 of your Information Security Architecture*** **-** An information security architecture (ISA) is your blueprint of how to fit together all the information risk management program components of your enterprise, from business risk analysis to hardware and software.

Understand the business risks involved in technical implementations.

- ***Build risk management skills of key staff and develop a risk-aware management style*** **-** Your technical staff must develop sufficient business skills to understand the business risks involved in technical implementations. Your business team must develop an understanding of the value of security technologies. All must develop the basic risk management skills necessary to help you effectively implement your information risk management program.

"...people with ultimate responsibility for operation of a system need to make sure that security is a consideration from day one."

- Sallie McDonald, Information Assurance / Infrastructure Protection, Homeland Security

The strategic principles, immediate-action tasks, and longer-term goals described in this chapter will help you get started in information risk management. The following chapters offer guidance on implementing your program.

Building Security into the Systems Development Lifecycle (Required Products)

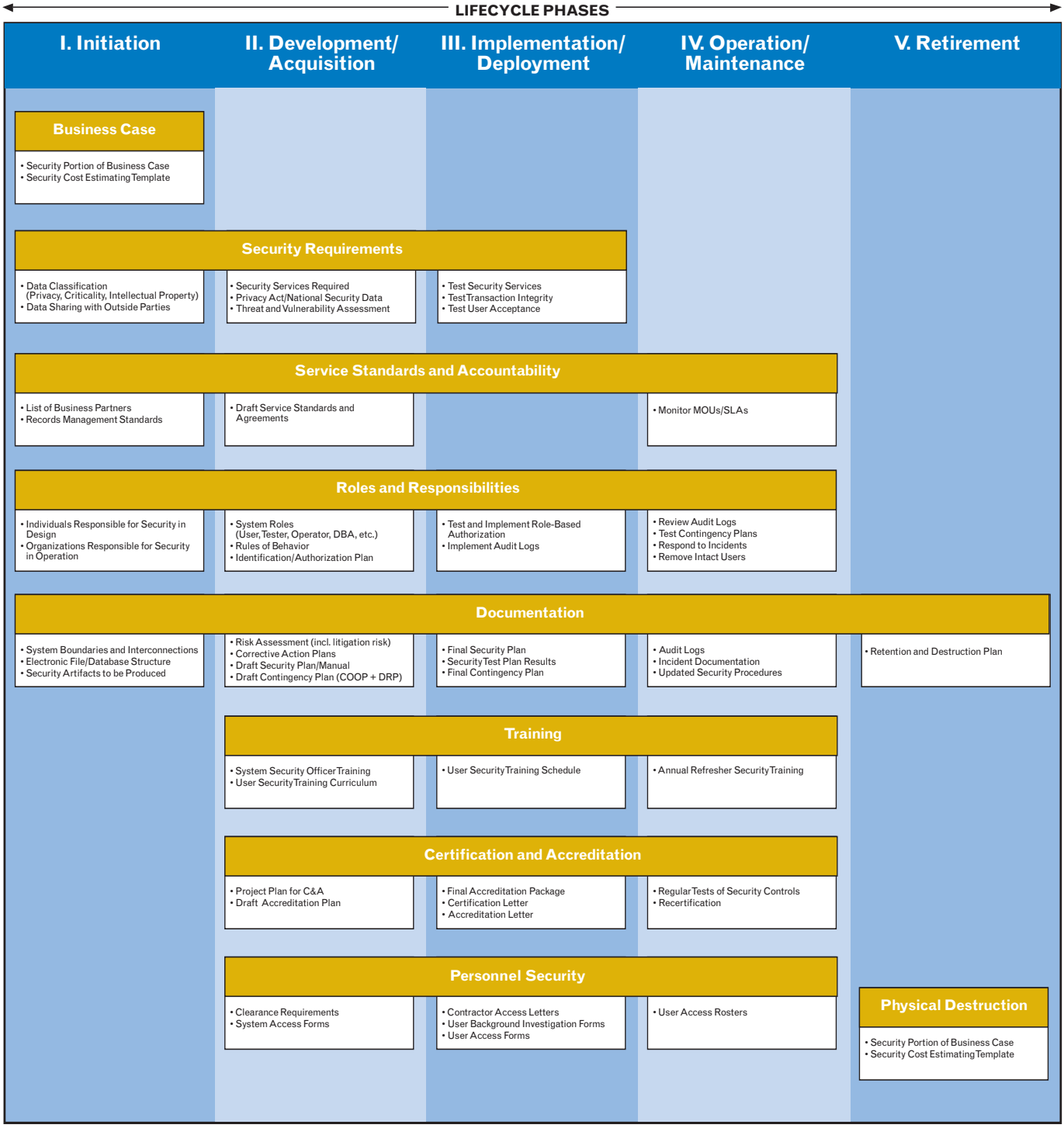

Figure 2, Building Security into the SLDC

Adapted from a graphic produced by the Department of Education, Office of Student Aid.

