The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management

Author
Richard A. Caralli

Principle Contributors
James F. Stevens
Bradford J. Willke
William R. Wilson

July 2004

TECHNICAL REPORT
CMU/SEI-2004-TR-010
ESC-TR-2004-010

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management

CMU/SEI-2004-TR-010
ESC-TR-2004-010

Author
Richard A. Caralli

Principle Contributors
James F. Stevens
Bradford J. Willke
William R. Wilson

July 2004

Networked Systems Survivability Program
Survivable Enterprise Management Team

Unlimited distribution subject to the copyright.

This report was prepared for the

SEI Joint Program Office
HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

Copyright 2004 Carnegie Mellon University.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use. Requests for permission to reproduce this document or prepare derivative works of this document for external and commercial use should be addressed to the SEI Licensing Agent.

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.
The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

To the Reader ..... **vii**

Acknowledgements ..... **ix**

Abstract ..... **xi**

1 Introduction **1**
1.1 Critical Success Factors 2
1.2 Enterprise Security Management 2

2 Background **5**
2.1 Lessons from OCTAVE 5
2.2 Challenges for Security Management 6
2.3 Addressing Challenges with CSFs 7

3 History of the CSF Method **9**
3.1 Beginnings 9
3.2 Evolution of the CSF Method 10

4 A CSF Primer **11**
4.1 CSFs Defined 11
4.2 Goals Versus CSFs 12
4.2.1 Relationship Between Goals and CSFs 13
4.2.2 Cardinality Between Goals and CSFs 15
4.2.3 The Superiority of CSFs Over Goals 15
4.3 Sources of CSFs 16
4.3.1 Industry CSFs 17
4.3.2 Competitive-Position or Peer CSFs 18
4.3.3 Environmental CSFs 18
4.3.4 Temporal CSFs 19
4.3.5 Management-Position CSFs 21
4.4 Dimensions of CSFs 22
4.4.1 Internal Versus External 22
4.4.2 Monitoring Versus Adapting 23

4.4.3 Importance of CSF Sources and Dimensions 23
4.5 Hierarchy of CSFs 23
4.5.1 Enterprise CSFs 24
4.5.2 Operational Unit CSFs 25
4.5.3 Relationship Between Hierarchy and Source 26
4.5.4 Other Considerations 28

5 Applying CSFs 29
5.1 Historical Application of CSFs 29
5.2 General Advantages of a CSF-Based Approach 30
5.3 Using CSFs in a Security Context 30
5.3.1 Enterprise Security Management 32
5.3.2 Information Security Risk Assessment and Management 34

Appendix A CSF Method Description 45

Appendix B Case Study 1: Federal Government Agency 91

Appendix C Case Study 2: Large County Government 103

Appendix D Glossary 113

References 117

List of Figures

Figure 1: Strategic Planning in Organizations 1

Figure 2: Alignment of Strategic Plan and Security Strategy 3

Figure 3: Goals vs. CSFs 13

Figure 4: Relationship Between Goals and CSFs 15

Figure 5: Example of Industry CSFs for an Airline 17

Figure 6: Example of Peer CSFs for an Airline 18

Figure 7: Example of Environmental CSFs for an Airline 19

Figure 8: Example of Temporal CSFs for an Airline 21

Figure 9: Example of Management-Position CSFs for an Airline Manager 22

Figure 10: Example of Hierarchy of CSFs in an Organization 24

Figure 11: Relationship Between Enterprise and Operational Unit CSFs 28

Figure 12: Affinity Analysis for Determining ISRM Scope 36

Figure 13: Affinity Analysis for Determining Critical Assets 38

Figure 14: Affinity Analysis for Determining/Validating Security Requirements 39

Figure 15: Affinity Analysis for Validating Evaluation Criteria 42

Figure 16: Affinity Analysis for Determining Which Risks to Mitigate 43

Figure 17: Sample Mission Statement 67

Figure 18: Example of Deriving Activity Statements from Mission 68

Figure 19: Example of CSF Interview Notes 71

Figure 20: Example of Activity Statements Drawn from CSF Interview Notes 71

Figure 21: Affinity Grouping Example – Activity Statements.....72

Figure 22: Affinity Grouping Example – Three Affinity Groups 73

Figure 23: Affinity Grouping Example – Refined Groups.....73

Figure 24: Example of CSF Affinity Grouping of Activity Statements.....76

Figure 25: Example of Three Emerging Supporting Themes 77

Figure 26: Illustration of Affinity Grouping of Supporting Themes 80

Figure 27: Illustration of Deriving CSFs from Supporting Themes 82

Figure 28: Example of Affinity Analysis.....86

List of Tables

Table 1: Matrix of CSF Levels to CSF Types 27

Table 2: CSF Interview Questions Proposed by Rockhart 59

Table 3: Additional Interview Questions to Consider 61

Table 4: Example of Activity Statements and Supporting Themes 66

Table 5: Qualities of “Good” and “Poor” CSFs 83

Table 6: Agency CSFs 93

Table 7: Vulnerabilities to Agency CSFs 98

Table 8: County CSFs 106

Table 9: Affinity Analysis – CSFs to Critical Assets 111

Table 10: Affinity Analysis – CSFs to Enterprise Security Strategies 112

To the Reader

This technical report is based on the work of John Rockhart and his colleagues at the Center for Information Systems Research (CISR) at the Massachusetts Institute of Technology in the area of critical success factors and information systems planning.[1] In our research at the Software Engineering Institute (SEI) in the areas of enterprise security management and enterprise resiliency, we found broad applicability of Rockhart's concepts as an important tool in developing and deploying an effective approach to security management. The use of Rockhart's concepts for this purpose forms the basis of this technical report.

In this report, we introduce readers to the critical success factors (CSFs) concept and a corresponding method for developing a working set of CSFs that we developed at the SEI. More importantly, we discuss our use of CSFs as a means for framing and focusing the security strategy, goals, and activities of an organization. For background, the history and early uses of the critical success factor method in the field of information systems planning are presented. With regard to enterprise security management and enterprise resiliency, we discuss our recent application of the CSF method in fieldwork with customers using the Operationally Critical Threat, Asset, and Vulnerability Evaluation[SM] (OCTAVE®) risk assessment methodology. The high-level steps we defined and applied to develop CSFs for these customers are codified in this report for further application and research. Finally, we discuss other ways in which the CSF method can be a powerful guiding and directing activity for the definition and improvement of enterprise security management processes and practices in organizations.

Depending on your level of familiarity with the concept of critical success factors, there are several ways to make effective use of the material presented in this report. To facilitate your use of this material, we suggest the following:

- If you have no familiarity with the concept of critical success factors or the work of John Rockhart, you should read each of the sections of this report in numerical sequence.
- If you are already familiar with the concept of critical success factors and are interested in our application of CSFs in the areas of enterprise security management and enterprise resiliency, you should begin reading this report at Chapter 5, "Applying CSFs," and con-

[1] Rockhart's concepts are documented in "A Primer on Critical Success Factors," published by the Center for Information Systems Research in June 1981 [Rockhart 81]. Our use of this material as the basis of our research has been granted by permission of the author.

[SM] Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.

[®] OCTAVE is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

tinue with Appendices B and C, which describe our field experience using CSFs in customer engagements.

- Finally, if you have familiarity with CSFs and are interested in obtaining a systematic method for developing a set of CSFs, refer directly to Appendix A, "CSF Method Description."

However you decide to read this technical report, it is our hope that you will see the potential benefits of deriving and applying critical success factors in your organization and will realize improvement in developing and deploying your organizational security strategy through this simple, yet powerful concept.

Acknowledgements

The authors would like to thank members of the Survivable Enterprise Management team of the Networked Systems Survivability Program who helped in the production of this report by applying the CSF method in fieldwork with customers and graciously sharing their experiences with us.

The authors would also like to thank Julia Allen of the Practices, Development, and Training team for her review of this material and her considerable feedback. We appreciate her support and willingness to explore these emerging ideas with us.

We are also grateful to David Biber for his extensive work in creating the graphics that so appropriately illustrate our thoughts and concepts and to Pamela Curtis for her careful editing of this report.

We would also like to thank our sponsors for their support of this work. It has already had great impact on our customers' ability to improve their security programs and in our ability to transition new technologies in the area of enterprise security management and enterprise resiliency.

Last, but certainly not least, we would like to thank John Rockhart, whose work in the area of critical success factors is still viable today. His work improved information systems planning for many organizations, and we hope that our application of CSFs will have the same impact in the field of information security and enterprise security management.

Abstract

Every organization has a mission that describes why it exists (its purpose) and where it intends to go (its direction). The mission reflects the organization's unique values and vision. Achieving the mission takes the participation and skill of the entire organization. The goals and objectives of every staff member must be aimed toward the mission. However, achieving goals and objectives is not enough. The organization must perform well in key areas on a consistent basis to achieve the mission. These key areas—unique to the organization and the industry in which it competes—can be defined as the organization's critical success factors.

The critical success factor method is a means for identifying these important elements of success. It was originally developed to align information technology planning with the strategic direction of an organization. However, in research and fieldwork undertaken by members of the Survivable Enterprise Management (SEM) team at the Software Engineering Institute, it has shown promise in helping organizations guide, direct, and prioritize their activities for developing security strategies and managing security across their enterprises. This report describes the critical success factor method and presents the SEM team's theories and experience in applying it to enterprise security management.

1 Introduction

An organization[2] primarily exists to serve its stakeholders—the customers, employees, business partners, shareholders, and communities that benefit from the organization's existence and growth. The organization's mission embodies this focus by stating the organization's purpose, vision, and values. Stakeholders are best served when an organization operates in a manner that ensures the mission is accomplished.

Accomplishing the mission in a logical and systematic way requires the organization to develop a strategy. The strategy encompasses a set of goals or targets that the organization must achieve in a specific period of time. These goals are transformed into lower level tactical plans and activities to be carried out at various levels throughout the organization. This process of strategic planning provides a means for ensuring that the entire organization is focused on a shared purpose and vision.

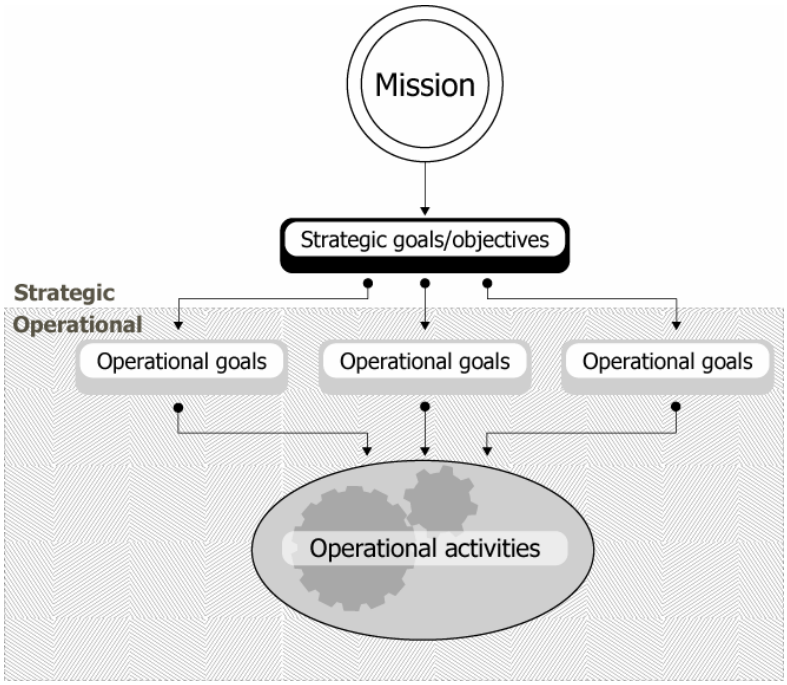


Figure 1: Strategic Planning in Organizations

[2] It is our intention to apply the term "organization" in this report universally to "for-profit" and "non-profit" organizations. While the bottom-line objectives may be different, we find no useful distinction between these types of organizations—both are in operation to accomplish a specific mission.

However, setting goals and developing plans to achieve them is only one factor in accomplishing the organization's mission. The organization must also perform well in a few key areas that are unique to its mission and to the industry in which it operates. In fact, failure to perform well in these areas may be a major barrier to achieving goals. These key areas can be described as a set of critical success factors—the limited number of areas in which satisfactory results will ensure competitive performance for the organization and enable it to achieve its mission [Rockhart 79].

1.1 Critical Success Factors

Critical success factors (CSFs) define key areas of performance that are essential for the organization to accomplish its mission. Managers implicitly know and consider these key areas when they set goals and as they direct operational activities and tasks that are important to achieving goals. However, when these key areas of performance are made explicit, they provide a common point of reference for the entire organization. Thus, any activity or initiative that the organization undertakes must ensure consistently high performance in these key areas; otherwise, the organization may not be able to achieve its goals and consequently may fail to accomplish its mission.

1.2 Enterprise Security Management

Managing security[3] across an enterprise is one of the many business problems that organizations must solve in order to accomplish their missions. Regardless of what organizational assets are to be secured—information or technical assets, physical plant, or personnel—the organization must have a security strategy that can be implemented, measured, and revised as the business climate and operational environment change. In the long run, the effectiveness of the security strategy depends on how well it is aligned with and supports the organization's business drivers:[4] mission, business strategy, and CSFs.

[3] Managing security broadly refers to the process of developing, implementing, and monitoring an organization's security strategy, goals, and activities.

[4] Throughout this document we use the term "business drivers" to collectively represent the organization's mission, values, and purpose; its goals and objectives; and its critical success factors.

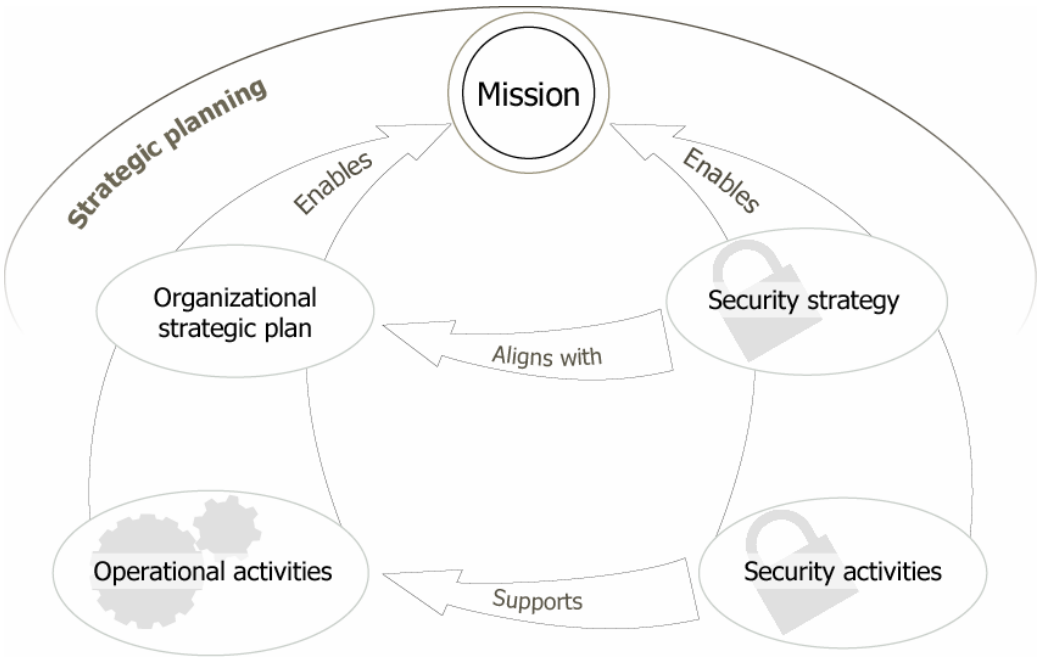


Figure 2: Alignment of Strategic Plan and Security Strategy

2 Background

The work of the Survivable Enterprise Management (SEM) team of the Networked Systems Survivability (NSS) program at the Carnegie Mellon® Software Engineering Institute (SEI) is focused on helping organizations improve their capabilities for managing security across their enterprises. A primary objective of this work is to establish strategic planning and risk management as essential components of a security management program.

In this section, we document some of the lessons learned from our development and fieldwork efforts. In addition, we introduce the use of CSFs as an important element of an organization's strategic plan for security.

2.1 Lessons from OCTAVE

One of the primary functions of executive-level management[5] is to manage risk across the organization. An organization's security strategy and goals must be framed in the context of risk to get the attention of executive-level management. Only those risks to critical assets that threaten the accomplishment of the mission are worth executive-level management's attention, and then only if the organization would be significantly impacted if the risks are realized.

A risk-based approach to security strategy and management enables organizations to direct their limited resources to the operational areas and critical assets that most need to be protected. Risks to operational areas and assets that can directly affect the organization's ability to accomplish its mission must be identified, analyzed, and mitigated. This perspective of "focusing on the critical few" is a foundation of the OCTAVE information security risk assessment methodology [Alberts 01].

In OCTAVE, this principle is put into practice by creating an assessment team that is composed of personnel from the organization who understand the organization's unique business drivers and conditions. Implicitly, these personnel are likely to consider the organization's

® Carnegie Mellon is registered with the U.S. Patent and Trademark Office.

5 In this report, term executive-level management is intended to refer to those personnel in C-level (e.g., CEO) positions, as well as their first-level senior managers (vice-presidents, executive directors, etc.). These personnel are involved in the organization's strategic planning process and are responsible for setting the direction and course for the organization.

mission when they decide which operational areas and assets to include in the risk assessment activity.

Identifying and focusing on the most important operational areas and assets is perhaps the most important activity that an organization performs when deploying a risk-based approach to security. However, as we have learned in our fieldwork with the OCTAVE method, this can be a difficult task in a large, complex organization particularly because there may be numerous operational areas from which to choose, each with its own set of important assets. An analysis team must apply their judgment in selecting the right areas and assets, and must ensure that their selection aligns with the business drivers of the organization. Failure to select (and validate) the right operational areas and assets can significantly diminish the value of a risk-based approach to security.

2.2 Challenges for Security Management

In the past three years, our research, fieldwork, and classroom interaction has provided much data regarding the challenges and barriers that organizations face in making the transition from vulnerability-based[6] to risk-based approaches to security management. Overall, we have observed that many organizations understand clearly that success depends on gaining the sponsorship of executive-level management and aligning security goals with the mission, goals, and objectives of the organization. In this way, security goals become an enabler of the organization's mission or strategy, rather than a burden or expense. However, our experience suggests that many organizations are ill-equipped to define their security goals, let alone to make an explicit connection between their security goals and the strategic drivers[7] of the organization.

This is not unlike a similar challenge that has been faced by information technology (IT) departments in organizations. The acceptance of the position of chief information officer (CIO) as a legitimate executive-level partner to the chief executive officer (CEO) and chief financial officer (CFO) has been a more recent accomplishment in many organizations. Legitimizing this position causes the IT department to become a strategic partner of the organization, helping it achieve its mission more efficiently and effectively. Many well-known organizations have indeed proven their ability to be competitive, to grow, and to accomplish their missions through innovative and strategic uses of technology.

---

[6] We describe a "vulnerability-based" approach to security as one in which the primary focus is to react to vulnerabilities (such as viruses or intrusions) as they are identified, rather than to take a proactive, strategy-driven approach to security. Vulnerability management is an important part of managing security but rarely is sufficient alone for securing a large organization or enterprise.

[7] In this report, the term "strategic drivers" is used to refer to the important components of an organization's strategic plan: mission, objectives, goals, and critical success factors. These drivers may sometimes be referred to as "business drivers" or "organizational drivers."

In the same way, an organization's security strategy must align with and enable its organizational strategy. But, with the increasing dependence of the organization's mission on information technology, security strategy must also ensure that the organization is resilient against attacks, particularly on technology, that could disable the mission.

Our conclusion is that a strong partnership is lacking between executive-level management and the parts of the organization responsible for setting and implementing security strategy. To assist our customers with this challenge, we began to search for ways that could aid in making this connection more explicit.

2.3 Addressing Challenges with CSFs

One of the ways in which IT departments have addressed these challenges (as early as the 1970s) is by involving the organization at large in their strategic planning process. This process—known by many names, such as business systems planning—explicitly takes into consideration the organization's key business processes and data to determine the technology needs of the organization. To further determine priority, these efforts also frequently include a direction-setting activity such as the development of CSFs. If the organization's accomplishment of the mission is tightly linked to its performance in a few key areas and the technology plan is based on enabling high performance in these same areas, the plan can enable the mission.

We drew upon the broad experience of the SEM team to address similar challenges for security management. At least one SEM team member had previously used CSFs in the development of an information technology plan. Other team members were also familiar with CSFs, and thus we began to explore the CSF method as a possible way to help our customers improve the focus of their security efforts. We began our investigation of the method specifically in response to the increasing number of questions and concerns of customers in their attempt to develop a scope for their risk assessment activities—selecting the right operational areas and critical assets to focus on. In our fieldwork, we also observed the value of the method for security management and strategy and goal development.

3 History of the CSF Method

The concept of identifying and applying CSFs to business problems is not a revolutionary new field of work. It dates back to the original concept of "success factors" put forth in management literature by D. Ronald Daniel in the 1960s.[8] However, the CSF concepts and approach are still very powerful today and are applicable to many of the challenges being presented in the information technology and security fields.

3.1 Beginnings

In the late 1970s and early 1980s, organizations found themselves in the midst of an information revolution. The growth of information systems in organizations resulted in the production of significant amounts of information for analysis and decision making. The advent of the personal computer and the evolution of the field of information "systems" to information "technology" were indicators that the information explosion would continue.

John F. Rockhart, of MIT's Sloan School of Management, recognized the challenge that the onslaught of information presented to senior executives. In spite of the availability of more information, research showed that senior executives still lacked the information essential to make the kinds of decisions necessary to manage the enterprise [Dobbins 98]. As a result, Rockhart's team concentrated on developing an approach to help executives clearly identify and define their information needs.

Rockhart's team expanded on the work of Daniel to develop the CSF approach. Daniel suggested that, to be effective in avoiding information overload, an organization's information systems must focus on factors that determine organizational success [Rockhart 79]. For example, in the automotive industry, Rockhart suggested that styling, an efficient dealer organization, and tight control of manufacturing costs are important success factors [Rockhart 79]. Using success factors as a filter, management could then identify the information that was most important to making critical enterprise decisions. Accordingly, the underlying premise is that decisions made in this manner should be more effective because they are based on data that is specifically linked to the organization's success factors.

[8] Daniel's concepts are described in "Management Information Crisis," *Harvard Business Review*, September-October 1961.

In 1981, Rockhart codified an approach that embodied the principles of success factors as a way to systematically identify the information needs of executives. This work, presented in "A Primer on Critical Success Factors," detailed the steps necessary to collect and analyze data for the creation of a set of organizational CSFs [Rockhart 81]. This document is widely considered to be the earliest description of the CSF approach. Our interpretation and application of Rockhart's approach, as documented in this report, is largely based on this description.

3.2 Evolution of the CSF Method

Most of the work in success factors performed by Rockhart and Daniel was focused on refining the information needs of executives. However, as a logical outgrowth of this work, Rockhart hinted at the usefulness of the method as a component of strategic planning for information systems or technology [Rockhart 81]. The CSF method has found its way into many formalized information or business systems and technology planning methodologies that are still being used today.

The CSF method and the analysis of CSFs have been used in many ways outside of the information technology planning arena. In their research on the use of CSFs in federal government program management, James Dobbins and Richard Donnelly [Dobbins 98] identify uses of CSFs to

- identify the key concerns of senior management
- assist in the development of strategic plans
- identify key focus areas in each stage of a project life cycle and the major causes of project failure
- evaluate the reliability of an information system
- identify business threats and opportunities
- measure the productivity of people

While this is not an exhaustive list of the ways in which Rockhart's original work has been applied, it suggests the broad applicability of the method. It speaks to the use of CSFs as a way for organizations to focus and validate many of the important activities they perform to accomplish their missions.

4 A CSF Primer[9]

CSFs are an explicit representation of the key performance areas of an organization. In this context, CSFs define those sustaining activities that an organization must perform well over time to accomplish its mission. They are found at every level of management, from executive to line management. Each organization also has a set of CSFs that it inherits from the particular industry in which it operates.

To apply the CSF method and to use CSFs as an analysis tool, it is important to understand how they relate to the organization's strategic drivers and competitive environment. This section provides a foundation for understanding CSFs and defines these important relationships.

4.1 CSFs Defined

The term "critical success factor" has been adapted for many different uses. Familiarity with the term is often presented in the context of a project or an initiative (i.e., the CSFs for the implementation of an ERP system or the deployment of a diversity program). In this context, CSFs describe the underlying or guiding principles of an effort that must be regarded to ensure that it is successful.

A slight distinction must be made when considering CSFs as a strategic driver at the organizational or enterprise level (as is done in this report). In this context, CSFs are more than just guiding principles; instead, they are considered to be an important component of a strategic plan that must be achieved *in addition to* the organization's goals and objectives. While this distinction is subtle, it is intended to point out that an organization's CSFs are not just to be "kept in mind"; their successful execution must drive the organization toward accomplishing its mission.

Many definitions of a CSF at the strategic planning level have already been provided in this report. In his seminal work on CSFs, Rockhart provides a useful summary of similar but distinct definitions [Rockhart 81]:

- key areas of activity in which favorable results are absolutely necessary to reach goals

[9] This section relies heavily on the description of CSFs as documented in the original primer by John Rockhart and Christine Bullen [Rockhart 81]. Their work is still widely recognized as the initial definition of CSFs and the CSF approach.

- key areas where things must go right for the business to flourish
- "factors" that are "critical" to the "success" of the organization
- key areas of activities that should receive constant and careful attention from management
- a relatively small number of truly important matters on which a manager should focus attention

The fact that CSFs can be defined in so many different ways speaks to their elusive nature. Managers generally recognize their CSFs (and the organization's) when they see or hear them, but may be unable to clearly and concisely articulate them or appreciate their importance. In fact, most managers are aware of the variables they must manage to be successful, yet only when problems arise and root causes are identified are these variables made explicit. For example, suppose an organization finds an alarming number of duplicate payments to vendors. They might conclude that this problem is related to poor staff training or high levels of staff turnover. As a result, the effective management of human resources (attracting, training, retaining) might be identified as an important factor that can impede the achievement of their strategic goals. In the process, they have explicitly defined a CSF for the organization.

