Operational Assessment of IT

Steve Katzman

Operational Assessment of IT

Internal Audit and IT Audit

Series Editor: Dan Swanson

PUBLISHED

Leading the Internal Audit Function
by Lynn Fountain
ISBN: 978-1-4987-3042-6

Securing an IT Organization through Governance, Risk Management, and Audit
by Kenneth Sigler and James L. Rainey, III
ISBN: 978-1-4987-3731-9

CyberSecurity: A Guide to the National Initiative for Cybersecurity Education (NICE) Framework (2.0)
by Dan Shoemaker, Anne Kohnke, Ken Sigler
ISBN: 978-1-4987-3996-2

Operational Assessment of IT
by Steve Katzman
ISBN: 978-1-4987-3768-5

FORTHCOMING

Practical Techniques for Effective Risk-Based Process Auditing
by Ann Butera
ISBN: 978-1-4987-3849-1

The Complete Guide to CyberSecurity Risks and Controls
by Anne Kohnke, Daniel Shoemaker, and Ken E. Sigler
ISBN: 978-1-4987-4054-8

Software Quality Assurance: Integrating Testing, Security, and Audit
by Abu Sayed Mahfuz
ISBN: 978-1-4987-3553-7

Internal Audit Practice from A to Z
by Patrick Onwura Nzechukwu
ISBN: 978-1-4987-4205-4

Operational Assessment of IT

Steve Katzman

CRC Press
Taylor & Francis Group
Boca Raton   London   New York

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

To my dear wife, Diana,
with love and admiration. Diana, thanks for consenting
to put up with a computer nerd like me for this lifetime.

Contents

Preface

Shortly after I retired from full-time employment, I received an e-mail from Dan Swanson, an interesting consultant and author from Canada, asking me if I would be interested in writing a book about auditing. I was intrigued about the prospect of sharing what I have learned over the years with other people.

Everything I know, I learned from other people who have written books, published articles, and provided online training (web based), as well as in-person seminars and briefings. My only contribution to the process is my assimilation of the data they so kindly shared.

You could consider this book as my way to say thank you and pass it forward.

Throughout my military career and civilian life, I have had the rare opportunity to meet some very interesting and informative people and to work in totally different environments with different computer systems throughout my information technology (IT) and audit career.

In fact, during my military career, I had only one assignment where I worked with a computer system that I had worked with during a prior assignment. In addition, while working as a military pay clerk, I had a special team assignment with a chemical, biological, and radiological response team to detect and identify chemical, biological, and radiation incidents or warfare. I also have an electronic background that started around the age of 12 when Herbie Levine and I built a

superheterodyne radio receiver out of scrap parts in his bedroom and continued through my time at Brooklyn Technical High School in New York City and even while I worked at PACAF headquarters, the Air Force Weapons Lab and through today.

I decided to write this book and present the ideas in such a way as to allow the business person, the IT professional, and the auditor an equal understanding of the concepts shared in this book.

The only downside is probably my inability to write. While stationed at the Strategic Air Command headquarters, Colonel Wilkowske said that I write like I talk and vowed to make me into a reasonable administrative writer. Unfortunately, she was reassigned prior to fulfilling that goal. She did make a great dent, but you will find that I still write as if we were having a conversation.

The focus of this book is to present ideas and concepts of optimization and what an operational assessment looks like. After you understand what an operational assessment is supposed to be, we look at how the IT teams support the business units and the organization's objectives.

Throughout this book, I present issues, concerns, and environments that I have encountered throughout my career to demonstrate the issues and how I or we used the tools that I present in this book.

For a doctor to prescribe a cure, he or she must first diagnose the root cause of the malady or pain.

For you to assess the operational readiness and capability to support the business and the customers, you must gain a thorough understanding of the process.

This book introduces you to or reminds you of tools that should assist you in gaining a 360-degree view of the process.

- Without a process, nothing is accomplished.
- A process is one or more steps that take input, use resources, and create output.

To accomplish an assessment, we first use some tools to answer the following questions: Who? What? Where? When? And how?