chapter 2: organizing to manage information risk

Getting the right executives and team members involved in information risk management is critical to making the best decisions. Bring together personnel from key functional and business perspectives to form an Information Risk Management Team in order to balance information risk against other considerations. Give the Information Risk Management Team clear guidance and the right information to assess and balance information risk against other mission priorities. High-performing organizations take a broad perspective on all types of risks to strategic objectives using this perspective to help set priorities and keep management focus on results.

Establish Accountability

Accountability is a foundation for reaching any management goal. Accountability for information risk management starts at the top with the Agency Executive. Successful implementation is driven through the management chain and each employee is accountable in accordance with organizational policy.

- ***Agency Executives -*** Ultimately, the success of the information risk management program depends on senior management. There is a direct correlation between the success of an information risk management program and the level of executive commitment. If you take the issue seriously, your organization will take the issue seriously. Get involved. Show the people you have assigned responsibility for the risk management program that you are behind them. Show your commitment in tangible ways, such as support for well-justified security initiatives during the budget process.

- ***Chief Information Officer -*** Within the top management team, the Chief Information Officer will be the key executive sponsor for the Information Risk Management Program and will have primary responsibility for program oversight and assessment, as well as for advice to the Agency Head on information risk issues. It is obvious that there must be particularly close cooperation between the CIO and executives responsible for security of physical facilities and human resources. However, the CIO cannot deliver a fully successful information risk program without input, guidance, and support from all members of the leadership team.

- ***Information Security Officer -*** A single point of accountability can keep important actions from "falling through the cracks". If it has not already been done, the agency CIO should immediately designate a senior manager as the ISO or Chief Security Officer (CSO) to coordinate the Information Risk Management Program.

  The ISO will serve as the organization's senior advisor on security methods and technology, but the ISO also must be a business-focused manager. Given its importance, the ISO position must be full-time in all but the smallest agencies.

Accountability for information risk management starts at the top.

The ISO establishes and maintains the institutional framework and overall architecture of the information security program, makes the framework operate, works with stakeholders and other groups on cross-cutting security issues, and tracks and develops the agency's response to changes in regulatory requirements and the risk environment. The ISO should not have the authority to make major decisions

on accepting risk or implementing policies in the name of information security that might impact mission performance. Those decisions are the responsibilities of the Agency Head, executives, and program managers.

- ***Program Executives*** **-** Accountability for information risk management should be assigned in writing to program managers in their individual performance plans. This assignment should include accountability for security of both automated and non-automated systems, e.g., all components of their business process. Program managers also should be designated in writing as ultimately responsible for any automated systems that support their programs. For a new system, this designation should be a formal step in the agency's investment control process and it should occur before initial project approval is given.

"...I'm responsible for the security risks for the systems that I manage..."

- Sallie McDonald, Information Assurance/Infrastructure Protection, Homeland Security

- ***End-users*** **-** Individual employees and contractors should be held accountable for following "rules of the system" for each system to which they have access. Penalties for infractions should be defined in the security program and system security plans. Signed acceptance of the rules will support enforcement. Disciplinary action for infractions should be a shared responsibility between the employee's supervisor and system owners.

Establish Performance Standards

The ISO is a functional program manager and should be held accountable for overall performance of the information risk management program. Keep the incentives of the ISO aligned with the overall goals of the agency, which means balancing cost and mission-impact concerns with information security requirements. The ISO's performance standards therefore, should also include some accountability for broad measures of information security costs. This measure should include direct costs of security hardware and software, security services and security staff, as well as program office staff time spent on training and other security-related activities, and costs of information-security failures like lost work time due to virus damage.

The key functional managers on the Information Risk Management Team should share responsibility for success of the overall program, preferably including a specific element in their individual performance plans. They should share accountability with the ISO for overall operation of the program, including both process measures (e.g., degree of compliance with required procedures) and outcome measures (e.g., agency-wide losses due to security failures). Aligning Information Risk Management Team objectives with those of the ISO promotes cooperative behavior.

