The Institute of Internal Auditors Research Foundation

Proudly Presents

Electronic Systems Assurance and Control

eSAC Model

Written by:
Jay H. Stott, CIA, Fidelity Investments

Edited by:
Xenia Ley Parker, CISA, CFSA

Project Review Team:

Charles H. Allen, Wilmington Trust Company
Angelina K. Y. Chin, CIA, General Motors Corporation
Charles H. Le Grand, CIA, Institute of Internal Auditors
David S. Lione, KPMG LLP
Steven S. Mezzio, CIA, CCSA, PricewaterhouseCoopers LLP
Kurt F. Reding, PhD, CIA, Pittsburg State University
Mark L. Salamasick, Bank of America
Jay H. Stott, CIA, Fidelity Investments
Roderick M. Winters, CIA, Microsoft Corporation

The Institute of Internal Auditors Research Foundation
Your Key to the Future

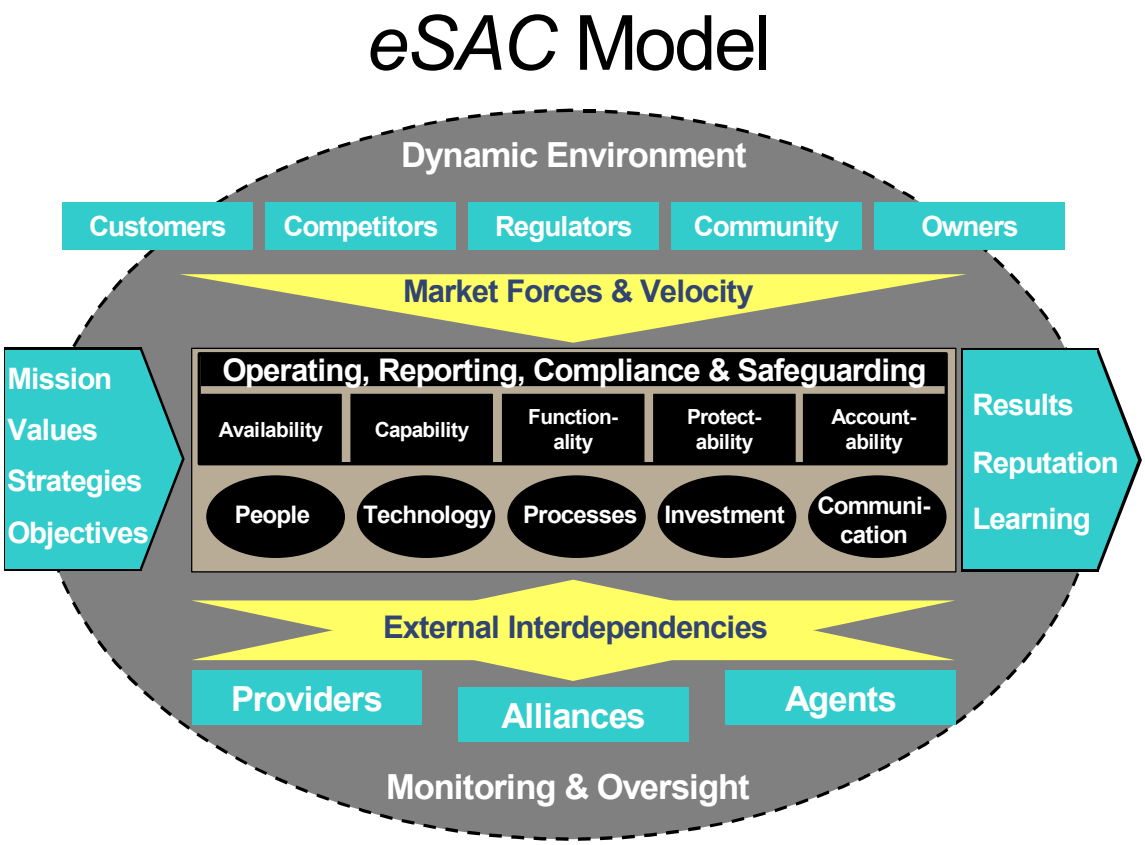
eSAC Model

Introduction

Internal auditors must understand the business risks resulting from changes in technology. They then need to be able to articulate responsive risk management strategies to management, and provide assurance on the availability, capability, functionality, protectability, accountability, and auditability of the systems involved.

