PRIVACY PROGRAM MANAGEMENT

Tools for Managing Privacy Within Your Organization

Executive Editor and Contributor

Russell R. Densmore, CIPP/US, CIPP/IT
Deputy Chief Privacy Officer, Lockheed Martin Corporation

Contributors

James M. Byrne, CIPP/US, CIPP/G, CIPP/IT
Elisa Choi, CIPP/IT
Ozzie Fonseca, CIPP/US
Edward P. Yakabovicz, CIPP/IT
Amy E. Yates, CIPP/US

An IAPP Publication

Cover design: Noelle Grattan, -ing designs, llc.

Copy editor: Sue Ducharme, TextWorks

Compositor: Ed Stevens, Ed Stevens Design

Indexer: Wendy Catalano, Last Look Editorial Services

ISBN: 978-0-9885525-1-7
Library of Congress Control Number: 2012955874

Contents

SECTION II: Privacy Operational Life Cycle

Figure List

Table List

SAMPLE FROM CHAPTER FOUR
Assess

2. Assess Key Areas of Your Business (Data, Systems and Process)

The functions of internal audit and risk management, information technology (IT), information security and privacy office/team are closely related and, in many companies, may form one team. A simple analogy may serve to describe this relationship. If you were to picture an information network in terms of plumbing, then IT would be directing attention to the pipes and how they fit together to allow for the proper flow of water (i.e., personal information). Internal audit/risk and information security, on the other hand, are more concerned with how securely the water flows through the pipes. They ask questions, such as: How can that water (data) be protected and who has access to it? Where does the water flow, which pipes are being used, and which pipes are inadvertently being exposed to wrong uses by wrong users (i.e., security breaches)?

A thorough privacy assessment approach should support these business areas.

- Internal audit and risk management
- Information technology: IT operations and development
  - Business continuity and disaster recovery planning

- Information security
  - Security, emergency services and physical access
  - Incident response and breach notification
- Human resources/ethics
- Legal and contracts
  - Compliance
  - Mergers, acquisitions and divestitures
- Processors and third-party vendor assessment
- Marketing/business development
- Government relations/public policy
- Finance/business controls

2.1 Internal Audit and Risk Management

Internal audit (IA) and risk management functions review and analyze the whole organization—all departments, functions and operations. They are responsible for discussing audit and risk with senior leaders, mid-level managers, first-level managers and employees. Based on the industry, these roles take on different meanings. Auditors and risk managers take on many roles and responsibilities based on the industry and organization, to include finance, performance, quality, project, operations and more. Their responsibilities include reviewing privacy assessment results and the identification of privacy risk for the organization.

Internal auditors evaluate the organization's risk management culture and identify risk factors within all systems, processes and procedures. In addition to evaluating control design and implementation to ensure proper risk management, internal auditors test those controls to ensure the proper operation. Risk managers ensure business and regulatory requirements through detailed market, credit, trade and counterparty analysis that communicate risk and issues throughout the organization.[8]

The nature of IA and risk management is different from other groups that may conduct internal risk assessments. Most IA departments report to an audit committee that reports to the board, assuming a predominantly independent role from the rest of the organization. While assessments come back with *recommendations* about what should be fixed, audits come back with findings that *must be* fixed. Since IA is independent of management in most cases (also a good best practice to separate the roles and responsibilities), the audit committee can be confident that internal audits are unbiased in the reporting of audit findings. Internal audits, or self audits, within an organization signify a commitment by the organization to be proactive in its approach to reducing corporate risk. This is evidenced by several positive contributions, such as:

- Focus on value-add activities beyond financial controls
- Use enterprise risk management (ERM) processes making risk a priority
- Hire auditors and risk managers with different skill sets (e.g. HR, IT, IA)
- Identify risk factors proactively, before they become incidents
- Ensure an independent perspective using audit committees and third parties on the governance, risk management, and control processes
- Identify and use best practices for recommendations to improve controls, performance, and reporting throughout the entire organization

2.2 Information Technology: IT Operations and Development

IT operations and development is a crucial piece of an organization's privacy program. Here is where the IT team implements controls and technical solutions in systems that include computers, networks and automated systems to provide a high degree of security technical controls in order to sustain the privacy program objectives and goals. It is important for IT operations and development to follow the organization's guidelines and incorporate privacy requirements from the outset.