For program managers, assuring that system-specific security procedures are followed is a minimum performance requirement. These procedures would include, for example, arranging for specialized training of users and administrators of their systems. Consider more outcome-oriented performance goals as well. For example, if a system security plan included acceptance of up to 20 days per year of lost work time due to unscheduled downtime, actual downtime could be part of the manager's performance plan standard.

As with all programs, accountability for information security should have incentives on the up side as well as on the down side. Individual or unit awards are in order where performance against process or outcome goals is exemplary, or for special achievements.

Involve Key Organizational Partners

A successful information risk management program requires involvement of a cross-functional team of individuals, not just the executive or the ISO. Personnel from Operations, Finance, Legal, and Public Affairs, as well as the CIO Office, constitute the members of the Information Risk Management Team.

The team also should have participation by security-related functional areas, including Facilities Management and Human Resources. The Information Risk Management Team serves as the ISO's business advisors and also may have policy oversight responsibility.

Apart from helping make good trade-off decisions, a business-oriented Information Risk Management Team may help the agency find non-technical alternatives for dealing with information risks that would not have been apparent or within the capability of the ISO or CIO to pursue. Non-technical alternatives are often cheaper and more effective than a technical fix.

For the Information Risk Management Team to function effectively, risk issues must be framed in business terms. IT and security professionals may have trouble translating technical issues into business language. It may be smart to bring in a risk management expert to help your technical staff re-orient toward "speaking business" on security issues. While it's essential to have a single coordinating point for the agency's information risk management activities, the most critical determinations that define tolerable risks must have informed buy-in from all affected agency executives.

Provide Information Risk Management Training - Knowledge is Power!

What do accountable managers need in order to carry out their information risk management responsibilities? Adequate resources and authority are essential, as are guides and information on what specific actions or determinations they are expected to make and training on how to apply the information.

It is obvious that the ISO and other technical staff involved in information security should receive specialized training and achieve recognized security certification, if possible. There is an abundance of technical security training aimed at the ISO and security staff available from public and private sources.

It's equally important that the other members of the Information Risk Management Team have sufficient understanding of information risk assessment and risk management to make sound decisions on risk tradeoffs and information risk policies for the agency. Unfortunately, there is little federal guidance tailored to the needs of this class of executives. The ISO and the CIO should take the lead to identify or develop agency-level guidance on information risk assessment and management and associated federal regulations and policies.

Effective training is essential to success.

An effective information risk management training program will teach how to:

- Identify agency business processes and supporting IT assets, including sensitive information; define business risk in terms of their threat to mission and assets;
- Define and communicate the organization's risk tolerance;
- Develop and implement information risk management strategies that balance identified business risk and organizational risk tolerance;
- Identify and understand the costs (financial, operational, and organizational) to implement risk mitigation tactics;
- Identify and quantify the business impact and cost of risks, threats, and vulnerabilities. For example, quantify the cost of one hour of downtime at peak, average, and low volume work times.

Effective training on the specific tasks of information risk management is essential to the success of any information risk management program.

chapter 3: implementing your information risk management program

Adopting a risk management-based model requires a fundamental shift in thinking away from viewing security as a technology problem and towards viewing security as a business issue.

Information Risk Management is a Business Issue, not a Technology Problem

Traditionally, information security has been viewed as a technical issue and delegated to IT managers and staff. In the days of the data center, with limited external access, this model worked. Connecting agency systems to the Internet has led to new threats, service interruptions, and other problems that land on executives' desks for resolution - and explanation! Information risk is now as serious a risk as any other risk with which an executive deals and should be treated as such. Therefore, incorporate information risk into your overall responsibility, assume responsibility for the requirement, and plan, staff, operate, and manage accordingly.

Program executives thinking about information risk management may be tempted to see security as a matter of using the appropriate technology. Avoid that temptation! Though technology is necessary to protect against certain risks and to provide the right kinds of technical controls, technology provides no more adequate systems security than a seatbelt provides driver safety.