Seek first to understand and then to be understood.

Stephen Covey

I also hope that the tools presented in this book make the job easier and more efficient and effective.

My father used to tell me, if a tool saves you an hour or more for a task you do multiple times, it is probably worth buying.

I hope this book provides you with ideas and concepts that you can use in your business as well as in your personal life.

Acknowledgments

About the Author

Steve Katzman is a retired master sergeant who spent four years in accounting and finance with a part-time (three-year) assignment with the chemical, biological, and radiological response team, and the rest of his 21-plus-year Air Force career in information technology (IT) and data communication before moving into civilian life.

After retiring from the U.S. Air Force, Katzman worked for an international manufacturer in Connecticut as a systems programmer, systems and network administrator, second- and third-level IT support, and project manager of networks.

When Katzman moved from Connecticut to North Carolina, he worked as an IT technical resource and contingency planner in banking and senior technology consultant in healthcare before joining KPMG as a senior consultant. After leaving KPMG, he joined the Bank of America as a vice president, internal IT audit, then as an independent consultant and subsequently for TIAA-CREF, a not-for-profit organization established by Andrew Carnegie in 1918 to help educators create retirement plans. He initially started with the IT Audit Team and subsequently was asked to move to the new Professional Practices Team, where he retired from full-time employment in April 2014.

Katzman is a past president and board member of the Charlotte chapter of the Institute of Internal Auditors (IIA). He was a volunteer

instructor for the Charlotte ISACA chapter "Certified Information Systems Auditor" (CISA) candidate review program and has been a learning facilitator for the IIA since 2010.

As a volunteer IIA facilitator, Katzman has provided many virtual and on-site seminars covering tools and techniques for beginning auditors and audit leads, risk-based auditing, operational auditing, and Lean Six Sigma tools for auditors.

Katzman has over 35 years of computer and technology experience and 14 years in auditing (internal and external).

Katzman earned a BS degree in management information systems with a focus on business from Central Connecticut State University. He maintains Certified Internal Auditor, CISA, Certified Information Systems Security Professional (CISSP), Certification in Risk Management Assurance (CRMA), Certified in Risk and Information Systems Control (CRISC), and Information Technology Infrastructure Library (ITIL) foundation certifications. During his military career, he held a top-secret/Special Background Investigation (SBI) security clearance.

PART I
PRELUDE

1
Introduction

Although this book is designed to help auditors, and especially information technology (IT) auditors, accomplish an operational assessment, I tried to write it in such a way to also help the business unit manager as well as the IT gurus in an effort to improve their operations.

The real focus of this book is to help you improve your organization's business processes, which should help the business unit meet the goals of the organization more effectively. The focus is not on any specific technology, computing environment, enterprise risk, or resource program, infrastructure, etc.; it is on the organizational processes. Although the writing may introduce the reader to some Lean and Six Sigma (6σ) tools, techniques, and concepts, it is not meant to prepare the reader for green or black belt certification. If you are interested in Lean Six Sigma certification or implementation, there are other books and a number of training organizations that are quite focused on those areas of interest. This book is focused on helping you determine better and more economical ways to meet your customer's requirements. Your customer may be someone internal or external to your organization. It doesn't really matter who or where your customer is. The goal of any process is to service or supply a customer with what they covet.

A word to the wise: Lean Six Sigma is not a get-rich-quick checklist. Lean 6σ merely provides you with the tools and concepts that help you visualize your processes using different and varied perspectives to help you determine process wastes and bottlenecks along with determining the value and nonvalue steps in the process.

The plan behind this book is to provide you with tools and techniques to help you review a process and help the business unit improve the delivery of a quality product or service to the customer. The assessment process will review the economics as well as the effectiveness and the efficiency of that process. Whether your organization is profit based, not-for-profit, or even governmental, you cannot provide services or products at a continuous loss.

I recognize that the federal government coined the phrase deficit spending and maintains that debt is good for the nation; however, no normal organization can continue to exist spending more than its income.