There is no one-size-fits-all solution regarding technical controls—every environment has its own specific needs, requirements and protections. Smaller companies will not necessarily have the same kinds of security concerns that confront larger companies, so this area needs proper research and evaluation. The goal is always the same—to protect the data for every organization—so controls should be implemented through refined engineering processes that are repeatable, documented and measured.

Numerous technical controls, devices, systems and products exist throughout the market today. The privacy professional should leverage internal offices, such as IT or security, to assist in discussions, evaluations, requirements and use. A simple rule to follow with any technical issue is to use an expert rather than attempt to become an expert. Although privacy professionals may know and understand certain technologies, they should always consult, document and collaborate on all things IT and strengthen those ties to privacy.

2.2.1 Business Continuity and Disaster Recovery Planning

Although not typically thought of as a part of audit or risk, business continuity and disaster recovery planning (BCDR) are two complementary processes that prepare an organization for crises and managing the business afterwards, thereby reducing risk. As stated by an audit executive, "Internal audit's job is to provoke [thinking about] the unthinkable and ensure we have a plan."[9] The focus is to recover from a disaster when disruptions of any size are encountered. The overall goal of any BCDR plan is to maintain your organization's operations by mitigating the effects of disruptions. In other words, developing a good BCDR plan is practicing sound risk management.

BCDR is sometimes considered a high-cost insurance policy that is never used; thus the privacy professional should understand the key role played by this critical function and how it impacts (both negatively and positively) the organization. As the Info-Tech Research Group states, "When risk and business impact are misinterpreted or miscommunicated [within the BCDR plan], many problems arise:

- Lack of unified incident response across the organization
- Failure to achieve consensus on standardized recovery processes
- Incomplete or nonexistent risk assessments, assumptions and objectives
- Insufficient communication plans to coordinate recovery/continuity efforts
- Inability to recover data and applications"[10]

An effective BCDR ensures critical business functions continue; thus, understanding which staff and systems are mandatory to continue as a business and how to resume operations are necessary components. Recovery and restoration of personal information must be handled appropriately during the recovery period. The stressful conditions experienced during disaster recovery operations can cause mistakes that result in data being exposed. It is essential, therefore, to have a plan in place prior to a crisis to safeguard all personal information that ensures the organization privacy objectives and goals. Info-Tech recommends the following BCDR practices:[11]

- Make BCDR clear to executives so they understand BCDR is more than technology and must be properly budgeted and tested
- Convince the business to get involved so they understand the cost of downtime in lost business, customer relationships and customer service
- Develop recovery time objectives and recovery point objectives and then communicate those throughout the organization to stakeholders at all levels to ensure collaboration, support and awareness
- Use BCDR best practices; do not create the wheel, and eliminate rework or duplicated work between IT, security and privacy

Because the BCDR plans include many components, the privacy professional should focus on the privacy aspects to protect and manage data privacy throughout BCDR planning, execution and reporting. As an example, during a pandemic, Rachel Hayward states, "Privacy professionals need to work with the business continuity planners and human resource departments to clarify any questions regarding the collection, use, and disclosure of personal employee information during the development of organizational [business continuity plans] that include considerations … The challenge is to balance these needs with the needs of the organization to plan for the potential of prolonged staff shortages caused by employee illness, and, potentially, employees staying home from

work to care for loved ones … a single department within an organization may be severely affected while other areas are less affected, or not affected at all."[12]

The privacy professional should ask the following questions for BCDR:

- Does our BCDR plan align with our organization's privacy policies and procedures?
- How will we protect personal information from loss and exposure before, during and after an event?
  - Maintaining a backup system off-site?
  - Training for backup employees to handle various tasks in an emergency?
- Are there business contingency plans in place that ensure data privacy?
  - Alternate locations for office operations with the same protections?
  - Alternate means of communicating within the organization and to outside contacts (e.g. supply chain networks, customers) with the same level of privacy controls?

It is recommended the BCDR be assessed from a privacy perspective.

2.3 Information Security

Information security is a complex topic that includes technical and physical controls that span the organization to form IT systems, building security, remote users, vendors and third parties. As controls change all the time based on newer releases of technology, software applications, upgrades, decommissions and rotation in staff, control management should be an agenda item at many privacy and security meetings to communicate, understand and provide proper management practices, information and collaboration of that data. These controls have to include the privacy requirements of the organization.