In the past, our notion of information security resembled a popular chocolate candy - hard on the outside, but soft and gooey in the middle. We put our computers in high-security buildings, let only pre-authorized people get access to the data, and concentrated on keeping everyone else out. But the Internet has changed all that. E-government not only means connecting to the Internet where untrustworthy characters abound, but it also means we have to allow our trusted users (employees, contractors, customers, partners) to by-pass that "hard candy protective shell." We have to implement flexible, but effective ways to manage access to assets in the "soft middle" of our networks.

The best way to make sure you have implemented effective information security measures in your enterprise is to design security into systems from the start. Then, you must make sure the right sorts of technology investments are budgeted, implemented, and monitored for effectiveness.

The Information Risk Management Program

This section introduces some practical concepts of information risk management that bring to life the Strategic Principles listed in Chapter 1.

The core of an information risk management program is assessing risk and developing alternative risk reduction strategies. But these tasks are very complex. The complexity arises from three sources: first, a very large number of bad things, in infinite combinations, can happen that might affect a business system. Second, new types and combinations of attacks are invented daily, often specifically aimed at defeating the defensive action you took yesterday. Third, even though some bad things are bound to happen, it's hard to get people to agree to an "acceptable" incidence of bad things or to quantify the impact of some of the most important ones (e.g., loss of the public's trust in your agency's ability to safeguard confidential data).

"It's about ensuring the accuracy and reliability of critical information. That is ultimately, in every organization, not a security problem; it's a business problem."

- Frank Reeder, Chair, Information Security and Privacy Advisory Board

While implementing procedures for making risk assessment and mitigation decisions, agencies should incorporate strategies to address the above problems.

1. **Focus on threat to the mission.** Resist the tendency of technical staff to concentrate on hacker threats. Instead, start by engaging the business manager to identify how compromise of a system might affect the mission, or impact customers. Then have technical staff focus on eliminating or minimizing those risks.

Design security into systems from the start.

2. **Use failure scenarios centered on business thresholds.** You can't plan for every combination of circumstances, so try to understand what must or must not happen to accomplish the mission at a few levels of success. This is what most agencies did to prepare for Year 2000 (Y2K). Here again, it may be easiest to begin by discussing the effects of system downtime. How long would it be before system downtime resulted in customer impact? Are some system components more critical than others? Are there backup procedures if automated systems fail?

It's not about technology.

3. **Use existing experience to establish a baseline of "acceptable" risk.** Every existing information system and business process operates with some degree of risk that, by definition, is acceptable. Baseline the existing risk as a starting point for discussions of acceptable risk in the new system or process.

4. **Try to place a cost on a specific amount of mitigation and not on a new technical tool.** Business executives can assess the value of less downtime better than they can a new backup system. They also will be more likely to consider non-technical alternatives to mitigating the risk, e.g., developing manual emergency procedures.

Cost-effective Information Risk Management

Effectively manage the financial aspects of your information risk management program as you would any other program. Understand what you are spending on security and develop metrics to measure the performance of your investments in information risk management.

Providing for information risk management is now a requirement of doing business in both the government and commercial worlds. However, security must be cost-effective - too much security and systems become cumbersome and wasteful; too little security and real damage may result. So how do you achieve a cost-effective investment in security?

- ***Know the Cost of Security*** **-** The first step is to get a handle on how much your organization is currently spending on security. Security spending often is embedded into overall IT systems. It's important to get some rough estimates as quickly as possible, so don't worry about perfection. Capture the categories of security spending - hardware, software, contractor services, staff time - and make estimates from whatever information is available. Once that's done, you've got a rough estimate of your current security budget.

With the current cost picture in hand, you're in a position to exercise real program management. Individual components of the information risk management program can be subjected to cost-benefit and portfolio-management techniques. New investments or moves to standardize across the organization can be shown to have value in terms of cost savings over current operations. Costs for information security compliance and reporting can be highlighted and compared to investment in operational security measures.

- ***Know the Result of Your Investment in Security -*** "To manage it, measure it" is the slogan of performance-based management. After you have identified your current cost picture, you can measure the effectiveness of your investments in security. To do this, develop metrics that can be used to determine the success of your program. Collect data on the results of the existing program in terms of lost work time, citizen confidence, and other measures of impact on mission. These data document the benefit or avoidance of loss produced by a given set of expenditures and the baseline of performance against which goals for the program can be established. Also, compliance is still important, so process-oriented metrics should be used to measure the degree of success in audit and other compliance reviews.

Integrate Information Risk Management into Your Enterprise Management Processes.