Another focus area of this book is on adding value. For an operational assessment to be of value, the ultimate goal must be to provide either of the following:

- Assurance that the business unit process is effective and efficient and employs the financial assets and resources appropriately
- Assessment recommendation(s) that helps the business unit make adjustments to improve the operation and use resources more efficiently and/or economically

Even if you think you are adding value, your business unit partner or assessment customer must be the one to recognize that value.

When I was a teenager I thought I was handsome and debonair. Unfortunately I was one of the few people who recognized that fact. In fact, I may have been the only one to recognize those qualities.

The organization's leadership must recognize your value to the organization. If the business unit manager is the only person besides you who recognizes your qualities and value, he or she will miss you when they

rightsize your area, division, or job. To help you visually show your value to the organization, I recommend using some of the graphical tools mentioned in this book to show the business manager and the senior leadership the current process steps and your proposed improvements, if improvements are economically worth it.

Tie any recommended changes to the organizational strategy, vision, and goals.

I have hopefully learned a number of things over my 4 years in accounting and finance, 35 years in IT, and 14 years in audit, plus a number of other part-time positions as a TV repairman, a garageman in New York, a good-humored ice cream vendor, bartender, etc., etc., etc.

Overview

Since most organizations have a mission, vision, and strategy,

- Chapter 2 focuses on the goals of the organization and the strategy that the organization employs to satisfy the needs of their customers. Chapter 2 also provides a perspective to gain insight into the needs, wants, thoughts, and ideas of the business or process customers.
  - In most cases, there is a stream of activity that focuses on providing a quality product or service to the external customer; however, there are normally even more business processes in support of that main artery of activity to satisfy the external customer. This secondary stream is focused on satisfying the internal customers.
  - We need to recognize and agree that every process in the organization must support the organizational goals and strategies either directly or indirectly.
  - If a process does not support the organizational strategies, then the question to answer is, why waste time and resources for that process?
  - Chapter 2 should provide some background into process improvement, measuring success, and productivity.
- Chapter 3 introduces operational auditing from The Institute of Internal Auditors' (IIA) perspective as well as its Barron's

financial dictionary definition. This chapter includes a focus on the following:

- The three Es (economic, effectiveness, and efficiency)
  - Triangle of process-independent and -interdependent entities
  - Value-added benefits balancing the three Es
  - Performance goals as opposed to market or financial goals
- Chapter 4 covers the operational assessment phases of planning.
  - The first phases of any assessment: Fieldwork and reporting will be covered later.
  - Here we introduce some Lean and Six Sigma tools and techniques to gain an understanding of the process and the lay of the land. By this, I mean that you do your reconnaissance of the territory.
    - Develop the project plan.
    - Develop a RACI (responsible, accountable, consulted, informed) matrix to accomplish a workload analysis and gain insight into the process and people—answer the question *who*.
    - Build an *as-is* SIPOC (source, inputs, process, outputs, customers) matrix to answer the questions *what*, *from where*, and *to where*.
    - Develop a value stream mapping to answer the questions *why* and *how long*.
    - Build an (*as-is*) spaghetti diagram to answer the question *where geographically*.
  - If you understand the business process before you show up on site, you will be more efficient and the business customer may accept the fact that you understand their business environment.

Some audit teams have gained a less-than-desired reputation by walking into a business unit, asking the business unit to teach them the business processes, and then weeks later the business unit reads the audit report about what the business unit is doing wrong.

Isn't this a Credibility gap?

- The more you know about the organization, business unit, and business process goals, the more confidence the business unit will have in your ability to help them improve.
- Chapter 4 also has an activity to provide insight into the business process in an effort to employ some of the concepts and ideas provided for the tools covered in this chapter.
  - The planning phase also includes a look into the technologies that will help or influence the business processes within an organization and a view of the latency delays caused by the various technologies.
  - We will also cover some insights into message traffic influenced by distance, speed, message size, appliances, and the Open Systems Integration (OSI) model.
- Chapter 5 moves us from the planning stage to the fieldwork stage.
  - Using the *as–is* information developed in the planning stage to answer the questions about bottlenecks, redundancies, business value that is no longer of value, waste, fraud, efficiency, and economy helps develop ideas for improvement.
  - Learn and employ other tools to recognize the *root cause* and establish the metrics needed to help with the process analysis.
    - Failure mode and effect analysis (FMEA)
    - The five whys
    - Control charts to analyze process capability, accomplish a trend analysis, determine anomalies, and find outliers (possible glitches or fraud)
    - IT metric collection (simple network management protocol [SNMP], etc.)
    - Metric analysis
    - Development of the *to-be* diagrams start during the analysis stage
- Chapter 6 moves the reader into the reporting stage of the assessment.
  - The use of value stream mapping and other tools to show the as-is and to-be environment as an illustration to your