CSFs are powerful because they make explicit those things that a manager intuitively, repeatedly, and even perhaps accidentally knows and does (or should do) to stay competitive. However, when made explicit, a CSF can tap the intuition of a good manager and make it available to guide and direct the organization toward accomplishing its mission.

4.2 Goals Versus CSFs

In traditional strategic planning and management, the definition of a goal or an objective is fairly well known; however, defining a CSF is much less clear [Rockhart 81]. Thus, CSFs are often confused with organizational goals. For the purpose of this report, we define organizational goals as targets that are established to achieve the organization's mission. They are very specific[10] as to what must be achieved, when it is to be achieved, and by whom. Effective goals have a quantitative element that is measurable to determine if the goal has been achieved. Goals can be decomposed into operational activities to be performed throughout the organization.

[10] Goals should be S.M.A.R.T.—specific, measurable, achievable, realistic, and tangible—to be effective. Goals that do not have this level of specificity can easily become confused with critical success factors. More information about the S.M.A.R.T approach to goal setting can be found in *Attitude is Everything!* by Paul J. Meyer [Meyer 04] or online at www.topachievement.com /smart.html.

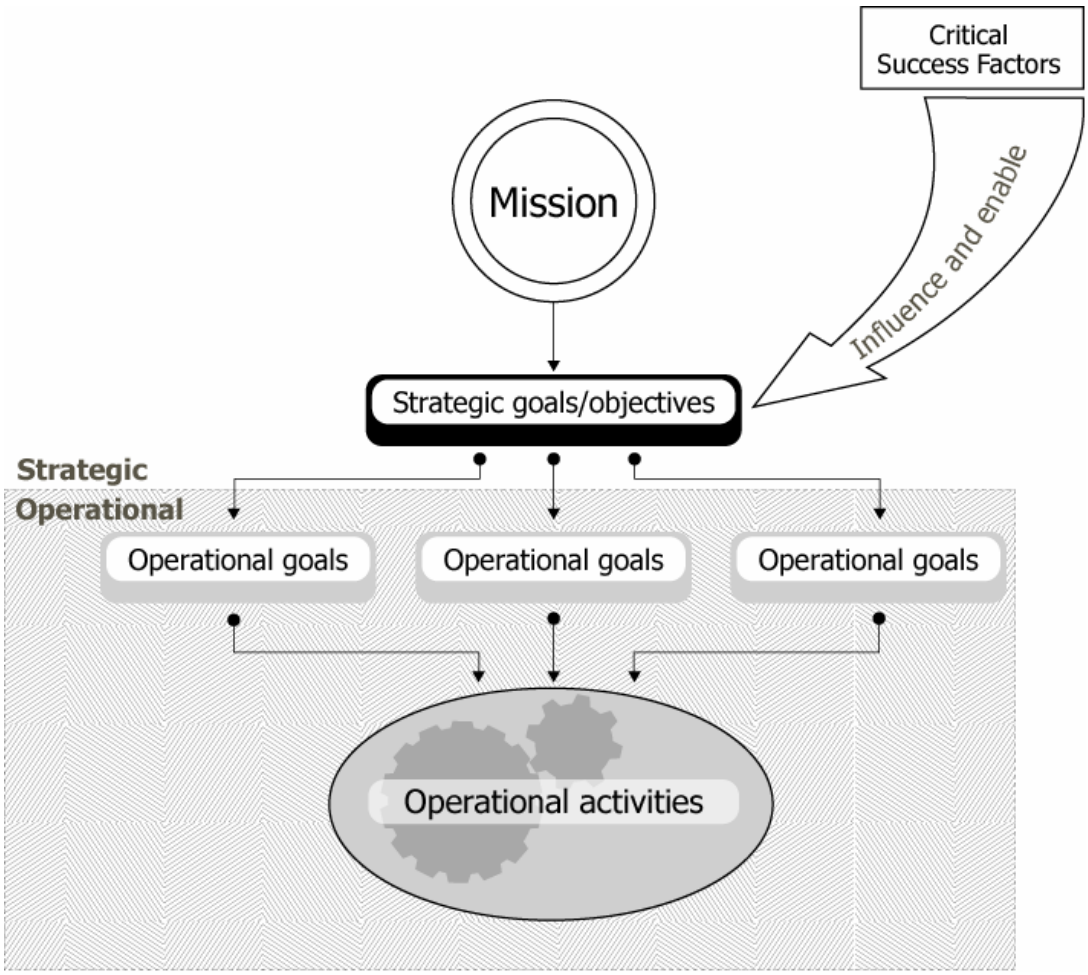


Figure 3: Goals vs. CSFs

Goals and CSFs go hand-in-hand. Both are needed to accomplish the organization's mission, and neither can be ignored without affecting the other. Because they are both integral parts of an organization's strategic plan, their relationship must be considered. For example, a person might have a goal of losing 10 pounds by the end of the year. To achieve this goal, the person would have to be mindful of a few key factors—improving his or her diet and nutrition, exercising regularly, and avoiding tempting social gatherings. Careful attention to these key factors will enable the person to achieve the goal of losing 10 pounds; conversely, inattention to these factors will inhibit achievement of the goal.

4.2.1 Relationship Between Goals and CSFs

The strong relationship between goals and CSFs results from the fact that managers are the origin of both goals and CSFs. When managers set goals, they also implicitly consider what they need to do to be successful at achieving the goals. Thus, it is likely that managers consciously consider their CSFs during goal setting and consequently create the bond between

goals and CSFs that is needed to contribute to accomplishing the organization's mission. In this way, the influence of CSFs on goal achievement is made explicit, even if the actual CSFs are not. Organizations that have been successful at achieving their goals have also likely achieved their CSFs, albeit in a less observable way. Thus, goals sometimes resemble CSFs because they embody the importance of a key performance area.

Usually a goal is immediately discernible from a CSF because of its specificity. A CSF for the organization may be more general and is likely to be related to more than one goal. Consider the following goals for a large manufacturing company:

- Increase sales in our Northeast division by 10% by 2nd quarter, 2004.
- Decrease travel expenses by 5% in the next 30 days.
- Expand product line to include widgets and gadgets.
- Increase expansion by opening at least two retail stores in at least two European markets by 3rd quarter 2006.

The first goal might be commonly found in many commercial organizations: to achieve a 10% increase in sales in a divisional unit. To achieve this goal, the manufacturing company is stating an implicit dependence on the organization's ability to perform well in a few key areas. While the goal is simple, it reflects many key underlying assumptions or conditions. Implicitly, this goal states that

- The growth of the company is dependent on the organization's capability for increasing sales.
- Sales staff must be empowered and enabled to meet the challenge of attaining an increase of 10%.
- The company must act quickly because it needs to retain and grow its market share in the Northeast as other competitors ramp up.
- The Northeast division is an important area in which sales expansion brings the company a competitive advantage.

These assumptions or conditions embody CSFs that are directly related to the potential success in achieving the goal. For example, consider the following dependencies between the goal, underlying assumptions and conditions, and CSFs:

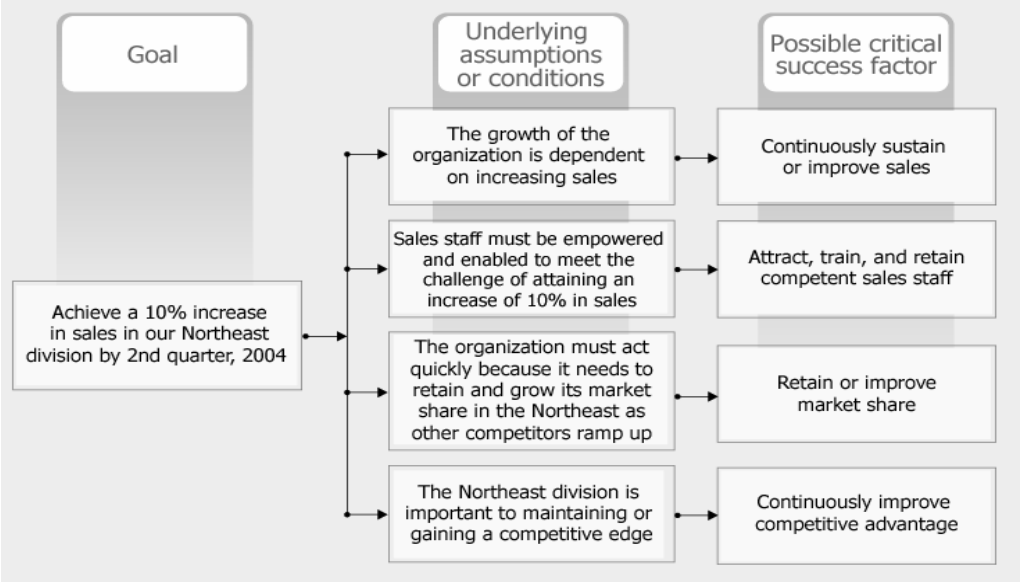


Figure 4: Relationship Between Goals and CSFs

The importance of the CSFs in helping the manufacturing company achieve its goals cannot be overstated. In this example, at least one of the CSFs—attract, train, and retain competent sales staff—is vitally important if the company wants to achieve the goal of attaining a 10% increase in sales. If the company fails to consistently retain qualified sales staff, the goal cannot be achieved, and in the long run, the manufacturing company's mission may be in jeopardy.

4.2.2 Cardinality[11] Between Goals and CSFs

As illustrated above, an organizational goal may be related to more than one CSF to be achieved. Conversely, a CSF may influence or affect the achievement of several different goals. The potential many-to-many relationship between goals and CSFs is indicative of their interdependent nature and the importance of CSFs in helping the organization accomplish its mission.

4.2.3 The Superiority of CSFs Over Goals

Goals alone can be an unreliable predictor of an organization's ability to successfully accomplish its mission. This is because goal-setting in many organizations is at best a subjective exercise and often is strongly influenced by or derived from a performance management system rather than a strategic planning exercise. Often, goals are set with an eye to their

[11] Cardinality refers to the extent of the relationship between two entities. A useful definition in the context of CSFs is "a business rule specifying how many times an entity can be related to another entity in a given relationship." (This definition can be found at www.vertaasis.com.)

achievability rather than how they contribute to accomplishing the mission. For example, an organization may realize that it is failing to accomplish its mission even though it has successfully achieved its goals. This can occur because the goals have not been aligned with the organization's strategic plan; thus their achievement does not propel the organization forward.

On the other hand, CSFs are less likely to be biased toward achievement. While CSFs are derived from and reflect the considerations of management, they are also inherited by the organization from the industry in which it operates, its position relative to peer organizations, and the effects of the current operating climate and environment. As a result, even though an organization may not achieve its goals, achieving CSFs may still get the organization closer to accomplishing the mission. Organizations that have achieved their goals but failed at their missions may have ignored the achievement of their CSFs.

The connection between an organization's operating environment and CSFs make them collectively more reliable as a predictor of the organization's capabilities for accomplishing the mission. To further develop this assertion, it is useful to explore the various sources of CSFs in more detail.

4.3 Sources of CSFs

CSFs are generally described within the sphere of influence of a particular manager. But there are many levels of management in a typical organization, each of which may have vastly different operating environments. For example, executive-level managers may be focused on the external environment in which their organizations live, compete, and thrive. In contrast, line-level managers may be concerned with the operational details of the organization and therefore are focused on what they need to do to achieve their internal, operational goals. Because of these different operational domains, the CSFs for the organization will come from many different sources. All are important for the organization as a whole to accomplish its mission, regardless of their source.

Rockhart defined five specific sources or types of CSFs[12] for the organization as follows: [Rockhart 81]

- the industry in which the organization competes or exists
- an understanding of the organization's peers
- the general business climate or organizational environment

[12] In our application of the CSF method to security activities, we did not concern ourselves specifically with ensuring that CSFs were identified in each of Rockhart's categories. However, consideration of each of these categories makes a set of CSFs more robust and representative of all of the various operating domains of an organization.

- problems, barriers, or challenges to the organization
- layers of management

To provide an accurate picture of an organization's overall key performance areas, it is important to identify CSFs from each of these sources. However, as we found in our use of the CSF method, deriving CSFs at the highest levels of the organization tends to bring an acceptable mix of CSFs from many of these sources, so long as a broad cross section of management is represented in the process.

Each source of CSF and its importance to understanding the organization's key performance areas is discussed in more detail in the following sections.

4.3.1 Industry CSFs

Every organization inherits a particular set of operating conditions and challenges that are inherent to the industry (or segment of the industry) in which it chose to do business. This results in a unique set of CSFs that organizations in a particular industry must achieve to maintain or increase their competitive positions, achieve their goals, and accomplish their missions. For example, consider an organization in the airline industry. As a member of this industry, the organization inherits CSFs such as "deliver on-time service" or "move away from the hub-and-spoke system." Failure to achieve these CSFs may render the organization unable to stay competitive in its industry and may ultimately result in its exit.

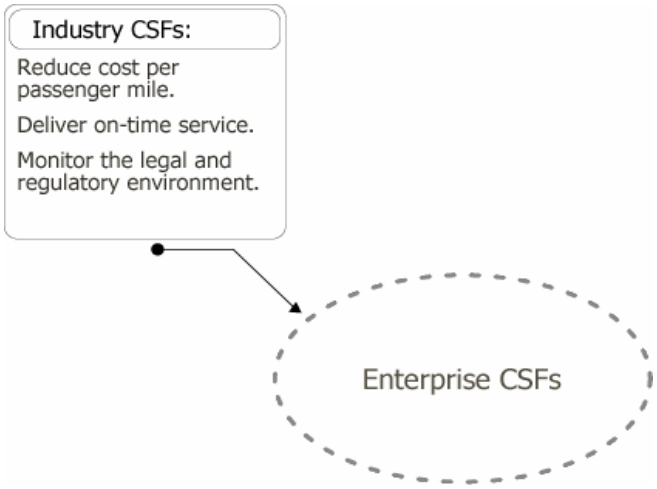


Figure 5: Example of Industry CSFs for an Airline

Industry CSFs do not necessarily apply only to a commercial or profit-oriented mission. In reality, the concept of industry CSFs can apply to organizations that have a commercial, educational, public-service, or non-profit orientation. Thus the term "industry" in this context

describes an organization whose purpose, vision, and mission is typically similar to those of its peers.

4.3.2 Competitive-Position or Peer CSFs

Peer-group CSFs are a further delineation of industry-based CSFs. They define those CSFs that are specific to the organization's unique position relative to their peer group in the industry in which they operate or compete. For example, an organization may be a leader or a laggard in a particular industry. If they are a leader, they may have CSFs that are aimed at ensuring they maintain or increase their market share against other organizations in the industry. On the other hand, if considered a laggard, the organization may have specific CSFs aimed at closing the gap and improving their competitive position relative to other organizations in their industry. In the case of the airline, an example of a peer-group CSF may be to "reduce cost per passenger mile" or "increase code share partnerships." These CSFs may be necessary for the company to increase market share in new geographical areas and to maintain or increase their competitive positions.

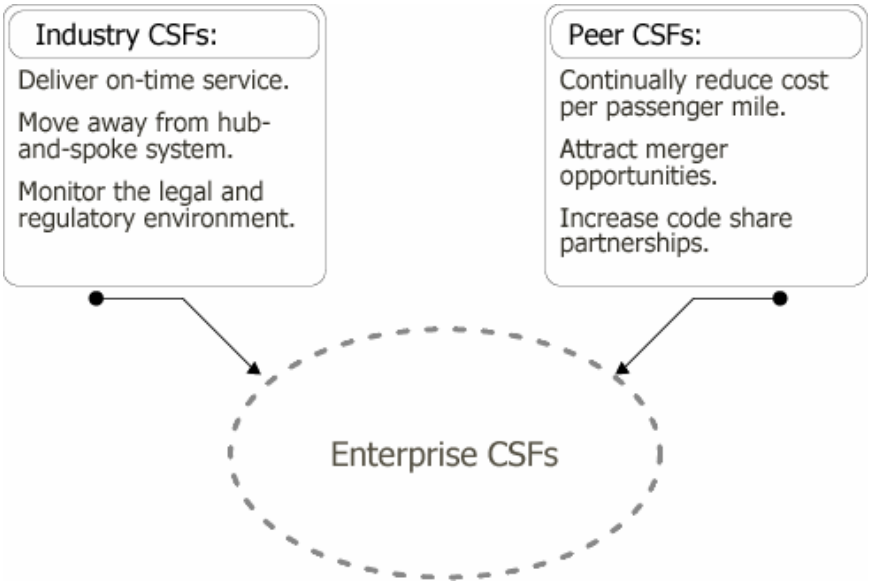


Figure 6: Example of Peer CSFs for an Airline

4.3.3 Environmental CSFs

To be successful, an organization must be mindful of the macro environment in which it operates. A closed organization—one that does not fully interact with its external environment—cannot survive in the long term. As a result, an organization must acknowledge the

environmental factors that can affect its ability to accomplish its mission. Environmental CSFs reflect the environmental factors over which the organization has very little control or ability to actively manage. By making these factors explicit, the organization can at least be mindful of them and actively monitor their performance relative to them.

Environmental CSFs describe such conditions as current socio-political issues, the industry's regulatory environment, and factors such as seasonality. For example, the airline industry has been dramatically affected by terrorist activities, which have forced changes in airport operations and scheduling and have brought about new regulations with which airlines must comply. Unfortunately, airlines have very little control over this problem.

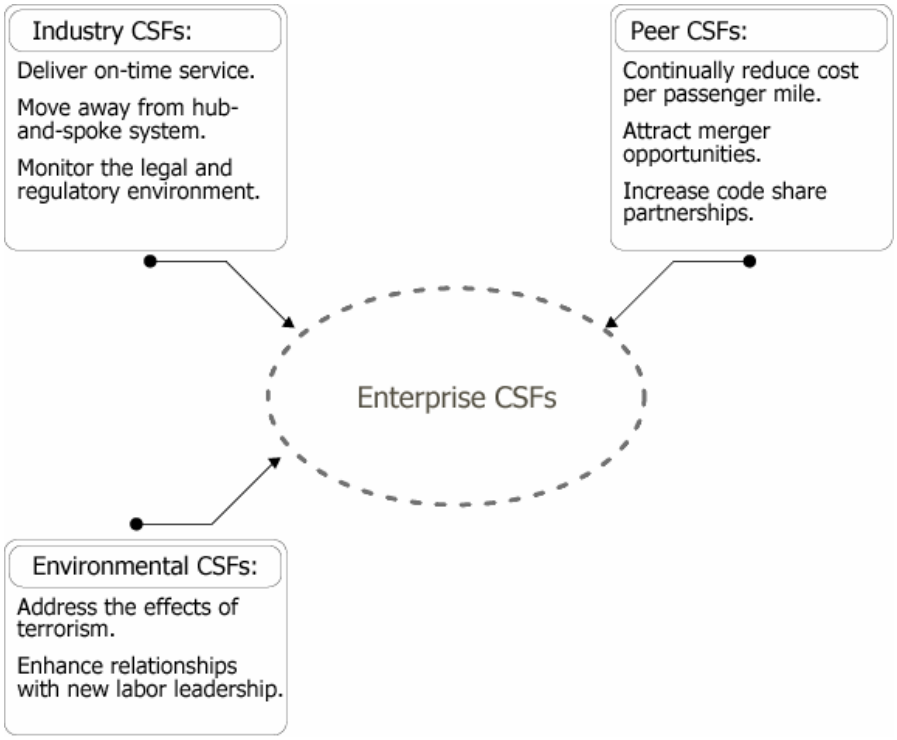


Figure 7: Example of Environmental CSFs for an Airline

4.3.4 Temporal CSFs

CSFs are tied to the long-term planning horizon of an organization. Over the strategic planning period the organization's CSFs may remain fairly constant, adjusted only when the organization makes major changes, such as changing its mission or the industry in which it competes. However, at one time or another, every organization encounters temporary conditions or situations that must be managed for a specific period of time, while continuing to maintain its performance in all other areas. These temporary conditions or situations can result in temporal CSFs—areas in which the organization must temporarily perform satisfacto-

rily in order to ensure that its ability to accomplish its mission is not impeded. For example, the following conditions can create temporal CSFs:

- threats that have been identified through SWOT[13] analysis
- temporary operating conditions, such as high inventory levels that must be reduced
- extreme changes in the organization's industry, such as the effect of the 9-11 terrorist attacks on the airline and travel industries
- barriers to entry to a new market or a new industry that arise when the organization takes on a new strategic direction
- temporary environmental factors, such as war, extreme weather, loss of key employees
- process or production problems that cause temporary changes in the organization's ability to produce its primary products or services
- lawsuits or legal actions brought against the organization that must be managed as a course of business until resolved

Keep in mind that a temporal CSF may be an indication of a *permanent* change in the organization's industry, operating environment, or competitive position and as a result may be adopted as a long-term organizational CSF because of its strategic importance.

[13] SWOT analysis is a commonly used strategic planning technique. It identifies the organization's strengths, weaknesses, opportunities, and threats that should be considered in developing a strategic plan.

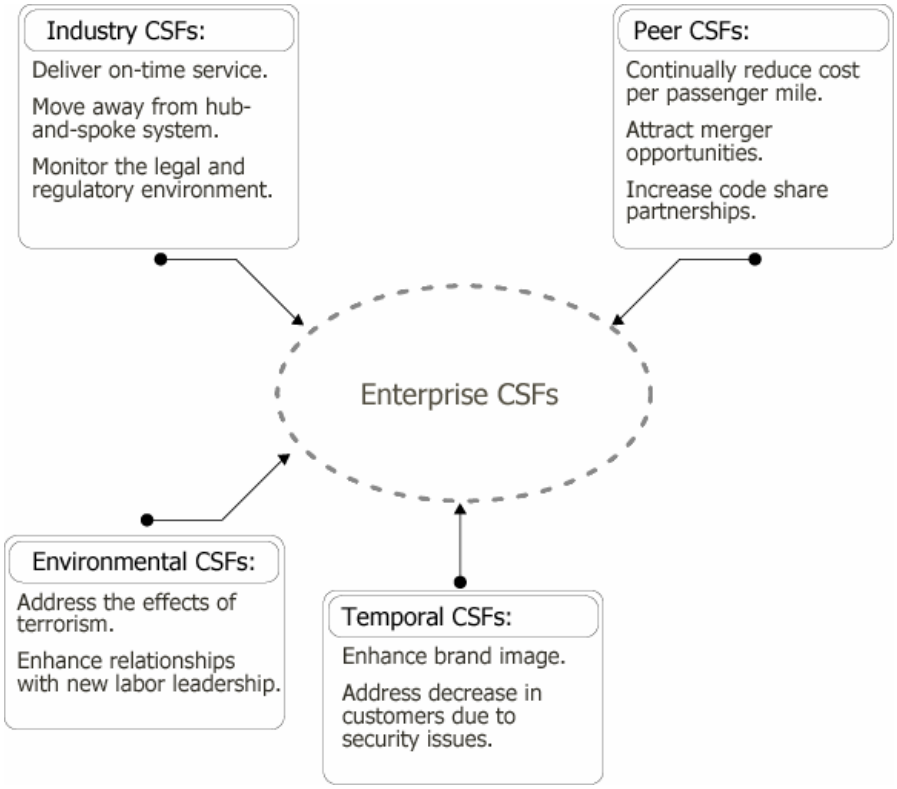


Figure 8: Example of Temporal CSFs for an Airline

4.3.5 Management-Position CSFs

Every layer of management has a different perspective and focus in the organization. This division of labor ensures that both tactical and strategic actions are taken to accomplish the organization's mission. Managers have different focuses and priorities depending on the layer of management in which they operate. This translates into a set of CSFs that reflect the type of responsibilities required by the manager's position in the organization. In fact, the CSFs that are inherent to the level of management may be universal across different organizations in the same industry. For example, executive-level managers may have CSFs that focus on risk management, whereas operational unit managers may have CSFs that address production control or cost control.

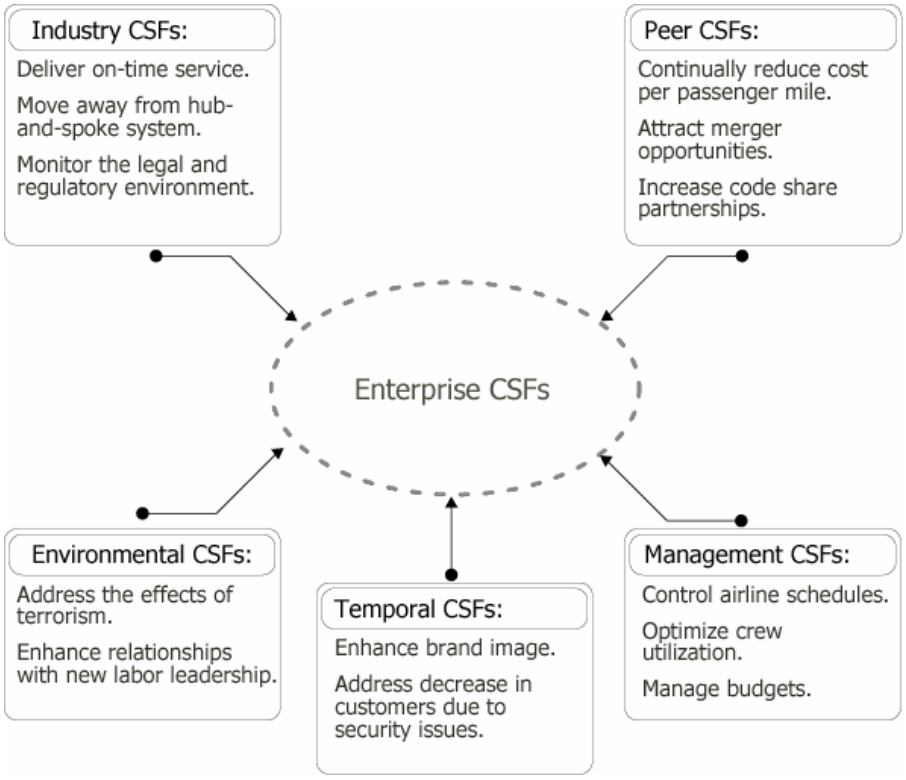


Figure 9: Example of Management-Position CSFs for an Airline Manager

4.4 Dimensions of CSFs

In his initial work, Rockhart also described various dimensions of CSFs that are useful for understanding a particular manager's view of the world [Rockhart 81]. CSFs can be categorized by these dimensions to further clarify the current focus of the organization and how it is positioned among its peers.