> *As privacy is concerned with an individual's ability to control the use of personal information, information security focuses on mechanisms for protection of information and information systems.*

At the high level, information security provides standards and guidelines for applying management, technical and operational controls to reduce the probable damage, loss, modification or unauthorized access to systems, facilities or data. This includes having a strategy for document destruction, sanitization of hard drives and portable drives, security of fax machines, imaging and copier machines. Many times there is confusion between applying all three of these controls, and information security is only considered within the technical controls of an enterprise, domain, system, etc. The privacy

professional should become an expert with all three as related to the policies, standards and codes of conduct of the organization's management structure, objectives and goals.

At the highest levels, these three controls are secured through three common information security principles from the 1960s, known as the C-I-A triad, or information security triad:

- **Confidentiality.** Prevention of unauthorized disclosure of information
- **Integrity.** Ensure information is protected from unauthorized or unintentional alteration, modification or deletion
- **Availability.** Information is readily accessible to authorized users

Further advanced information security concepts developed years after the principles from above were established include:

- **Accountability.** Entity ownership is traceable
- **Assurance.** All other four objectives are met

These practices apply high-level reasoning to risk management and define the organization's objectives and goals for data security. Since security practices are based on geographical, legal, regulatory and other considerations, the privacy professional should understand the organizational strategies to meet those and determine stakeholders for communication, collaboration and information sharing. Information security in general is a complex topic that may span the organization. By becoming familiar with the stakeholders, the privacy professional will have open channels of communication to and from those key players throughout the life cycle management aspects.

It is important the security controls are an integral part of the privacy assessment process.

2.3.1 Security, Emergency Services and Physical Access

All security-related services should be aligned with the organization's privacy policies and procedures. Physical security measures implemented at each facility should reflect the sensitivity of the information housed at that location. Procedures should be in place to control access to the organization's facilities and to prevent unauthorized access to resources within those facilities.

Monitoring physical access to the organization's facilities is a function of the security department. Procedures should be in place to confirm that the data being used to monitor access (e.g., surveillance videos, access logs, etc.) is handled, stored and destroyed appropriately, in accordance with the entity's privacy and security requirements. The security department should also be aware of the organization's incident response protocol, as they may be required to notify or otherwise provide evidence of potential breaches to the designated parties (e.g., privacy office, incident response team, information security, etc.) and to help support investigations regarding unauthorized access or compromise. It is also important these services, wherever they collect personal information, also undergo a privacy assessment.

2.4 Human Resources/Ethics

Depending on the organization's size, industry, geographical location and more, HR and ethics management cross boundaries or are totally separate. Smaller organizations might be forced to merge the offices, while larger organizations could devote many more resources to these tasks.

2.4.1 Human Resources

Staff in the HR department looks at the personal information life cycle of specific HR data to ensure that the handling of all information by HR personnel is in compliance with the organization's privacy policies and procedures.

The human resources function will include personal information in areas such as:

- Talent acquisition and hiring
- Performance management
- Training and development
- Compensation and benefits
- Employee relations
- Employee records
- Succession planning

Multinational organizations are required to meet local regulations and the privacy expectations of their employees in all countries in which they operate. Obligations do not simply disappear because the office or employees are in another state, country or continent. Specifically, cross-border data transfers should be monitored to regulate the export of personal data to ensure regulatory compliance and data privacy. The employment contract provides overall employee consent for certain work-related activities. Some surveillance/monitoring in the workplace will require additional privacy considerations.

Employee privacy considerations are other important activities for HR to review:

- Investigations of fraud and criminal activities
- Handling of organization trade secrets for the protection of that information
- Prevention of discrimination, sexual harassment and other human rights concerns
- Compliance with workplace safety
- System integrity with compliance of security and privacy practices[13]

2.4.2 Ethics

Not all companies have a separate ethics office, but all companies need to have an ethics function. This may be tied in with compliance or HR, but there needs to be accountability for people doing the right thing within the organization.

There needs to be a trusted place in your organization where people can take their complaints, concerns and possible whistle blowing when necessary. If an allegation should arise, for example, concerning someone invading another individual's personal information, there needs to be a procedure for responding, resolving and documenting the situation. Usually this is a function of the privacy office.