business partner and any reader in support of your pro-
posed recommendations
- The report distribution and my recommendations
- The issue and the impact, which are the key to any
  recommendations
- The five elements of an IIA finding
- A state auditor's report—great report—great effort—great
  issues/findings—no management action—was it worth it?
- Draft and final report

- Chapter 7 reminds you about the IT business process as it
  is expected to run according to an ISACA framework called
  Control Objectives for Information and Related Technology
  (COBIT). Most Certified Information Systems Auditor
  (CISA)–certified auditors use COBIT 5 to assess the IT
  functions.
  - In an effort to deal well with your external and internal
    audit teams, you should gain an awareness of COBIT.
  - COBIT is the framework that IT auditors expect the IT
    division to follow.
  - In this chapter we will look at the management steps that
    the audit teams will invariably check.
  - For the IT business manager, this should help you under-
    stand the auditor as well as performing a self-inspection in
    advance of an audit visit.
  - This chapter should help the IT auditor as well as the IT
    business manager.

Rationale

This book is written based on what I have learned over the length of
my career and life. As I was growing up, my father used to tell us that
"when we became adults, we would wake up each morning and go to
work. If you learned something that day, then it was worth getting
out of bed."

The information that I am sharing is based on various books and
white papers that have influenced my thoughts along with a multi-
tude of training classes provided by many different leaders, facilita-
tors, teachers, and organizations.

Three really great influences pertaining to optimization and Six Sigma are *The 7 Habits of Highly Effective People*, the training presented by Stephen Covey, and the books called *The Goal* (Goldratt & Cox, 1986) and *Rath & Strong's Six Sigma Pocket Guide* (Rath & Strong Management Consultants, 2002).

Stephen Covey and *The 7 Habits of Highly Effective People* focus on communicating and building an understanding between you and the people in your life, whether it be business or personal relationships as well as career building.

Eliyahu Goldratt's book *The Goal* changed the way many manufacturers approached productivity. In the book, Goldratt presented the idea that productivity is not based on cost per unit production; what productivity is and the goal of the organization is to deliver the product or service to the customer and get paid. Goldratt's focus is on throughput as the process value, while resources and inventory are costs. Producing large or even huge lots of a product uses resources and builds inventory. Resources and inventory (raw material, work in process, and finished goods) are costs.

Some years ago a vendor provided me with *Rath & Strong's Six Sigma*. I don't even recall the vendor or whether I received the book at a technology show or from whom, but I use it quite frequently as a reference to gain ideas of tools and possible uses.

Throughout this book, I will be sharing information that I gleaned from people through demonstrations, newspapers, periodicals, books, webinars, conferences, etc.

In fact, *I firmly believe that everything I know, I have learned from other people.*

My only contribution to this book is how I assimilated the facts provided by others and put what I have learned over the years in this book.

I believe that it was Socrates who said something to the effect of "I cannot teach anybody anything; I can only help you think."

This book is intended to provide you with information to help you improve your operations or at least help you think about your processes and how you can help to ensure that they are effective, efficient, and economically sound.

When I was stationed at the Strategic Air Command headquarters in Offutt Air Force Base, Nebraska, Colonel Kathleen Wilkowske

said that I write like I speak and vowed to make me into a reasonable administrative writer. As you review this book, you will realize that the good colonel was reassigned before she completed that quest.

Considering that I was born in Brooklyn, New York, where English was considered a foreign language, I sincerely hope that you will gain what I am trying to share.