The dimensions of CSFs as described by Rockhart are

- internal
- external
- monitoring
- adapting

4.4.1 Internal Versus External

Internal CSFs are those CSFs that are within the span of control for a particular manager. In contrast, *external* CSFs are those over which a manager has very little control. For example,

in the airline industry example, an internal CSF could be "managing ground operations," while an external CSF may be "fuel costs."

Categorizing a CSF as either internal or external is important because it can provide better insight for managers in setting goals. For example, a manager can set very specific, achievable goals that complement the achievement of internal CSFs because the manager has control over them. However, if a manager has an external CSF, he or she must set goals that aim to achieve the CSF and minimize any impact on operations that may result because the CSF is not in his or her direct control.

4.4.2 Monitoring Versus Adapting

Monitoring CSFs emphasize the continued scrutiny of existing situations [Rockhart 81]. Because monitoring the organization's health is a primary function of management, almost all managers have some type of monitoring CSF. In fact, in our work with CSFs, we have found that many enterprise CSFs (those that apply to the entire organization) are focused on monitoring the organization's performance in a few key areas, such as compliance with regulations. Conversely, *adapting* CSFs are focused on improving and growing the organization. We have also found that many enterprise CSFs are adapting CSFs because they state the organization's desire to improve their competitive position or to make a major change in their mission. In these cases, the distinction between a goal and a CSF is less clear—what appears to be a goal of the organization is actually an adapting CSF.

4.4.3 Importance of CSF Sources and Dimensions

The source and dimension of a CSF provides additional information for understanding the importance of a CSF and its contribution to the accomplishment of the organization's mission. To be effective, managers must consider and monitor a wide range of activities, events, and conditions that occur throughout the organization and in the external environment in which the organization operates. Gathering CSFs that incorporate and reflect various CSF sources and dimensions provides an effective delineation of a manager's field of vision—a representation of the depth and breadth of the manager's responsibilities.

4.5 Hierarchy of CSFs

As explained previously, CSFs exist throughout all levels of the organization and can come from many sources. As with strategic planning and goal setting, CSFs at higher levels of the organization are related to (or dependent on) those at lower levels in the organization. Higher level CSFs cannot generally be achieved unless lower level CSFs are achieved as well.

Higher level CSFs influence lower level CSFs. In fact, if lower level CSFs differ significantly from higher level CSFs, the organization must consider whether there is proper alignment between the activities of lower level management and the strategic direction of the organization.

Goal setting also tends to follow a hierarchical pattern throughout an organization. However, in contrast to goal setting, there may not be a one-to-one relationship between CSFs as they cascade through the various layers of the organization. This is because CSFs are often closely tied to a particular manager or management layer and any specific concerns at that level. Thus, there may be some CSFs at lower levels in the organization that are important to achieving higher level CSFs and accomplishing the organization's mission but are not explicitly related or subordinate to a higher level CSF.

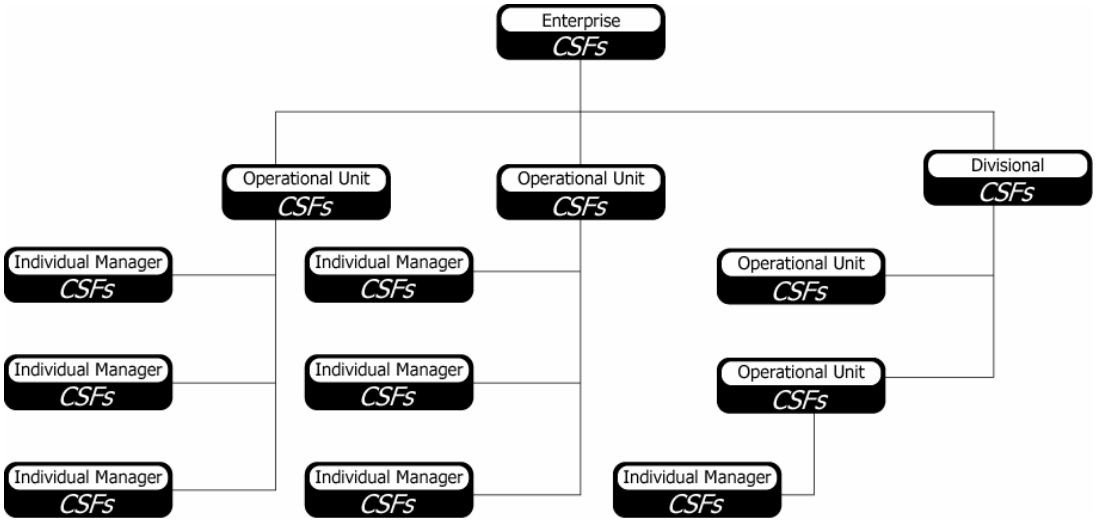


Figure 10: Example of Hierarchy of CSFs in an Organization

In our experience with CSFs, we have found it useful to describe two levels of CSFs: enterprise CSFs and operational unit CSFs.

4.5.1 Enterprise[14] CSFs

The numerous sources of CSFs illustrate the broad array of challenges and demands facing management in modern organizations. Each layer of management has a set of conditions that must be monitored and acted upon. They also have a unique set of CSFs to consider.

[14] Rockhart refers to these types of CSFs generically as "corporate CSFs" because of the focus of his work on the corporate world. However, throughout this report, and particularly in the case studies, we use the term "enterprise CSFs" whenever we make a general reference to the critical success factors for an organization.

But a simple gathering of the CSFs of each manager (and management layer) in the organization does not necessarily form a superset of enterprise CSFs. This approach could result in hundreds or possibly thousands of CSFs that the highest levels of management would need to consider. (Imagine the difficulties that strategic planners, for example, would have in attempting to align their planning activities with hundreds of CSFs.) It could also derail the organization's ability to focus on those five to seven areas that can truly "make or break" their efforts to accomplish the mission.

As with other managers in the organization, executive-level managers must be guided by their own set of unique CSFs. However, because of the role of executive-level management, their CSFs also typically represent the organization's truly critical and key areas of performance. This is not to say that the CSFs of other layers of management are not important—executive-level managers' strategic direction strongly influences the CSFs of other layers of management, and their ability to achieve enterprise CSFs is highly linked to success in achieving lower level CSFs.

Thus, an organization can develop a high-level set of CSFs that represent the top activities, concerns, strategies, and goals of executive-level management. These "enterprise CSFs" are derived from the top two or three layers of management and reflect the various CSFs found throughout the organization. In our work with CSFs, we have found that enterprise CSFs provide the most effective strategic view of what is important to the organization and to accomplishing the organization's mission. Enterprise CSFs represent the entire organization, and each operational unit in some way contributes to (or detracts from) achieving them by achieving its operational unit CSFs.

4.5.1.1 Nature of Enterprise CSFs

Enterprise CSFs often reflect both the current concerns of executive-level managers as well as the longer term strategic direction of the organization. As a result, enterprise CSFs can comprise a blend of temporal CSFs (reflecting the current "hot issues" of management) and industry, peer, and environmental CSFs (which reflect such indicators as the state of the economy, current business climate, and geopolitical issues). This is important because executive-level managers often must be agile and able to react to changes in addition to planning for the long run.

4.5.2 Operational Unit CSFs

An operational unit can be described as an organizational department, division, subdivision, or any other grouping of activities that share a common function, purpose, or mission. For example, the finance department in an organization might be an operational unit. Regardless of how organizations define their operational units, each may have its own set of CSFs.

As noted with enterprise CSFs, operational unit CSFs are not necessarily a simple collection of the CSFs of managers in the operational unit. Instead, operational unit CSFs may reflect the concerns and strategic direction of senior managers in the unit, as well as the strategic direction of the organization (as embodied in enterprise CSFs).

It is important not to confuse operational unit CSFs with management-function CSFs. Management-function CSFs reflect the generic responsibilities that are inherent in the manager's position in the organization. In contrast, operational unit CSFs are similar to enterprise CSFs in that they reflect the operating perspective and strategic direction of executive-level managers in the operational unit. The management layer is certainly a source of CSFs for the operational unit but is not entirely reflective of it.

4.5.2.1 Nature of Operational Unit CSFs

In our definition, operational unit CSFs tend to be less influenced by the organization's industry and more focused on the contributions necessary to support the organization's strategic goals and mission. For example, in the airline example, the operational unit CSFs for four divisions or departments—reservations, scheduling, flight operations, and freight operations—are very different, but each contributes vitally to the organization's overall achievement.

Operational unit CSFs may also have a temporal component, particularly if a specific division in the organization has temporary changes in operating conditions that it must consider. For example, if the airline industry as a whole must contend with overcapacity, the "scheduling" department may have a CSF that seeks to reduce flights and destinations served until demand increases.

4.5.3 Relationship Between Hierarchy and Source

Each of the sources of CSFs (industry, environment, etc.) can supply CSFs at the enterprise or operational unit level. However, because of their nature, some sources are more likely to supply CSFs at either the enterprise or operational unit levels. For example, industry CSFs may supply more CSFs to the enterprise level than to the operational unit level. Table 1 summarizes the possible relationships between enterprise or operational unit CSFs and the various CSF sources.

Table 1: Matrix of CSF Levels to CSF Types

CSF Level	Type of CSF				
	Industry	**Peer**	**Environmental**	**Temporal**	**Management-Function**
Enterprise	Industry CSFs strongly influence enterprise CSFs. Executive-level managers have a direct responsibility for interacting with the external operating environment of the organization as reflected in industry CSFs.	Executive-level managers must be mindful of the competitive position of the organization and calculate their role to ensure they plan accordingly.	Factors such as seasonality and the current geopolitical environment affect the current and long-term plans of the organization. Executive-level managers must consider the impact of the environment on their strategic plans.	A temporary problem or change in the organization's strategy can affect the overall CSFs for the organization. The hottest issues for executive-level management (such as security) must be considered and addressed.	Enterprise CSFs reflect the unique responsibilities of executive-level managers. Their position generally reflects their unique roles, such as risk management, financial management, and shareholder interaction.
Operational Unit	Industry CSFs could influence operational unit CSFs, especially if a particular division is affected. However, on the whole, there is less focus on the industry at this level than at the organizational level, particularly if the operational unit is fairly low in the organization.	Operational units may have less responsibility for the competitive positioning of the organization; therefore this may not be a source of CSFs. However, if the operational unit is a division that competes in a unique industry, competitive position CSFs will arise similar to those that could be found at the organizational level.	Environmental factors may filter down to an operational unit, particularly if it is a division competing in a unique industry, resulting in some environmental CSFs.	Temporary problems or changes affecting the organization as a whole may filter down to any operational unit that is critical to dealing with these problems or helping to implement changes. Therefore, some temporal CSFs may be found at the operational unit level.	Operational unit CSFs are highly influenced by management layer CSFs. Operational units tend to reflect many different unique layers of management (middle, line, etc.) and therefore are a rich source of management-function CSFs.

4.5.4 Other Considerations

Enterprise and operational unit CSFs must fit together and relate to one another, but they are generally much more loosely coupled than goals. Goals tend to cascade throughout the organization so that there is a tight one-to-one fit between the goals of each management layer. For example, the goals of a production line worker are directly related to the goals of the production line manager, whose goals in turn are focused on helping to achieve the goals of the chief operating officer and the organization.

The strict balancing and leveling inherent in goal setting is not typically found with CSFs. There may not be a one-to-one match between every operational unit CSF and an enterprise CSF. This is because each layer of the organization has its own focus and operating conditions, including executive-level management. However, there must be congruence; otherwise there may be a disconnection between what an operational unit views as important and what is good for the larger organization.

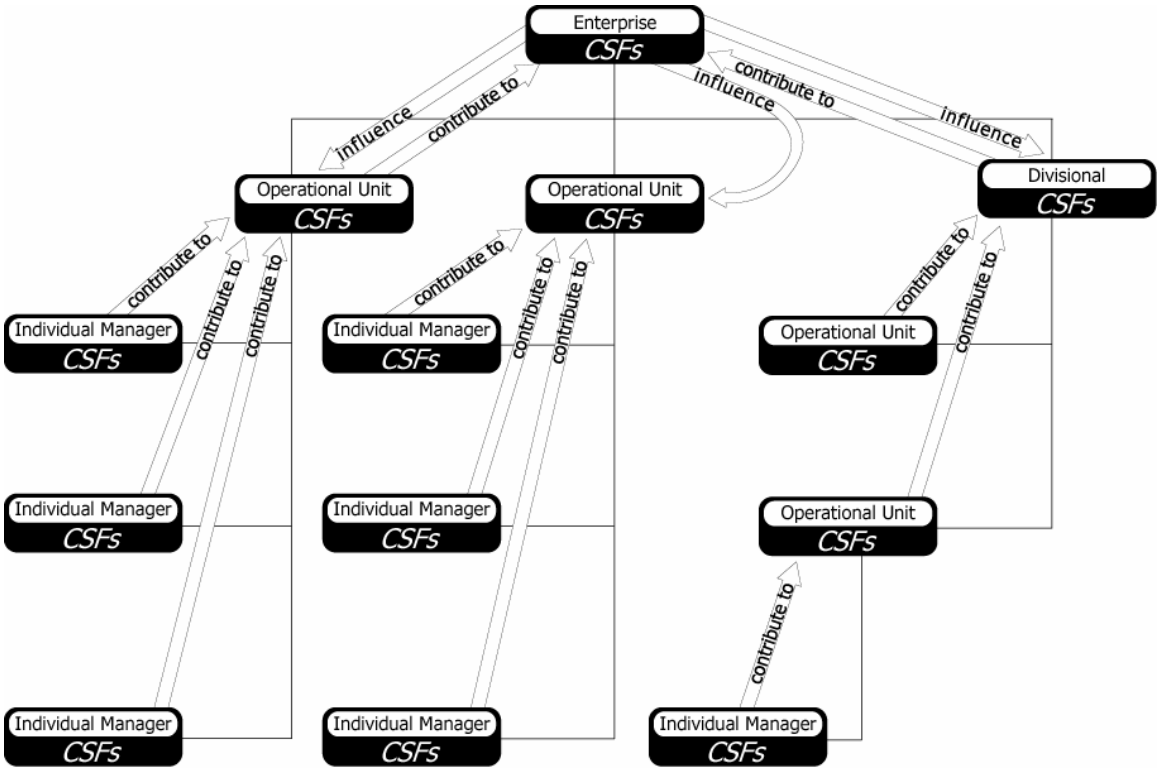


Figure 11: Relationship Between Enterprise and Operational Unit CSFs

5 Applying CSFs

At the core, CSFs relate to the functions of management[15]—what needs to be done, how well, and how often to meet a personal or organizational mission. In their simplest form, CSFs can be viewed as a management tool for making better-educated decisions that consciously support the mission of the organization. In fact, applying CSFs to validate and ensure alignment with the direction and intent of the organization can enhance any decision, initiative, effort, or process.

In this section, we describe the traditional uses of CSFs and some general advantages of a CSF-based approach to organization-wide efforts and initiatives. Most importantly, we explore the potential benefits of the CSF method as specifically related to addressing security strategy, goals, and activities. Finally, other potential uses of the method that we believe merit further research and field testing are presented.

5.1 Historical Application of CSFs

As noted in Section 3.1, much of the contemporary literature regarding CSFs (certainly that which postdates Rockhart's introduction of the CSF approach in the *Harvard Business Review* [Rockhart 79]) focuses on the connection between CSFs and information systems and technology. Even the creator of the concept, D. Ronald Daniel, had information systems in mind when he coined the phrase "success factors" and created the concept that Rockhart eventually transformed into CSFs. Ironically, Daniel's underlying objective was to help organizations manage more effectively; however, he quickly acknowledged that this was increasingly dependent on high-quality information and technology. Thus, the bond between CSFs and information systems was created and has continued to evolve.

[15] Henri Fayol's classic view of management includes the functions of planning, organizing, commanding, coordinating, and controlling. The effectiveness of each of these functions can be greatly enhanced if performed within the context of the organization's critical success factors. More information on Fayol's management functions can be found at www.onepine.info/htm.

5.2 General Advantages of a CSF-Based Approach

Throughout this report, the advantages of developing and applying CSFs are presented. The seemingly endless ways in which they can be of use to an organization speaks to their simple nature and broad applicability.

Of note is Rockhart's view that one of the most powerful uses of CSFs is to enhance communication among the organization's managers [Rockhart 79]. The ability to get managers "on the same page" can aid in mobilizing all areas of the organization toward the same goals. Regardless of how CSFs are used, there are several advantages to having this type of common focus for the organization:

- CSFs can reduce organizational ambiguity. Developing and communicating a set of CSFs can reduce the dependence on the *perceived* aims of the organization. CSFs reflect the implicit, collective drivers of key managers and as a result are a more dependable and independent articulation of the organization's key performance areas.
- CSFs are more dependable than goals as a guiding force for the organization. An organization can set good goals that, in theory, will move the organization toward its mission. However, if the goals are poorly articulated or developed, this is not guaranteed. CSFs are reflective of what good managers do well to move the organization toward its mission, regardless of the quality of the goals that have been set.
- CSFs are more likely to reflect the current operating environment of the organization. Goal setting tends to be a cyclical (i.e., yearly) activity that is seldom revisited until performance measurement. Used properly, CSFs are likely to be more dynamic and to reflect current operating conditions (particularly because of the many sources of CSFs).
- CSFs provide a key risk-management perspective for the organization to consider. The risk perspective of executive-level managers is built into CSFs, so their "radar screen" is exposed to the organization as a whole.
- CSFs can be valuable for course correction. When CSFs are made explicit, managers often realize that their perception of what is important to the organization may not match reality or they may realize that they don't fully understand the current operational climate. Thus, they can use CSFs to realign their operating activities.

5.3 Using CSFs in a Security Context

Our interest in the CSF approach evolved from our recurring observation that customers often have difficulty developing and implementing a security strategy when they do not maintain an explicit focus on business drivers. This can occur for a number of reasons:

- The organization may have decided that security is the domain of the information technology department, which may not play a strategic role or is unable to articulate the overall goals of the organization.

- Security is viewed as a cost or burden that must be managed and not as an activity that contributes to success, profitability, or growth.
- Personnel in charge of security are disconnected from the organization's mission because of their role or function (i.e., they are external to the organization, as with consultants, or they have a strict technology focus) or because of the layer of the organization where they operate (i.e., staff or line functions).
- The organization's business drivers or factors for success simply are not well known or communicated to all who have a need to know.

Regardless of the reason, the result is often the same: the security strategy fails to reflect what's important to the organization, to the accomplishment of its mission, and to its long-term resiliency. It fails to answer the basic questions: What is to be protected? How is it threatened or why does it need to be protected? What happens if it is not protected? Certainly, these questions are fundamental to a risk management approach to security, but the answers are often embedded in the organization's mission, goals and objectives, and the factors that affect the organization's potential success or failure in pursuit of the mission and goals—the CSFs.

Unfortunately, many organizations with whom we have worked have only a vague understanding of their CSFs. They often rely on their perception of "important" or "critical" rather than relying on an explicit articulation of these factors. They also tend to rely on external influences (such as laws and regulations) to provide them with a default security strategy or initiative instead of developing an internal strategy, consistent with their mission, that can position them to address ever-increasing and changing regulations.

Overall, it is our contention that organizations that have a clear "eye on the prize" are better positioned to make meaningful decisions about security and to implement them in a way that not only protects the organization but actually contributes to the accomplishment of the mission. Properly positioned and managed, organizations can turn the burden of security into a competitive advantage—an enabler that directly affects an organization's achievement of its goals and its bottom line. Some organizations have had to adopt this perspective on security because it is required by the nature of the industry in which they compete. For example, the business model for many e-commerce organizations is built on trust and security. Thus, their security strategy is inextricably linked to their mission—if the strategy is effective, they meet their goals; if not, the bottom line suffers.

In this section, we provide some of our theories and share our experiences regarding the use of the CSF method to enable the effective development of security strategy and the application and management of security throughout an enterprise.

5.3.1 Enterprise Security Management

Several years ago, we were called upon to assist a federal government agency in its security efforts. The agency had recently decided to develop its own information security capability, through which it would not only serve itself but several other high-profile government agencies. Our scope of work was to perform a risk assessment for the agency to identify the issues that it would need to address first. However, it soon became clear that a risk assessment activity would not answer some of the basic questions and issues the agency needed to confront.

A team with a broad array of technology and security skills was assembled to staff the information security capability. However, what the agency had in terms of human resources did not compensate for what it lacked in other key ingredients for success—there was no existing security policy or strategy, no shared vision or objectives for strategy across the various agencies, and, more importantly, no clear vision of what it wanted to accomplish and why. In addition, the team appeared to lack clarity on its role and responsibilities.

Our work promptly took the form of helping the team to determine its security goals and objectives and to take an inventory of its strengths and challenges. The team members understood that they needed to "secure the organization" but were not able to clearly articulate the meaning of "secure" and, further, how they would know when they had accomplished it.

We observed that, as a newly formed group, one of their major challenges in defining "secure" or "security" was that the team lacked context—members had no comfort or familiarity with the mission of the larger agency or the missions of the other very diverse agencies that they were charged to protect. Before our work progressed any further, we suggested that it might be a good idea to collect these agencies' mission statements and study them to get a sense of what was important. This information could then help to determine the capabilities that the team would need to meet its requirements for managing security across such a vast enterprise.

In hindsight, what we were attempting to do was to get the agency to set the context for its security efforts—to develop a guiding "position" or a "posture" as we described it at the time. We prompted the agency to look clearly and explicitly at the drivers used by the organization to accomplish its operational goals and to align its security strategies and activities to those drivers. In that way, agency personnel might not only be supporting but contributing to the operational goals through their work. While we didn't perform a CSF exercise with the agency, it became clear to us that in the future, this type of exercise would be a valuable context-setting exercise for customers facing similar problems.

It also became apparent during our engagement that the small security staff that the agency had assembled would not be able to accomplish its security goals alone. It would need to

draw upon and mobilize existing capabilities of the organization, both technical and managerial, to be successful.

5.3.1.1 Enterprise Security Management Defined

Our experience with this federal government agency (and subsequently several other organizations) evolved into a management- and process-oriented view of security as a business process that is pervasive across and dependent on the enterprise. Our continuing exploration of these theories is the focus of an emerging body of work in the Networked Systems Survivability program at the SEI, referred to as enterprise security management (ESM). The core assertion of this work is that managing security across an enterprise is a complex endeavor that depends on several fundamental principles:

- The skills, capabilities, and efforts of the entire organization must be utilized and mobilized.
- Key functions and processes in the organization must collaborate on shared security goals and strategy.
- The organization's security objectives or an articulation of its "desired state" must be developed and understood.
- Critical assets that are essential to achieving the organization's mission must be identified and protected.
- Information technology operations and support must enable security goals.

One of the keys to achieving such an extensive undertaking, particularly where many diverse parts of the organization must work together, is to ensure that it is properly focused on a shared understanding of organizational values—such as CSFs.

5.3.1.2 ESM and CSFs

The complexity of undertaking an enterprise-wide view of security management can be illustrated in the challenges facing chief security officers (CSOs). Often, CSOs are tasked with "securing" the organization, but may not be clear on what that means. Indeed, in some organizations, the role of the CSO has been relegated to the information technology department, further separating it from organizational strategy and business drivers. As a result, the CSO is often left to answer some very important organization questions without specific guidance:

- What needs to be secured? Why, and in what priority?
- What parts of the organization must be involved in this effort? How will I convince these units to work together, especially if I don't have direct control over them?
- How will I know when the organization has been "secured?" What will be used to measure success?

Our assertion is that some of the answers to these important questions are found in the organization's business drivers, and in particular its CSFs, because they represent a common, shared focus. Why?

- The "field of vision" of top management (and management in general) is represented in CSFs. This provides a powerful clarification of what is important and valued in the organization. Failure to achieve CSFs directly affects the organization's ability to accomplish its mission. Thus, security efforts need to align with CSFs *and* ensure that the accomplishment of CSFs is not impeded.
- CSFs reflect the goals of the organization. Managers operate toward the achievement of goals. What needs to be protected in the organization can be identified relative to these goals—assets and processes that support these goals and the organization's mission must be protected.
- Rallying around a common purpose is an effective means for getting disparate parts of the organization to take on a common cause, such as security. Security is a business problem that requires the effort of everyone in the organization to solve and to manage. CSFs provide a unifying effect, if only because most employees prefer to avoid the stigma of failing to contribute to an effort that is clearly good for the organization.
- The drivers for security should be the same as the business drivers used by the organization to accomplish its mission. Security should be a way for organizations to enhance their operations, help them achieve their goals, and provide them with an appropriate level of resiliency commensurate with their long-term strategies. CSFs can be shared drivers for security and the organization.

For these reasons, we see great promise for the CSF method as a catalyst for setting the direction of an organization's enterprise security management activities. Chief security officers can confront the challenges of enterprise security management by using CSFs as a foundation from which security professionals and the rest of the organization can collaborate, plan, and execute. They can also qualitatively measure the success of their security programs by determining how they contribute to achieving the organization's enterprise CSFs.

5.3.2 Information Security Risk Assessment and Management

One of the key activities in managing security is to perform periodic risk assessments. In general, risk assessments are a diagnostic tool that helps the organization to determine the success of its security efforts relative to its security strategy. The CSF method shows particular promise in helping organizations conduct more meaningful (and valid) information security risk assessments in a number of areas.

Most of our fieldwork experience in information security risk assessment is in the use and application of the OCTAVE[16] method. The OCTAVE method provides specific guidance for the major activities of a risk assessment, but also allows for significant tailoring to meet the needs of unique organizations. As a result, many users with whom we have worked have asked us for additional guidance on developing scope, selecting critical assets to assess, and in prioritizing risks to mitigate. Without the advantage of the CSF method, we often provided no specific guidance to customers except to encourage them to align risk assessment activities with business drivers. However, the term "business drivers" is often ambiguous and subject to interpretation. Unless an organization has a clear definition of its business drivers, they cannot be used in a practical way to guide important organizational efforts or initiatives.