Information risk management should be part of overall agency management processes, including strategic planning, human resource planning and budgeting. In this section, we concentrate on three processes where security considerations are most important.

You should incorporate security considerations explicitly into the following business management processes:

- The Agency Enterprise Architecture
- The Agency Capital Investment Management Process
- The Agency Systems Development Lifecycle (SDLC) Guidance

- ***Leverage the Enterprise Architecture Approach -*** Enterprise architecture (EA) is a management process particularly well suited to information-intensive organizations implementing performance-based management. It complements agency and IT strategic planning and can help agency executives focus technology assets on business goals.

Non-technical alternatives are often cheaper and more effective.

An EA includes a blueprint of the desired future state of the organization—the "to-be" architecture. To create this "to-be" blueprint, the organization has to identify and reconcile all major stakeholders' key objectives and constraints into a single consistent whole. The resulting "to-be" architecture is a powerful tool for aligning strategic goals and capital planning. In brief, any investment in a component of the "to-be" architecture has a strong justification, while others face careful scrutiny.

An enterprise information security architecture should be included as an integral component at each layer of the agency's overall enterprise architecture. It promotes enterprise-wide standardization of security policies and implementations that enhance assurance. By showing how all the pieces of the information security program fit together, it helps technical and non-technical executives see the big picture.

Start immediately to develop a first version of the enterprise security architecture, keeping the following in mind:

"Once we've defined the architecture, then you have the map by which you can begin to identify vulnerabilities."

- Steve Cooper, CIO, Homeland Security

1. ***Make the security architecture a joint responsibility of the information risk program manager and the agency's enterprise architecture function.*** The security architecture must fit the rest of the agency EA and the EA staff establishes an overall "framework" that should be followed in the security architecture. The EA staff also can guide the information risk program manager through the substantial body of specialized forms and terminology that develops around the EA.
2. ***Get an initial security architecture published and don't worry about making it perfect.*** Recording what is known or planned is an appropriate goal for version 1.0 of the EA. Feedback from publishing version 1.0 will improve the product faster than doing more research. Wherever possible, incorporate existing plans, documentation, flowcharts, and slideshows into the EA rather than developing information from scratch.
3. ***Focus on the business (upper) layers of the security architecture, rather than "wiring diagrams"*** of the technology.
4. ***Focus on the "to-be" security architecture***, rather than on developing a detailed "as-is" blueprint, even though the "as-is" is easier!
5. ***Don't forget to provide adequate resources for this effort.*** Developing an EA is not an "additional duty."
6. ***Use the security architecture to manage information risk in relation to the whole enterprise.*** Managing risk system by system misses the opportunity to implement shared security services. Enterprise-wide services (e.g., a common authentication or log-in system) can simplify and unify an agency's operations for both administrators and customers. They also can save money by eliminating duplicative investment.

Figure 3, IT Security Framework, is an example of the type of information found in enterprise IT security architecture.