Ethics will often function in a manner similar to IA; that is, independent of the normal chain of command and properly empowered and staffed to perform necessary tasks. Ethics will usually report directly to the board, or as close to the board as possible. This is necessary to guard the integrity of the ethics function, protect the data and protect the organization from possible misconceptions of data confidentially. If an allegation were to be made against the chief executive officer of the corporation, for instance, you could not have your ethics department reporting to the very person being investigated. By guarding the independent operations of the ethics function, your organization sends a strong message about its commitment to privacy protection.

Wherever the ethics function is located within your organization, you need to make sure that you are addressing the issue of people doing the right thing with other people's personal information, investigating matters as they arise and reporting those to proper stakeholders to protect the individuals and the organization.

2.5 Legal and Compliance

As with many other categories, legal and contracts can overlap in layers or be two distinct topics, depending on the organization's size, geographical location and other factors. These tasks may overlap within administrative, clerical and research duties.

> *Legal, security, audit, risk and compliance may overlap or be separate based on the organization.*

2.5.1 Legal

"Privacy policies have become long legal documents that most attorneys, let alone the average consumer, have difficulty understanding. They are meant to provide notice to individuals about data collection, use and disclosure policies. However, they are often complicated, long, and unintelligible and, as a result, rarely read by the average consumer … Your organization's privacy practices must align with its privacy promises to minimize legal liability. You can do so by conducting factual and legal due diligence. The factual due diligence allows you to determine what information your organization uses. The legal due diligence allows you to determine what laws govern the use of that information. You need to understand both in order to competently draft a privacy policy that minimizes legal risk for your organization."[14] The legal office is therefore the necessary owner of this task, to perform legal liability activities in conducting the due diligence.

To perform this due diligence, a legal office, team or person with the legal roles, responsibilities and empowerment must be appointed to act for the organization. This role will then have the responsibility for ensuring that the organization is in compliance with all legislative, regulatory and market requirements that are specific to your industry. They should also understand local privacy obligations and requirements that pertain to that organization in the countries from which the data is collected. This includes, for example, registering and obtaining international transfer approvals with data protection authorities (DPA) in those countries where this is required.

Administrative, clerical and research duties may apply across the organization or be delegated to a small group. Administrative duties may include legal advice, translation of laws and regulations into plain language, lawsuits, and senior leadership to the organization. Clerical duties include contracts (e.g., assisting the contracts office, writing contracts, etc.), legal document management and possible budget and expenditure assistance.

Research is another legal duty to ensure the organization is acting in accordance with laws, regulations, industry, geographical location, etc. The privacy professional should become familiar with the legal staff and how the organization performs the legal duties, as well as how privacy is impacted, managed, addressed, and considered or *scrutinized* by the legal team.

Legal should have controls, documentation management practices and tracking mechanisms to identify, track and record all procurements, contacts, service-level agreements and performance measurements for privacy management. Are there established procedures in place, for instance, to review contracts with vendors who handle personal data while representing your business? Is that data tracked and reviewed on an ongoing basis? Do the organization customers have a need to review this material for auditing or reporting purposes? The vendors must be held to the same standards as employees, and all vendor functions must be aligned to the privacy requirements you've established through your privacy framework.

An incident management and breach response team should include IT, security, the privacy office, legal and HR as required. This team manages the breach notification activities, as necessary, with guidance and leadership from the legal office to ensure understanding of the regulatory aspects and internal control of the information, the findings and the impacts that result. The legal office—as a privacy management stakeholder—should be aware of the privacy governance in the organization, roles and responsibilities, lines of communication, joint planning and coordination of risk.

2.5.2 Compliance

Privacy compliance is no less complicated than the legal aspects. For example, in the EU, the EU Data Protection Directive requires member states to adopt laws that protect personal information, to disclose who is collecting the data and why, and who will ultimately have access to it. The Directive also gives the person the right to access

the data and make corrections to it. Some multinational organizations doing business between the EU and U.S. may use Safe Harbor, while companies operating solely with the U.S. have federal, state and local regulations and laws that are sectoral, based within finance, healthcare and other industries. Compliance to the privacy standards and laws is challenging and not getting any easier. As stated in Chapter 2, because penalties for violation of privacy laws and regulations are increasing, the privacy professional must be prepared to address, track and understand any penalty that could affect the organization.

Compliance to privacy standards and laws is challenging and not getting any easier, regardless of geographic location, industry or organization size.