Because of this issue, we began to search for a more precise and practical way to apply the concept of business drivers to security. Through further research and fieldwork, we decided to explore the use of CSFs. CSFs are inextricably linked to and representative of the other components of business drivers (i.e., the organization's mission, values, and purpose and its goals and objectives). CSFs are also a conduit to achieving the organization's goals and objectives and accomplishing its mission. Thus, the use of CSFs can be an effective way to link business drivers to various aspects of security, including developing and implementing security strategy, managing security activities and operations, and conducting security risk assessments. On this premise, the following sections highlight the ways in which CSFs can enhance key risk assessment activities.

5.3.2.1 Determining Risk Assessment Scope

One of the most important (and difficult) tasks in performing a risk assessment is to determine its scope. A risk assessment performed on an area of the organization that is not essential to accomplishing the mission generally will not yield meaningful results. Unfortunately, failing to properly scope the risk assessment also diminishes the purpose and intent of using a risk-based approach.

For example, the OCTAVE method for risk assessment guides users to choose three to five important operational areas to include in the scope. This guidance is perfectly acceptable for users who have a good sense of the organization's mission and can be objective about which areas contribute most to accomplishing the mission. However, for many users, particularly those in the lower levels of the organization, this guidance is difficult to put into practice. Frequently, users need an explicit set of criteria against which to evaluate operational areas and to decide which areas should be included in the risk assessment. CSFs are useful for this purpose because they represent the organization's business drivers and they embody the risk-management perspective of executive-level management.

[16] More information on the OCTAVE method can be obtained from www.cert.org/octave.

Using CSFs, an affinity analysis[17] can be performed between enterprise (or operational unit) CSFs and the various departments or operational areas of the organization being considered for assessment. Those operational areas that provide significant support for the achievement of CSFs will be strong candidates for risk assessment because of the implied contribution they make toward accomplishing the organization's mission.

Figure 12 provides an example of the possible intersections between enterprise departments and CSFs for the purpose of identifying areas in which to perform a risk assessment.

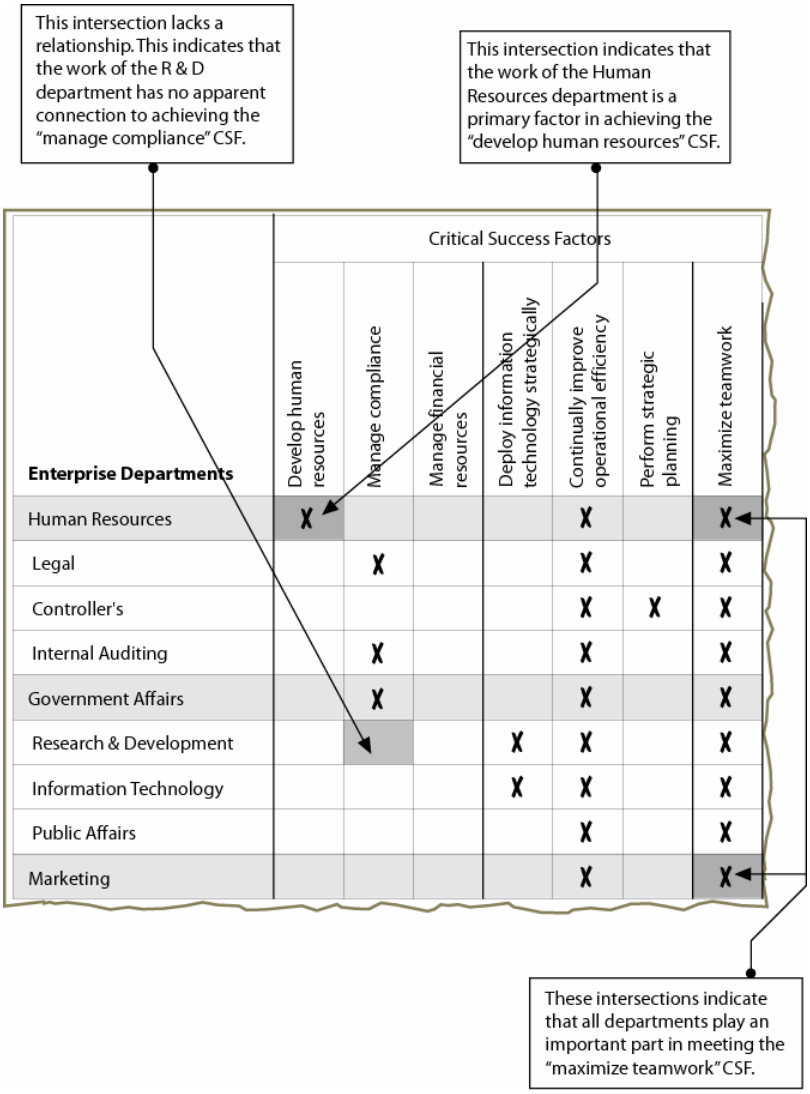


Figure 12: Affinity Analysis for Determining ISRM Scope

[17] The technique used to perform affinity analysis is provided in Appendix A, "CSF Method Description."

5.3.2.2 Selecting Critical Assets for Assessment

A risk-based approach to security encourages organizations to direct their limited resources to protecting the organization's most critical assets—information and technical[18] assets that are essential to supporting the organization's mission. The selection of critical assets for risk assessment is often left to the judgment of those performing or participating in the assessment, whether they are inside or outside of the organization. Thus the importance of the asset may be based on its perceived value, rather than a more concrete method of asset valuation. While desirable, assigning a qualitative or quantitative value to assets may be prohibitively expensive for an organization.

The use of CSFs can be a simple yet effective compromise for selecting critical assets. As a byproduct of using CSFs to help define the scope of a risk assessment, the pool of potential assets can be effectively limited to those operational areas that are most important. Conversely, for organizations that have a solid inventory of information and technical assets, affinity analysis can be performed to compare assets to CSFs. The result of this type of analysis is the identification of assets that are essential to achieving CSFs and, by default, to accomplishing the mission of the organization. In summary, CSFs can help to validate the importance of an asset by confirming its overall significance to the organization.

Figure 13 portrays an example of affinity analysis between critical assets and a set of enterprise CSFs. In this case, there is an intersection between the "financial data" asset and the "manage compliance" CSF. This indicates that the "financial data" asset is critical to the organization because it is essential to achieving the "management compliance" CSF, and thus needs to be protected.

[18] Information assets represent the data and information, in either physical or electronic form, that is critical to the organization. Technical assets represent those assets that support the storage, transmission, and processing of data and information and therefore are important to transforming data and information for use by the organization. People can be an asset to the organization as well for similar reasons—they can be a primary way of storing, transporting, or processing data.

The asset "Financial data" is critical to achieving the "Manage compliance" CSF.

Critical Assets	Critical Success Factors						
	Develop human resources	Manage compliance	Manage financial resources	Deploy information technology strategically	Continually improve operational efficiency	Perform strategic planning	Maximize teamwork
Customer information					X		
Payroll information			X				
ERP system					X		
Financial data		X	X				
Widget formulas					X		
EIS system						X	
Skills database	X						X

Figure 13: Affinity Analysis for Determining Critical Assets

5.3.2.3 Identifying and Validating Security Requirements

An important component of protecting critical assets is the development of security requirements in the areas of confidentiality, integrity, and availability.[19] As an asset is stored, transported, and processed throughout the organization, these security requirements must be met and protected by all who use or take custodial control of assets. Defining security requirements can be a difficult task; significant thought must be given to the potential misuse of the assets and the consequences of this misuse. In addition, a substantial number of requirements could be developed for each asset. This poses a problem for devising a protection strategy for an asset: Which requirements are most important? Which requirements, if unmet for any reason, would impact the owner of the asset or the organization as a whole? Further, which assets, if impaired, would impact the achievement of CSFs?

Answering these questions requires consideration of the priority of the security requirements. CSFs can be very useful for this purpose because they represent management's priorities. For example, a comparison of an asset's security requirements to CSFs will highlight those requirements that are essential to ensuring that the achievement of CSFs is not impeded. Prioritizing requirements in this manner can help the organization to develop and implement

[19] Security requirements in these categories are commonly applied only to information assets. Technical assets have security requirements as well, but are not often described in terms of confidentiality, integrity, or availability.

meaningful security controls for assets to ensure that they continue to contribute to the organization's pursuit of its mission.

Figure 14 provides an example of affinity analysis for security requirements. In this example, the security requirement of "confidentiality" for the "medical records" asset has been identified as important to the "manage compliance" CSF. This is because failure to meet the confidentiality requirement for medical records could impede the organization's ability to be successful at managing compliance activities.

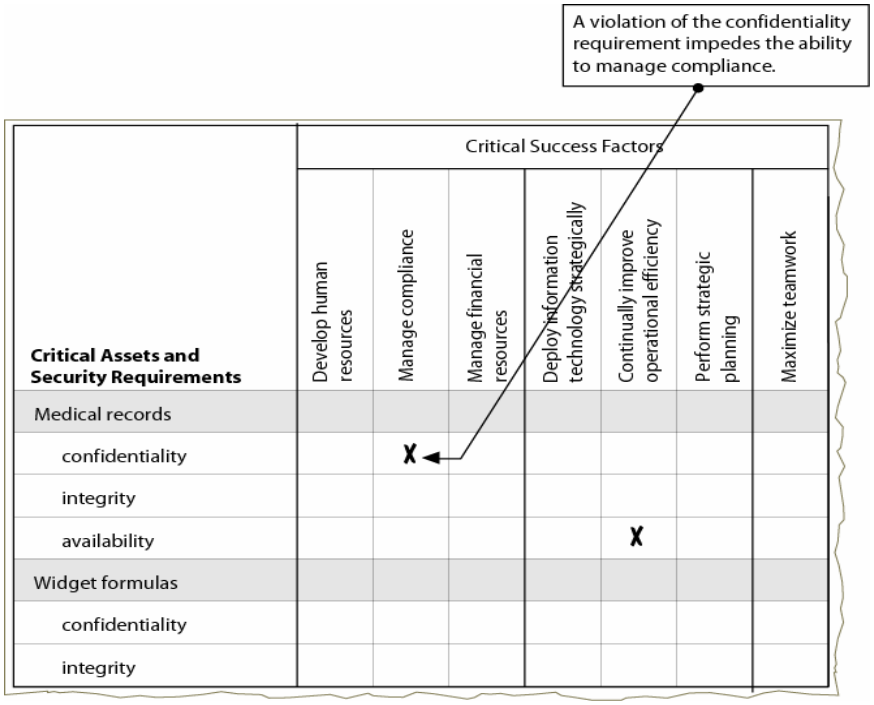


Figure 14: Affinity Analysis for Determining/Validating Security Requirements

5.3.2.4 Identifying Risks to Critical Assets

Risk identification is at the core of a risk-management approach to securing critical assets. Properly characterizing a risk is essential to understanding the potential impact on the owners of the asset if it is somehow compromised, temporarily lost, or permanently destroyed. While this task is essential, it can also be the most elusive for an organization to undertake. As noted previously, defining the scope of a risk assessment and determining the critical assets on which to focus the assessment is an important first step. However, the organization still has to decide upon which risks to direct limited resources. To do this, an organization has two options:

1. Use a generalized taxonomy to identify risk. This approach is popular with federal government agencies and is often effective because it provides an orderly and somewhat comprehensive guide for examining many potential areas of risk.

2. Elicit risk information directly from the organization. This is the approach used by the OCTAVE method and, depending on the organization, can also be very effective. It attempts to ensure that the experience and intuition of managers and staff in the organization is relied on to identify risks that are most associated with the business drivers of the organization.

While effective, there are potential problems with each of these approaches. For example, exclusively using a taxonomy may cause the organization to overlook certain risks that are unique to its business environment or to spend valuable time considering risks to which it is not specifically exposed. In addition, success in using a knowledge elicitation approach is highly dependent on ensuring that the right participants are interviewed and that they fully understand the risk assessment approach and objectives. While it may be effective in identifying risks that are unique to the organization, this approach can result in overlooking many common risks that the participants are not familiar with because they have a limited understanding of information, technical, and physical security issues. Thus, the results from this approach are only as good as the quality of the participants in the process.

One way to enhance the effectiveness of either of these approaches is to use CSFs. For example

- CSFs can be used to properly focus risk identification. With a taxonomy approach, CSFs can help to focus in on those areas of the taxonomy that directly affect (encourage or impede) the accomplishment of CSFs. In this way, the taxonomy is more effectively linked to the organization's business drivers and areas that are unimportant to the organization are not considered.
- In the case of the knowledge elicitation approach, CSFs can be a very powerful means for shaping and guiding the responses of participants. Knowledge of enterprise (or operational unit) CSFs can enable participants to identify areas of concern and risks that explicitly consider the potential impact on achieving CSFs. In this way, the participants are providing information that is more certainly linked to the organization's business drivers. (This is illustrated in the case study presented in Appendix B.)
- Likewise, once risks have been identified, CSFs can be used for validation. Risks to critical assets that do not impair the achievement of the organization's CSFs may be given a lower priority because they are unlikely to impact the organization's ability to accomplish its goals and mission. As a result, risks that interfere with the organization's ability to achieve CSFs can then be focused on because they have the greatest potential for harm.

5.3.2.5 Setting Evaluation Criteria for Measuring Risk

In most commonly used risk assessment methods, a set of criteria is used to evaluate the extent of risks to critical assets. In risk assessment methods such as OCTAVE, the risk evaluation criteria is developed by the organization so that it uniquely reflects their business drivers

and conditions; in other methods, the extent of risk is standardized in that the developer of the method has defined and weighted the criteria used for evaluating risk.

In our experience, a risk assessment is more meaningful when it is based on and connects directly to an organization's unique business drivers. Risk evaluation criteria that are developed by the organization are likely to reflect the values of the organization, but this is not guaranteed. The validity of the criteria is dependent on a number of factors, including: Who developed the criteria? What is that person's role (or perspective) in the organization? What is that person's level of familiarity with the organization's business drivers? This can be particularly problematic when risk assessments are performed at the operational unit level—evaluation criteria that are important to the unit may not be in synch with the organization's business drivers. Thus, the consequences of risk are only measured with respect to the unit and not the organization as a whole.

CSFs can be used to mitigate some of these issues with evaluation criteria. For example, affinity analysis can be performed between CSFs and the impact areas being considered for inclusion in the risk evaluation criteria. This comparison is a means for validating that the evaluation criteria accurately reflect what is important to the organization. As a result, there is more assurance that the evaluation criteria being used in the risk assessment will reflect a more accurate representation of risk.

Figure 15 shows affinity analysis for validating evaluation criteria. In this example, the organization has decided that the impact area "productivity" is directly related to its ability to meet the "continually improve operational efficiency" CSF. Consequently, any risk that impacts the organization's productivity also impacts its ability to successfully meet this CSF.

Evaluation criteria	Critical Success Factors						
	Develop human resources	Manage compliance	Manage financial resources	Deploy information technology strategically	Continually improve operational efficiency	Perform strategic planning	Maximize teamwork
Reputation			X		X	X	
Life & health		X	X				
Fines & legal penalties			X				
Finance			X				
Productivity	X				X		X

Continous improvement of operational efficiency is dependent on productivity. As productivity is impacted, there is a direct effect on the "Continually improve operational efficiency" CSF.

Figure 15: Affinity Analysis for Validating Evaluation Criteria

5.3.2.6 Evaluating Threats and Mitigating Risk

Organizations are vulnerable to many different threats and risks. Which threats should an organization be concerned about? Which risks need to be mitigated? The purpose of applying a risk-based approach to assessment is to focus on only those threats and risks that could have a significant impact on the organization. Implicitly, a risk impacts the organization by impeding its ability to conduct its normal course of business and to achieve its goals. For example, a risk that results in negative publicity impacts an organization by interfering with its ability to keep its customer base, attract new customers, obtain financing, etc. However, the organization is really impacted only if these consequences affect business drivers—goals, objectives, mission, and CSFs.

Comparing threats and risks to CSFs identifies those that are strong candidates for mitigation. Thus, as an important component of business drivers, CSFs can help an organization to identify and prioritize threats and risks by providing additional criteria to evaluate the potential impact to the organization. Traditionally, in risk assessment methodologies such as OCTAVE, the organization's evaluation criteria are used to identify those risks that need to be mitigated. Using CSFs to determine which risks to mitigate can enhance this process because it provides an explicit tie to the organization's business drivers. This can make up for potential errors caused by poorly developed evaluation criteria or a misapplication of the criteria.

Risk mitigation is a burden on the organization that must be considered within the context of the potential benefits (i.e., prevention of risk or reduction of impact) that can be achieved. By using CSFs as a guide, an additional and important variable can be considered in the cost-benefit analysis of risk mitigation strategies.

Figure 16 provides an example of affinity analysis between CSFs and risks that have been identified for critical assets. In this example, the organization is stating that the threat of alteration of "employee records" directly impacts the ability to "manage compliance." If this risk is realized, the "manage compliance" CSF will be impacted, and thus the risk should be mitigated.

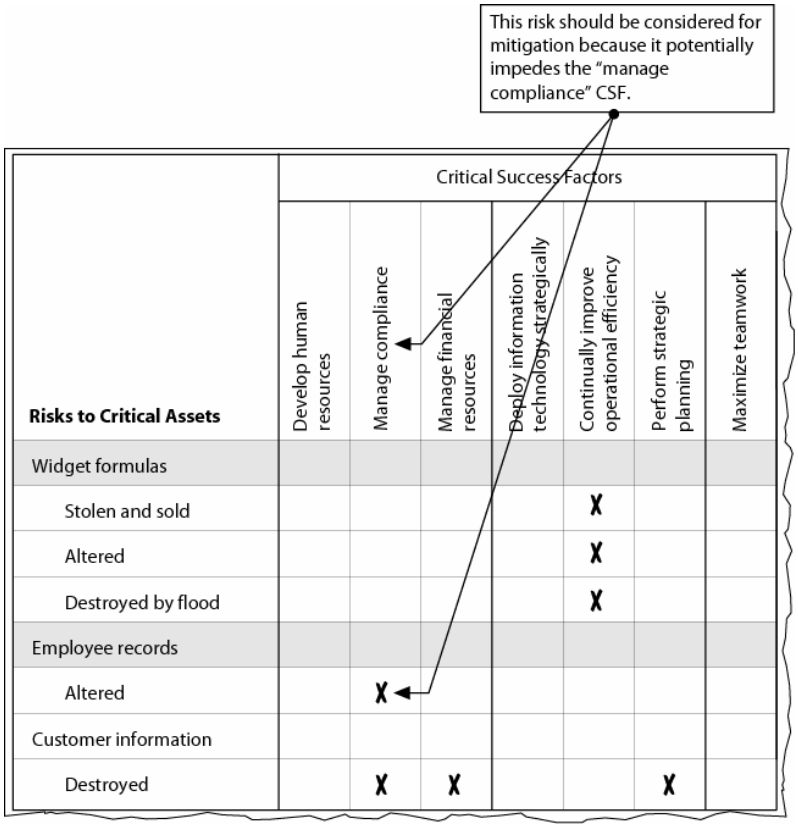


Figure 16: Affinity Analysis for Determining Which Risks to Mitigate

Appendix A CSF Method Description

In this section, we outline and describe our approach to developing organizational CSFs. This approach is largely based on the work of Rockhart and his colleagues; however, we have codified a more structured process for analyzing collected data and deriving CSFs.

It is important to note that our approach was applied and refined in two customer engagements with a primary focus on risk management and security. Therefore, our description of the method is aimed at deriving a set of enterprise CSFs that can be used to align security goals, objectives, and activities with the strategic direction of the organization. With slight modification, our approach can be used to align any important organizational initiative with the strategic direction of the organization.

Introduction

The goal of the CSF method is to tap the knowledge and intuition of the organization's managers. Many experienced managers act with a "sixth sense" that makes them successful. The CSF method attempts to make this "sixth sense" explicit so the organization can use it as an aid in setting strategic direction and in directing resources to those activities that can make it successful.

Thus, CSFs are actually *derived* from the organization rather than created. (Every organization already has a set of CSFs but may not know them. This is certainly true of industry CSFs that the organization inherits.) The CSF method is a way to harvest these factors from a review and analysis of the goals and objectives of key management personnel in the organization. They are also shaped by talking with key management personnel about what is important in their specific domain and discussing the barriers they encounter in achieving their goals and objectives.

Document review and interviews provide the basic raw data for deriving an organization's CSFs. To perform the CSF method, this information is formed into statements that represent the activities that key managers perform or, sometimes more importantly, should be performing. These statements are analyzed and placed into affinity groupings from which the CSFs are derived.

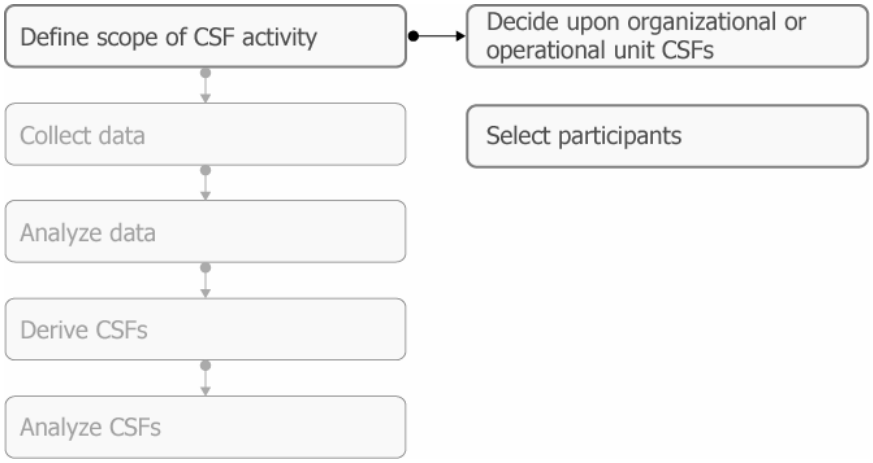
To describe the CSF method, we have identified five basic activities:

- defining scope
- collecting data
- analyzing data
- deriving CSFs
- analyzing CSFs

Each of these activities, along with the steps necessary, is provided in the following sections. Throughout the activities, we distinguish the steps where necessary depending on whether a set of enterprise CSFs or operational unit CSFs are being developed.

Activity One: Defining the CSF Scope

There are two primary steps in Activity One:



Because CSFs exist throughout the many layers of management in the organization, the hierarchy of CSFs (see Section 4.5) and the level of CSFs to be developed (i.e., enterprise or operational unit) must be considered when determining the scope for applying the CSF method. Once the CSF level is determined, the participants to be included in the exercise can be identified.

Defining the Appropriate CSF Type

In reality, enterprise CSFs are highly related to and derivative of the collective CSFs of the organization's operational units. However, many organizations who want to use the CSF method may not have time to derive the CSFs of each of their operational units. Instead, they will want to create a set of enterprise CSFs that are *representative* of the operational units of the organization.

There are a few factors that can be considered when determining which level of CSFs to develop. For example, if the organization's structure is flat (i.e., there are not many layers of management), a set of enterprise CSFs may in fact be highly representative of the operational units of the organization. In addition, if the purpose of deriving CSFs is to provide a comprehensive and consistent guide that can be used across the organization to align activities with the organization's strategic direction, a set of enterprise CSFs will be appropriate.

On the other hand, if the organization has many layers of management, and many divisions that are each involved in different industries, it is best to develop operational unit CSFs because each operational unit is essentially a separate, functioning organization. For example, a natural gas company that is involved in many segments of the industry, such as drilling wells and producing natural gas (production), moving natural gas from the well to regional delivery points (transportation), and delivering natural gas to customer locations (delivery), may have three very distinct sets of CSFs at the operational unit level. All of the operational unit CSFs would influence the CSFs for the organization as a whole, and in some cases might be identical.

Defining Scope

Enterprise CSFs

To create a set of enterprise CSFs, the scope of the exercise must traverse the entire organization so the domain of each executive-level manager is included and considered. Each operational unit must be represented either by including managers from that unit or the executive-level manager who has responsibility for a particular operational unit or units. Some organizations have a corporate office or headquarters that is responsible for all lines of business and each operational unit. In this case, the corporate office should be included in the scope.

In addition, enterprise CSFs are most likely to be influenced by or to include industry CSFs, so these must be developed and integrated to the organizational CSFs as well.[20]

Keep in mind that in some organizations it makes sense to develop operational unit CSFs and use them as a source for the development of enterprise CSFs. An acceptable shortcut for many organizations is to create only a set of enterprise CSFs—so long as consideration is given to ensuring that the enterprise CSFs accurately reflect the organization's operational units as well.

[20] We do not provide any explicit guidance for developing industry CSFs in this document. However, experienced executives generally identify some industry CSFs because they are part of their management domain. Other sources of industry CSFs could include trade or professional groups that represent a particular industry or a review of competitor/peer CSFs if available.

Operational Unit CSFs

If a set of operational unit CSFs is being developed, the scope of the exercise may be limited to the operational unit and some of the corporate or organizational areas that are important to the operational unit's success. Thus, when focusing on an operational unit, it may only be necessary to include managers within the particular operational unit and their representatives at the executive level of the organization. However, because some operational units are often dependent on others (for example, where corporate services are provided to subordinate units), it may also be necessary to expand the scope of the CSF exercise to include other specific operational units as appropriate.

In addition, the CSFs of individual managers[21] in the operational unit may be important to developing the CSFs at the operational unit level.

Selecting Participants

Determining who to include as participants in the CSF activity is dependent on several considerations:

- the type of CSFs being developed (enterprise or operational unit)
- the structure of the organization (many layers vs. a flat structure)
- the unique operating conditions of the organization (international presence, large divisions in different industries, etc.)
- the purpose and objective for developing CSFs

Each of these is explored in more detail below.

CSF Type

The type of CSFs being developed strongly influences decisions about whom to include in the CSF activity.

Enterprise CSFs

For enterprise CSFs, the broad perspective of executive-level and other senior managers in the organization is vitally important to deriving a set of valid and representative CSFs. Thus, consideration should be given to including personnel that represent the following areas:

[21] Rockhart speaks of the concept of individual manager CSFs in his work. This refers generically to the CSFs that are important to each manager in the organization. However, depending on his or her position in the organization, a manager's CSFs are likely to be the same as the CSFs at the operational unit level over which the manager has responsibility. In lower levels of the organization, line managers, for example, may have their own unique CSFs, but it is likely that they also reflect most of the CSFs for the operational unit as well. If individual managers have developed their own CSFs, they can certainly be used as input to the development of the CSFs for the operational unit, but may not be necessary.