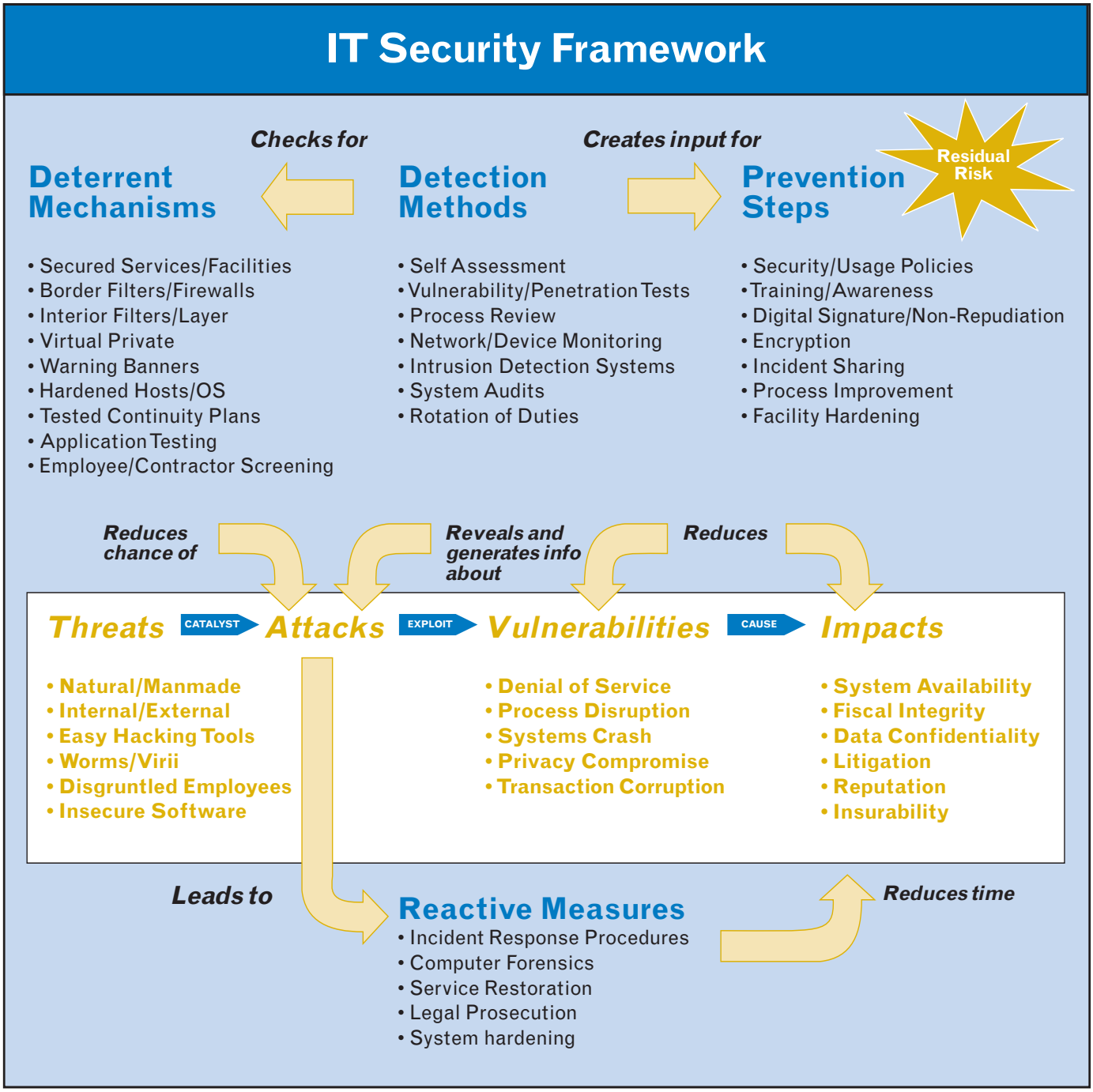

Figure 3, Security Architecture Framework
Adapted by the U.S. Department of Education from a graphic produced by Georgia Institute of Technology.

- ***Integrate Capital Investment*** - The Capital Investment Management process provides a framework to manage the entire IT portfolio of an enterprise, infused with business insight. If the organization's objective is better service to its constituents and increased efficiency, then systems must properly maintain confidentiality, integrity, and availability in order to maintain public trust. It is a business case argument, rather than a security argument.

- ***Build Security into the Systems Development Lifecycle*** - The SDLC provides a framework for rigorously managing the integration of security requirements of each system development project *(See Figure 4)*. To assure secure delivery of the mission, an enterprise view is needed. The SDLC is a way to ensure the quality of software - good quality means the system does what is expected, no more, no less. Integrating security requirements into the SDLC not only ensures that they are addressed, but also that costly rework is avoided in "retrofitting" security into a software product.

  Explicit integration of security-related activities and milestones into enterprise management processes, such as the SDLC, assures appropriate visibility, by appropriate levels of management, into key security and business decisions.