Compliance can exist within any of the core business functions: legal, security, IT, audit or others. There are specific merits to the layering, overlapping or separation of each as defined by the organization objectives or goals. Regardless, the roles and responsibilities of each function must still be performed in one way or another to ensure the success of the organization. Mark Ruppert states that the advantages and disadvantages of combining these include:

- Separation of legal, compliance, internal audit and security functions: "collaboration is more challenging, but functional independence is assured."
- Combining legal, compliance, internal audit and security functions: "collaboration is assured, but functional independence is more challenging."[15]

He also highlighted the fact that twenty-two comparative compliance categories exist within a *generic* organization to reflect the complexity in the compliance roles and responsibilities that may include:[16]

- Requirement
- Purpose
- Reporting
- Internal authority
- Span of responsibility
- Professional standards
- High-level focus
- Primary risk focus
- Activity focus
- Relationship management
- Training
- Auditing
- Monitoring
- Expertise
- Compliance plan
- Risk
- Follow-up
- Investigation
- Hotline
- Information systems
- Internal controls
- And others that overlap from this list

Access to the organization, proper governance, lines of reporting and authority, organization placement and organizational access impact all of these categories to

achieve effective privacy management and governance. The privacy professional will need to define the roles and responsibilities of compliance for the organization and document when, where and how privacy is managed within many of these layers. The starting point to complete this task may be within several offices or unique roles that depend greatly on the organizational structure and purpose. It may be the legal office, internal audit, risk management or privacy office itself.

Because of the overlap for compliance, the privacy professional should be prepared to track and investigate all possible roles and responsibilities within the organization. Remember that each organization completes this role differently by combining or separating them. The key will always be found in the organizational governance structure, joint planning and coordination of risk management in the organization. Risk is typically the driving factor for establishment of many offices, including privacy, security, audit and compliance, so the starting point will be to understand the organizational risk approach, the supporting offices and the governance.

2.5.3 Mergers, Acquisitions and Divestitures

Mergers, acquisitions and divestitures contain many legal and compliance aspects, with their own sets of concerns related to privacy. Mergers form one organization from others, while acquisitions involve one organization buying one or many others; divestitures remove one aspect of an organization for several motives, which may include selling off part of the business not integral to the core.

An organization can be exposed to unnecessary corporate risk by acquiring companies that may have different regulatory concerns than the current business environment. Examples below illustrate the need to consider the variety of regulatory considerations that may be involved in any of these actions, to include:

- Acquiring an organization that is a U.S. Health Insurance Portability and Accountability Act (HIPAA)-covered entity if the parent organization is not
- Acquiring an organization that needs to meet PCI-compliant standards or other regulatory compliance, such as Statement on Auditing Standards, No. 70, Service Organizations (SAS 70) reporting
- Acquiring an organization that has employees in countries with specific privacy legislation; for example, PIPEDA, EU Data Protection Directive, etc.
- The acquisition of an organization with existing client agreements requires a review by the new ownership in regards to the control, movement and use of the data, including marketing
- New resources, technologies and processes need to be assessed in order to identify all actions that are required to bring them into alignment with privacy and security policies before they are integrated into the existing system

2.5.3.1 Divestitures

With respect to both partial and total divestitures, the organization should conduct a thorough assessment of the infrastructure of all, or any part of, the entity being divested prior to the conclusion of the divestiture. These activities are performed to confirm that no unauthorized sensitive information, including personal information, remains on the organization's infrastructure as part of the divestiture, with the exception of any pre-approved proprietary data.

It is important to the organization to include a privacy checkpoint as part of the merger, acquisition, and divestiture processes.

2.6 Processors and Third-Party Vendor Assessment

Processors, third-party vendors and business process outsourcers who are now a part of the standardized business practice must also be part of the privacy management program to remain vigilant about data protection. In the majority of the legislations, accountability remains with the organization; therefore, privacy controls that determine how data is to be protected and handled must exist in the contracts with the processors and third-party vendors. Compliance factors, the ever-changing landscape of privacy and security regulations, multinational considerations, geographical location and other factors relevant to storing, processing, and transmitting privacy data must maintained.