To facilitate discussions of these issues, the *eSAC* Model was developed. As the COSO *Internal Control--Integrated Framework* provided a common control language for management and auditors, the *eSAC* Model facilitates the discussion of objectives, risks, and mitigation responses within the context of e-business. Its purpose is to focus on how the risks resulting from rapid technology and e-business model changes can be managed, both in discussion and implementation.

There are, of course, many different risk and control models, and they must all be tailored to a given organization. Topics such as the rapidly evolving regulatory environment, how much capacity is enough, and making realistic technology choices are a few of the significant issues that can be reviewed through the lens it provides.



Model Description

The COSO framework of objectives, risks, and controls (mitigating responses) is an integral part of this model, since it has been successfully employed in numerous organizations. From a global perspective, similar reports that have been issued worldwide, such as Cadbury in the UK, have the same general concepts, so this should be easily adapted in any environment.

An organization typically pursues its mission (purpose) through establishing strategies and objectives consistent with its values. This process is indicated by the arrow at the left side of the model. The organization aims to achieve desired results while enhancing or preserving its reputational standing and learning how to improve its future performance. These outcomes are shown as the arrow at the right of the framework.

A sound control environment helps an organization stay on its intended path as it moves from mission to results. The broad control context — effectiveness and efficiency of operations, financial and other management reporting, compliance with laws and regulations, and safeguarding of assets (COSO objectives) — is captured in the top center of the framework. These are abbreviated for presentation as Operating, Reporting, Compliance, and Safeguarding.

Availability, Capability, Functionality, Protectability, and Accountability, in the next row, capture control attributes that are particularly pertinent for e-business activities. They can equally be called business assurance objectives, since they are broader than the way in which some people view control. These assurance objectives provide the "framework" through which *eSAC* topics or modules are discussed. For instance, Privacy concerns will be addressed under Protectability and Accountability.

Availability
Information, processes, and services must be available when needed. Specifically, the organization must be able to receive, accept, process, and support transactions in a manner acceptable to its customers. Access via the Internet can mean availability 24/7/365. To ensure availability, the auditor evaluates controls that deal with potential causes of business interruption. These might include:

- Physical and logical security of system resources
- Mechanical failure of file storage devices
- Malfunction of software or unexpected incompatibilities
- Inadequate capacity planning

In the event of a problem, controls must provide for swift recovery.

Capability
Capability means end-to-end reliable and timely completion and fulfillment of all transactions. This means that the system has adequate capacity, communications, and other aspects to consistently meet needs, even at peak demand. For systems to provide such services, monitoring of usage, service-level agreements with Internet service providers, application service providers,

and others are important controls. It is critical that system and process bottlenecks be identified and eliminated or carefully managed — the goal is to achieve and maintain an efficient and effective balance across the organization.

Efficiency of systems is an aspect of capability that leads to effective use of resources. A key is controlling system development and acquisition methodologies to prevent cost overruns and systems that do not perform as required. To help ensure efficiency of IT, the auditor evaluates controls that deal with causes and risks of excessive costs, characterized as waste and inefficiency. Some of the problems might include:

- Weaknesses in controls that result in excessive correction of errors; prevention is usually more efficient.
- Controls that consume more resources than the benefits they deliver.

The objective is an optimal balance of control, which means acceptance of some risk. Systems that are inefficient may foster user creation of shadow systems that work around the official system. Such duplicate costs are clearly inefficient. The unreliable system must be fixed before the shadow system is halted. The objective of system development controls is to avoid such issues. Methodologies should result in efficient and appropriate design and development of an application, and ensure that controls, auditability, and security are built into the system.

An information system that is not maintained effectively becomes unreliable. Controls over maintenance, often called change controls, provide continuity while hardware or software changes are made, and ensure that all changes are documented, approved, and confirmed. Maintenance controls include things like adequate user involvement in requesting, testing, and approving program changes; creating appropriate audit trails, including program change history logs; IT and user personnel approval; and sufficient documentation of program changes. Once complete, controlled production transfer procedures reduce the risk of programmers having the ability to introduce unapproved test versions of programs into production.

Functionality

Functionality means the system provides the facilities, responsiveness, and ease of use to meet user needs. Good functionality goes well beyond the minimum transaction processing. It should also provide for recording control information and other issues of concern to management. Preventing problems in functionality includes considering the perspective of untrained, possibly unknown online users. Users can become impatient and may quit without completing a transaction or may resubmit input, causing duplicates. To help ensure functionality, the auditor evaluates controls that monitor and provide feedback. Some of these might include the display of progress indicators following input, positive confirmation of transactions, or monitoring user abandonment of transactions, or “hang-ups.”

Effective information is relevant to the business process, delivered by a functional system Relevance of information is based on system design, which requires user and management participation to reach functionality. Problems often stem from inadequate specifications due to lack of user involvement in development, which usually means the resulting application will be ineffective.

To help ensure effectiveness, the auditor evaluates controls over timely, correct, consistent, and usable information. The format in which information is delivered can have a substantial effect on effective communication. The system should permit flexible display and reports that can be tailored to different audiences.

Protectability

Protectability includes protection of hardware, software, and data from unauthorized access, use, or harm. Robust security is difficult to maintain due to the vast access possible via the Internet, whose structure has inherent weaknesses. Controls are needed to safeguard IT assets against loss, and identify when such loss has occurred. Many current controls focus on reducing risks of catastrophic damage, internal fraud, or embezzlement. To ensure protectability, the auditor evaluates general controls over IT that are often grouped as follows:

- *Data Security and Confidentiality* — Access to data, an important asset, should be limited to those authorized to process or maintain specific data or records. Protecting organizational data is the key responsibility of the information security function and its administrator(s). The security functions may include restricting access to data through various logical access paths, based on user requirements; restricting access to program libraries and data files on a "need-to-know" basis; and providing the ability to hold users accountable for activities performed.

- *Program Security* — Access to program files and libraries should be restricted to authorized personnel through use of access control and other security software. Program updates should be monitored and controlled using library management software. Appropriate segregation of duties should ensure that the programming function does not have unrestricted access to production programs.

- *Physical Security* — Access to processors and storage devices should be limited to those (e.g., management and operations staff) requiring access to perform job functions. Access to the host server computer room should be monitored and controlled (e.g., card access systems). Physical control over reports containing confidential data should be implemented (e.g., distribution procedures). Physical safeguards include fire prevention, preventive maintenance, backup of data files, and property insurance.

Many protectability objectives are designed to ensure that data retains its integrity. In other words, that data is complete, accurate, and up-to-date, and cannot be changed on an unauthorized basis. To help ensure integrity, the auditor evaluates controls over causes of erroneous data, often characterized as application controls, complemented by general controls over access, described above. More detailed integrity control objectives include:

- Authorized transactions are initially and completely recorded.
- All transactions are completely and accurately entered into the system for processing.
- Approved transactions entered are accepted by the system and processed to completion.
- All transactions are processed only once; no duplicate transactions are processed.
- All transactions are processed accurately, updating the correct files and records.

Procedures should minimize the opportunity for application programmers and users to make unauthorized changes to production programs. Access to system software should be controlled to avoid direct compromise of the integrity of program code, data on file, or results of processing.

Confidentiality and privacy are issues of accountability in compliance, and protectability in making it possible. As one industry expert put it at one of The IIA's Critical Infrastructure Conferences: "Without security, there is no privacy." Confidentiality usually refers to intellectual property, trade secrets, competitive plans, or national security. Privacy is usually viewed in the context of personal information, including customers, employees, and stockholders, but not corporate entities. The Internet facilitates a new level of low-cost collection. Organizations need to maintain essential data about individuals to accomplish their missions, but some go far beyond the minimum. Collection of information has become an industry in itself.

Accountability

Accountability identifies individual roles, actions, and responsibilities. It includes the concepts of data ownership, identification, and authentication, all fundamental to being able to identify who or what caused a transaction. The audit or transaction trail should have enough information — and be retained long enough — for transactions to be confirmed, if necessary.

This also includes the concept of non-repudiation. This means that once authenticated, a user cannot disclaim a transaction, as might happen when an online brokerage user seeks to break a trade that turned out to be a bad idea that they nonetheless actually caused.

It also includes issues in granting traceable access to restricted information and software functions. This is a particular problem in IT, where systems analysts and the like resist controls over their own activities. In some cases, monitoring of such use, while seemingly appropriate, can be turned off by the very system administrators it is designed to watch.

Organizations need to authenticate the identity of people entrusted with authority to change data files or software. Similarly, an organization holding private information has an obligation to authenticate the identity of inquirers before disclosing information. In such cases, accountability and privacy may appear to be in conflict. Accountability means identifying the source of a transaction, while privacy might deny meaningful identification. These objectives can be reconciled with care. Accountability protects everyone, for example where a seller has a legitimate need to authenticate the identity of a buyer for credit purposes, while the holder of the credit card has a legitimate need to authenticate the seller to prevent fraudulent misrepresentation.

To support accountability, information must be sufficient, accurate, timely, and available to management to meet its responsibilities. To help ensure reliability of information, the auditor evaluates controls over unacceptable processing and reporting. These might include:

- Information can be supported irrefutably. Controls that provide support are variously known as transaction trails or audit trails.

- Information should be timely. It must be available when decisions are made. This is a common criticism of financial statements issued months after the events.
- Information must be consistent, in accordance with applicable policies. Errors of inappropriate processing, whether programmed or human, are common causes of this effect. Management override can be another.

Achieving Assurance Objectives

Achieving Availability, Capability, Functionality, Protectability, and Accountability requires an adequate infrastructure, resources, and organizational commitment. Areas to make this possible include the building blocks: people, technology, processes, investment, and communication, shown in the ovals in the third band at the center of the model.

This already complex environment has to effectively respond to external forces. Depicted as multidirectional arrows, the impact of ever-increasing interaction, interconnectivity, and system sharing with external market forces (customers, competition, regulators, community, and owners) and speed of change (velocity), compounded by the external interdependencies (providers, alliances, and agents), shows just how many forces are affecting the e-business environment.

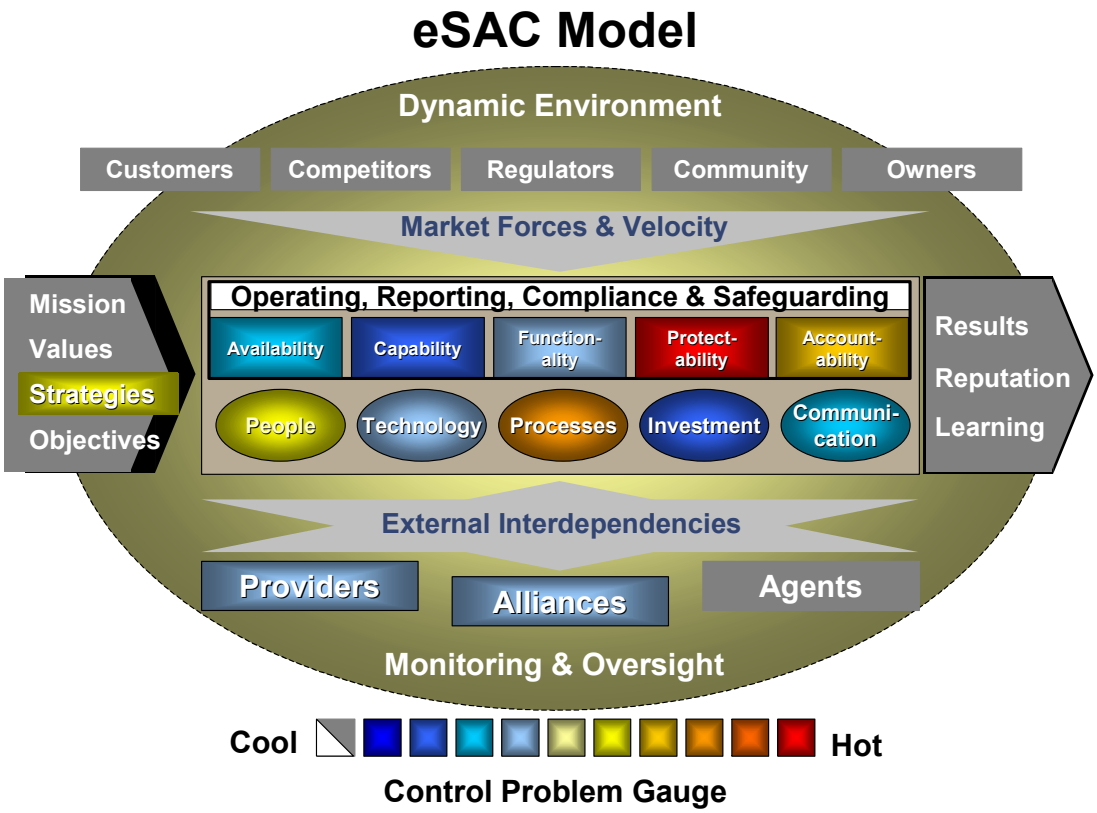
Dynamic Environment

The context to all of this is shown by the gray oval. The dynamic environment is what many call the control environment, although today people prefer to talk about risks and responses rather than controls. To enable the environment to retain stability and control, Monitoring and Oversight are key elements. Monitoring and oversight means that pertinent risks, whether internal or external to the organization, are recognized and addressed on an ongoing basis and controls are confirmed to be functioning as intended. These requirements are shown as the background, and must be effectively designed for all this to work, whatever it is called.

Auditors are moving to other areas of monitoring, such as logging, and are testing to understand where deficiencies and problems may occur. In a world where electronic records are the order of the day, and paper is truly disappearing, auditors can no longer expect to rely on familiar tangibles such as source documents. Today's source can be a Web-based input form, or an electronic transmission from another system. For example:

- What is the business objective? The goal of an e-business may not be clearly articulated, and those depending on it may require after-the-fact definitions and strategies
- What are the risks? Technology platforms are non-homogenous and interlinked, often with outside agents — how can network security in a network of networks be assessed (the Internet and those of business allies)?
- Where are the controls? Traditional views may not work, since there is a need to look to the infrastructure, business processes, and middleware glue that hold it all together (where formerly one reviewed general controls and application controls).

To provide a further example, below is a "heat map" version of the *eSAC* Model, which shows how the framework can report the status of controls. Since the ovals in the third central band are control building blocks, the heat map illustrates how the model might be used to drill down to highlight root cause issues, discussing each according to its priority and potential consequences.



Summary

Availability, Capability, Functionality, Protectability, and Accountability are business assurance objectives. What they mean in this context is:

- Availability
  - Able to receive, accept, process, and support transactions at all times, as required (e.g., 7/24/365)
- Capability
  - There is end-to-end reliable, timely completion and fulfillment of all transactions
- Functionality
  - System provides necessary facilities, responsiveness, and ease-of-use to meet user needs and expectations
- Protectability
  - Logical and physical security controls ensure authorized access, and deny unauthorized access, to servers, applications, and information assets
- Accountability
  - Transaction processing is accurate, complete, and non-refutable (non-repudiation concept)

Appendix A
Relating Control Objectives to the *eSAC* Model

There is a variety of depth and coverage in statements of control objectives. For example, integrity is a top-level control criterion in COBIT, and an inherent requirement in the COSO Study report on reliability of financial reporting. The level of detail varies, with COBIT's four domains, seven information criteria, 34 high-level control objectives, and 318 detailed control objectives, to address specific issues and control concerns.

Based on those widely used sources, components of major pronouncements as they apply to the *eSAC* model are shown in the table below:

Control Objectives and Consequences					
***eSAC* Model**	***COSO***	***SysTrust***	***COBIT Information criteria***	**Objectives -- consensus**	**Consequences**
Availability		Available	Available	Reliable	Business interruption
				Available	Loss of customers
Capability	Reporting	Integrity	Integrity		Erroneous record keeping
	Efficient		Efficient	Effective	Excessive costs / deficient revenues
Functionality	Effective		Effective	Capability	Erroneous management decisions
				Efficient	Fails user & business needs
		Maintainability		Functionality	Fails user & business needs
Protectability	Safeguarding	Security		Compliance	Loss or destruction of assets
			Confidential	Accountability	Fraud
Accountability	Reliable		Reliable	Integrity	Unacceptable accounting
	Compliance		Compliance	Maintainability	Statutory sanctions
				Confidential	Competitive disadvantage
				Security	Deniable / anonymous actions