Integration of Investment Management, Project Management and Security

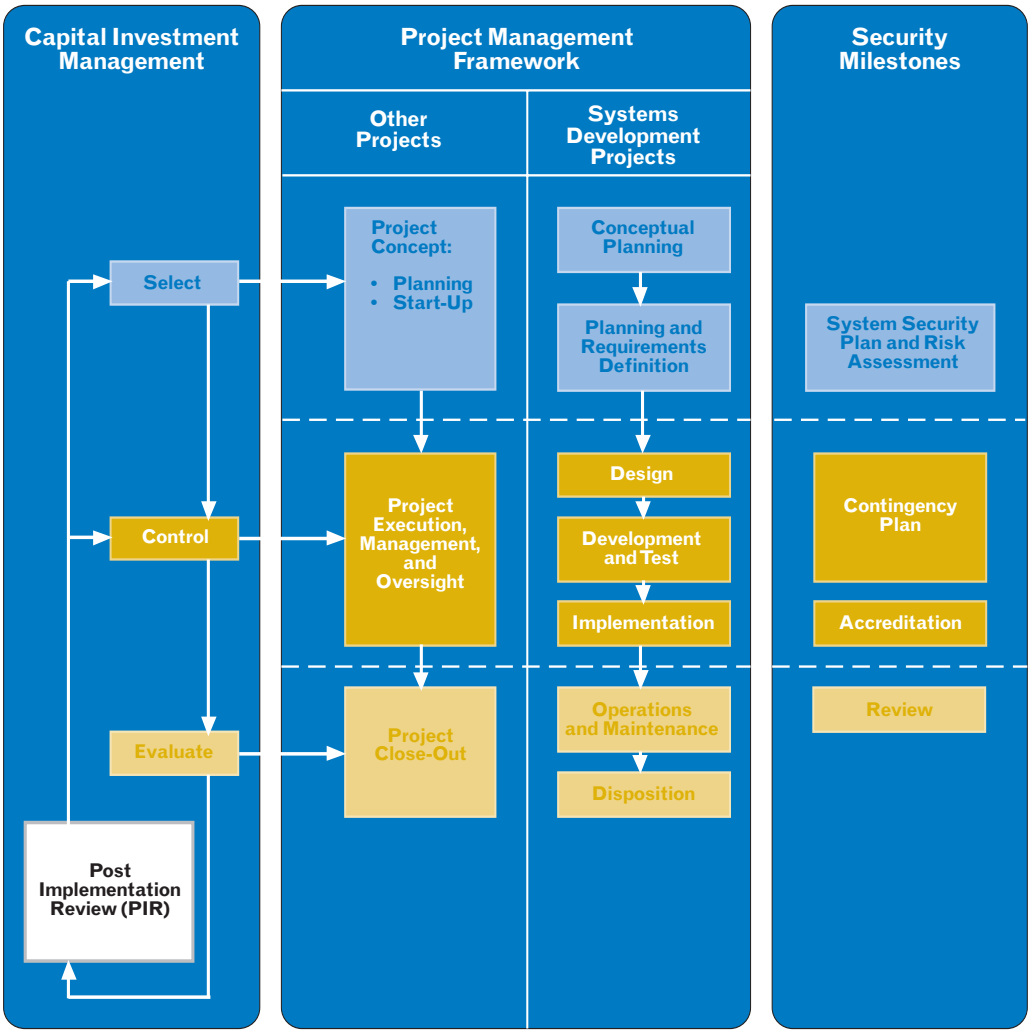

Figure 4, Integration of Investment Management, Project Management and Security
Adapted from a graphic produced by the Department of Labor
(IT Project Management, January 2002, Prepared by the Office of the Chief Information Officer, Department of Labor)

chapter 4: epilogue

The challenge of information security will continue to evolve with changes in technology and business requirements. This Guide has offered concrete ways to improve information security at your agency, but it is critical for your technologists and your Risk Management Team to keep abreast of emerging threats to information security facing the federal government.

As this publication goes to press, several trends confront us with complex security problems:

- The transition to e-government;
- The war on terrorism; and
- The rise of pervasive computing.

The Transition to E-government

E-government is an effort to remove organizational boundaries by providing seamless governmental services through the application of information technology. It includes services coordinated horizontally across agencies and vertically through local, regional, national, and other countries' government service providers. However, the road to e-government has some formidable information-security hurdles. Citizens will only use new on-line services if they trust the security of the systems. And as we bring more and more information together to improve service to citizens, we raise the stakes on protecting the vast databases that make this possible.

The War on Terrorism

The events of September 11, 2001 revealed shocking gaps in the government's ability to share information and coordinate actions. These gaps can be minimized when we are able to manage security across organizational boundaries, including the federal, state, county, local, and tribal governments, as well as the private sector.

The Rise of Pervasive Computing

"Pervasive computing" is the proliferation of device types, media, and locations of networks that is creating an always-on, always-connected global society. As new technology products and services are introduced into the market, the associated risks to security and privacy often are not clearly identified and addressed. Use of wireless devices is an example of pervasive computing that can result in introduction of technology-enabled vulnerabilities into the enterprise. Security policy on the use of these devices and application of appropriate security technologies must be established as early in the life cycle of the product as possible.

In the final analysis, you are the only one who can make sure a sound information risk management program is implemented at your agency. Good program management and security practices are essential. More importantly, as has been found in all ITRB reviews of mission-critical projects, the success of initiatives is directly related to the constructive involvement of senior management.

ITRB members participating in publication development

Participating ITRB Members

Kay Clarey	Department of the Treasury
Martin Smith*	U.S. International Trade Commission
Andy Boots	Office of Comptroller of the Currency
Sandra Borden	United States Coast Guard
Gary Christoph	National Institutes of Health
Ken Heitkamp	Department of the Air Force
George Hyder	Office of Personnel Management
Frank Maguire	Department of Defense

**Publication Team Leader*

ITRB Management Staff

Nora Rice	General Services Administration
Lee Barnes	General Services Administration
Judith Douglas	Electronic Data Systems
June Crosby	Electronic Data Systems
Jim Galie	Electronic Data Systems

People Interviewed for this Publication

Steven Cooper	Chief Information Officer, Department of Homeland Security
Robert Dacey	Director, Information Security Issues, Information Technology Team, General Accounting Office
Sallie McDonald	Information Assurance / Infrastructure Protection, Department of Homeland Security
Mary Mitchell	Deputy Associate Administrator, GSA Office of Electronic Government and Technology
Franklin Reeder	Chair, The Information Security and Privacy Advisory Board Chair, The Center for Internet Security President, The Reeder Group
Marianne Swanson	Senior Advisor for Information Technology Security Management, Computer Security Division, National Institute of Standards and Technology (NIST)

Acceptable Risk A concern that is acceptable to responsible management due to the cost and magnitude of implementing countermeasures.

Accountability The property that allows auditing of information system activities to be traced to persons or processes that may then be held responsible for their actions.

Accreditation The authorization and approval granted to a major application or general support system to process in an operational environment. It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate system security.

Attack Attempt to gain unauthorized access to an Information System's (IS) services, resources, or information, or the attempt to compromise an IS's integrity, availability, or confidentiality.

Availability Ensuring timely and reliable access to and use of information.

Certification The comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements.

Confidentiality Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

FISMA Federal Information Security Management Act of 2002 - Purpose(s): (1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets; (2) recognize the highly networked nature of the current federal computing environment and provide effective government-wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities; (3) provide for development and maintenance of minimum controls required to protect federal information and information systems; (4) provide a mechanism for improved oversight of federal agency information security programs; (5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and (6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

Information Security Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—*(A) integrity* - guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; *(B) confidentiality* - preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (*C) availability* - ensuring timely and reliable access to and use of information.

Information System Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation,

management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data (digital or analog); includes software, firmware, and hardware.

Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

ITRB The Information Technology Resources Board was formalized in July 1996 by Executive Order 13011 to provide peer review assessments of mission critical information systems by: identifying critical issues and findings; framing these in management and/or technical perspectives; and by recommending actions to mitigate risks or resolve issues.

OMB Circular A-130 OMB A-130, Management of federal Information Resources, Appendix III, Security of Federal Automated Information Resources: Establishes a minimum set of management controls that are to be included in federal automated information security programs. These include assigning responsibility for security, developing a system security plan, screening and training individual users, assessing risk, planning for disasters and contingencies, and reviewing security safeguards at least every three years. It recognizes that all federal computer systems require some level of protection. It also requires agencies to clearly define responsibilities and expected behavior for all individuals with access to automated systems and to implement security incident response and reporting capabilities.

Risk The possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

Risk Management The ongoing process of assessing risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

Risk Management Team Cross-functional, cross-organizational group of personnel (e.g., Operations, Finance, Legal and Public Affairs, as well as the CIO Office) that are responsible for organizational information risk management.

Social Engineering Use of psychological tricks on legitimate users of a computer system to gain information (usernames and passwords) needed to gain access to a system. Techniques that rely on weakness in human nature rather than software; the goal is to trick people into revealing passwords or other information that compromises security.

Technical Controls Consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

Threat An activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity.

Vulnerability A flaw or weakness that may allow harm to occur to an automated information system or activity.

Information Technology Resources Board
U.S. General Services Administration
Office of Electronic Government & Technology
1800 F Street, NW
Washington, DC 20405
Attn: ITRB Program Manager

Web: ***www.itrb.gov***
e-mail: ***itrb.support@gsa.gov***