- c-level executives (CEO, CFO, chief operating officer, CIO, CSO [22])
- vice president and other director-level personnel
- division heads (or the equivalent of divisional CEOs or presidents), particularly if the organization is involved in diverse industries or has international divisions
- unique *roles* in the organization, including
  - vice president of internal auditing or general auditor
  - chief legal counsel or general counsel (whether internal or external to the organization)
  - corporate secretary
  - vice president of investor relations or similar role
  - vice president (or similar level) for merger and acquisition activities
  - vice president (or similar level) for marketing and sales
  - vice president (or similar level) for public relations and affairs
  - strategic planners, both financial and operational
- unique *functions* in the organization, including
  - asset management
  - corporate reporting and taxes
  - risk management
  - controller and treasurer
  - government and regulatory relations, including lobbyists, etc.
- select members of the board of directors or trustees, such as the heads of various board committees (such as the audit committee) or the chairman of the board
- significant external personnel, particularly if primary business functions such as information technology or legal have been outsourced or where advisors have been brought into the organization to help shape and execute strategic direction

Operational Unit CSFs

For operational unit CSFs, the broad perspective of senior managers in the *operational unit* is necessary. This requires the inclusion of high-level managers in the unit as well as first-level supervisors. It is also important when developing operational unit CSFs to remember that the operational unit is part of the larger organization, so inclusion of some of the positions and roles noted above may be helpful as well.

[22] The perspective of a CSO can be very valuable, particularly if the CSFs are to be used in guiding the organization's security strategy.

Organizational Structure

The organization's structure also influences the selection of participants. A hierarchical organizational structure tends to have more functional areas and executive-level roles (such as those noted above for organizational CSFs). Thus, there is a larger pool of available personnel that can be included in the CSF activity.

On the other hand, an organizational structure that is flat (i.e., personnel have many similar, homogeneous roles) presents a bigger challenge for selecting participants because there are generally fewer specifically defined functions. For example, a research organization may have hundreds of employees who are essentially employed in similar jobs but perform these jobs to varying degrees and in different subject matter areas. In this case, consideration should be given to choosing personnel based on their unique role or contribution in the organization rather than their title or job level.

Operating Conditions

Some organizations do not have complex operating conditions—that is, they are generally involved in a single line of business or focus and are located in few geographical areas. For example, a county government is in operation to serve the needs of citizens (a single purpose) and is generally contained in a limited geographical area (the county in which it provides services).

However, other organizations essentially comprise many "mini-organizations" that act according to their own strategic direction and goals. For example, this is found frequently in

- large, multinational corporations that are involved in many lines of business or have divisions located in many countries
- organizations with very distinct operating lines
- organizations with other natural divisions or groupings of functions, such as universities with distinct schools and support organizations

Whenever these types of organizations are encountered, consideration must be given to including personnel not only from the operating unit but also in higher levels of the organization such as the corporate office or headquarters. This will provide both operating unit and enterprise perspectives.

Purpose and Objective

The goals for developing a set of CSFs can also affect the selection of participants. For example, if the CSFs will be used to influence the strategic direction of the organization or to help it diagnose and correct problems, a broader, more general perspective may be appropriate. Thus, consideration should be given to covering the horizontal dimension of the organi-

zation, but not going very deeply into any one area. This is a common approach when developing a set of enterprise CSFs.

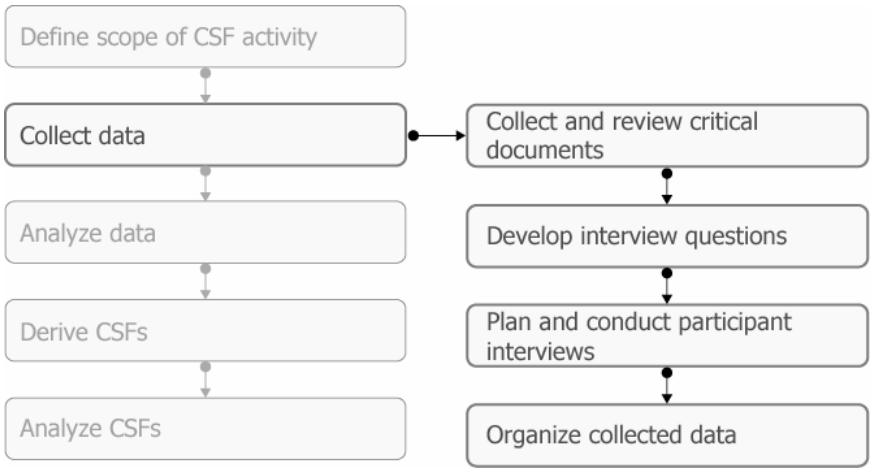
However, if the focus is on an operational unit, the purpose may be to reset the operating objectives and goals of the unit and to bring them in line with the broader goals of the organization. In this case, the selection of participants should be robust enough to support all layers of functionality in the operational unit.

Other Considerations

Because much of the raw data for developing CSFs comes from personnel in the organization, selecting the right participants for the CSF activity is very important to success. Reflecting the various roles in the organization or operational unit may be far more productive than focusing on particular positions or personnel. In addition, including more participants as a way of ensuring that enough data is gathered should be considered. The process of deriving CSFs is data analysis-centric, and having more data (rather than a smaller quantity of high-quality data) is not necessarily a benefit. Include participants if their perspective is important and their role is vital to the organization or the operational unit in meeting their respective missions, goals, and objectives. However, failing to identify all of the necessary participants up front will not impede the CSF activity; other important participants may be identified as interviews are conducted and can be included in the activity later.

Activity Two: Collecting Data

There are four primary steps in Activity Two:



These steps are centered on two means for obtaining the data needed to derive CSFs: reviewing critical documents and conducting interviews. Each of these data collection techniques is discussed in this section. Where possible, both of these data gathering techniques should be

used; however, if only one technique is to be used, it is preferable that personnel interviews form the basis for data collection.

Other data collection methods can be used, such as questionnaires and surveys, but these techniques can introduce bias and impede dialog and thus are not recommended.

Performing a Document Review

A document review is a very effective means for obtaining an understanding of the focus and direction of an organization or operational unit. Most organizations document their purpose, vision, and values in a mission statement that is known to all employees. In addition, many organizations have a formal process for documenting short- and long-term strategies, as well as the related goals and objectives of personnel for achieving these strategies. All of this information provides a good foundation for determining the activities that are most important to managers and to which they devote much of their time.

A document review, for the purposes of defining CSFs, can include an examination of the following:

- the stated, documented mission and vision of the organization and/or operational unit
- the stated goals and objectives for the current year (fiscal or calendar) for participants in the CSF activity
- performance metrics that have been gathered against any stated goals and objectives
- the organizational or operational unit short-term plan or long-term strategic plan
- internal auditing reports or relevant subject matter
- annual reports and similar documents
- industry reports for the primary industry in which the organization operates[23]
- existing CSFs[24]
- CSFs of peer or industry organizations

In some cases these documents will not be available, and therefore a document review will not be possible. This will affect the data collection process but can be mitigated by appropriate planning and execution of participant interviews.

---

[23] Industry reports can be a good source of industry CSFs.

[24] If the organization has performed a CSF activity in the past and is actively using a set of CSFs, this can be valuable input to a future CSF activity. One caution: reviewing existing CSFs can result in a propensity to affirm existing CSFs rather than to use the process to develop a new set. This bias should be considered before existing CSFs are reviewed.

Conducting Interviews

The most important data collection activity is conducting interviews with participants. In this activity, the participants have an opportunity to talk about their management challenges and their contributions to the organization and/or the operational unit's successes and failures. The interactive nature of the interview process provides opportunities for clarification and for guiding the interview in areas that might expose particular barriers and obstacles to accomplishing the mission.

Interview Process

One of the purposes of Rockhart's primer on CSFs was to codify the information gathering and analysis techniques for developing CSFs [Rockhart 81]. In particular, Rockhart provided detailed instructions on conducting a CSF interview. Appropriately, this included several suggestions on effective interviewing and a set of questions that are directly intended to elicit CSFs.

In our experience in applying the CSF method, we made modifications to both the processes of eliciting data and analyzing it to derive CSFs. Rockhart's original work asserts that CSFs can be developed and documented during the interview in such detail that they can be restated to participants for their confirmation or correction [Rockhart 81]. However, we have found that producing CSFs is a more involved process.

Rockhart's method requires the interview team to explicitly ask a participant to describe his or her CSFs. However, meaningful answers to this question are highly dependent on the participant's level of familiarity with CSFs and, further, that their definition of CSFs is consistent with that of the interview team. Because the concept of CSFs can be difficult to grasp, the likelihood of success using this method is low in our opinion.[25] We have found that significant additional analysis is required to create a set of CSFs for an individual manager and that this work is generally performed after the CSF interview.

In our view, it is more effective to help the manager draw out his or her set of CSFs through a process of interviewing and discussion. Rockhart developed a series of questions that can be used for this purpose, but his original objective was to use these questions to assist in facilitating a difficult interview [Rockhart 81]. We consider Rockhart's questions to be an integral part of the process for deriving CSFs and recommend that they play a stronger part in shaping and conducting the interview. (More information on Rockhart's questions is presented in Table 2, which is included later in this section.)

[25] One of the major problems with this method is that it doesn't ensure a good mix of CSFs across the various sources unless the manager fully understands the nature of CSFs.

Interview Considerations

Before beginning the interview process, there are a few areas that require further consideration.

Order of Interviews

There is no prescribed order for interviewing participants. This is highly dependent on the organization or operational unit for which CSFs are being developed. However, in our experience with CSFs (and with risk assessment data collection), it is sometimes desirable to interview senior personnel first. They often can provide insight and information that is important to keep in mind as other interviews are conducted with lower level staff. Executive-level managers can also provide guidance on additional personnel who should be included in the interview schedule earlier in the process.

Interview Team

In this document, we do not provide any specific guidance in assembling an interview team or, more importantly, a CSF activity team.[26] However, those conducting the interviews should be comfortable asking questions of managers who may be either higher or lower in the organizational hierarchy. The interviewer must also not be so scripted as to prevent a spontaneous dialog to unfold. The interviewer should always be prepared to follow structured questions with follow-up, clarifying questions, so an ability to quickly comprehend and restate the participant's responses is vital. Finally, the interviewer must be comfortable acting as a facilitator, using reasonable judgment to determine how to allocate time most effectively during the interview. The most undesirable outcome of an interview is to run short on time without gathering vital information—the participant may not be willing to extend the interview or set up a follow-up interview.

Interview Etiquette

There are several key behaviors that will ensure success in the interview.

1. **Use engaged listening.**

   Participants will tend to respond to questions as thoughts come to mind, so it is important to stay engaged and ask follow-up and clarification questions as necessary. In addition, be aware of non-verbal clues that provide additional information. Often, non-verbal clues tell a story that participants may not choose to verbalize.

[26] The selection of a CSF activity team is addressed in "Final Considerations" at the end of this appendix.

2. **Avoid leading the responses of participants.**

   If the same personnel are involved in conducting all participant interviews, there is a tendency in later interviews to prompt participants into providing answers that confirm observations or conclusions that have already been drawn. It is easy to become biased as more interviews are conducted, and all efforts should be made to keep this bias out of the later interviews.

3. **Do not position the interview as an audit, an assessment, or an examination.**

   The purpose of the interview is not to gather information to render an opinion on the effectiveness of managers and their operational domain. Participants should understand that the interview is one of their contributions to the CSF activity, which is vitally important to the long-term survival of the organization.

4. **Ensure that participants understand that their input is confidential.**

   Participants will be more likely to freely provide accurate and meaningful information if they are assured that this information will not be directly attributed to them. It should be clear to participants that their input is confidential and, to the extent possible, will be used in a way that does not directly implicate them. This is especially important when interviewing lower-level management—they may be concerned that their input could be provided to their superiors without proper context or intent.

Preparing for the Interview

Because of the importance of the interview activity to developing solid CSFs, there are a number of preparatory activities and techniques that should be considered:

1. **Review documents such as the participant's goals and objectives, if available, before the interview.**

   This will provide a fresh view of the conditions and constraints under which the manager operates and could provide additional follow-up questions during the interview. At the very least, being able to speak comfortably about the participant's sphere of influence will show a sincere interest in the participant's viewpoint and open the door to a productive conversation. Note any areas in documents that need to be clarified so that this can be accomplished during the interview as well.

2. **Keep the interview as short as possible and to the point.**

   The interviewer must balance keeping the interview on track with the additional information that might be gained in general conversation. Participants are more likely to buy into the CSF process if it appears to them to be productive and professional. A suggestion is to aim for a 30-minute interview but not to exceed one hour.

3. **Conduct interviews one-on-one where possible.**

   Group interviews, particularly among operating peers, can be very effective because participants can build from each other's responses. However, there are also some disadvantages to a group interview, including the potential that some participants will not discuss their area of responsibility and expertise openly. In addition, some participants may want to divulge concerns or barriers in the organization and may not want to have this information attributed to them after the interview. Finally, in group settings, less assertive participants may be intimidated and will resort to just nodding to the comments of others. This defeats the aim of the interview.

4. **Develop a robust, consistent set of questions for the interview.**

   Do not rely on having a general conversation where, for example, the participant's goals and objectives are discussed. The interview should be scripted and participants should know what to expect throughout. Also, use open-ended interview questions. Open-ended questions encourage discussion and thought and facilitate stream of consciousness thinking. (A set of candidate questions is provided in Table 2 and Table 3.)

5. **Enlist a scribe or use another method to capture the details of the interview.**

   Attempting to take notes and to facilitate an interview at the same time is very difficult and can disrupt the natural flow of the conversation. Notes taken in the interview are very important to developing CSFs, so they must be accurate and complete. Recording the interview session either by scribing it to paper or recording it (if approved by the participants) should be strongly considered.

Conducting the Interview

Based on Rockhart's guidance [Rockhart 81] and our field experience with the method, the following procedure is recommended for conducting a CSF interview:[27]

1. **State the purpose of the interview.**

   The participant in the CSF interview must understand the purpose of the interview and the larger CSF activity. Clarify, if necessary, that the activity is not an assessment or an audit.

   If possible, it is a good idea to provide reading material in advance that describes CSFs and the process used to develop them. If it is clear that the participant doesn't understand the purpose and outcome of the CSF activity, this should be discussed before proceeding. Be clear as well on the type of CSFs being developed—enterprise or operational unit—and keep the interview properly focused.

[27] There are many commercially available structured interviewing techniques that can assist in this process. The procedure recommended here was used in our application of the CSF technique and should be considered even if a structured interview technique is used.

2. **Clarify the participant's view of the organization or operational unit's mission.**

   Setting a common context for the interview will help to keep it focused and properly scoped. If the participant's view of the organization or operational unit's purpose is skewed, it will affect the responses they provide to the interview questions. Obtaining this information up front will provide insight to the interviewer and can prompt additional clarification questions later in the interview.

3. **Clarify the participant's view of his or her role in the organization or operational unit.**

   It is important to understand the participant's view of the world. It explains his or her unique context and provides the underlying premise for the types of CSFs he or she identifies. This information can be helpful later when analyzing interview notes and deriving CSFs.

4. **Discuss the participant's goals and objectives.**

   If a document review has not been performed, it is vitally important to obtain a concise understanding of the participant's short- and long-term goals and objectives. This provides some of the raw data for developing CSFs, as well as an indication of the participant's role and importance in the larger organizational or operational unit goals.

5. **Ask a series of open-ended questions to elicit CSF data.**

   Responses to these questions provide much of the core data needed for analysis and development of CSFs. As noted above, avoid leading the participant by asking questions that reflect information or data gathered in previous interviews. In the case where an interview must be cut short, this step is the most important and should be completed.

6. **Summarize the interview by playing back the important points.**

   It is a good idea to summarize and paraphrase the interview before closing. This gives the participant an opportunity to correct any inaccurate data (or assumptions) that have been recorded as well as to prompt them for additional details if necessary. Remember, this step is difficult if a scribe is not available to record the interview session. Also, look at the types of information received—does it cover industry, peer, environment, temporal, and management-function responsibilities? If not, ask clarifying questions at this point.

7. **Ask for priority.**

   Where possible throughout the interview and at the close, ask the participants for prioritization of important details, particularly if goals or CSFs are provided. This is one way to sift through all of the details collected throughout the interview and to focus on the truly critical data.

8. **Ask for measures.**

   If possible, ask the participants for any measures they have implemented to determine if they are meeting their goals, objectives, and, if known, CSFs. This may provide further insight into whether they are achieving less-important goals in lieu of those that can impact the organization if left unaccomplished.

9. **Reserve the right to follow up and get confirmation of interview notes if necessary.**

   At the close of the interview it is a good idea to set the expectation that the participant will continue to be involved in the process as CSFs are created. Obtain approval from the participant to reconnect at several points in the process.

After the Interview

After each interview, it is important to obtain the notes taken by personnel involved in the CSF interview and consolidate where possible. In addition, reviewing notes immediately after a CSF interview provides an opportunity to add more detail because the experience is recent. It will be more difficult to do this after many CSF interviews have been conducted over an elapsed period of time.

Interview Questions

During the CSF interview, a series of questions can be asked to help managers to identify their CSFs. Simply asking the question "What are your critical success factors?" is only successful if the manager understands the CSF concept and has the same definition as that being used to guide the activity. Thus, several open-ended questions can be posed to help participants think about those areas of their responsibility that are most important and must be done well.

In Rockhart's primer on CSFs, a series of questions[28] is provided that can accomplish this task [Rockhart 81]. We used these questions in our application of the CSF method, with a few variations. Table 2 and Table 3 provide a list of Rockhart's questions and our own, along with explanations on the intent of the questions, the sources of CSFs that the questions are most likely to address, and the relationship to the two types of CSFs—enterprise and operational unit—that we have identified.

[28] One note of caution: to ensure consistency of responses, the same set of questions should be used for all participants. The questions to be used should be decided on before interviewing begins and should be asked of all participants.

Table 2: CSF Interview Questions Proposed by Rockhart[29]

Interview Question	Intent	CSF Source	CSF Type
What are the critical success factors in your job right now?	The intent of this question is to directly elicit CSFs from the participant. However, meaningful responses are highly dependent on the participant's understanding of the CSF concept and the consistency of the participant's definition to those conducting the CSF activity.	This question can identify CSFs from all sources—industry, peer, temporal, etc.—depending on the perspective of the participant.	This question can identify both enterprise and operational unit CSFs, depending on the manager's perspective and the scope of the CSF activity.
In what one, two, or three areas would failure to perform well hurt you the most?	This question helps to draw out CSFs from a different perspective—by getting participants to think about possible failures that would interfere with or interrupt their ability to achieve their goals and mission. Answers to this question generally reflect CSFs for the manager.	Industry, peer, environmental, and temporal CSFs are more likely sources than management-function CSFs.	At the organizational level, this question can bring about a distinct set of enterprise CSFs that the entire organization should be mindful of, particularly if they are repeated by different participants across various interviews.

[29] These questions appear in Rockhart's codification of the CSF method [Rockhart 81].

Interview Question	Intent	CSF Source	CSF Type
In what area would you hate to see something go wrong?	The implication of this question is that the participant will identify areas where poor performance might interfere with achieving goals and accomplishing the mission. This question gets to the impact of failure and where the impact would be most felt and destructive. If the impact is on achieving goals or mission, it may signify a CSF.	Industry, peer, environmental, and temporal CSFs are more likely than management-function CSFs.	Depending on the manager's level, this question might be very useful for identifying operational unit CSFs.
Assume you are placed in a dark room with no access to the outside world, except for daily food and water. What would you most want to know about the organization when you came out three months later?	The purpose of this question is to identify what is most important to the manager. By providing a scenario where the manager "must take their eyes off of the road," a manager can reflect abstractly on their role and articulate what parts of their information dashboard they most need to pay attention to.	This question might identify industry and peer CSFs because of the focus on attempting to get reacquainted with the organization's industry and competitive position.	This question is beneficial for identifying enterprise CSFs.

Table 3: Additional Interview Questions to Consider[30]

Interview Question	Intent	CSF Source	CSF Type
What is your personal mission and role in the organization?	This question helps to set context for the remainder of the participant's responses. For example, if senior managers have different views of what they are there to accomplish, it provides insight into the things that they consider to be most critical. Often, a particular manager has a CSF that appears to be out of line with the rest of management and management's goals. Responses to this question can help to identify such CSFs during analysis so that a determination can be made as to whether they are something the entire organization or operational unit should be concerned about.	May be useful for identifying industry, peer, or environmental CSFs, depending on the level of the participant being interviewed. Management-function CSFs may also be identified if the participant focuses on the unique role they play in the organization or operational unit.	Either enterprise or operational unit CSFs can be identified by this question.

[30] We developed and used these questions, along with the Rockhart suggestions shown in Table 2, in our application of the CSF method with customers.

Interview Question	Intent	CSF Source	CSF Type
What are your most critical goals and objectives?	This question is very important if there are no documents to review before the interview. In addition, this question is highly recommended if the organization does not have a formal goal setting and performance management process. Responses to this question often characterize what an individual manager believes is his or her role, which may be completely out of line with what is expected or necessary to help the organization or operational unit accomplish its mission.	Highly useful for identifying temporal CSFs if managers have short-term goals related to operating conditions, seasonality, etc. Could bring about industry CSFs depending on the management level of the participant. Management-function CSFs are also possible, particularly if the manager holds a common role (such as Manager, Accounts Payable).	Depending on the management level of the participant, both enterprise and operational unit CSFs are possible.

Interview Question	Intent	CSF Source	CSF Type
What are your three greatest business problems or obstacles?	This question is essential for identifying CSFs that the individual manager, organization, or operational unit may not be aware of explicitly. By considering opportunities or accomplishments that are impeded because of obstacles, this question can identify not only those CSFs that are in the manager's scope of view but those he or she may not have thought about.	Many temporal CSFs can be derived from this question, but industry, peer, and environmental are possible as well. Management-function CSFs might be identified if the manager feels that the position he or she holds is a barrier to effectively meeting his or her goals and objectives in the organization.	Depending on the management level of the participant, both enterprise and operational unit CSFs are possible.

Data Consolidation and Preparation for Analysis

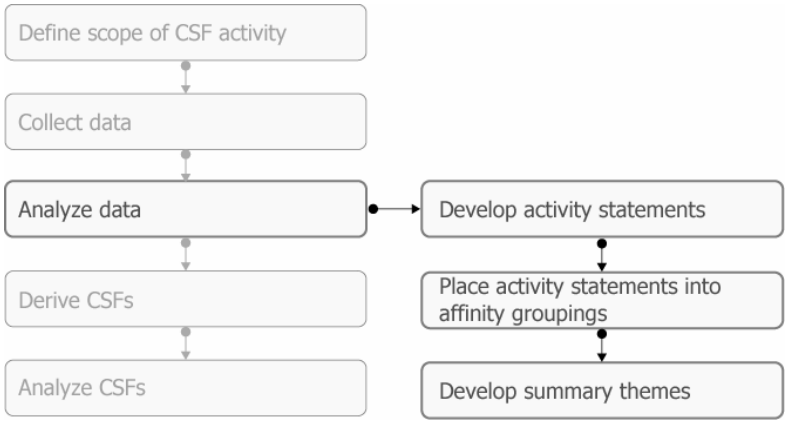
Document review and interview notes provide the core data for developing CSFs. Thus, all of the documents collected and the interview notes that have been recorded must be compiled and organized to facilitate analysis. There is no prescribed means for doing this; however, a few suggestions can be offered to ensure collected data is ready for the analysis activities:

- Group common pieces of data. If managers' goals and objectives are collected, keep them together and arrange them in a way that groups similar organizational functions, management levels, or issues.[31] This may be very useful when performing analysis and deriving CSFs.
- Arrange interview notes into a common format so that similar information gathered across interviews can easily be located. In some cases, it can be effective to group together all of the responses for a particular question from all interview participants. When performing analysis, this may highlight particular trends or overall confirmation of important points and opinions.
- Scan the information for accuracy and completeness. If information is missing, it is a good idea to "fill in the blanks" now before the analysis process begins. Once analysis begins, it will be difficult to remain objective with participants when asking for additional information.

Once data has been arranged and checked for completeness, it can be analyzed and shaped into a set of CSFs.

Activity Three: Analysis

There are three primary steps in activity three:



[31] The questions used in CSF interviews attempt to draw out particular important aspects and challenges of management. One way to group data is by common response areas such as personnel issues, market issues, sponsorship and leadership, competition, etc. However, use caution with these groupings so that they are not used directly to develop CSFs without performing analysis activities.

The purpose of the analysis activity is to categorize and analyze raw data so that it can be used to derive CSFs. This requires some molding and shaping of raw data into the basic components of a CSF. This "normalization" process prepares data so that it is

- detached from the personnel who provided it (to avoid bias and attribution going forward),
- condensed to its essential meaning or thought (to eliminate ambiguity), and
- formed into manageable pieces or entities that can be analyzed.

In our application of the CSF method, we have found it useful to transform raw data into CSFs by using a series of repeatable and consistent processes, rather than relying on participants to directly identify CSFs. For our application of these processes, we created two important concepts: activity statements and supporting themes. We also made use of a common technique called affinity analysis as a structured means for working with activity statements and supporting themes. The use of affinity analysis provides not only a consistent process for deriving CSFs but also a self-correcting mechanism that affords the user many opportunities to re-examine analysis decisions without interjecting additional bias.

The concepts of activity statements and supporting themes are introduced below.

Activity Statements

Activity statements are statements that are harvested from interview notes and documents that reflect what managers do or believe they and the organization should be doing to ensure success. They collectively describe the operational goals, objectives, and activities performed by managers throughout the organization or in the operational unit that supports the existence and/or attainment of a CSF. It is important to note that activity statements can reflect something that the organization is already doing, paying attention to, or monitoring (as established in goals, objectives, or operational activities), or reflect something that the organization should be doing (such as barriers and challenges to effectiveness). Examples of activity statements include

- Comply with state and federal regulations.
- Manage migration to a new financial system.
- Train accounting staff.
- Increase customer sales by 10% this year.
- Focus on customer needs.
- Recognize core competencies.