Organizations should carefully vet vendors prior to selection and continue to monitor and audit them through the life of the contract to ensure proper privacy and security risk management practices. Contract language should be written to call out privacy protections and regulatory requirements within the statement of work and then mapped to service-level agreements to ensure there are no questions about the data privacy responsibilities, breach response, incident response, media press releases on breaches, possible fines, and other considerations, as if the vendor were part of the organization. Privacy/security questionnaires, privacy impact assessments and other checklists can be used to assess the vendor risk and should include consideration for the vendor's privacy and information security policies, access controls, where the personal information will be held and who has access to it. Results may indicate improvement areas that may be fixed or identify higher-level risk that may limit the ability of that vendor to properly perform privacy protections.

Once risk is determined, the organization best practices may also be leveraged to assist a vendor too small in size or with other limited resources by offering security engineering, risk management, training through awareness and education, auditing and others.

The vendor contract should include specific information about what services the vendor will be providing and what the vendor's responsibilities are. The following list gives a few examples of the kind of information you may want to consider including:

- Specifying the type of personal information the vendor will have access to at remote locations
- How the vendor plans to protect personal information
- The vendor's responsibilities in the event of a data breach
- How the data will be disposed of when the contract is terminated
- Limitations on the use of data that ensure that it only be used for specified purposes
- Rights of audit and investigation
- Liability for data breach

The purpose of the vendor contract is to make certain that all vendors are in compliance with the requirements of your organization's privacy program.

2.7 Marketing/Business Development

Aligning marketing/business development means that any activities where information is collected and shared as a function of marketing must conform to regulatory privacy practices.

2.8 Finance/Business Controls

Finance is linked to many of the other organizational functions discussed in this chapter. Finance will typically control the money and budget of an organization, including employee payroll, investments, expenditures and many other sensitive key business indicators that may or may not be within the scope of privacy. Financial functions should align with requirements in the privacy framework and legal, security, risk and many other governance factors of the organization. Internal lines of communication and control are necessary to establish and observe privacy practices to ensure organizational objectives and goals.

Finance must have some effective means to track any changes to regulatory requirements and to update finance employees' awareness of those changes. All financial functions must handle financial information that aligns with current regulatory requirements) and the overall privacy program.

Examples of financial functions include:

- Accounts receivable
- Accounts payable
- Payroll
- Securities
- Investments

Don't be reluctant to phone a friend. *Conducting a gap analysis using some or all of someone else's maturity model is not necessarily an intuitive activity. Professionals usually study and pass exams in their chosen subject fields—it takes time to become proficient. If you've never conducted a review before, ask relevant and experienced colleagues for help and advice. The IA function may have templates you can adapt and use. You may be lucky, and they may offer to partner with you in conducting the assessment. Use the internal resources and skills available to you; they know your business best. You don't necessarily have to hire expensive internal consultants.*

All processes in the above functions should undergo a privacy assessment if/when personal information is handled.

3. Summary

Assessment of your organization's privacy program is one stage of the privacy operational life cycle. There are a variety of models and frameworks—including maturity models—that provide guidelines for measuring and aligning privacy activities. These models can be used in whole or in part to help your organization conduct an effective assessment.

Endnotes

1 AICPA/CICA, Privacy Maturity Model, March 2011, www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/DownloadableDocuments/10-229_AICPA_CICA%20Privacy%20Maturity%20Model_FINALebook_revised0612.pdf.

2 *Id.* at 2.

3 *Id.* at 3.

4 *Id.* at 2.

5 Information and Privacy Commissioner, *Executive Summary*, www.ipc.on.ca/site_documents/achieve-goldstnd_execsumm.pdf.

6 Federal Trade Commission, *Protecting Consumer Data in an Era of Rapid Change: Recommendations for Businesses and Policy Makers*, p.iii, p. vii, March 2012, http://ftc.gov/os/2012/03/120326privacyreport.pdf.

7 Information and Privacy Commissioner, Ontario, Canada, *Privacy by Design: From Policy to Practice*, September 2001, www.ipc.on.ca/images/Resources/pbd-policy-practice.pdf.

8 Counterparty: commonly used in the financial services industry to describe a legal entity, unincorporated entity or collection of entities to which an exposure to financial risk might exist.

9 Ernst & Young, *Executive Summary: Internal Audits Evolving Role: A Proactive Catalyst of Business Improvement* (2011), www.energycollection.us/Board-Of-Directors/Audit/Internal-Audits-Evolving.pdf.