As you read through the information presented in this book, you may find that I repeat various statements throughout the book. I don't believe that this is a sign of Alzheimer's, but I did want to express to you that I believe these points are important enough to repeat.

PART II
GOALS

2
The Organization

Before we can consider committing resources and impeding any business productivity to accomplish any assessment, we must understand the organization. Without this understanding, you will not be recognized as adding value to the organization. You will be considered a cost center, similar to the overhead expense of the building, equipment, etc.

If any business process is to be considered a value-added activity, the business process must be viewed as a partner and contributor to the productivity of the organization either directly or indirectly. Since the IT unit was formed to help make the business processes more efficient, we should look at some business processes and then determine how the technologies can help the business and organization be successful.

Based on the strategy and goals set down in the organization's strategic plan, each business unit and process should support the strategy either directly or indirectly. If you try to assess any process or business unit that does not help the organization meet its goals and strategic plan, then you are not providing real value.

Organizational Goals

Organizational goals are based on the mission and the strategy of the organization.

- *Profit-oriented organizations* are primarily focused on making money. No matter how many statements about helping humanity by providing a product or service are included in the mission statement, the organization is designed to provide a product or service to a customer in an effort to gain a profit over costs.

- *Not-for-profit organizations* are focused on providing a product or service that someone is willing to pay for.
  - Not-for-profit organizations cannot survive without income.
  - To obtain income, they must provide the service or product that meets or exceeds the contributor's expectations.
  - The contributor may be the recipient of the product or service or some benevolent person or group of people who will sponsor the delivery of that product or service.
- *Government organizations* are similar to not-for-profit organizations; however, the reputational risks to the political party in power sometimes overcome the effective use of resources, including monetary resources. (Deficit spending and the constantly growing national debt may be an example of the unbalanced checkbook.)

As a data center manager in the military, I requested a staff of 10 computer operators for our data center in an effort to maintain 2 members on duty at all times in accordance with the Occupational Safety and Health Administration (OSHA) guidance.

When Congress provided 75% of the U.S. Air Force budget request, my supervisor informed me that according to Congress, I could provide the OSHA required staffing for a 7-day-by-24-hour operation with 7.5 people.

Measuring the Success of an Organization

For a profit-oriented organization, the measures of success that they probably consider are the following:

- *Increasing net profit*—The revenue received from the customer less the organizational costs to providing the product or service
- *Increasing cash flow*—Having the cash flow to cover the costs for resources and inventory and/or providing for expanding the market and product research without borrowing against future sales

- *Increasing return on investment (ROI)*—Increasing the percentage of dollars returned to the organization for dollars spent on resources, buildings, equipment, people, etc.

For a not-for-profit organization, to measure their success they may look at the following:

- *Increasing donations*—Increasing donations so that the organization can service or provide for a larger number of users
- *Increasing cash flow*—Having the cash to pay for resources and inventory without going into debt to provide for the participants
- *Increasing ROI*—Increasing the number of people serviced for the donated dollars

For an organization, the above goals and measures may fit the need to measure the success of the organization; however, most processes and business units within the organization cannot be directly measured against the three organizational measures of success. Of course, each business unit, each process, and each step in the process very likely adds to the cost and influences the success of doing business; however, it may or may not have a direct quantifiable influence or impact on the revenue stream, cash flow, or ROI.

Most organizations are governed based on the strategy and goals of that organization. Those strategies have a direct influence on the way the external customer or recipient of the product or service is treated and how the organization will respond to their needs.

As you can see by the triangle in Figure 2.1, an organization can be depicted by three tiers:

- Tier 1—The pinnacle of the triangle is the strategy and goals of the organization. This tier is also considered the organizational governance tier.
- Tier 2—The area under the strategy and goals in the triangle is the external customer value stream. These business processes must support the organization's strategies and provide for the sales, production, and delivery of the goods or services to the external customer.

  The reason for depicting this structure as a triangle is to denote the importance of the customer-focused business processes as a foundation to successfully achieve the goals of the