As illustrated, in addition to reflecting operational goals and objectives, activity statements can represent a general action[32] that is being taken (or must be taken) to support goals or can convey a general sense of something that is beneficial to the organization.

The creation of activity statements is a technique for transforming raw data into manageable, consistent entities that can then be subjected to analysis to derive CSFs.

Supporting Themes

Supporting themes highlight the underlying content or intent of a CSF. In essence, supporting themes provide a description or definition of a CSF.

Supporting themes are drawn from an initial grouping and analysis of activity statements. For example, the following activity statements could be grouped and analyzed to derive supporting themes:

Table 4: Example of Activity Statements and Supporting Themes

Activity Statements	Supporting Themes
Maintain a qualified, properly-trained workforce. Ensure that personnel are technology literate and competent. Address diversity issues. Perform succession planning for key employees. Ensure that the organization is attractive to a demographically shrinking workforce. Monitor staffing changes and human resources issues. Empower employees and reduce micromanagement.	*Attract high-quality employees from the available workforce.* *Develop, train, and prepare employees to contribute to the growth and effectiveness of service delivery.* *Empower employees to act and take responsibility for their actions.*

Supporting themes essentially represent the intention and substance of the activity statements as they have been grouped together. However, there is no one-to-one relationship between

[32] Activity statements should reflect an action or activity. We do not provide a strict format for activity statements, but for consistency and usability we recommend that they begin with an action verb.

activity statements and supporting themes; supporting themes summarize the intention of the activity statements as an aid in deriving a CSF.

Developing Activity Statements

The first step in creating CSFs is to develop activity statements. These are created from the documents and interview notes that have been collected.

Using Document Review

Activity statements can be drawn directly, without much interpretation, from relevant documents provided by participants or the organization. Most often, the documents that will produce the majority of activity statements will be the organization's or the operational unit's mission, vision, or purpose statement and the individual managers' goals and objectives. Guidance for developing activity statements from each of these document sources is provided below.

Mission Statement

The organization (or operational unit's) mission statement is a rich source of broad-based activity statements. Often, the mission statement describes the vision and purpose of the organization and reflects the organization's values. For example, consider the mission statement for a large county government:

Our County Mission Statement

The mission of our county is to *provide progressive, service-oriented, responsible government* that is *responsible and accountable to the people* and their need for low-cost government. Our vision is to be a dynamic, service-driven organization *built on community values and needs, continuously improving the way local government does business.* To achieve this, our goals are to *create partnerships with common interest groups* and the people in our community, *accelerate infrastructure to meet growth* and challenges, *maximize service delivery and human resource utilization,* and to *ensure financial stability through a fair revenue and expenditure system.*

Figure 17: Sample Mission Statement

This mission statement can be summarized into several key activity statements:

- Focus on community values and needs.
- Continuously improve the way that local government does business.
- Provide progressive, service-oriented, responsible government.
- Remain responsive and accountable to the people.
- Create partnerships and relationships with common interest groups.
- Accelerate infrastructure to meet growth.
- Maximize service delivery.
- Maximize human resource utilization.
- Ensure financial stability.

Notice that these activity statements do not provide any information on *how* the mission, vision, and goals are going to be met—they are just broad statements of intention that characterize what is important to the organization. The following illustrates how the activity statements were derived from the county mission statement:

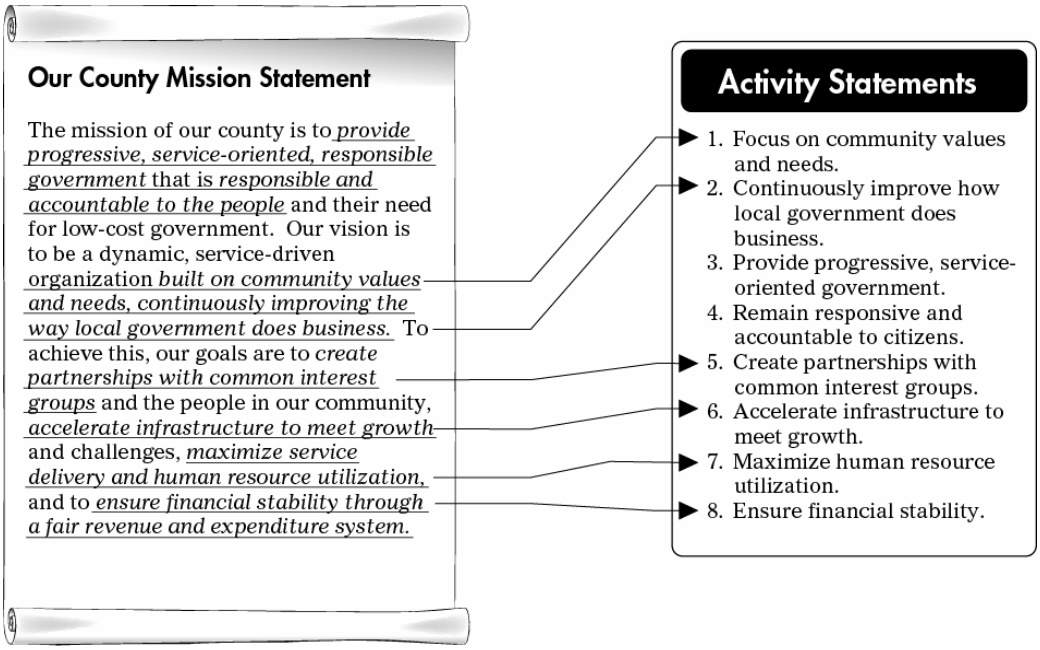


Figure 18: Example of Deriving Activity Statements from Mission

Goals and Objectives

The goals and objectives of managers generally prove to be an abundant source of activity statements. Ideally, a manager's goals and objectives depict statements of action or intention that the manager must accomplish to support the larger goals of the organization or opera-

tional unit. While performance goals tend to be more specific than the broad goals stated in the organization's mission, they can still be easily transformed directly into activity statements without much interpretation or alteration. For example, the following goals could easily pass for activity statements as well:

- Implement a HIPAA compliance program by 12/31/2003.
- Reduce labor costs by 30% by 1st quarter 2004.
- Increase participation in frequent flyer programs by 10%.
- Perform a risk assessment on the widget system by 3rd quarter 2005.

As stated, these goals could represent activity statements or could be altered[33] to remove specific performance metrics and focus on the intent of the goal. For example, "implement a HIPAA compliance program by 12/31/2003" could be restated as "ensure HIPAA compliance" to create a less specific activity statement that retains the underlying intent of the goal. However, this transformation may not be entirely necessary unless the underlying intent of the goal cannot be determined or is ambiguous. In this case, it is wise to talk with the individual manager (in the interview, for instance) and gain clarification.

Using Interview Notes

Obtaining activity statements from interview notes is a more difficult exercise because it requires some interpretation and over time may be affected by the biases of those performing the analysis. The main challenge in creating activity statements from interview notes is to ensure that the intent of the participant's responses to questions is captured and transformed into an activity statement.

Interview notes can provide several types of information from which to develop activity statements. Each must be considered differently.

Direct Statement of CSFs

In some cases, participants will directly provide a set of CSFs. There are reasons to be cautious when using this information.

- First, the statement may be based on the participant's unique perspective and may not fit the definition of a CSF. Thus, it may be a valid point, but should be put through the CSF process as a check. At a minimum, what appears to be a CSF can be considered an activity statement that will later support a higher-level CSF.
- Second, the participant may provide a valid CSF. However, it may be too soon in the process to determine whether the CSF provided will stand alone or be subsumed by a

[33] Alteration of goals and objectives should not result in changing the intent or to interject biases; rather, it can be used to eliminate extraneous information or provide clarification.

higher level CSF. Again, the CSF that is identified by the participant can constitute an activity statement (or supporting theme) that will eventually support a higher level CSF.

Responses to CSF questions

Participants will provide data in response to interview questions. This data must be carefully parsed and transformed into activity statements, which can be challenging.

- Frequently, participants don't provide complete information. The urge to "fill in the blanks" must be resisted; otherwise bias will be infused. If clarification is needed, talk to the participant.
- Participant responses may be ambiguous. Look to the intent of the interview question for clarification or, if necessary, talk to the participant.
- Sometimes participants answer a different question than the one that is asked or go back to previous questions and provide more information. This is not necessarily a problem unless the intent of the participant's responses cannot be determined. Again, in this case, ask the participant for clarification before using this data to develop activity statements.

Other information

Additional information is often provided during interviews. This information can be very valuable because it comes from the participant's stream of consciousness thinking during the interview. It can be turned into activity statements in much the same way as responses to interview questions. However, it may be harder to interpret the underlying meaning of the information because it is unsolicited and may lack context.

Example of Using Interview Notes

Consider the interview notes shown in Figure 19 in response to the question "In what two or three areas would failure hurt you the most?" There are many activity statements that can be extracted from the interview notes; some are straightforward and others must be interpreted as to intent. (Candidates are underlined.) In one instance during the interview, the manager points out what he believes to be a CSF for his department. This may or may not be a CSF for the organization.

Interview Notes – J. Brown

Q1: In what two or three areas would failure hurt you the most?

A1: Well, we must be careful not to use public funds inappropriately. Taxpayers don't take kindly to having their dollars wasted. This is also why we must keep an eye on our budgets and manage them wisely. By the way, we have an excellent finance manager to whom we can go to make sure we are keeping our financial commitments. The public perception of our agency is also very important. If we are seen as ineffective....

Figure 19: Example of CSF Interview Notes

Referring to the underlined areas in the interview notes, the following subset of activity statements can be created:

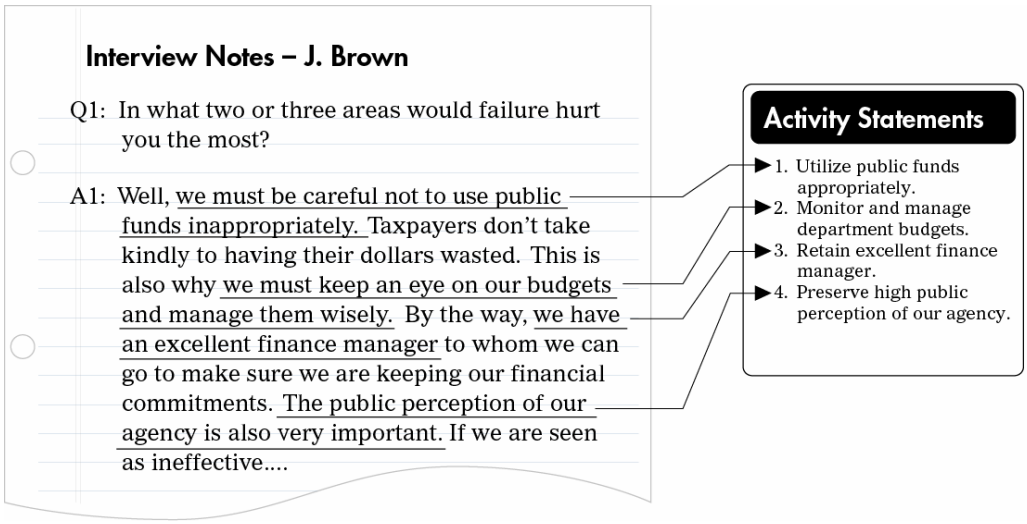


Figure 20: Example of Activity Statements Drawn from CSF Interview Notes

With practice, developing activity statements from interview notes becomes less difficult. However, it is important to periodically examine how activity statements are being derived to ensure that the process is not influenced by experience gained in earlier interviews. Over time, activity statements from different interviews may begin to look similar; this may be valid, but should be checked to ensure that the intent of the participant is captured accurately.

Activity statements should be developed for each participant for whom documents have been collected and an interview has been conducted. If no interview has been conducted, but relevant documents such as a manager's goals and objectives are available, the development of activity statements may still be possible. Good judgment should be used to determine whether the lack of a corresponding interview interferes with gathering sufficient and appropriate data from the participant.

Performing an Initial Affinity Grouping

The next step in creating CSFs is to perform an initial affinity grouping of the activity statements gathered from document review and interview notes. Simply stated, affinity grouping is a process for organizing ideas, thoughts, concepts, etc. It is a broadly used technique, often found in activities such as requirements elicitation for software development. Affinity grouping enables the categorization of data that share common characteristics, traits, or qualities so that a common description of the data can be developed.

Example of Affinity Grouping

To illustrate the affinity grouping concept, consider the following example. Suppose the following words represent 10 activity statements:

Activity Statements

1. Shetland
2. Doberman
3. Siamese
4. Poodle
5. Tabby
6. Zebra
7. Clydesdale
8. Calico
9. Cougar
10. Mule

Figure 21: Affinity Grouping Example – Activity Statements

As you examine these words, specific groupings begin to appear. If each activity statement is placed into a group that shares similar characteristics, the following groups might be created:

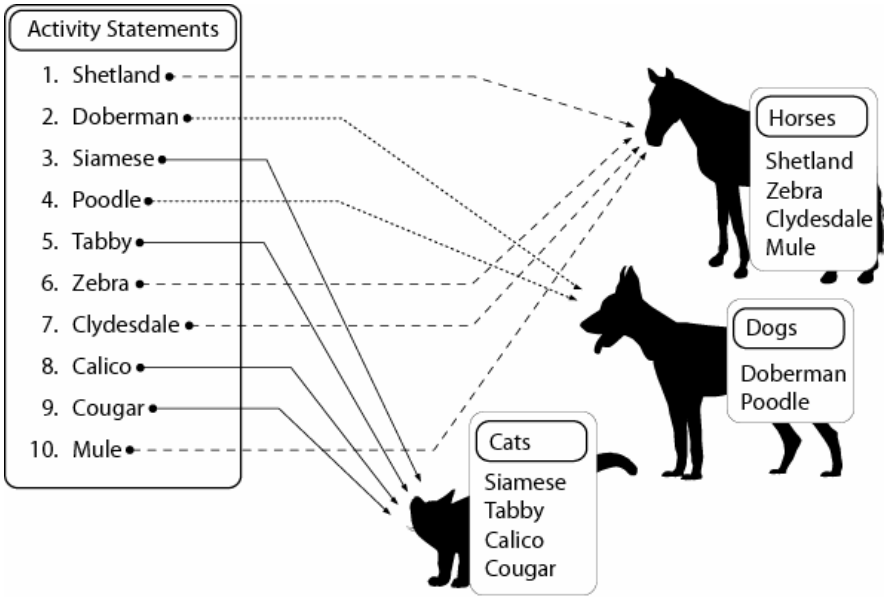


Figure 22: Affinity Grouping Example – Three Affinity Groups

However, in examining the groups that have been created, it is clear that we have accounted for the similar characteristics of the statements, but perhaps have not properly labeled the groups. A refinement of the group names might look like this:

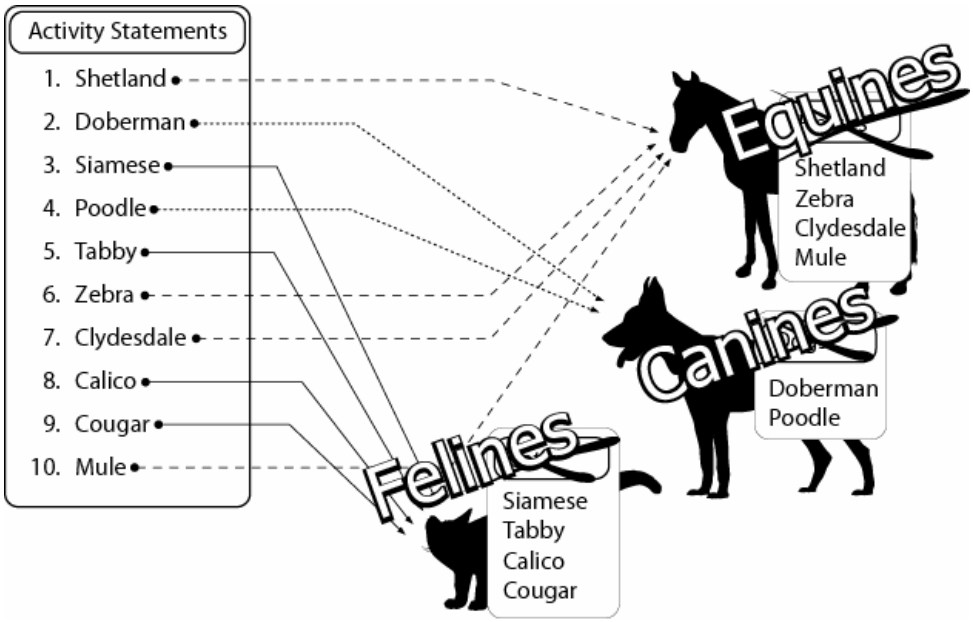


Figure 23: Affinity Grouping Example – Refined Groups

As a result of this exercise, the 10 original activity statements can be placed into three meaningful groups, each of which has its own distinct theme. In much the same way, activity statements can be grouped to begin to form themes that will eventually suggest CSFs.

Performing Affinity Grouping

CSFs tend to be more representative of the organization or operational unit when they are gleaned from raw data provided by managers, rather than from asking managers directly to identify their CSFs. The affinity grouping of activity statements is a way to summarize the core thoughts and concepts from managers regarding those activities they most need to pay attention to. Affinity grouping also provides a documented foundation for making decisions about which CSFs are created and why. Looking to the activity statements and supporting themes that support a particular CSF provides insight into why it was developed and how it is important to the organization or operational unit.

There are many existing techniques available for performing an affinity grouping activity. The extent to which a formal technique is necessary is dependent on the degree of precision required and other factors such as how many statements are being grouped, the number of persons involved in the activity, etc.

A simple process of affinity grouping may be all that is necessary to derive CSFs. The following is our suggested process for performing affinity grouping of activity statements:

1. **Mark the origin of each activity statement.**

   Later, it may be important to be able to trace back to the interview or document from which the activity statement was created. Thus, it is a good idea to tag each activity statement for origin. (One suggestion is to apply line numbers to interview notes and to use the line number and the participant's initials to identify the origin of the statement, such as "RAC22.") However, be careful not to make this origin tag so prominent a part of the activity statement that it becomes a primary criterion for categorizing activity statements. The core content, intention, or meaning should always be the primary driver for categorizing the activity statements.

2. **Use only the activity statements when creating affinity groupings.**

   The activity statements should be the only initial source for this activity. If an activity statement is difficult to categorize with other statements, it may need further clarification. This can be accomplished by referring to the raw data from which the activity statement was created, if necessary. Be careful, however, not to derail the grouping process by delving too deeply into the source data. The essence of the affinity grouping activity is to make immediately recognizable connections between somewhat disparate pieces of data.

3. **Work each activity statement individually.**

   The essence of the affinity grouping activity is to make immediately recognizable connections between similar data elements by using the core content, intention, or meaning portrayed by the activity statement as the primary decision criteria.

Each activity statement should be considered individually and placed into an affinity group. It is sometimes helpful to have several people consider each statement together and agree on placement in a group. If a statement cannot be grouped after reasonable consideration, it may appropriately indicate the creation of a new group. If not, place the statement aside and continue with the affinity grouping process.

4. Stabilize the affinity groups.

As a final check, once all activity statements have been grouped, each group should be examined to determine if subgroups are emerging and should be extracted. For example, during an affinity grouping activity (particularly when considering a large number of activity statements) the team performing the grouping may lose sight of the meaning of the groups it has created or may inadvertently change the definition of a group as the process unfolds. Eventually, this can result in the creation of groups that, in actuality, contain more than one distinct group. If this is the case, additional distinct groups should be separated. (One caution: looking for additional groups within a group is not the same as defining emerging themes that underlie or support all of the activity statements in a group. This activity is referred to as "developing supporting themes," and is the final abstraction required to create CSFs.)

In addition, this is a good time to consider duplicate activity statements. Duplicate statements (particularly if they are from different participants) can serve to confirm a particular affinity group, and later a CSF. However, duplicates can be eliminated if necessary. Also, consideration should be given to the traceability of the activity statements at this point. Moving forward, the origin of the statement should be removed (certainly before presentation to the organization), but it is a good idea to keep a copy of the groups with origin information in case further analysis is required later in the process.

5. Address any left over activity statements or small groups of statements.

After the affinity grouping exercise, a set of activity statements may remain that cannot be placed into a group.[34] Each statement that doesn't fit into a group must be re-examined. In some cases, several remaining statements will form a new group; however, there is a possibility that some will never fit into a group. For those that cannot be grouped, a decision must be made as to their value. Keep in mind that a single activity statement may be so compelling that it eventually defines its own CSF; conversely, an activity statement might be found to be extraneous, and a decision might be made to discard it.

[34] Groups that have fewer than two or three activity statements should be re-examined. These groups may need to be combined with other existing groups. Or, the activity statements in these groups may need to be assigned to one or more existing groups.

Developing Supporting Themes

A final step required before the development of CSFs is to develop supporting themes. Supporting themes represent a group of activity statements and will be used as the foundation from which to create the CSFs.

Developing supporting themes can be easy or difficult depending on a particular affinity grouping. In some cases, the supporting themes are readily apparent; in others, the themes must be developed through group discussion and, occasionally, by regrouping activity statements where necessary.

The objective of the supporting themes activity is to draw out the underlying concepts or intentions that represent the activity statements in a particular grouping (and will eventually represent a CSF.) This is best illustrated through an example. Consider the following affinity grouping of activity statements:

Affinity Group #1

1. Manage migration from legacy systems.
2. Position IT as a partner to business and operational units.
3. Attain efficiencies in service delivery through e-commerce.
4. Implement new technologies to fulfill mission needs.
5. Position IT as an enabler of new initiatives and strategies.
6. Increase the number of e-commerce services provided this year by 15%.
7. Manage impacts on efficiency and effectiveness from use of legacy systems.
8. View IT as an investment, not an expense.

Figure 24: Example of CSF Affinity Grouping of Activity Statements

This affinity grouping contains statements that have "the use of technology as an enabler" as their underlying premise. However, within this affinity grouping, several subgroups emerge as well. Using these subgroups, a set of supporting themes can be created that collectively represents the activity statements that have been placed in this group. Thus, when these activity statements are rearranged by subgroup (common ideas or concepts), a few supporting themes emerge, as shown in the three tables of Figure 25.

Activity Statements	Supporting Theme 1
2. Position IT as a partner to business and operational units.	**Align information technology with strategic planning.**
5. Position IT as an enabler of new initiatives and strategies.	
8. View IT as an investment, not an expense.	

Activity Statements	Supporting Theme 2
3. Attain efficiencies in service delivery through e-commerce.	**Expand service delivery through e-commerce.**
6. Increase the number of e-commerce services provided this year by 15%.	

Activity Statements	Supporting Theme 3
1. Manage migration from legacy systems.	**Move away from people-intensive, legacy systems to newer technologies.**
4. Implement new technologies to fulfill mission needs.	
7. Manage impacts on efficiency and effectiveness from use of legacy systems.	

Figure 25: Example of Three Emerging Supporting Themes

At this point, the three supporting themes represent the eight activity statements that have been placed in the affinity grouping. Moving forward to the derivation of CSFs, these supporting themes will be easier to work with than the activity statements from which they are derived. The process of abstracting up to the supporting themes reduces the amount of data that must be interpreted and handled and reduces the potential for error later in the process.

Developing supporting themes is a somewhat subjective process. The objective is to develop a statement that represents or summarizes the underlying intent of the activity statements. For example, in Theme 1, the underlying intent of the activity statements is that the information technology efforts of the organization should be aligned with strategic planning so that information technology becomes an enabler of the organization, rather than a burden.

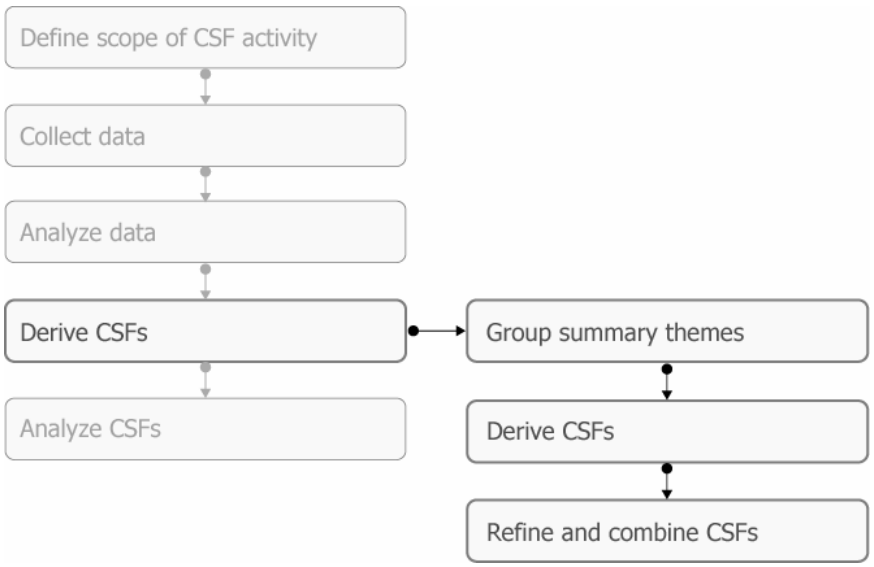
There are some additional considerations, however, for developing supporting themes.

1. During theme development, it may become apparent that a particular subgroup of activity statements no longer fits with the larger group from which it originated. This may indicate a need to separate the subgroup into its own affinity grouping or to place it in a different existing group. Using the emerging supporting themes to guide these decisions is a self-correcting mechanism that helps to double-check the accuracy of the initial affinity grouping exercise.
2. Sometimes, one or two activity statements may not appear to support a particular theme. When this occurs, it is wise to examine these statements and determine whether they support other themes or whether they may belong in a different affinity grouping. Again, in this case it is best to either find an affinity grouping that is a better fit or determine that the statement can be discarded.

Because the supporting themes activity is subjective, it may help to involve experts in the organization to obtain feedback on the emerging themes and advice on handling activity statements that cannot be grouped. For example, participants in the document review and interview processes might be able to assist by providing additional feedback and clarification on their comments.

Activity Four: Deriving CSFs

There are three primary steps in Activity Four:



CSFs are derived rather than created. They are extracted from raw data collected throughout the process and formed into activity statements, affinity groupings, and finally supporting themes. In our experience, we have found that CSFs can be derived easily based on supporting themes alone if the process described herein is followed.

CSFs seem to have more clarity, usability, and impact when they can be reduced to a brief, concise statement that captures the CSF's essential intent and description. For example, one of the reasons that mission statements often cannot be recited by employees is because they are generally too long and contain too much detail. A similar issue can be found with CSFs—if it takes hundreds of words and paragraphs to define a CSF, there's a good chance that it isn't a key performance factor that the organization can reasonably achieve.

In our method for creating CSFs, we have limited ourselves to as few words as possible (generally fewer than 10) when describing a CSF. For certain, a more detailed description of the meaning of the CSF, its origin, and potential impact on the organization can be developed, but won't be as useful or practical as a statement that can capture the CSF and can be easily recalled and communicated.

Affinity Grouping of Supporting Themes

Once supporting themes have been developed for each group of activity statements, it is important to perform an additional affinity grouping exercise using the supporting themes. This helps to bring together similar supporting themes into groups that will result in CSFs. Often, this is a simple exercise because many of the supporting themes that result from an affinity grouping of activity statements are already closely related. Where a theme is not related, it can be regrouped with other supporting themes that are a closer match. In this way, the process of performing affinity grouping of supporting themes essentially can correct any errors made in previous CSF activities. This is illustrated as follows:

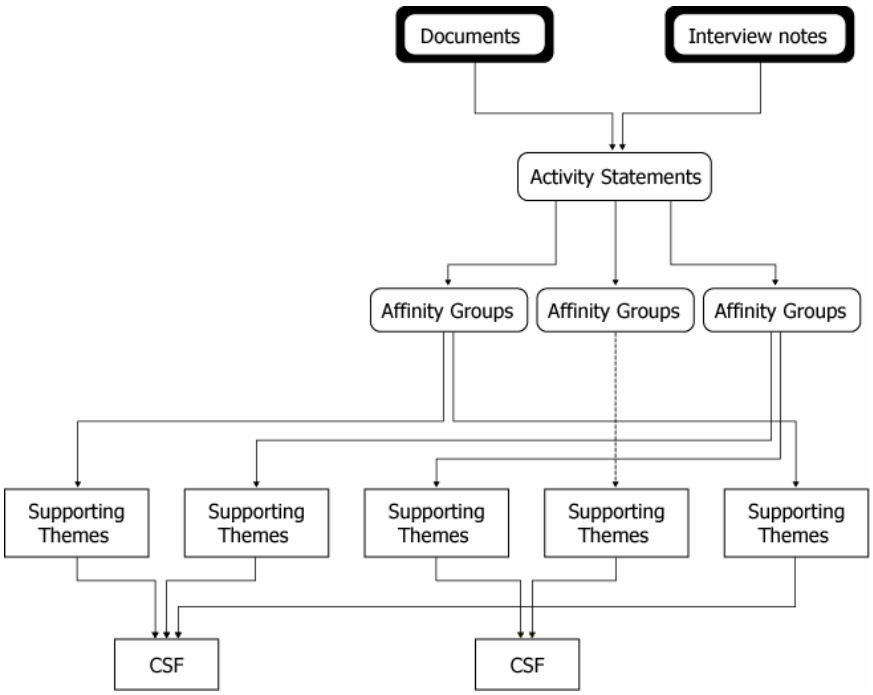


Figure 26: Illustration of Affinity Grouping of Supporting Themes

Deriving CSFs

A simple process for deriving CSFs is to use supporting themes as a guide. The reason for developing supporting themes is to represent, in as few summary statements as possible, the things that managers are concerned about as reflected in activity statements. If the process of creating supporting themes is done correctly, the resulting themes should provide enough insight to "name" a CSF. For example, consider the following summary themes:

- Align information technology with strategic planning.
- Expand service delivery through e-commerce.
- Move away from people-intensive, legacy systems to newer technologies.

These supporting themes communicate several key notions. For example, information technology is an important part of the organization. Second, it is important to create a solid relationship between the information technology activities of the organization and the organization's strategic plan. Finally, the organization must use new technology to help it expand and meet its mission.

In essence, these points describe a set of CSFs for the organization that can be restated more concisely as "Deploy information technology strategically." In this way, a CSF is derived from one or more supporting themes and is representative of the activity statements and affinity groupings that preceded it.

As an additional example, consider the following supporting themes that have been drawn from various affinity groups of activity statements:

- Attract high-quality employees from the available workforce.
- Develop, train, and prepare employees to contribute to the growth of the organization.
- Empower employees to act and take responsibility for their actions.

These supporting themes can be summarized into a single CSF for the organization: "Attract and develop human resources." This CSF suggests that the organization can meet its mission only by selecting and training the best employees available and by giving them the resources and decision-making capabilities they need. Achieving this CSF on a consistent basis will help the organization achieve its mission.

Deriving CSFs is a skill for which consistency can be gained through practice. The following are a few additional guidelines for success in deriving CSFs.

1. Let the supporting themes do the work.

If the other activities in the CSF process have been performed well, the supporting themes will accurately represent the operational environment of managers. Thus, supporting themes can be relied on to derive the CSFs. If this is not the case, then errors may have been made in developing activity statements, performing affinity groupings, or in developing supporting themes. Although most of the CSF process is self-correcting, bias can be introduced along the way and can eventually affect the CSFs that are derived.

In addition, be aware that there is no specified or intended cardinality between supporting themes and CSFs; that is, a CSF can be derived from a group of 20 supporting themes or just one supporting theme.[35]

[35] Some organizations may decide to conclude the CSF method at the point of development of supporting themes. In some cases, supporting themes may already fit the description of a critical success factor. However, this will result in a generous number of CSFs. Whether this is acceptable for an organization depends on how they will eventually use the CSFs. Abstracting from supporting themes to a smaller set of CSFs is a way to manage the number of CSFs derived, but may not be useful for all organizations. Bottom line: quit when you have accurately characterized the key performance areas for the enterprise or an operational unit.

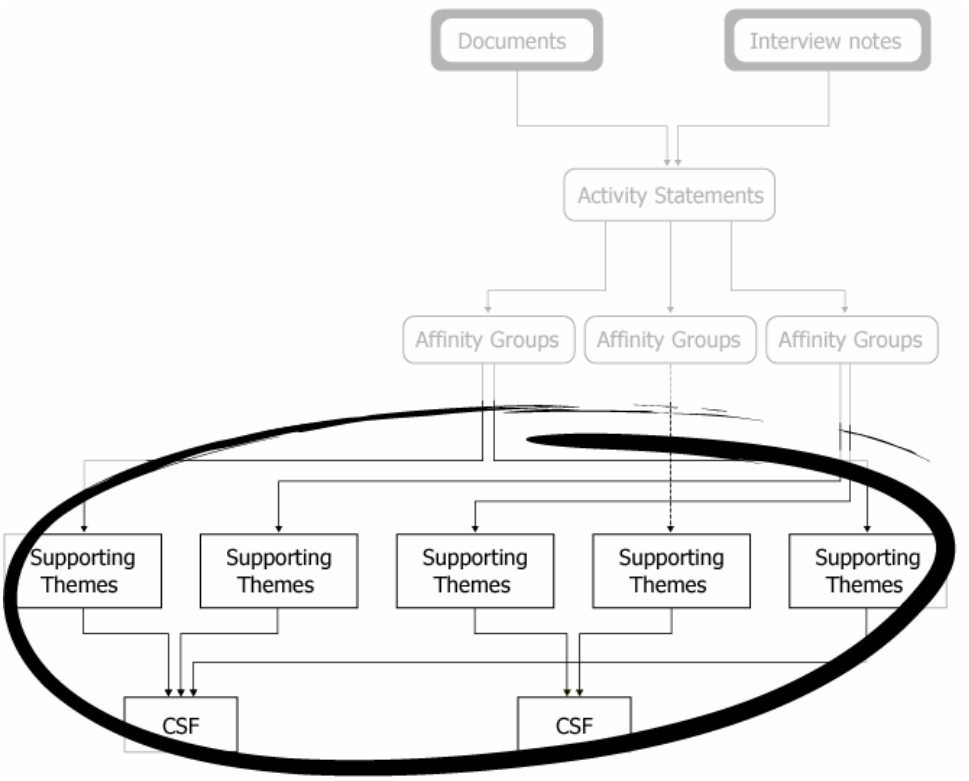


Figure 27: Illustration of Deriving CSFs from Supporting Themes

2. Aim for the fewest number of CSFs that can accurately and completely characterize the organization or operational unit.

The intent of CSFs is to identify those activities that are most important to managers to achieve the organization's mission. Managers cannot focus on an unrealistic number of CSFs—just as with driving a vehicle, the more things needing attention may cause the focus to be drawn away from the mission at hand (to arrive safely at the intended destination.) As a result, the number of CSFs derived should be kept to the minimum necessary to reflect the truly important key performance factors. (In our experience, an acceptable number of CSFs is around 5 to 7, but generally no more than 10.[36])

[36] These ranges have not been scientifically tested or proven. Rather, they are based on experience with the CSF method and field observation of the use and comprehension of CSFs. A larger set of CSFs might be developed at the organizational level, particularly if the organization has many divisions, lines of business, international units, etc. As always, determining the number of CSFs that is appropriate requires using good judgment and reducing the number to a level that is most appropriate for the organization.

3. **Recognize the difference between the composition of "good" CSFs and "poor" CSFs.**

A "good" CSF begins with an action verb and clearly and concisely conveys what is important and should be attended to. A "poor" CSF is vague and requires extensive explanation to be conveyed. Consider the following qualities of CSFs to determine the difference between "good" and "poor" CSFs:

Table 5: Qualities of "Good" and "Poor" CSFs

Qualities of Good CSFs	Qualities of Poor CSFs
Clear, concise, and readily understandable. The meaning of the CSF is not left to interpretation by different managers.	Vague, requiring extensive explanation. The CSF can be interpreted differently by different managers.
Suggests actions or activities performed by the organization in the course of operations or doing business.	Suggests improvements or recommendations that the organization should undertake.[37]
Begins with verbs that characterize actions or activities—attract, perform, expand, monitor, manage, deploy, etc.	Begins with verbs that convey enhancements, improvements, or error correction—improve,[38] implement, execute, enhance, upgrade, correct, etc.

4. **Determine if additional combining of CSFs needs to be performed.**

As with the repeated grouping of activity statements and supporting themes, CSFs should be examined to determine if additional combining can be performed. This is a final self-correcting mechanism of the CSF process that can correct for errors in the affinity grouping of supporting themes. In some cases, a larger number of CSFs may be justified, but this is also a signal for caution and re-examination.

[37] A critical success factors activity is not an assessment or audit of the organization's practices or activities. Although a lack of a certain activity may result in the creation of a CSF, the CSF process should not result in "findings." Repeated use of the method in this manner may impair the ability to gain the commitment of participants and affect their willingness to provide data.

[38] "Improve" can be valid in one exception: where the critical success factor conveys the need to continually improve some aspect of the business, such as "continually improve efficiency." In this case, the word "improve" in a CSF does not convey a recommendation so much as it captures the desire to progress and expand.

5. **Take an objective look at the CSFs that have been created.**

An objective review should be performed on the resulting CSFs. Consider the following questions for the group of CSFs that have been created:

- Do any of the CSFs overlap or appear to have the same underlying intent? (If so, combine again!)
- Do the CSFs appropriately characterize the organization or operational unit?
- Are there obvious CSFs that are well known in the organization but that failed to be identified through the process?
- Is there a good (or acceptable) distribution of CSFs across different sources (i.e., industry, temporal, etc.)?
- Have the various dimensions of CSFs been considered and reflected (i.e., internal vs. external, monitoring vs. adapting)?
- For organizational CSFs, have major operational units, divisions, or lines of business been represented?
- For operational unit CSFs, do the CSFs complement or support the organization's CSFs?
- Do any of the CSFs convey the goals and objectives (or the mission) of the organization or operational unit? (These CSFs might be suspect—they may be a restatement of the mission statement or a particular manager's goals and objectives.)

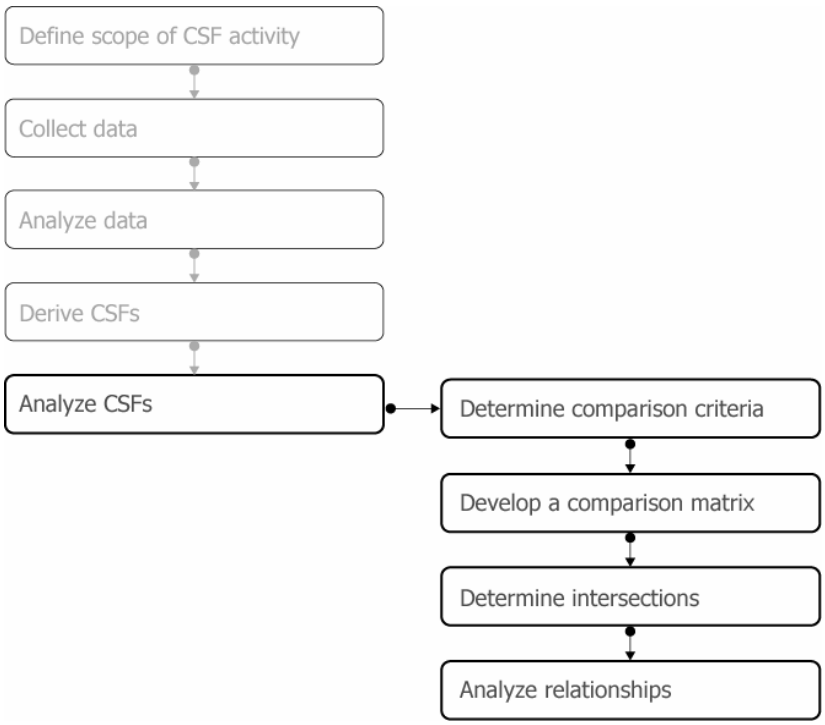
Final Considerations for Deriving CSFs

Keep in mind that the process of deriving CSFs from document review and interviews is only one means for obtaining CSFs. Industry, peer, and environmental CSFs may not always emerge from this process, particularly if managers are disconnected with the industry in which their organizations exist. As a final process check, it is recommended that a set of industry CSFs be obtained from outside sources such as professional organizations, peer organizations, or trade journals.[39] Once these CSFs have been obtained, they can be used for comparison, and any CSFs that apply to the organization should be used to augment the set that has been derived from the process presented herein.

Activity Five: Analyzing CSFs

There are four primary steps in Activity Five:

[39] The Internet provides a rich source for this information. However, because of the different uses of the term "critical success factors," you may have to sift through considerable information before you find CSFs as we have defined them in this report.



CSFs can be used for many purposes, as described throughout this report. They are a target at which many important initiatives of the organization can be aimed and compared. One of the keys to doing this comparison is to perform affinity analysis[40] using the CSFs as one of the comparison criteria. This section provides some guidance and examples for setting up and performing affinity analysis, which essentially primes the CSFs for further use and analysis.

Description of Affinity Analysis

Briefly described, affinity is the inherent or perceived similarity between two things. Affinity analysis is a way of studying this similarity to understand relationships and draw conclusions about the effect of one thing on another.

Affinity analysis is at the foundation of why the CSF method can be so powerful. In a simple way, comparing any organizational criteria to the organization's CSFs can expose gaps and problems and provide insight into why the organization is failing to accomplish its mission.

To illustrate affinity analysis using CSFs, consider the following table, which compares an organization's departments to its CSFs:

[40] Do not confuse affinity analysis with the activity of performing affinity grouping for deriving CSFs. Affinity analysis is focused on identifying and analyzing the intersections between different sets of comparison criteria. For example, comparing goals and objectives to CSFs is one way of performing an affinity analysis.

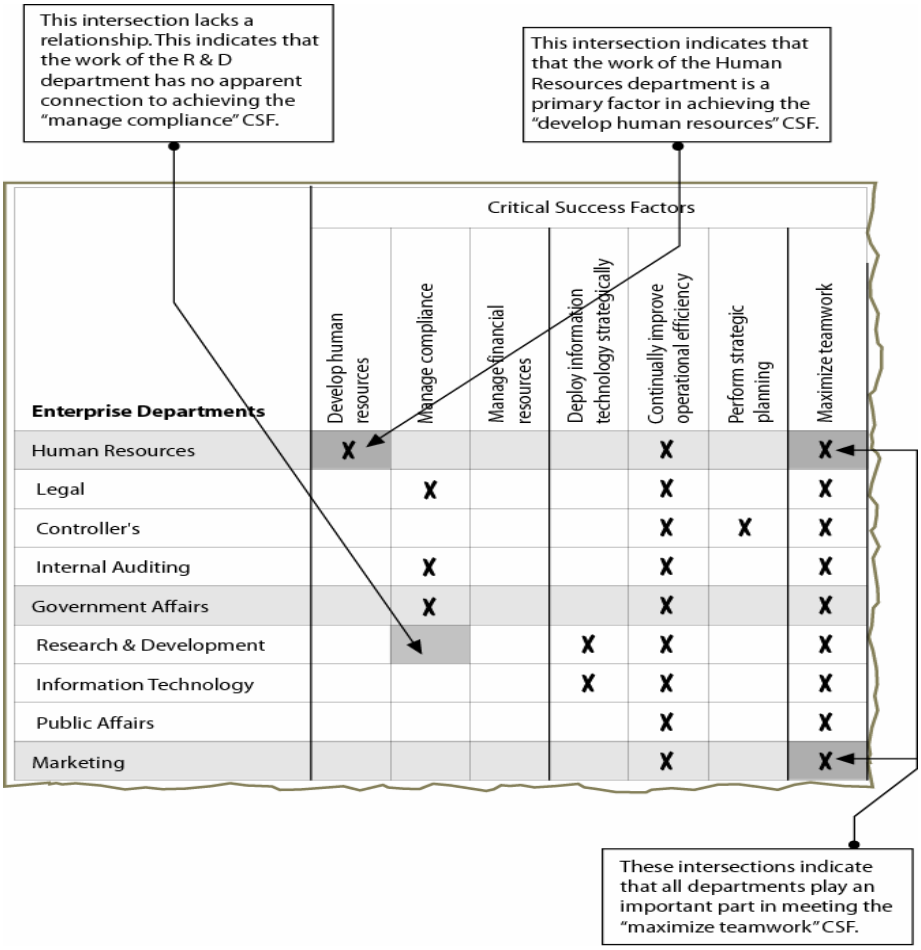


Figure 28: Example of Affinity Analysis

In this example, the comparison of departments to CSFs is used to determine which departments contribute primarily to (or have the strongest relationship to) achieving the organization's CSFs. By gathering this information, the organization can ensure that each respective department's goals reflect the tasks necessary to support, achieve, and monitor the CSF for which they have primary responsibility.

In the example provided, the Organizational Departments column could be substituted with many other comparison criteria to perform different types of analysis. For example, affinity analysis could be performed between CSFs and

- data elements (this would provide information on which data elements in the organization are vitally important to the achievement of CSFs)
- organizational processes
- assets, both information and physical
- security requirements

- assessment and audit findings
- performance metrics
- operational unit goals and objectives
- operational unit CSFs (to determine the "fit" between what managers see as important at the operational unit level and what is important to the organization as a whole)

As illustrated, the flexibility of the affinity analysis technique makes it an ideal instrument for implementing or "institutionalizing" the use of CSFs in an organization or operational unit.

Performing Affinity Analysis

The following characterizes the steps necessary to perform affinity analysis using CSFs:

1. **Determine comparison criteria.**

   The initial step in performing affinity analysis is to determine which comparison criteria to gather. Many organizations perform more than one type of affinity analysis with CSFs, so this may require the gathering of significant data outside of the CSF activity. Consider the objectives for performing the analysis to determine which data to collect and compare.

2. **Develop a comparison matrix.**

   Once the comparison criteria are established, a matrix similar to that shown in Figure 28 should be developed using a spreadsheet or other method that can be easily reconfigured and sorted if necessary.

3. **Determine the intersections.**

   Next, the intersections between CSFs and the chosen criteria must be decided on. This can be a large and somewhat difficult task, but it is very important for analyzing relationships. It may be necessary to consult with other organizational and operational unit personnel to determine which relationships exist. One caution—performing this activity haphazardly can result in flawed and inaccurate analysis.

4. **Analyze relationships.**

   Finally, look at the relationships between CSFs and the chosen criteria. Ask questions about all intersections, not only those that have been marked. For example,

   – If a relationship appears to exist, what does this mean?
   – If there is no relationship, what does this indicate? Does a relationship exist that is not marked? Should a relationship exist that has not yet been identified?
   – Are there too many or not enough intersections? If so, what does this mean?

Final Considerations

This section outlines the activities we have performed and codified for creating CSFs. Two other considerations must be made in performing these activities and applying the CSF method: Who performs the CSF activity and how often?

CSF Team

Purposefully, we do not provide extensive guidance in this report regarding the "optimal" composition of a team that would perform the CSF activity. In reality, this decision is highly dependent on the type of organization, the type of CSFs being developed, and the purpose for performing the activity.

In our field experience, we conducted the CSF activity to better understand our customer's business drivers so that we could work more effectively with the customer to develop security strategies, plans, and activities. Being outside of the core organization did not appear to have any measurable impact on our effectiveness; however, we were also highly dependent on having sponsorship inside of the organization for the CSF activity and a few highly competent individuals who were able to effectively guide us through the organization's hierarchy.

Conducting a CSF activity is not unlike any other activity undertaken to collect and understand an organization's experience and knowledge and use it to improve decision-making and to solve complex problems. This approach is basic to activities such as requirements elicitation for new systems and implementing cross-cutting initiatives such as new performance management approaches. Common to all of these activities is the need for the team conducting the activity to have a broad range of skills. For the CSF activity, this includes but is not limited to

- strong oral and written communications
- ability to interact with personnel in lower and higher level positions and responsibilities, particularly senior managers
- strong facilitation and interviewing skills
- an effective working knowledge of the scope area (organization, operational unit, department)
- an effective working knowledge of the organization's mission, purpose, vision, values, goals, and objectives
- strong analytical skills
- an ability to control biases and to think in the abstract, independent of the current operating environment and organizational structure

The selection of a team to conduct a CSF activity is highly dependent on the organization's culture. Certain organizational groups, such as internal auditors, are potential candidates for performing a CSF activity based on their skill sets. However, consideration must be given to the group's core roles and responsibilities in the organization to ensure that this would not affect the activity. For example, auditors certainly have many of the skills necessary to perform the CSF activity, but they may be biased or could portray a false perception of the activity as an assessment or audit.

Consideration should also be given to whether the personnel involved in the CSF activity should be internal or external to the organization. There are advantages to either choice; the aim is to ensure that the least amount of bias possible is interjected into the process.

Because of the amount of judgment that must be used in deriving CSFs, careful consideration should be given to assembling a cross-functional team that understands the value of the CSF activity and is willing and able to perform it.

Frequency

As with developing a CSF team, determining how often to perform a CSF activity is also highly dependent on many factors. Above all, it is dependent on how the CSFs will be used. For example, if the CSFs are part of the strategic planning process, they should be revisited whenever strategic planning is performed to ensure they are current and still representative of the organization. In addition, significant events might trigger the need to redo the CSF activity. For example, if the organization significantly changes its business focus, adds a new industry or exits an existing one, or is trying to implement an organization-wide initiative such as software engineering process improvement, a new set of CSFs can be invaluable as a guiding influence.

Finally, an organization that effectively uses CSFs to make decisions (e.g., through affinity analysis) will find that keeping them current (reflective of the current operating and industry environment) is very important to ensuring their validity and dependability.

Appendix B Case Study 1: Federal Government Agency

Introduction

This case study documents the use of the CSF method at a federal government agency of the United States. The CSF activity was undertaken as part of an information security risk assessment conducted by a team from the Networked Systems Survivability program at the SEI. The risk assessment focused on identifying the information security risks of a publicly available government Web service and developing a corresponding protection strategy to address those risks. The primary motivation for the CSF activity was to ensure that the assessment findings and the resulting protection strategy were aligned with the agency's organizational goals and objectives.

Acceptance of the CSF activity by the agency's management was not considered a criterion for success of the overall risk assessment. Instead, it was our belief that the CSF activity could be a catalyst for senior management support (of security activities) by characterizing IT security and risk findings in terms of business drivers. The agency's use of CSFs beyond this activity was always viewed as a secondary goal because, at the time, the use of the CSF method for the purpose of linking risk assessment and business drivers was still being researched and developed by the SEI team.

The Need for a CSF-Type Activity

Background

In 2002, we conducted an initial information security risk assessment for the federal agency presented in this case. The output of that assessment activity was a collection of information security vulnerabilities and risks to the public Web service and a suggested protection strategy. Since that time, a number of significant changes have occurred. For example, the immediate sponsorship, geographic location, contractor relationships and strategic partnerships, and architecture of the public Web service have changed. The agency also experienced a change in senior management, including the chief technology officer and a senior administrator. Similarly, some of the agency's operational units underwent changes not only in personnel but also in their placement in the organization's hierarchy. For example, the systems support and development personnel and their immediate supervisors were separated into functional teams instead of remaining in one organizational unit.

Because of these significant changes and the agency's previous assessment engagement, the SEI was asked to once again perform an information security risk assessment and to help the agency to develop a protection strategy. The assessment team began by conducting interviews with various staff members at the agency in order to get a better understanding of the current operational environment and to develop an appropriate scope. Immediately, it became apparent that there were a number of organizational disconnects. For example, the goals and objectives of senior management appeared to be significantly different from the goals and objectives of the operational staff. We also observed that the mission of the agency had changed since our last engagement and that all levels of the organization did not share a common view of the mission.

Positioning the CSF Activity

Considering these changes and challenges, it became evident that the assessment team and the agency would benefit from developing a set of CSFs. Thus, we initially proposed the CSF activity as a way to help us better understand the current direction of the agency and to ensure that the risk assessment was properly focused on those areas most important to the agency. However, the primary goal of the assessment was to identify security risks and to develop mitigating strategies. Because risk is highly relative to those assets and processes that are important to accomplishing the agency's mission, we also proposed that CSFs could help us prioritize and understand the agency's security risk in terms of how they may impede the accomplishment of CSFs. Thus, for these reasons, identifying CSFs became a logical first step to properly characterizing the current relationship between information security and the organization's business drivers.

Specific CSFs Derived for the Agency

This section describes the specific CSFs derived at the agency as well as the supporting themes and activity statements of each CSF. Activity statements for each CSF were logically organized against the general, technical, or customer management focus that the statement represented. Originally more than five CSFs and many more activity statements were derived for the agency. For the sake of brevity, consistency, and sanitization of the actual developed CSFs, this report only portrays a subsection of the original information to illustrate the type and nature of the content yielded through the activity.

The following information was broken into two subsections: first, the actual CSFs, supporting themes, and activity statements; and second, the threats and risks that exist or are perceived as impediments to the agency in meeting the CSFs.

Table 6: Agency CSFs

CSF 1 – Manage the Technical Production Environment
Supporting Themes Manage production operations to provide services and achieve customer requirements. Manage risks to production environment and impacts to customers and business partners.
Activity Statements **General Goals and Objectives** – Ensure that the production environment is capable of accommodating the anticipated requirements of customers, partners, and users. – Ensure that responsibility for the security and availability of the environment is accepted by the contractor. – Perform periodic stress testing to ensure system performance in the environment. **Customer-Specific Goals and Objectives** – Ensure that heightened availability requirements are maintained for the Web service under conditions where availability is paramount. – Maintain performance requirements for the Web service. – Maintain the accuracy and integrity of Web service content with documented procedures. **Technical Goals and Objectives** – Perform appropriate monitoring of the health of systems and information assets. – Patch and maintain software in the technical production environment on a regular basis. – Document, communicate, and test procedures for backup/restorative processes. **Other Related Themes** – Technical/change management of the production environment is an essential function. – System monitoring services are important to overall information system health.

CSF 2 – Provide High Value Customer Products and Services
Supporting Themes Maintain the integrity and availability of the Web service. Support cross-agency portals. Support e-government initiatives and activities. Promote products and services to a broader audience.
Activity Statements **General Goals and Objectives** – Provide services and support to the other government initiatives. – Develop a thorough understanding of government initiatives in order to provide service and support. – Clearly articulate the agency vision, goals, and objectives to remain relevant among the growing e-government initiatives. **Customer-Specific Goals and Objectives** – Ensure that Web service content is timely and relevant. – Maintain the appearance and availability of Web service services in accordance with the agency priorities. **Technical Goals and Objectives** – Implement a content management system to support future growth. – Implement effective government-wide customer relationship management capabilities. – Implement profile management capabilities. **Other Related Themes** – Web search services are an important component of providing the Web service functionality and for meeting the agency's mission. – Supporting cross-agency portals is a major future objective.

CSF 3 – Develop and Manage Human Resources

Supporting Themes

Develop, train, prepare, and support employees to participate in the growth of the agency.

Manage partner human resources to achieve the common goals of the agency.

Activity Statements

General Goals and Objectives

- Ensure that a capable, trained contractor staff is available to successfully meet contract requirements and objectives.
- Ensure that the agency and agency personnel fully understand security requirements and convey them to contractors.
- The skill and experience of subcontractors' personnel is critical to the successful delivery of security services to the agency.

Customer-Specific Goals and Objectives

- Obtain senior management support for increasing the size of the Web service team to support additional objectives.
- Ensure that time and local human resources can support increasing requirements for the Web service development and cross-agency coordination.

Other Related Themes

- Effective technical support is essential to managing the Web service.
- Professional development and training of contractor personnel is important to providing essential services.

CSF 4 – Manage Information Security Issues[41]

Supporting Themes

Manage threats and risks to achieving agency goals and objectives.

Protect customer data and privacy.

Activity Statements

General Goals and Objectives

- Implement complete and up-to-date security plans for the agency and the Web service.
- Effectively manage physical security as an important component of overall system and network security.
- Restrict physical access to production environment critical assets to key contractor personnel.

Customer-Specific Goals and Objectives

- Ensure that subcontractors' service offerings support the agency's security requirements for the Web service.
- Perform accurate and timely monitoring and reporting of Web service security incidents.

Technical Goals and Objectives

- Ensure system hardening as an essential component of security over the production environment.
- Perform periodic vulnerability scanning to ensure the security of the production environment.
- Effectively manage access privileges for terminated users or users whose need has expired.

Other Related Themes

- Data center security is an important component of overall system and network security.

[41] An interesting outcome of the critical success factors exercise for this agency is the identification of information security as a CSF. While this technical report proposes the use of CSFs to guide security efforts, this finding illustrates that for many organizations, managing security is a critical success factor.

CSF 5 – Manage Business and Operational Partners

Supporting Themes

Provide direction to business partners to achieve agency goals and objectives.

Communicate effectively with business partners.

Collaborate with business partners to maintain and improve operations.

Establish formal agreements with business partners.

Maintain effective government relationships and partnerships to promote agency goals and objectives.

Activity Statements

General Goals and Objectives

- The agency and Web service team must provide clear, consistent, and prioritized direction to contractors and other stakeholders.
- Formal agreements between contractors and the agency should be documented in contract language that is clear and concise.
- Ensure that contractors effectively manage their relationships with subcontractors to avoid impact on the agency production environment.

Technical Goals and Objectives

- Provide decision authority for system administration and security issues.
- Provide documentation of process or content of communications/actions required to perform or expedite service within the agency production environment.

Other Related Themes

- Identification and communication of explicit technical goals is critical to the relationship between the agency and contractor.
- A shared "product/service vision" is essential to the relationship between the agency and contractor.
- Effective communications among all the agency contractors and stakeholders is critical to successful service delivery.

Relationship of Risks to CSFs

In this section, we present an alternate view of the agency's CSFs. Instead of using the CSFs as an alignment factor, we characterize the agency's known or perceived vulnerabilities in terms of how they would impede or prevent the achievement of the CSFs. In this way, we provided the agency with another way to assess the importance of risk that was identified through the risk assessment. This illustrates the potential use of CSFs as a metric for determining which risks to mitigate and which to accept.

As with the supporting themes and activity statements for CSFs, each CSF vulnerability is arranged by the general, customer, or technical focus that it represents.

Table 7: Vulnerabilities to Agency CSFs

CSF 1 – Manage the Technical Production Environment
General Vulnerabilities – Management's lack of understanding and past misrepresentation of the state of the agency's technical security sets a basis for harm to the agency's reputation and its ability to effectively manage and control budgetary matters. – The agency's statement that the mission of the agency is to "make sure that the Web service works" cannot be executed in the absence of tangible strategy and objectives. – Agency management is unfamiliar with the multiple technical environments supported by the agency.
Customer-Related Vulnerabilities – lack of a content management system and lack of effective configuration management – lack of trouble-ticket system (for content and system administration needs of the agency) between contractor and the agency/the Web service to identify, track, and resolve business processes
Technical Vulnerabilities – lack of specific software engineering practices to develop, manage, and mature software and content – necessity for informal communications based on informal relationship to perform or expedite service in the environment – poor notification to the agency of equipment changes for hardware in the environment

CSF 2 – Provide High-Value Customer Products and Services
General Vulnerabilities – lack of consistency and coordination in the management, architecture, and administration of the multiple agency technical environments – lack of documented software engineering practices and a content release strategy
Customer-Related Vulnerabilities – A single conduit (such as through the project manager) does not exist to pass customer requests and demands to the contractor. – Lack of a content management system hinders a collaborative workspace.

CSF 3 – Develop and Manage Human Resources
General Vulnerabilities – Lack of personnel and funding create the possibility for a single point of failure to exist in the agency technical projects and support. – Lack of personnel in critical positions is a threat to the agency technical environments. – There is no continuity plan or procedure for dealing with the loss of key personnel. – Agency management doesn't adequately communicate expectations to the agency.
Technical Vulnerabilities – Lack of appropriate personnel in information security management positions is a threat to meeting the agency technical environments' security requirements. – Program management skills are lacking.

CSF 4 – Manage Information Security Issues
General Vulnerabilities – Lack of a documented policy stating the time requirements and detail necessary for incident notification and management is a threat to the environment. – Lack of a security policy and plan are threats to incident response and recovery efforts. – Lack of a regular risk assessment or a risk assessment driven by events (e.g., changes to the infrastructure, major contractual change affecting technology) poses a possible threat to the environment and the agency's survivability.
Technical Vulnerabilities – Subcontractors' standards for service, administration, and implementation are, by default, less secure than desired and may not meet the requirements for security of contractor. – Contractor system hardening does not follow procedures prescribed by subcontractors or the agency, but rather ad hoc procedures (done with "best intentions"). – Miscommunications between contractor and subcontractors have led to threats in the agency production environment.

CSF 5 – Manage Business and Operational Partners
General Vulnerabilities – The agency security advisory board is not being used as a partner in the agency's information protection and strategy formation. – Lack of documented policies, procedures, or specialized contracting vehicles (SLAs, etc.) between contractors and the agency is a threat to the agency production environment. – The agency is poor at describing the larger philosophy of service (and the business requirements to be maintained) and relies on only describing the technical goals and specifications.
Technical Vulnerabilities – The agency does not possess the technical skills to demand, require, or suggest specific hardening or administration of systems performed by contractors. – Due to contracting and funding specifications, the contractor has failed to provide enough technical staff to support the needs of the agency.

Conclusions and Results

As the agency's operational model and technical architecture evolved, the information security risk identification and analysis activities became paramount to short- and long-term decision making. The risk assessment activities performed in our engagement focused on the agency's ability to manage and control its operational partners and other contractors. This capability is essential for the protection of information assets for which the agency is responsible as a security and service provider.

Using the CSF method afforded a way for the SEI team to identify the links between the mission of the agency and the goals of technical operations. Thus, threats to operations could be presented and understood in both a technical and operational context. This allowed agency managers to broaden their view of the assessment findings to include organizational impacts and considerations. In the end, the CSFs played an important role not only in identifying the need for alignment of the agency's protection strategy to operational drivers, but as a means for communicating the importance of risk mitigation in a context that is familiar to, and on the minds of, executive-level managers.

Appendix C Case Study 2: Large County Government

Introduction

This case study documents the application of the CSF method within a local (county) government. The CSF activity was undertaken following pilots of the OCTAVE information security risk evaluation in the county. These pilots were conducted by analysis teams in two of the county's operational units, with training and assistance provided by a team from the SEI. The risk assessments were conducted in support of the county's efforts to adopt electronic methods of conducting business (e-government and e-commerce) and to ensure an appropriate level of security for transactions with constituents. Following the completion of the risk assessments, the two operational units encountered significant challenges in their attempts to transform the assessment findings and results into tangible strategies, plans, and actions. The development and analysis of CSFs were conducted to assist the county in addressing these challenges and in focusing its mitigation strategies and activities to ensure that they directly support the achievement of the county's mission.

The Need for a CSF-Type Activity

Background

In 2002, pilots of the OCTAVE risk assessment methodology were conducted in two of the county's operational units. Two analysis teams composed of county staff from the selected operational areas were involved in all aspects of the evaluation. A team from the SEI provided targeted on-site and hands-on assistance, guidance, and facilitation throughout the pilot assessments to the analysis teams, the two operational units, and county management. The assessments resulted in an initial view of the information security risks that exist in the two targeted operational units. Protection strategies were developed by assessing the operational units against a catalog of common security practices and identifying strengths and weaknesses in the county's current practices. In addition, asset mitigation plans were developed to address specific identified risks to selected critical assets within each operational area. The assessment results provided the county with an initial risk-based view of its information security posture.

The county encountered significant challenges in its efforts to complete the pilot assessments and to develop and implement the protection strategies. The assessments were conducted on a protracted schedule, with the analysis teams suffering numerous interruptions that required

them to respond to organizational changes and to frequently reacquaint levels of county management with the purpose and goals of the assessments. Throughout the assessments, the analysis teams struggled with the description and definition of several of the critical assets that were assessed. The analysis teams also had difficulty in evaluating and prioritizing the identified risks. Finally, the analysis teams and operational units experienced problems and delays in analyzing and selecting risk mitigation strategies, assigning responsibility for the selected strategies, and effecting the needed changes in policy, practice, and procedure. As a result, after successfully completing the assessment activities, the operational units were unsure of the relevancy and applicability of a portion of the assessment results.

In 2003, the SEI was asked to provide continued assistance and expert guidance to the county as it attempted to interpret the assessment findings and to implement its chosen protection strategies and mitigation plans. The second engagement with the county began with an extensive review of the pilot risk assessment activities and results. These review activities provided the SEI team with a better appreciation for the potential barriers to successful mitigation of risks identified within the operational units and the county. The SEI team recognized that the root cause for many of the county's challenges was the lack of a clear tie between the assessment activities and the county's business drivers.

Positioning the CSF Activity

Building on emerging field experience and research results, the SEI team proposed the use of the CSF activity to (*a*) confirm the criticality of the assets selected for the risk assessment, (*b*) guide the selection of operational units and assets for future assessments, and (*c*) provide a foundation for initiating improvements in the way that information, technical, and physical security are addressed throughout the county. The CSFs derived would also help the SEI and county teams to better understand the current direction of the county.

As the SEI and the county entered the second phase of their collaborative activities, the county appointed a new chief information officer. The new CIO was approached as a potential sponsor of the CSF activity. The SEI team felt that the timing and results of the CSF activity would provide a foundation for improvements in enterprise security and potentially other county business processes, benefiting the office of the CIO as well as the assessed operational units. The CSF activity would also identify enablers within the county that could be used to initiate future enterprise improvements.

Deriving CSFs for the County Government

CSF Activity Scope and Participants

The application of the CSF method was originally focused on assisting one of the county's operational units. However, the CSF activity was initiated with several senior county managers, including the CIO. Key senior managers from other operational units were also included

in the process. As a result, while the derived CSFs may not fully represent the entire county organization, they are more representative of enterprise CSFs than operational unit CSFs.

Data Collection

The county's CSFs were derived from data collected through reviewing critical documents and conducting interviews. The document review focused on the mission and vision statements of the county and the selected operational units. In addition, the SEI team reviewed the CSFs of several county governments in an attempt to identify industry and peer group CSFs.

Approximately one dozen data collection interviews were conducted with county participants. In all interviews, the following questions were used to assist managers, and the SEI team, in identifying CSFs:

- What is your mission and role in the organization?
- What are your most critical goals and objectives?
- What are your three greatest business problems or obstacles?
- In what areas would failure hurt you the most?
- If you were away from your job for three months, what three pieces of information (or things you would want to know) would you need after you returned?

County Government CSFs

This section presents the specific CSFs derived at the county. The data collection and analysis activities resulted in the generation of a significant number of activity statements for each CSF. In the interest of brevity and anonymity, these supporting statements have been omitted. The information in Table 8 is provided for all of the organizational CSFs derived for the county: the actual CSFs, a detailed description of each CSF, the CSF type, and the summary themes. The CSFs are numbered for reference purposes only; no priority is intended.

Table 8: County CSFs

CSF 1 – Manage Financial Resources
Description The County must operate with a high level of fiscal responsibility, deploying scarce resources efficiently and effectively. **CSF Type:** Industry
Supporting Themes – Expend taxpayer revenues efficiently and in accordance with the law. – Invest in high-payoff capital improvements, including information technology. – Collect, measure, avoid, control, and recover costs.

CSF 2 – Maximize Interlinking and Collaboration
Description The County must encourage and promote effective communication between operational areas and coordinate work and resources. **CSF Type:** Temporal
Supporting Themes – Maintain interfaces and communications between departments and operational areas. – Promote information sharing and teamwork. – Eliminate stovepipes and duplication of effort. – Manage culture and resistance to change. – Eliminate aversion to technology. – Promote a shared vision of the County's mission, goals, and vision. – Coordinate planning to maximize overall value to citizens. – Avoid allowing political barriers to disable the County's ability to deliver core services to citizens. – Communicate with elected officials more effectively.

CSF 3 – Attract and Develop Human Resources
Description The County must attract and develop human resources to provide services to citizens effectively and efficiently. **CSF Type:** Competitive-position
Supporting Themes – Attract high-quality employees from the available workforce. – Develop, train, and prepare employees to contribute to the growth and effectiveness of service delivery. – Empower employees to act and take responsibility for their actions.

CSF 4 – Improve Operational Efficiency
Description The County must continually improve their operational efficiency to meet growing demands for service delivery. **CSF Type:** Industry
Supporting Themes – Implement a higher degree of best practice throughout the County. – Utilize technology more efficiently and pervasively. – Streamline decision making. – Review and re-engineer processes pervasively.

CSF 5 – Perform Strategic Planning
Description Decisions made throughout the County must be focused on long-term goals, objectives, and mission. **CSF Type:** Temporal
Supporting Themes – Conduct strategic planning. – Move away from decisions based purely on financial constraints. – Manage proactively instead of reactively. – Define and prioritize long-term goals and objectives.

CSF 6 – Deliver Citizen Services
Description The County must continually improve its core focus: delivering high-quality services to citizens. **CSF Type:** Industry
Supporting Themes – Focus on citizen needs. – Implement technology to service citizens better and more efficiently. – Confront growth issues and their impact on service delivery.

CSF 7 – Manage Compliance
Description The County must ensure that it complies with all relevant guidelines, legislation, regulation, and standards in the delivery of services to citizens. **CSF Type:** Environmental
Supporting Themes – Maintain awareness of the regulatory climate. – Comply in an effective and efficient manner. – Monitor compliance activities.

CSF 8 – Deploy Technology Strategically
Description The County must gain efficiencies by enabling the achievement of its mission through strategic deployment of information technology. **CSF Type:** Competitive-position
Supporting Themes – Align information technology with County strategic planning activities. – Migrate from legacy systems. – Expand services delivery through e-government. – Automate people-intensive activities.

Analyzing the County's CSFs

The following information demonstrates the results of two affinity analyses performed using the CSFs derived for the county government. The affinity analysis included in Table 9 is a comparison of selected critical assets to CSFs. Such a comparison can be used to validate the importance or criticality of an asset by investigating its overall significance to meeting the organization's mission and day-to-day business objectives.

Somewhat in parallel with the CSF activity, the county's security strategies and plans were analyzed by the SEI and the analysis teams and were revised and formed into areas of improvement. Identified areas of improvement included enterprise security policy, security training and awareness, human resources, collaborative security management, and business continuity. The affinity analysis in Table 10 is a comparison of the enterprise strategies and areas of improvement to the derived CSFs. A detailed analysis can be used to ensure that the selected security strategies are properly aligned to the county's business drivers. This affinity analysis can also help the county to prioritize the strategies, identify interdependencies between selected strategies, and better prioritize the county's enterprise security initiatives.

Conclusions and Results

This case study demonstrates a number of the ways in which the development of CSFs can help organizations to guide, direct, and prioritize their activities to effectively manage security across the enterprise. The county's exposure to the CSF activity has provided it with a management tool for making better-educated decisions regarding its strategic investments in information security.

Identifying the CSFs helped the SEI and operational unit assessment team confirm the criticality of most of the assets chosen and assessed under the OCTAVE pilots. The comparison of assets to the county's CSFs validated the importance of each selected asset by confirming its overall significance to the county. The activity also identified a number of additional assets that should be included in future assessments. Additional affinity analysis conducted on the CSFs should assist the county in targeting operational areas for future information security assessment activities.

The CSF activity resonated with the operational area managers and selected county managers. The CSF activity served to enhance communications among the county's management teams, raising awareness for the pilot assessment program and the proposed mitigation strategies. The activity made explicit a candidate set of CSFs for the county, providing a common point of reference for the operational unit and the larger county organization. All of the participants in the CSF activity recognized the applicability of the CSFs and the supporting artifacts beyond their intended use in developing security strategies and managing security within the county. As a result of the initial CSF activity described above, the county is in the process of expanding the CSF method to all key managers and the remaining operational units within the county. The resulting organizational CSFs can be used as a benchmark against which major county initiatives and projects can be compared for validity and viability.

Table 9: Affinity Analysis – CSFs to Critical Assets

Critical Assets[42]	Critical Success Factors							
	Manage financial resources	**Maximize interlinking**	**Attract and develop human resources**	**Improve operational efficiency**	**Perform strategic planning**	**Deliver citizen services**	**Manage compliance**	**Deploy technology strategi-cally**
Asset #1						✓		
Asset #2				✓		✓	✓	✓
Asset #3				✓		✓	✓	✓
Asset #4	✓			✓			✓	
Asset #5	✓						✓	

[42] We have chosen to eliminate the names of these assets because they would identify the source of this information. However, in most cases, these assets represented either a significant information asset (stored in both physical and electronic form) or a significant information system for the organization.

Table 10: Affinity Analysis – CSFs to Enterprise Security Strategies

Enterprise Security Strategies	Critical Success Factors							
	Manage financial resources	Maximize interlinking	Attract and develop human resources	Improve operational efficiency	Perform strategic planning	Deliver citizen services	Manage compliance	Deploy technology strategically
Establish an enterprise-wide security initiative.		✓		✓	✓		✓	✓
Develop and implement a comprehensive enterprise-wide security policy.		✓					✓	
Develop and implement an enterprise-wide security training and awareness program.			✓					
Support enterprise security strategies, policies, and procedures through Human Resources activities.			✓					
Ensure business partners cooperate and collaborate in the security initiatives.		✓						
Develop and implement adequate contingency/disaster recovery plans.				✓		✓		

Appendix D Glossary

activity statements Activity statements are brief descriptions of what managers do or should do in an organization to ensure the organization's success. They are one of the essential elements in creating CSFs. They are harvested from interview notes and documents, and are the input for performing affinity grouping activities.

affinity analysis Affinity analysis is an activity in which the perceived similarity between two things is studied to understand relationships and draw conclusions about the effect of one thing on another.

affinity grouping Affinity grouping is a process for organizing ideas, thoughts, concepts, and so forth. For CSFs, affinity grouping is used to group similar activity statements as an element in defining CSFs.

business drivers The mission, goals, objectives, and CSFs form the elemental business drivers for an organization. These are sometimes referred to as "organizational drivers" or "strategic drivers."

competitive-position CSF A competitive-position CSF reflects the key performance factors that arise due to an organization's position relative to its peer group in the industry or the environment in which it operates or competes.

critical success factors The limited number of areas of performance that are essential for an organization to achieve its goals and accomplish its mission. They are the key areas of activity in which favorable results are absolutely necessary to reach goals. Critical success factors are often referred to as "CSFs."

enterprise CSF Enterprise CSFs are the set of critical success factors that represent the top activities, concerns, strategies, and goals of upper level management. They are derived from the top two or three layers of management and reflect the various CSFs found throughout an organization.

enterprise security management A management- and process-oriented view of security as a business process that is pervasive across and dependent on the enterprise.

environmental CSF An environmental CSF reflects the environmental factors over which the organization has very little control or ability to actively manage.

goals Specific, measurable targets of performance necessary to achieve the organization's objectives and ultimately its mission.

industry CSF An industry CSF reflects the unique operating conditions and challenges that are inherent to the industry in which an organization chooses to operate.

management-layer CSF A management-layer CSF reflects the unique focus and priorities that are inherent in a specific management layer, such as executive management or middle management.

mission The mission of the organization reflects its vision and purpose. It is the reason that the organization exists and describes what it is there to accomplish. The mission is accomplished through the setting of objectives and the achievement of goals.

objectives General directional statements [Rockhart 81]. Objectives are a more specific restatement of the organization's mission and are the aim of the organization's goals.

OCTAVE OCTAVE is an acronym for the Operationally Critical Threat, Asset, and Vulnerability Evaluation. It is a self-directed information security risk assessment methodology developed by the Software Engineering Institute. OCTAVE is available for download at www.cert.org/octave.

operational unit CSF Operational unit CSFs reflect the activities, concerns, strategies, and goals of an organizational department, division, or subdivision.

supporting themes Supporting themes are one of the essential elements in creating CSFs. Supporting themes summarize the intent of a group of activity statements and are the final input to deriving CSFs.

temporal CSF A temporal CSF is one that reflects a temporary condition or situation that must be managed for a specific period of time.

References

URLs are valid as of the publication date of this document.

[Alberts 01] Alberts, Christopher J. & Dorofee, Audrey J. *OCTAVE Criteria V2.0* (CMU/SEI-2001-TR-016, ADA3399229). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001. http://www.sei.cmu.edu/publications/documents/01.reports/01tr016.html.

[Meyer 04] Meyer, Paul J. *Attitude is Everything!* http://www.pauljmeyer.com (2004).

[Rockhart 79] Rockhart, John F. "Chief Executives Define Their Own Data Needs." *Harvard Business Review 57*, 2 (March-April 1979).

[Rockhart 81] Rockhart, John F. & Bullen, Christine V. *A Primer on Critical Success Factors*. Cambridge, MA: Center for Information Systems Research, Massachusetts Institute of Technology, 1981.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE July 2004	3. REPORT TYPE AND DATES COVERED Final
4. TITLE AND SUBTITLE The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management		5. FUNDING NUMBERS F19628-00-C-0003
6. AUTHOR(S) Richard A. Caralli		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213		8. PERFORMING ORGANIZATION REPORT NUMBER CMU/SEI-2004-TR-010
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116		10. SPONSORING/MONITORING AGENCY REPORT NUMBER ESC-TR-2004-010
11. SUPPLEMENTARY NOTES		
12A DISTRIBUTION/AVAILABILITY STATEMENT Unclassified/Unlimited, DTIC, NTIS		12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

Every organization has a mission that describes why it exists (its purpose) and where it intends to go (its direction). The mission reflects the organization's unique values and vision. Achieving the mission takes the participation and skill of the entire organization. The goals and objectives of every staff member must be aimed toward the mission. However, achieving goals and objectives is not enough. The organization must perform well in key areas on a consistent basis to achieve the mission. These key areas—unique to the organization and the industry in which it competes—can be defined as the organization's critical success factors.

The critical success factor method is a means for identifying these important elements of success. It was originally developed to align information technology planning with the strategic direction of an organization. However, in research and fieldwork undertaken by members of the Survivable Enterprise Management (SEM) team at the Software Engineering Institute, it has shown promise in helping organizations guide, direct, and prioritize their activities for developing security strategies and managing security across their enterprises. This report describes the critical success factor method and presents the SEM team's theories and experience in applying it to enterprise security management.

14. SUBJECT TERMS critical success factors, enterprise security management, strategic planning, information security, risk management	15. NUMBER OF PAGES 134
16. PRICE CODE	

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL