United States Government Accountability Office

GAO

Report to Congressional Requesters

September 2005

CHIEF INFORMATION OFFICERS

Responsibilities and Information and Technology Governance at Leading Private-Sector Companies

GAO

Accountability ★ Integrity ★ Reliability

GAO-05-986

September 2005

G A O
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-986, a report to congressional requesters

CHIEF INFORMATION OFFICERS

Responsibilities and Information and Technology Governance at Leading Private-Sector Companies

Why GAO Did This Study

To help address the many challenges being faced by federal agencies, Congress has enacted a series of laws designed to improve agencies' performance. The Clinger-Cohen Act of 1996, for example, requires that each agency head designate a Chief Information Officer (CIO) to lead reforms to achieve real, measurable improvements in the agency's performance through better management of information resources.

Recognizing the importance of the CIO position, congressional requesters asked GAO to conduct two reviews. The first, reported in July 2004, discussed the extent to which federal CIOs had responsibility for 12 functional areas that GAO had identified as either required by statute or critical to effective information and technology management, including information technology (IT) capital planning, strategic planning for information resources, and information security and privacy. This report focuses on the responsibilities of CIOs at 20 leading private-sector organizations. The questions GAO addressed were (1) What are the responsibilities of these CIOs, and how do they compare with those of federal CIOs? (2) What are the key challenges of these private-sector CIOs? (3) How do these organizations govern their information and IT assets enterprisewide?

www.gao.gov/cgi-bin/getrpt?GAO-05-986.

To view the full product, including the scope and methodology, click on the link above. For more information, contact David Powner at (202) 512-9286 or pownerd@gao.gov.

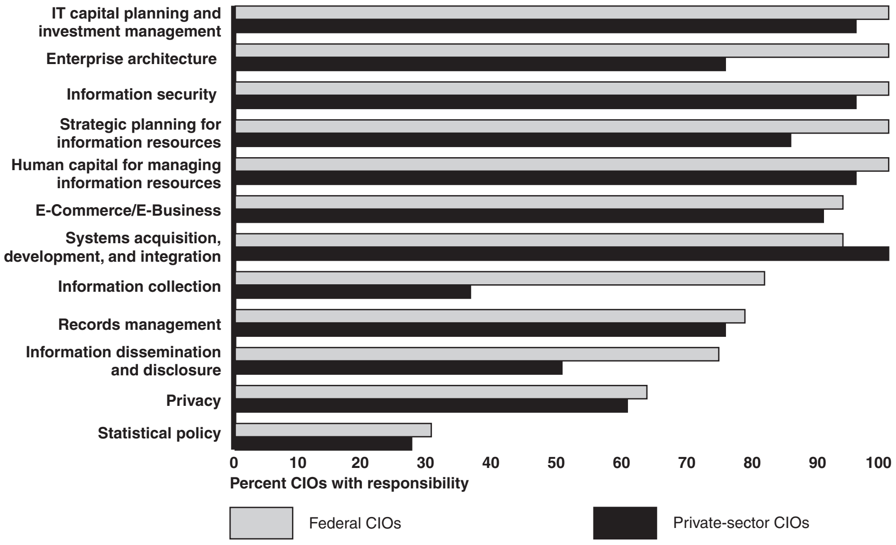
What GAO Found

The CIOs of most of the 20 leading private-sector organizations GAO met with had either sole or shared responsibility for 9 of the 12 information and technology management functional areas. Almost all of the private-sector CIOs had responsibility for five areas: (1) systems acquisition, (2) IT capital planning, (3) information security, (4) IT human capital, and (5) e-commerce. In only three areas—information dissemination and disclosure, information collection, and statistical policy—did half or fewer of the CIOs have responsibility. The chart below shows that in most of the functional areas there was little difference between the percentages of private-sector and federal CIOs who had or shared a given responsibility.

Eleven of the private-sector CIOs reported that aligning IT with business goals was their greatest challenge. Other major challenges that the CIOs frequently cited include controlling IT costs and increasing efficiencies, ensuring data security and integrity, and implementing new enterprise technologies.

The private-sector CIOs described several approaches to governing their companies' IT assets, including utilizing an executive-level committee with the appropriate decision authority and establishing cross-organizational teams to drive broad collaborative efforts such as enterprisewide business processes. Several CIOs also described their ongoing efforts to balance between centralization and decentralization of decision authority as their companies' competitive environments evolve.

Comparison of the Extent to Which Private-Sector and Federal CIOs Are Responsible for Each of Twelve Functional Areas



Source: GAO.

Contents

GAO
Accountability ★ Integrity ★ Reliability

United States Government Accountability Office
Washington, D.C. 20548

September 9, 2005

The Honorable Susan M. Collins
Chairman, Committee on Homeland Security
and Government Affairs
United States Senate

The Honorable Tom Davis
Chairman, Committee on Government Reform
House of Representatives

The Honorable Adam H. Putnam
House of Representatives

Over the past decade, Congress has enacted a series of laws designed to improve the federal government's performance with respect to information and technology management. For example, the Clinger-Cohen Act of 1996 requires agency heads to designate Chief Information Officers (CIO) to, among other things, lead reforms to help control system development risks; better manage technology spending; and achieve real, measurable improvements in agency performance through better management of information resources. We have long advocated that agencies put strong CIOs in place to address the government's many information and technology management challenges.[1] As we have previously reported, an effective CIO can make a significant difference in building the institutional capacity needed to implement improvements to an agency's information and technology management capabilities.

Recognizing the importance of this position, you asked us to perform two reviews in this area. The first, reported in July 2004, discussed the status of federal CIOs at major departments and agencies.[2] In that study, we found that most of this group had responsibility for many—but not all—of the functional areas we had identified as either required by statute or critical to

[1] GAO, *Improving Government: Actions Needed to Sustain and Enhance Management Reforms*, GAO/T-OCG-94-1 (Washington, D.C.: Jan. 27, 1994); *Government Reform: Using Reengineering and Technology to Improve Government Performance*, GAO/T-OCG-95-2 (Washington, D.C.: Feb. 2, 1995); and *Government Reform: Legislation Would Strengthen Federal Management of Information and Technology*, GAO/T-AIMD-95-205 (Washington, D.C.: July 25, 1995).

[2] GAO, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, GAO-04-823 (Washington, D.C.: July 21, 2004).

effective information and technology management. These responsibilities, which include functions pertaining to the management of government information as well as the technology that supports it, are listed in attachment 1 to the appendix of this report.

This report responds to your request that we contact private-sector organizations to answer these questions: (1) What are the responsibilities of leading CIOs in the private sector, and how do they compare with the responsibilities of their federal counterparts; (2) what are the key challenges of CIOs of leading organizations in the private sector; and (3) how do leading private-sector organizations govern their information and IT assets enterprisewide?

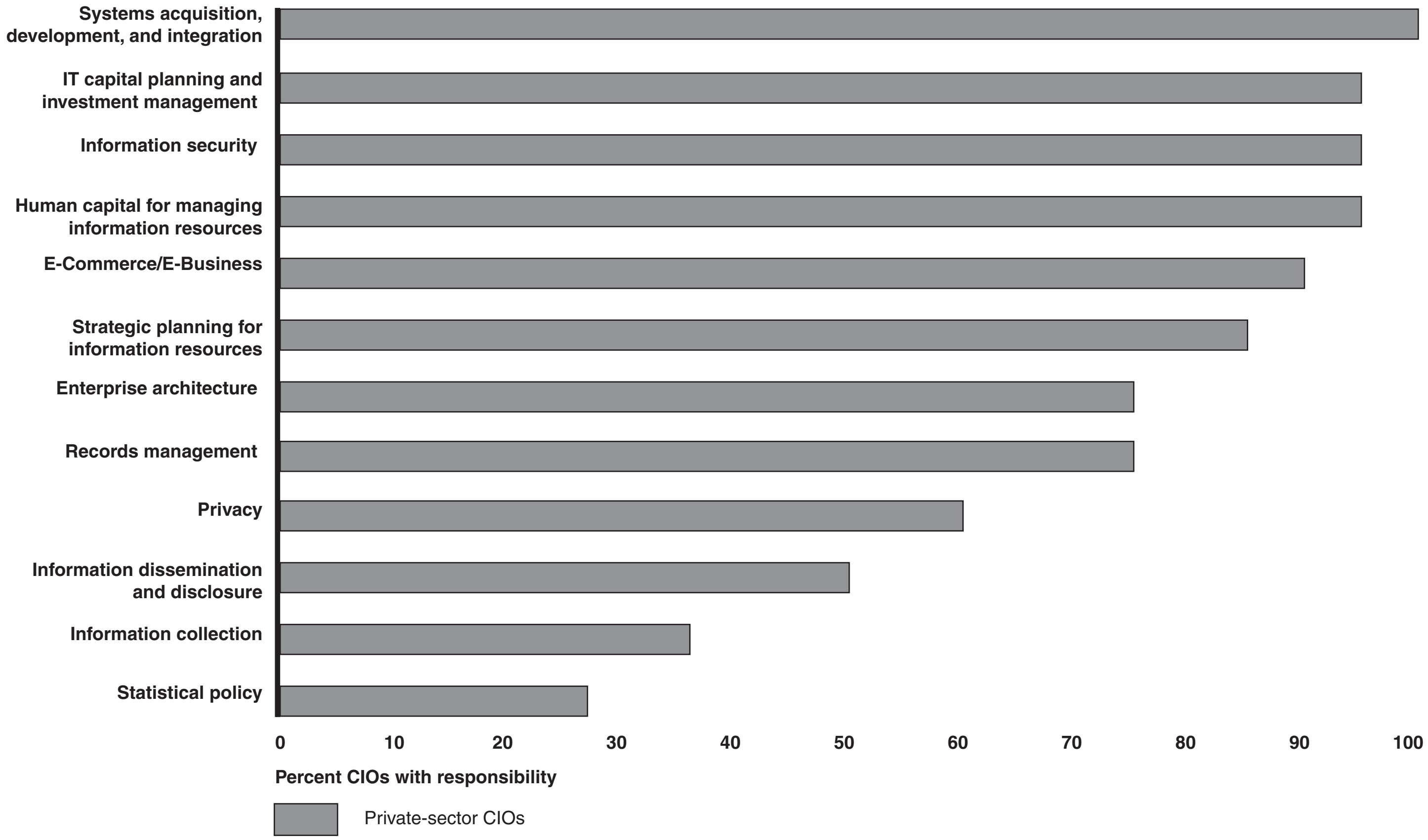
To address these objectives, we reviewed existing literature, held discussions with academic and IT professionals, and interviewed CIOs—as well as other IT executives—at 20 leading companies about their role and responsibilities. We identified prospective companies to interview based on their recognition as leaders in information and technology management. In addition, we chose companies that performed activities similar to those performed by federal agencies (e.g., supply chain management, education, and income security). We also selected both medium-sized and large companies, to ensure a broad representation. While our sample of 20 companies represents a wide array of high-performing organizations, the companies we selected are not representative of all private-sector companies, and the CIOs we interviewed are not representative of all of those in the private sector. Attachment 2 to the appendix of this report lists the companies that participated in our study. In our meetings with the CIOs and other IT executives, we used a set of structured interview questions based on the functional areas that we had addressed during our previous study of federal CIOs.[3] We had identified these 12 functional areas as either required by statute or critical to effective information and technology management, including information technology (IT) capital planning, strategic planning for information resources, and information security and privacy. The full list is included in attachment 3 to the appendix of this report.

On July 1, we briefed your staff on the results of our study. The slides from this briefing are included as appendix I to this report. The purpose of this letter is to formally publish the briefing slides.

[3] GAO-04-823.

In summary, most of the private-sector CIOs we spoke with had either sole or shared responsibility for 9 of the 12 functional areas we explored. These functional areas corresponded to the areas that we reviewed in our federal agency report and are listed in figure 1. Among the functional areas in which most of the private-sector CIOs had or shared responsibility, 18 or more of the 20 we spoke with had responsibility for the following five areas: (1) systems acquisition, (2) IT capital planning, (3) information security, (4) IT human capital, and (5) e-commerce. In only three areas—information dissemination and disclosure, information collection, and statistical policy—did half, or fewer, of those we interviewed have responsibility. Figure 1 shows the 12 functional areas that are covered in this study and the percentage of the private-sector CIOs in our study who had or shared responsibility for each area.

Figure 1: Percentage of Private-Sector CIOs with Responsibility for Information and Technology Management Areas



Source: GAO.

The set of responsibilities assigned to these CIOs in the private sector was similar to the corresponding set in the federal sector. In most functional areas, there was little difference between the private and federal sectors in the percentage of CIOs who had or shared a particular responsibility. In 4 of the 12 functional areas—enterprise architecture, strategic planning, information collection, and information dissemination and disclosure—the difference between the private- and federal-sector CIOs was greater; in each case, fewer CIOs in the private sector had these responsibilities. In all, the six functions least likely to be the CIO's responsibility in the federal sector were equivalent to the five functions[4] least likely to be his or her responsibility in the private sector. Some of the federal CIOs' functions, such as information collection and statistical policy, did not map directly to the functional areas in several of the private-sector organizations we contacted.

The private-sector CIOs in our study described four major challenges that they faced in their work:

- Eleven described aligning IT with business goals as a challenge. This challenge requires them to develop IT plans to support their companies' business objectives.

- Eight cited implementing new enterprise technologies (e.g., radio frequency identification, enterprise resource planning systems, and customer relationship management systems) as a challenge.

- Nine described controlling IT costs and increasing efficiencies as a challenge.

- Nine also described ensuring data security and integrity as a challenge.

When asked to describe how the governance of information management and technology is carried out in their companies, 16 of the 20 private-sector companies told us that they had an executive committee with the authority and responsibility for governing major IT investments. As part of the governance of IT assets in their companies, nine of the CIOs said that they shared responsibility for IT investment management and that their involvement ranged from providing strong leadership to reviewing plans to ensure that they complied with corporate standards. Six also described using cross-organizational teams to drive broad collaborative efforts, such as the development and implementation of standards and enterprisewide business processes. Several spoke of the work they were doing in balancing between centralization and decentralization of their responsibilities and described their efforts to move between the two extremes while finding the right balance.

[4] In our private-sector study, we combined information dissemination and information disclosure into a single functional area to increase their relevance to private-sector CIOs.

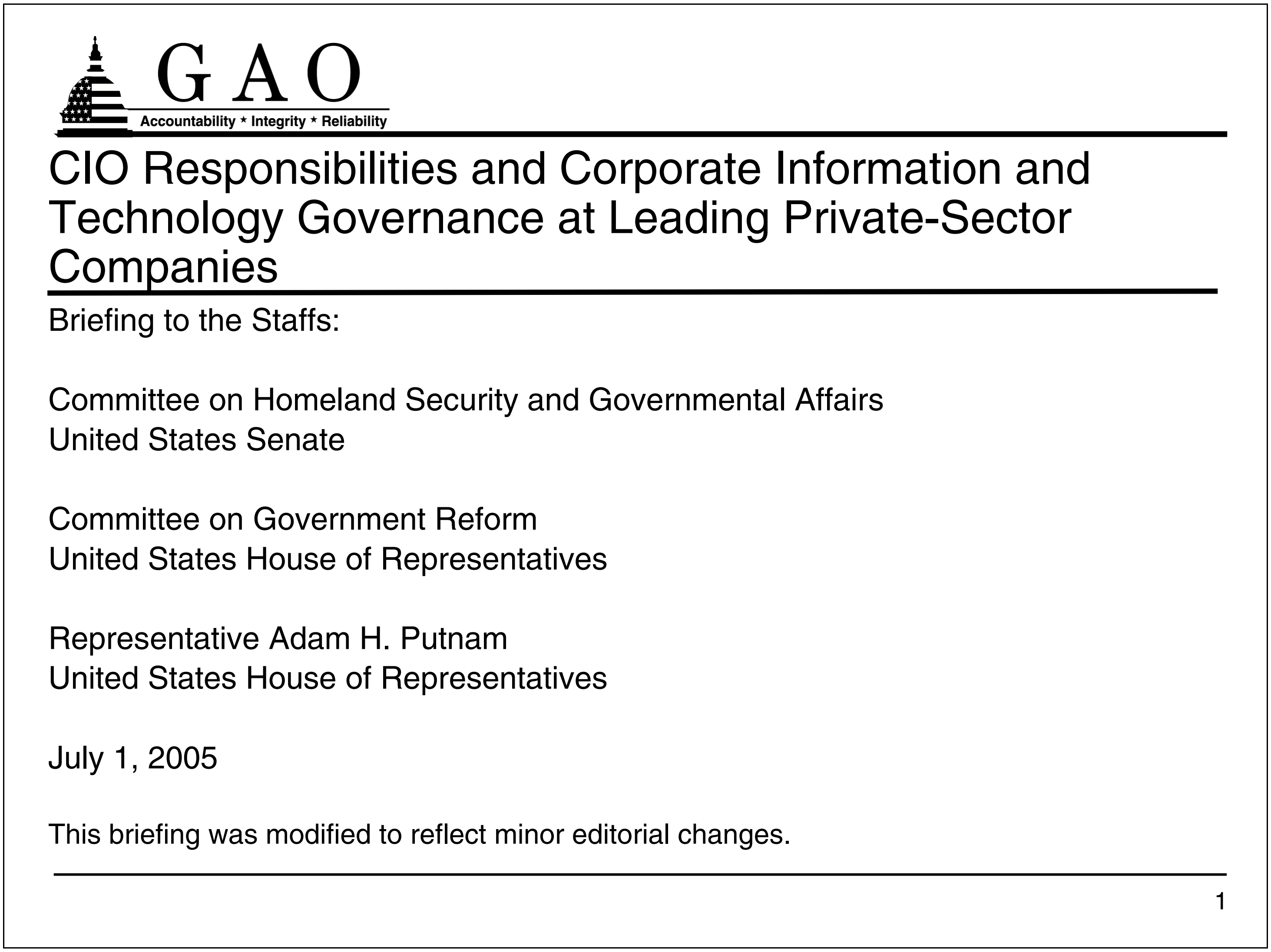
As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the date of this letter. At that time we will send copies of this report to the Ranking Minority Member, Senate Committee on Homeland Security and Governmental Affairs; the Ranking Minority Member, House Committee Government Reform; and other interested congressional committees. In addition, this report will be available at no charge on the GAO web site at www.gao.gov.

If you have any questions concerning this report, please call me at 202-512-9286 or at pownerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report were Barbara Collier, Lester Diamond, Neil Doherty, Joanne Fiorino, Ashfaq Huda, Tomás Ramirez, and Glenn Spiegel.

David a. Pow

David A. Powner, Director
Information Technology Management Issues

CIO Responsibilities and Corporate Information and Technology Governance at Leading Private-Sector Companies



GAO
Accountability * Integrity * Reliability

CIO Responsibilities and Corporate Information and Technology Governance at Leading Private-Sector Companies

Briefing to the Staffs:

Committee on Homeland Security and Governmental Affairs
United States Senate

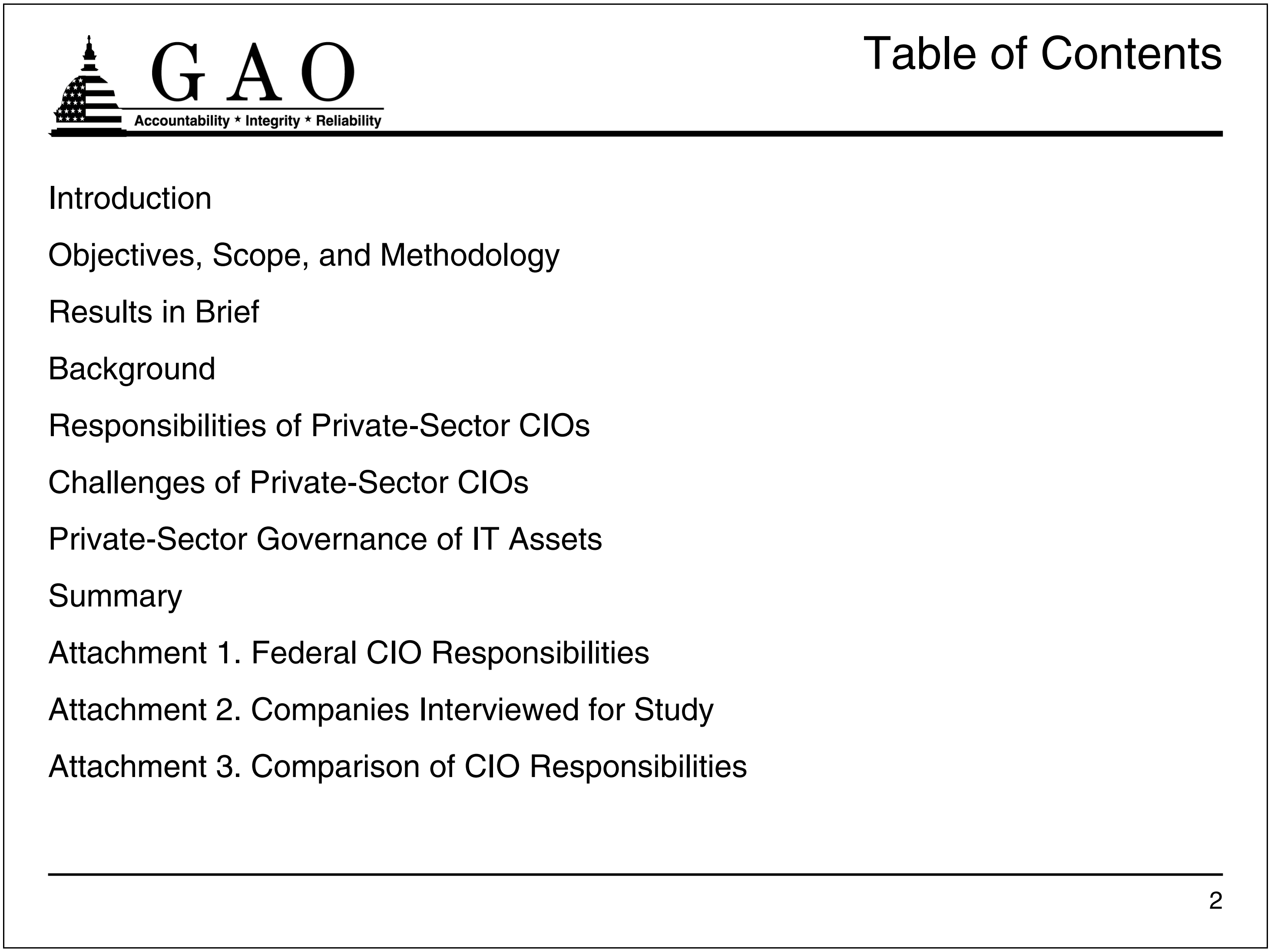
Committee on Government Reform
United States House of Representatives

Representative Adam H. Putnam
United States House of Representatives

July 1, 2005

This briefing was modified to reflect minor editorial changes.

1



GAO
Accountability * Integrity * Reliability

Table of Contents

Introduction

Objectives, Scope, and Methodology

Results in Brief

Background

Responsibilities of Private-Sector CIOs

Challenges of Private-Sector CIOs

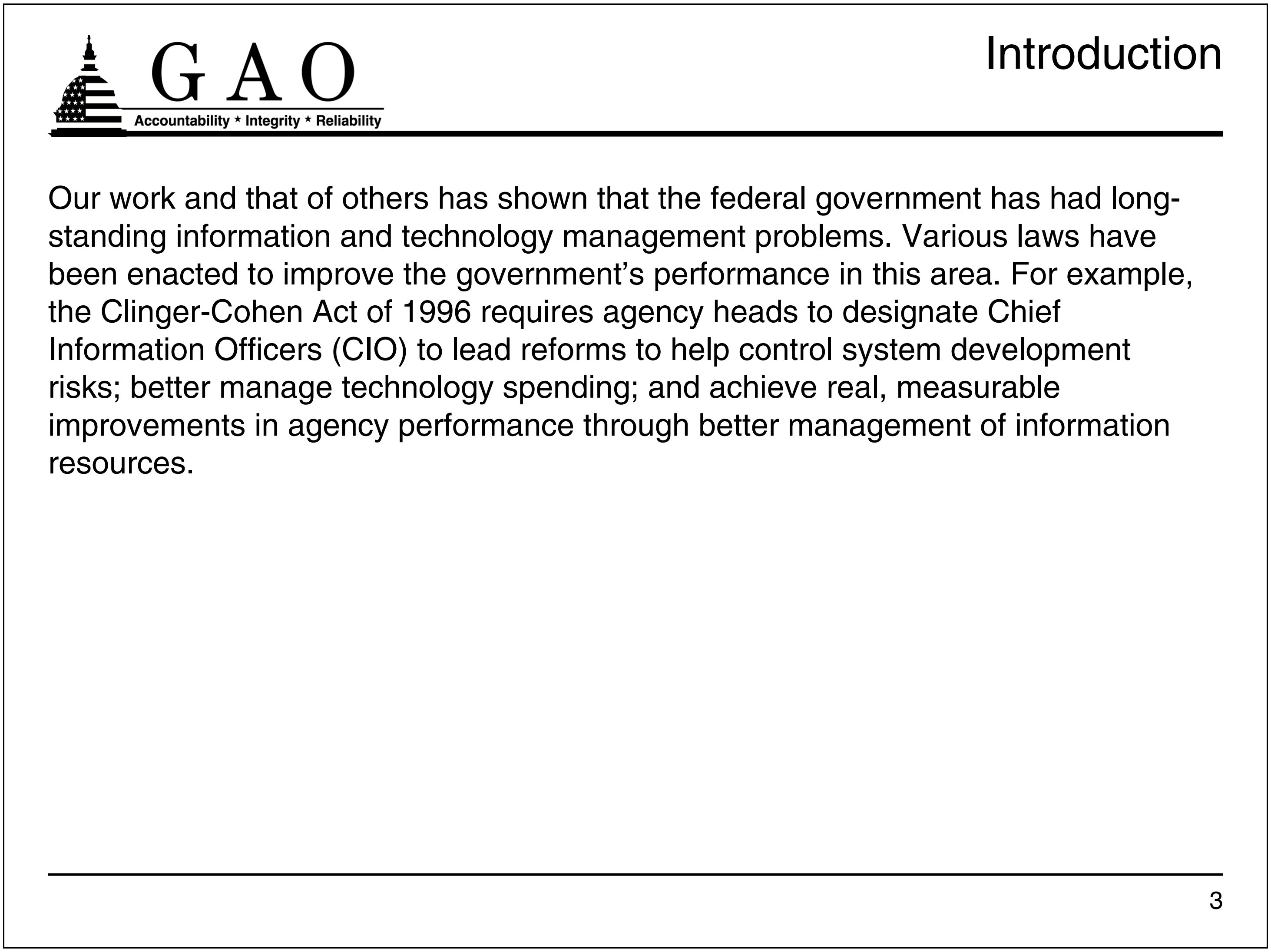
Private-Sector Governance of IT Assets

Summary

Attachment 1. Federal CIO Responsibilities

Attachment 2. Companies Interviewed for Study

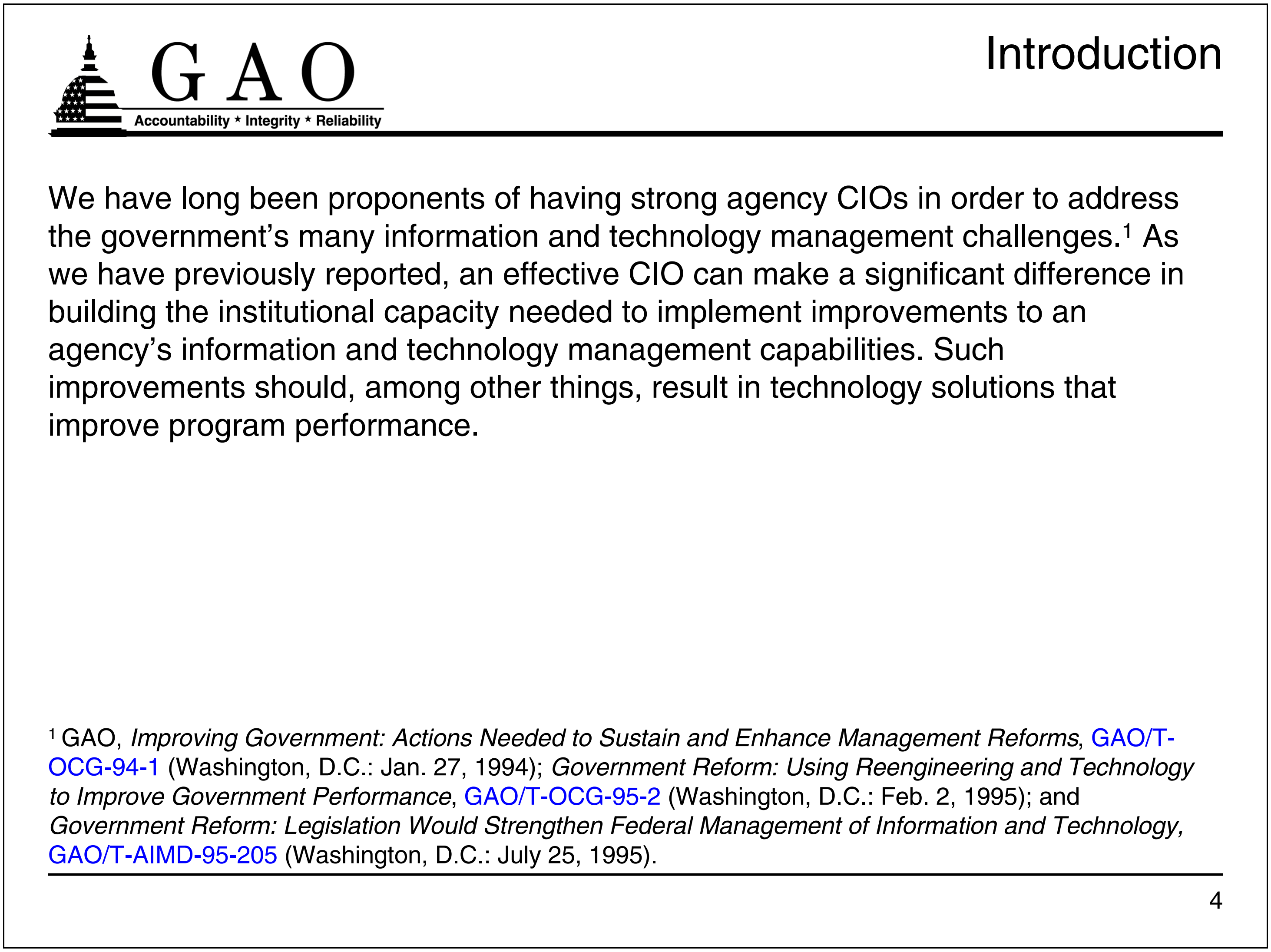
Attachment 3. Comparison of CIO Responsibilities



GAO
Accountability * Integrity * Reliability

Introduction

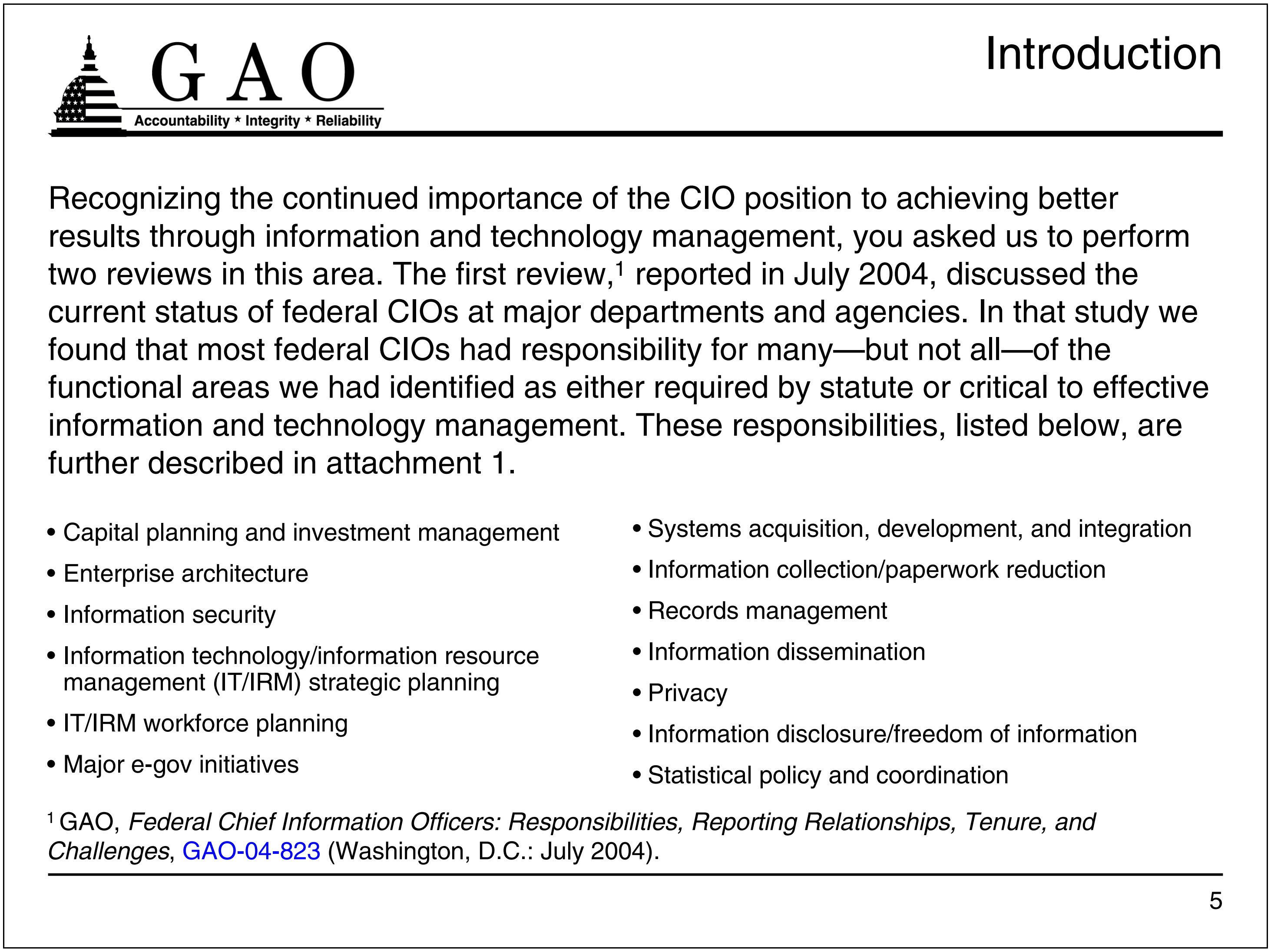
Our work and that of others has shown that the federal government has had long-standing information and technology management problems. Various laws have been enacted to improve the government's performance in this area. For example, the Clinger-Cohen Act of 1996 requires agency heads to designate Chief Information Officers (CIO) to lead reforms to help control system development risks; better manage technology spending; and achieve real, measurable improvements in agency performance through better management of information resources.



Introduction

We have long been proponents of having strong agency CIOs in order to address the government's many information and technology management challenges.[1] As we have previously reported, an effective CIO can make a significant difference in building the institutional capacity needed to implement improvements to an agency's information and technology management capabilities. Such improvements should, among other things, result in technology solutions that improve program performance.

[1] GAO, *Improving Government: Actions Needed to Sustain and Enhance Management Reforms*, GAO/T-OCG-94-1 (Washington, D.C.: Jan. 27, 1994); *Government Reform: Using Reengineering and Technology to Improve Government Performance*, GAO/T-OCG-95-2 (Washington, D.C.: Feb. 2, 1995); and *Government Reform: Legislation Would Strengthen Federal Management of Information and Technology,* GAO/T-AIMD-95-205 (Washington, D.C.: July 25, 1995).



GAO
Accountability * Integrity * Reliability

Introduction

Recognizing the continued importance of the CIO position to achieving better results through information and technology management, you asked us to perform two reviews in this area. The first review,[1] reported in July 2004, discussed the current status of federal CIOs at major departments and agencies. In that study we found that most federal CIOs had responsibility for many—but not all—of the functional areas we had identified as either required by statute or critical to effective information and technology management. These responsibilities, listed below, are further described in attachment 1.

- Capital planning and investment management
- Enterprise architecture
- Information security
- Information technology/information resource management (IT/IRM) strategic planning
- IT/IRM workforce planning
- Major e-gov initiatives
- Systems acquisition, development, and integration
- Information collection/paperwork reduction
- Records management
- Information dissemination
- Privacy
- Information disclosure/freedom of information
- Statistical policy and coordination

[1] GAO, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, GAO-04-823 (Washington, D.C.: July 2004).

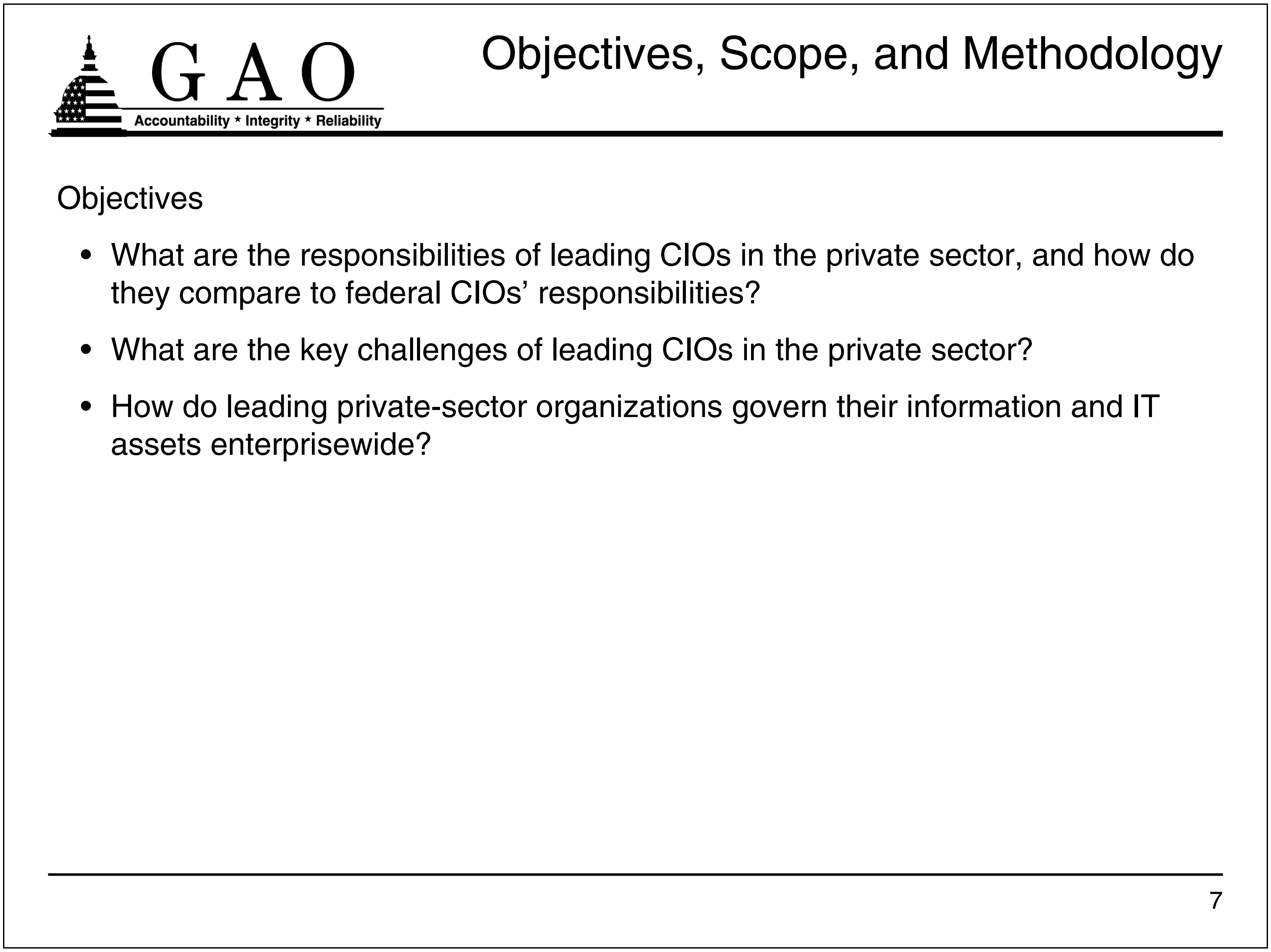
GAO
Accountability * Integrity * Reliability

Introduction

This briefing summarizes what we found regarding the responsibilities of 20 CIOs of leading organizations in the private sector. Along with our earlier report reviewing the responsibilities of federal CIOs[1] and work addressing the high-level organization and support of the CIO position in the private sector,[2] these reports provide Congress and others with information describing the responsibilities of CIOs in both the federal government and the private sector.

[1] GAO-04-823.

[2] GAO, *Maximizing the Success of Chief Information Officers: Learning from Leading Organizations*, GAO-01-376G (Washington, D.C.: February 2001).



GAO
Accountability * Integrity * Reliability

Objectives, Scope, and Methodology

Objectives

- What are the responsibilities of leading CIOs in the private sector, and how do they compare to federal CIOs’ responsibilities?
- What are the key challenges of leading CIOs in the private sector?
- How do leading private-sector organizations govern their information and IT assets enterprisewide?

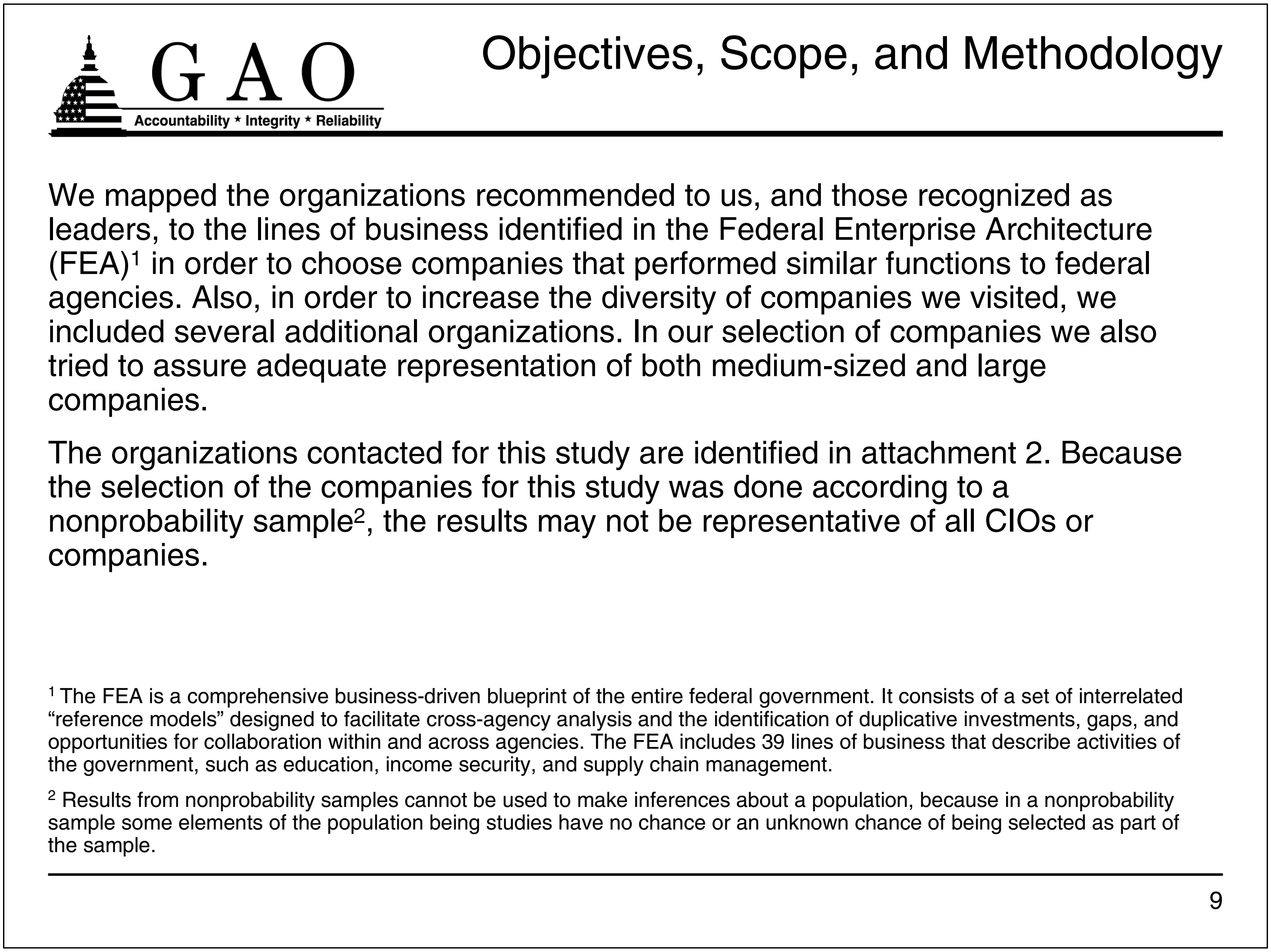
GAO
Accountability * Integrity * Reliability

Objectives, Scope, and Methodology

To address our objectives, we identified prospective companies based on their recognition as leaders in the field of information and technology management and the likelihood that they would perform functions similar to those of federal agencies.

First, we selected companies that had been identified as leaders in IT by industry organizations, publications, and experts. Specifically:

- We solicited recommendations from consulting firms and from academic and industry experts.
- We searched published and Internet sources for the names of companies and CIOs that were recognized as leaders by industry organizations and publications, for example, *CIO* magazine and *InfoWorld*.



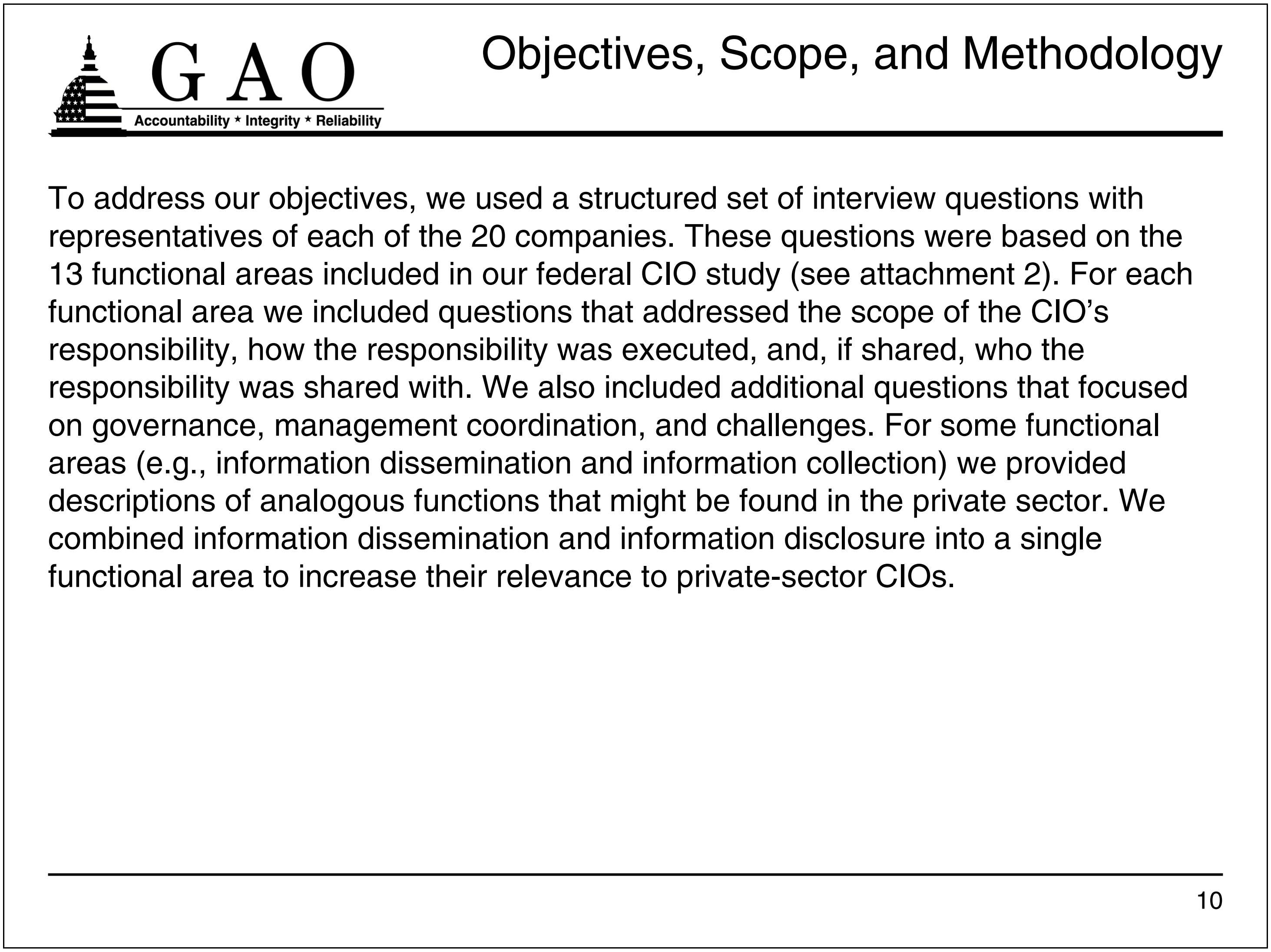
Objectives, Scope, and Methodology

We mapped the organizations recommended to us, and those recognized as leaders, to the lines of business identified in the Federal Enterprise Architecture (FEA)[1] in order to choose companies that performed similar functions to federal agencies. Also, in order to increase the diversity of companies we visited, we included several additional organizations. In our selection of companies we also tried to assure adequate representation of both medium-sized and large companies.

The organizations contacted for this study are identified in attachment 2. Because the selection of the companies for this study was done according to a nonprobability sample[2], the results may not be representative of all CIOs or companies.

[1] The FEA is a comprehensive business-driven blueprint of the entire federal government. It consists of a set of interrelated “reference models” designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across agencies. The FEA includes 39 lines of business that describe activities of the government, such as education, income security, and supply chain management.

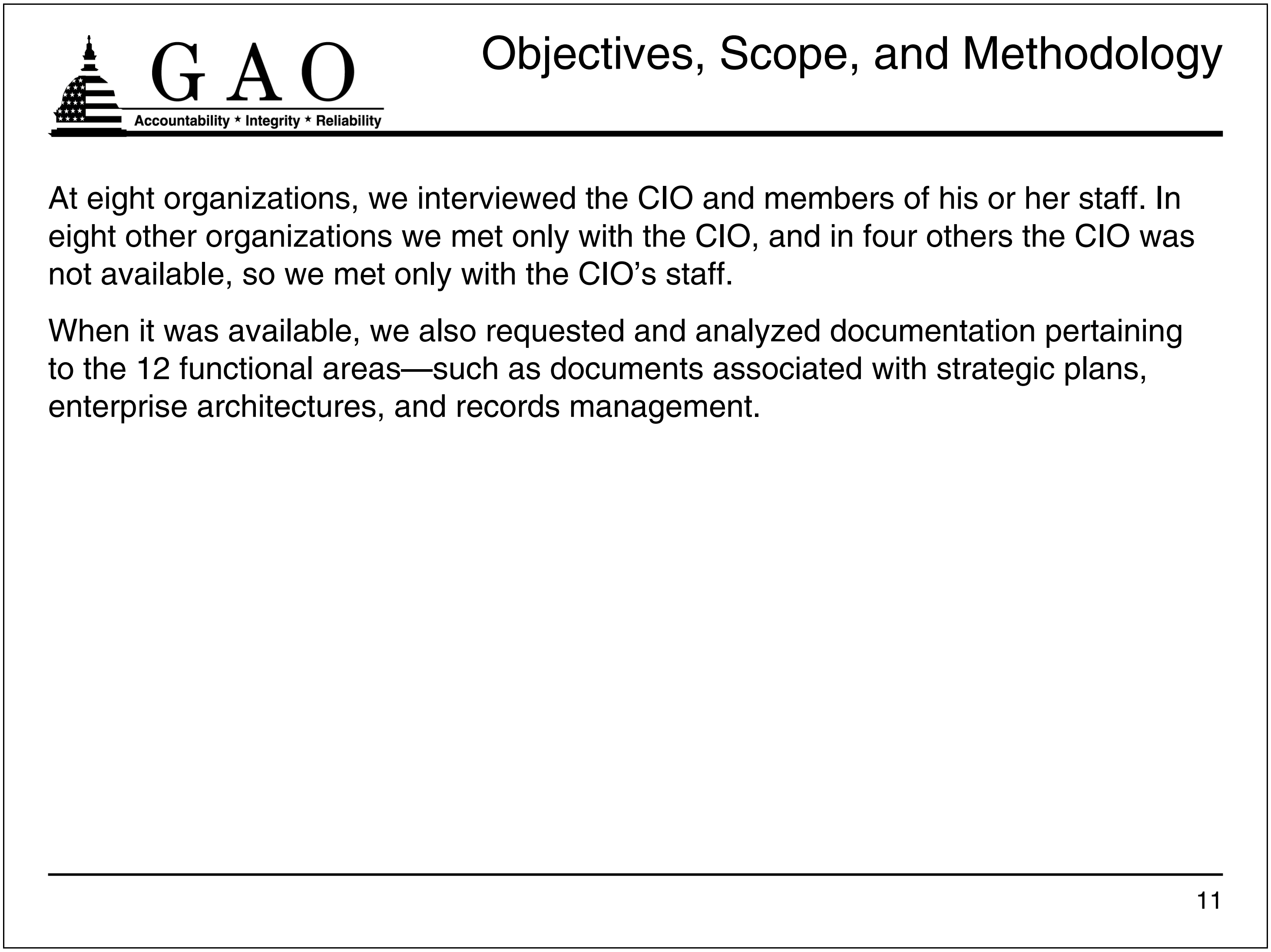
[2] Results from nonprobability samples cannot be used to make inferences about a population, because in a nonprobability sample some elements of the population being studies have no chance or an unknown chance of being selected as part of the sample.



GAO
Accountability * Integrity * Reliability

Objectives, Scope, and Methodology

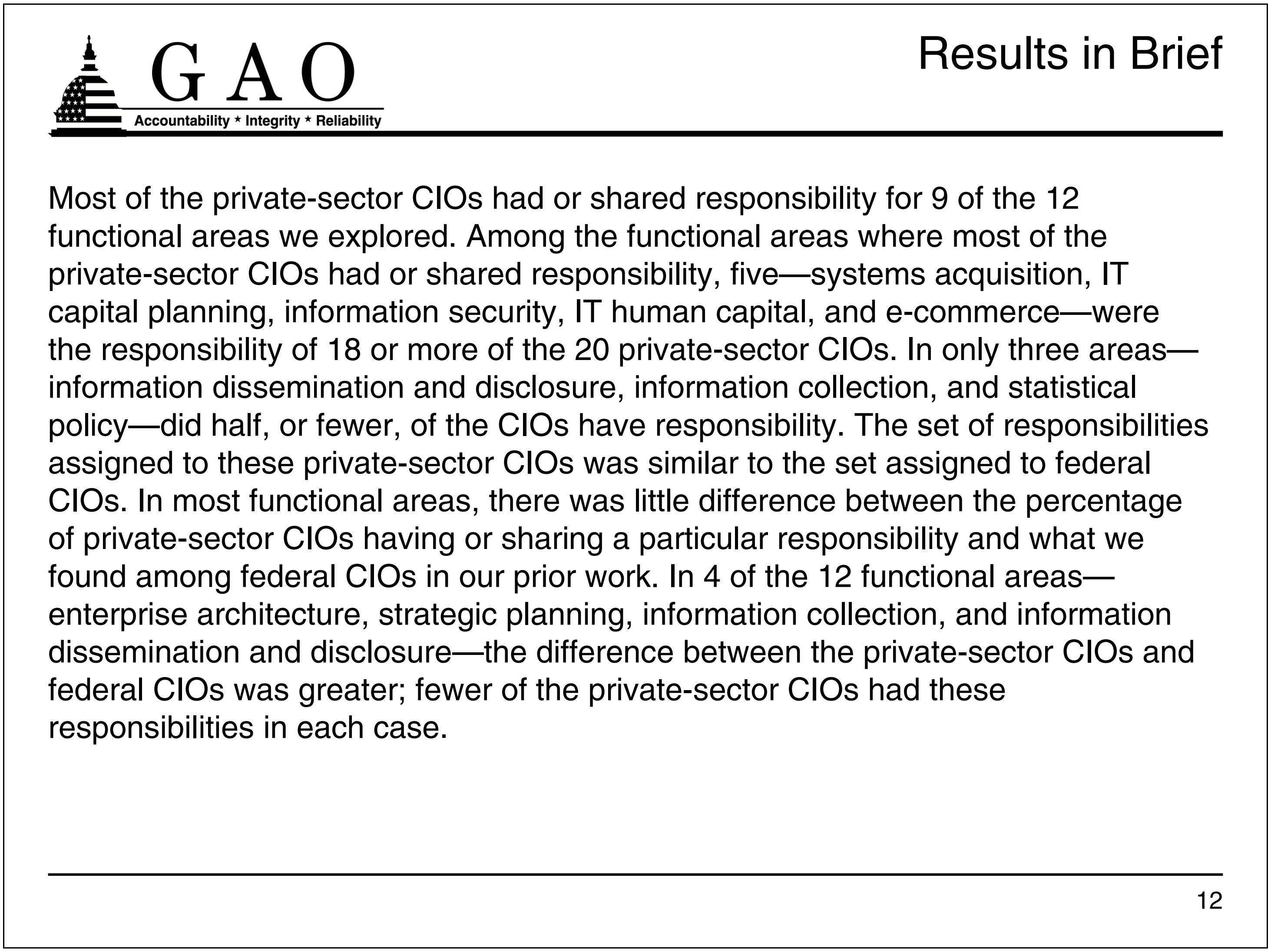
To address our objectives, we used a structured set of interview questions with representatives of each of the 20 companies. These questions were based on the 13 functional areas included in our federal CIO study (see attachment 2). For each functional area we included questions that addressed the scope of the CIO's responsibility, how the responsibility was executed, and, if shared, who the responsibility was shared with. We also included additional questions that focused on governance, management coordination, and challenges. For some functional areas (e.g., information dissemination and information collection) we provided descriptions of analogous functions that might be found in the private sector. We combined information dissemination and information disclosure into a single functional area to increase their relevance to private-sector CIOs.



Objectives, Scope, and Methodology

At eight organizations, we interviewed the CIO and members of his or her staff. In eight other organizations we met only with the CIO, and in four others the CIO was not available, so we met only with the CIO's staff.

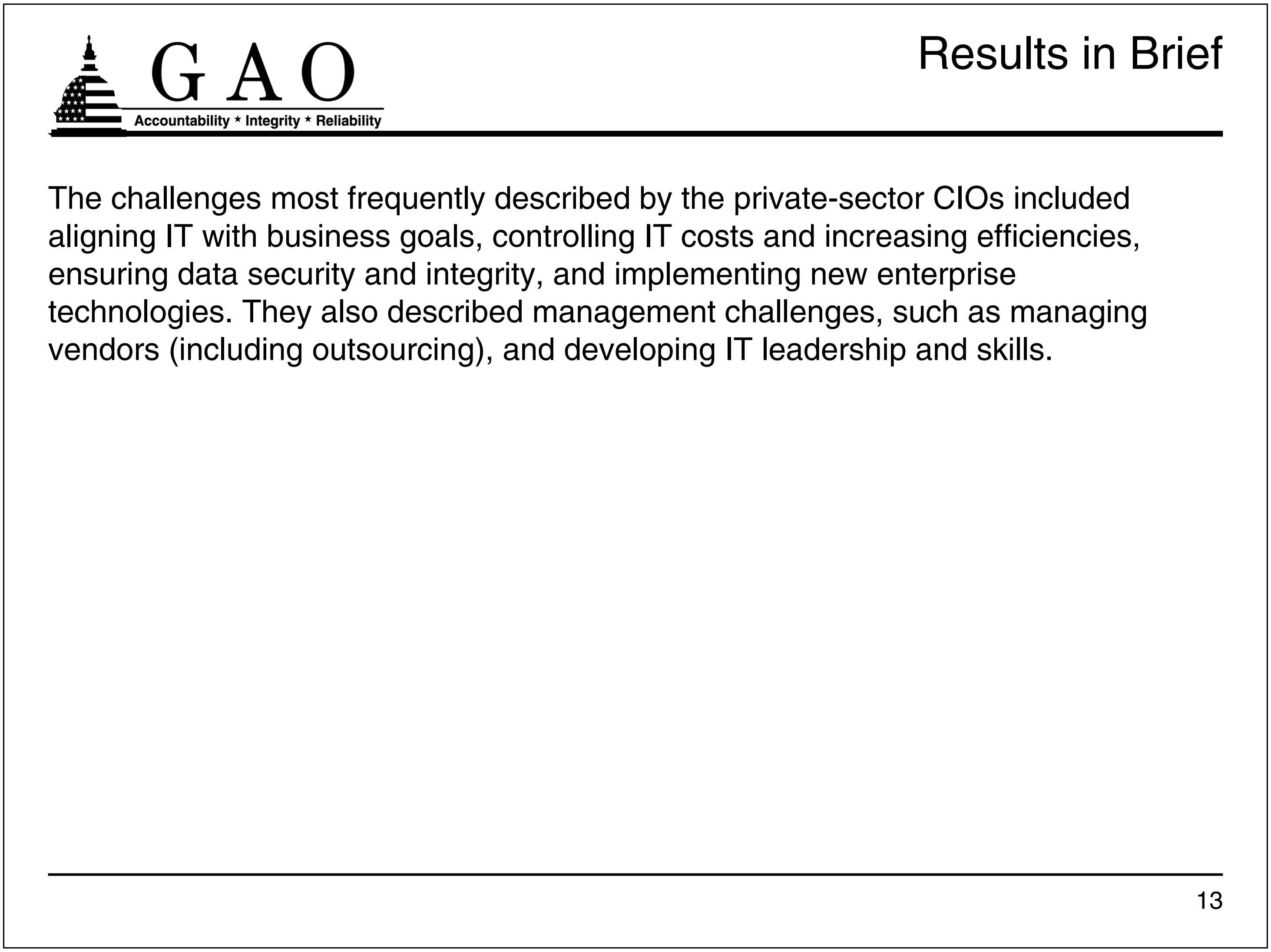
When it was available, we also requested and analyzed documentation pertaining to the 12 functional areas—such as documents associated with strategic plans, enterprise architectures, and records management.



GAO
Accountability * Integrity * Reliability

Results in Brief

Most of the private-sector CIOs had or shared responsibility for 9 of the 12 functional areas we explored. Among the functional areas where most of the private-sector CIOs had or shared responsibility, five—systems acquisition, IT capital planning, information security, IT human capital, and e-commerce—were the responsibility of 18 or more of the 20 private-sector CIOs. In only three areas—information dissemination and disclosure, information collection, and statistical policy—did half, or fewer, of the CIOs have responsibility. The set of responsibilities assigned to these private-sector CIOs was similar to the set assigned to federal CIOs. In most functional areas, there was little difference between the percentage of private-sector CIOs having or sharing a particular responsibility and what we found among federal CIOs in our prior work. In 4 of the 12 functional areas—enterprise architecture, strategic planning, information collection, and information dissemination and disclosure—the difference between the private-sector CIOs and federal CIOs was greater; fewer of the private-sector CIOs had these responsibilities in each case.

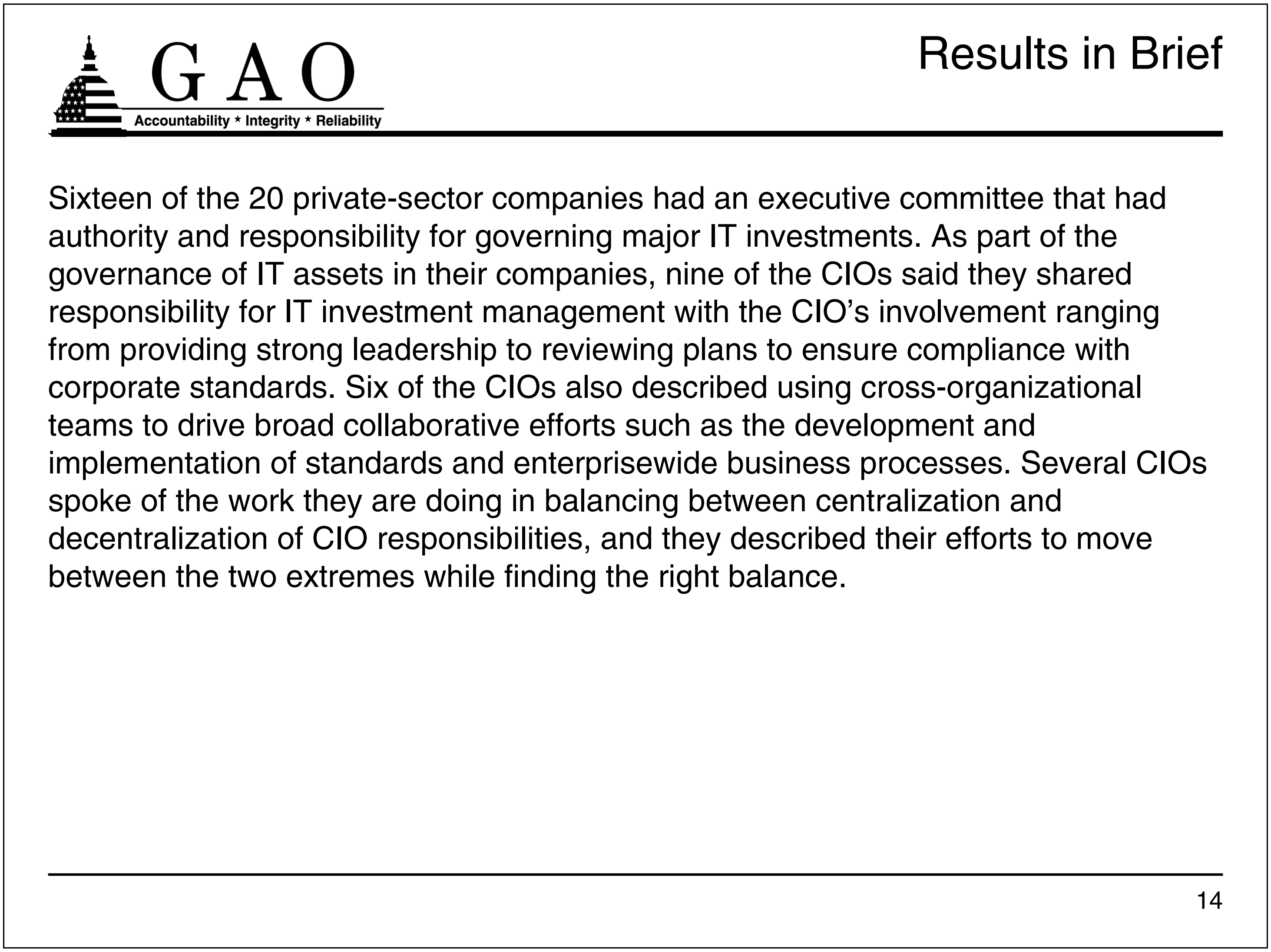


GAO
Accountability * Integrity * Reliability

Results in Brief

The challenges most frequently described by the private-sector CIOs included aligning IT with business goals, controlling IT costs and increasing efficiencies, ensuring data security and integrity, and implementing new enterprise technologies. They also described management challenges, such as managing vendors (including outsourcing), and developing IT leadership and skills.

13

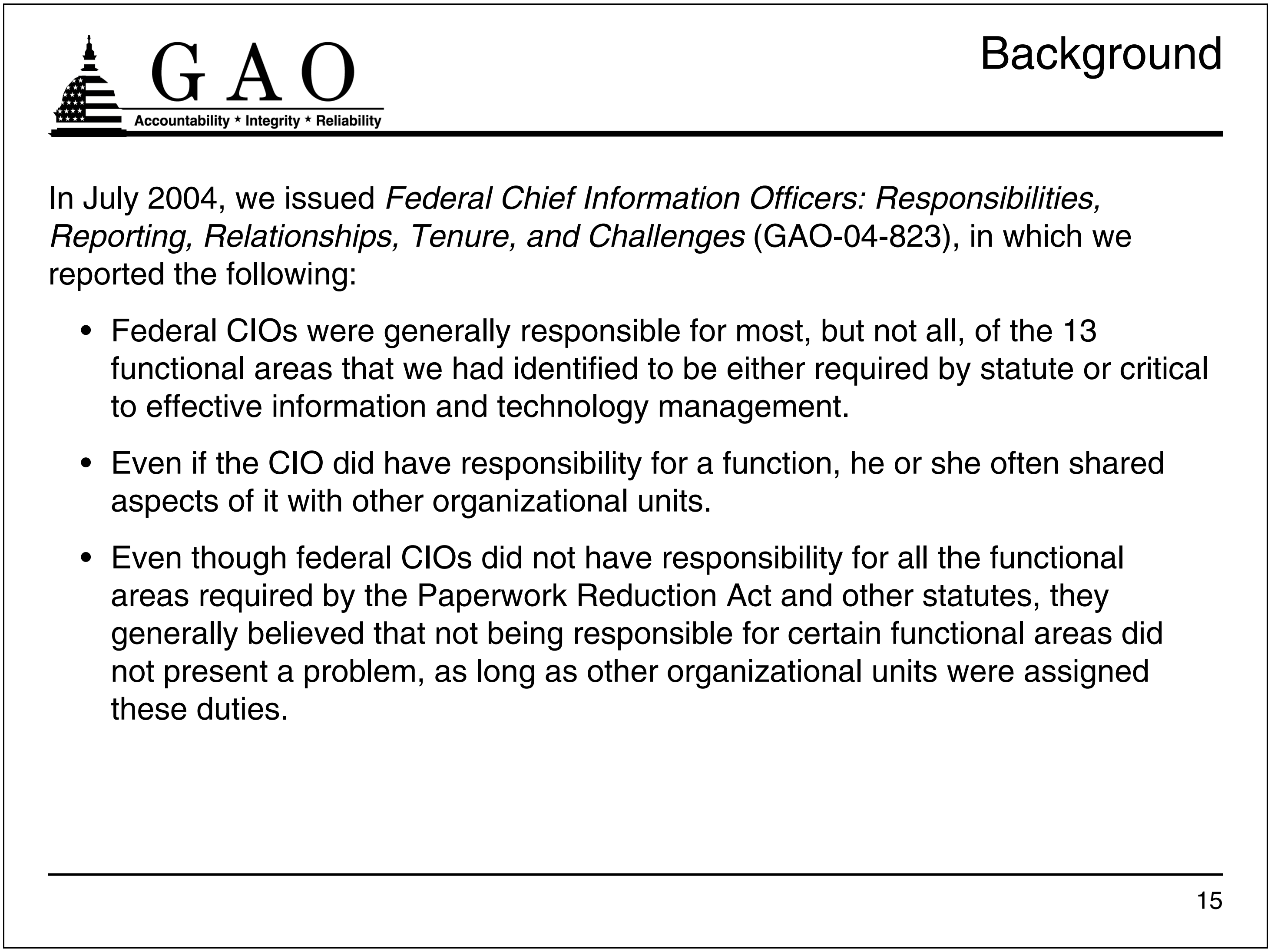


GAO
Accountability * Integrity * Reliability

Results in Brief

Sixteen of the 20 private-sector companies had an executive committee that had authority and responsibility for governing major IT investments. As part of the governance of IT assets in their companies, nine of the CIOs said they shared responsibility for IT investment management with the CIO’s involvement ranging from providing strong leadership to reviewing plans to ensure compliance with corporate standards. Six of the CIOs also described using cross-organizational teams to drive broad collaborative efforts such as the development and implementation of standards and enterprisewide business processes. Several CIOs spoke of the work they are doing in balancing between centralization and decentralization of CIO responsibilities, and they described their efforts to move between the two extremes while finding the right balance.

14



Background

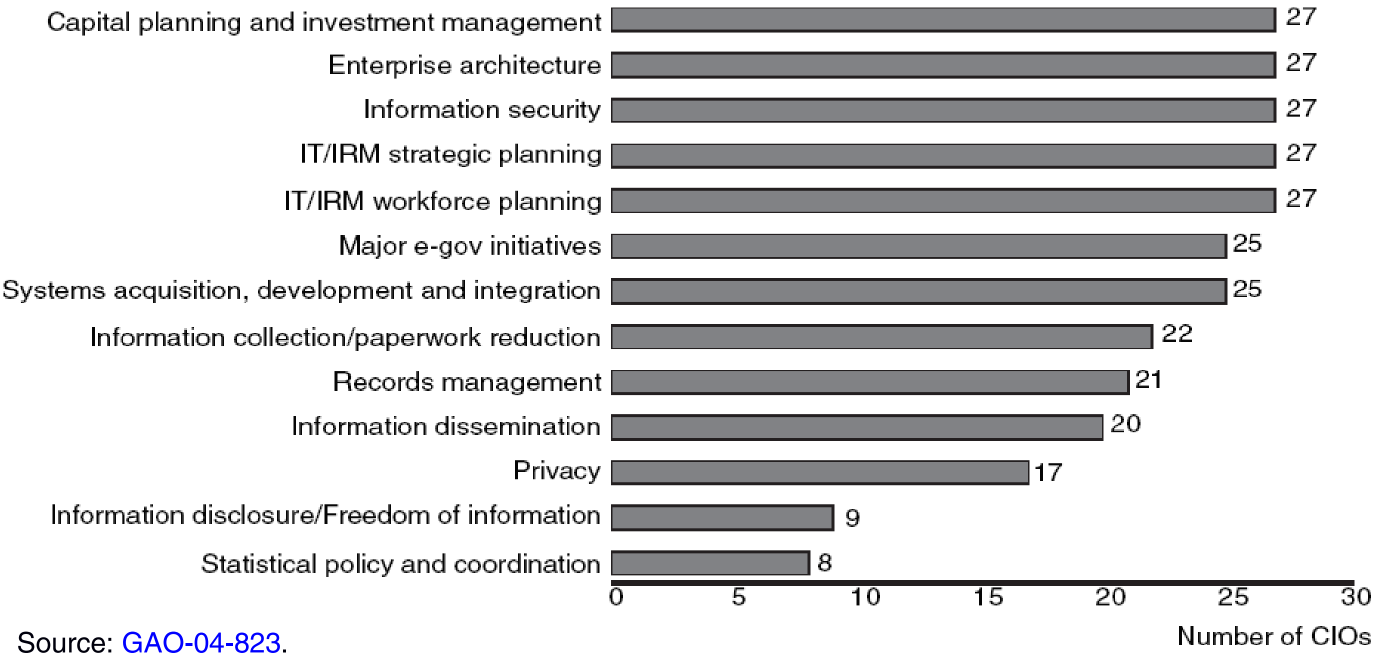
In July 2004, we issued *Federal Chief Information Officers: Responsibilities, Reporting, Relationships, Tenure, and Challenges* (GAO-04-823), in which we reported the following:

- Federal CIOs were generally responsible for most, but not all, of the 13 functional areas that we had identified to be either required by statute or critical to effective information and technology management.
- Even if the CIO did have responsibility for a function, he or she often shared aspects of it with other organizational units.
- Even though federal CIOs did not have responsibility for all the functional areas required by the Paperwork Reduction Act and other statutes, they generally believed that not being responsible for certain functional areas did not present a problem, as long as other organizational units were assigned these duties.

GAO
Accountability * Integrity * Reliability

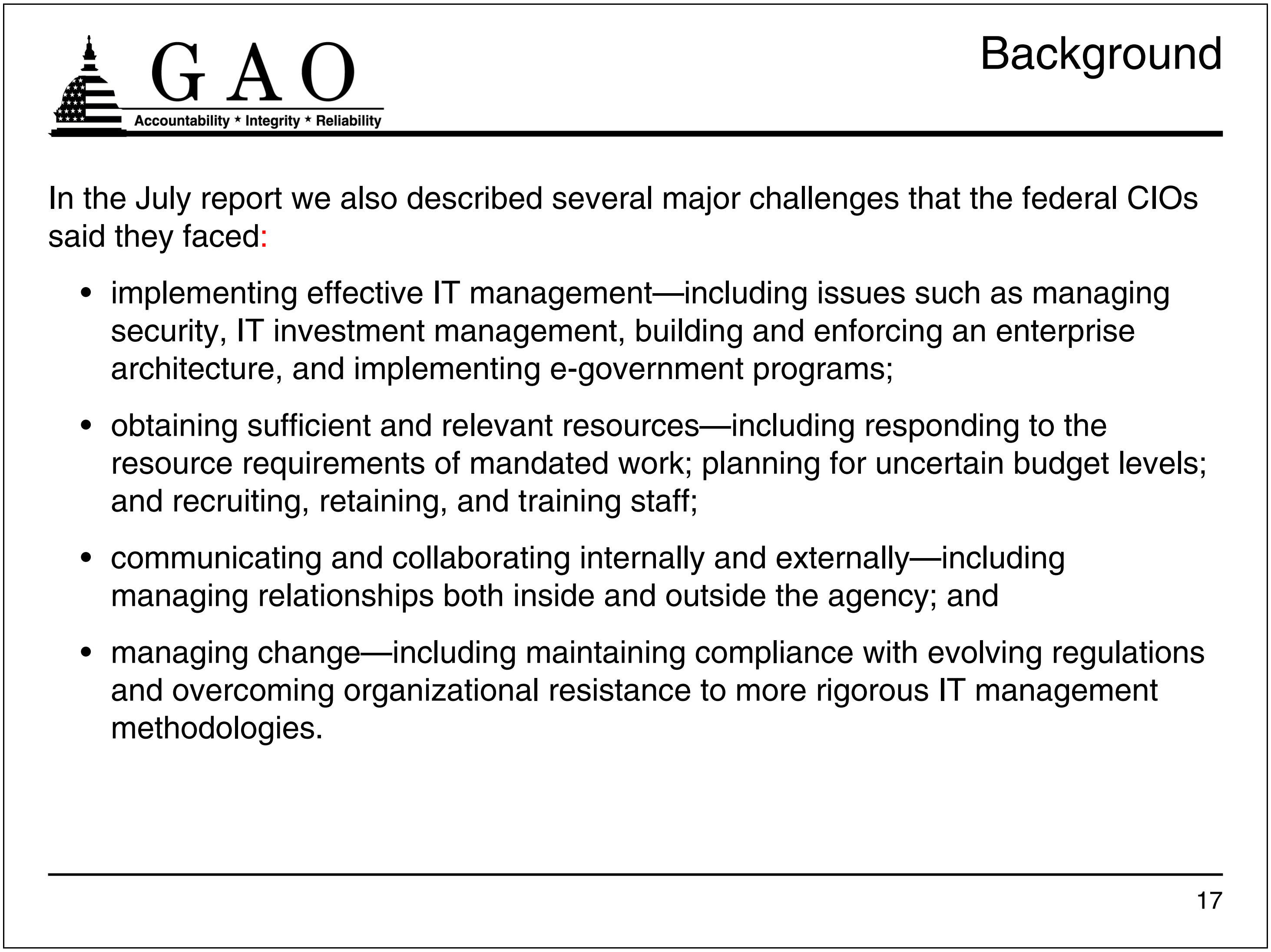
Background

Number of Federal CIOs with Responsibility for Information and Technology Management Areas (n = 27)



Source: GAO-04-823.

16



GAO Accountability * Integrity * Reliability

Background

In the July report we also described several major challenges that the federal CIOs said they faced:

- implementing effective IT management—including issues such as managing security, IT investment management, building and enforcing an enterprise architecture, and implementing e-government programs;
- obtaining sufficient and relevant resources—including responding to the resource requirements of mandated work; planning for uncertain budget levels; and recruiting, retaining, and training staff;
- communicating and collaborating internally and externally—including managing relationships both inside and outside the agency; and
- managing change—including maintaining compliance with evolving regulations and overcoming organizational resistance to more rigorous IT management methodologies.

17

GAO
Accountability * Integrity * Reliability

Responsibilities of Private-Sector CIOs

Most of the private-sector CIOs had or shared responsibility[1] for 9 of the 12 functional areas. Among the 9 functional areas where the majority of the private-sector CIOs had or shared responsibility, 5 of them—systems acquisition, IT capital planning, information security, IT human capital, and e-commerce—were the responsibility of 18 or more of the 20 private-sector CIOs. In only three areas—information dissemination and disclosure,[2] information collection, and statistical policy—did half, or fewer, of the CIOs have responsibility.

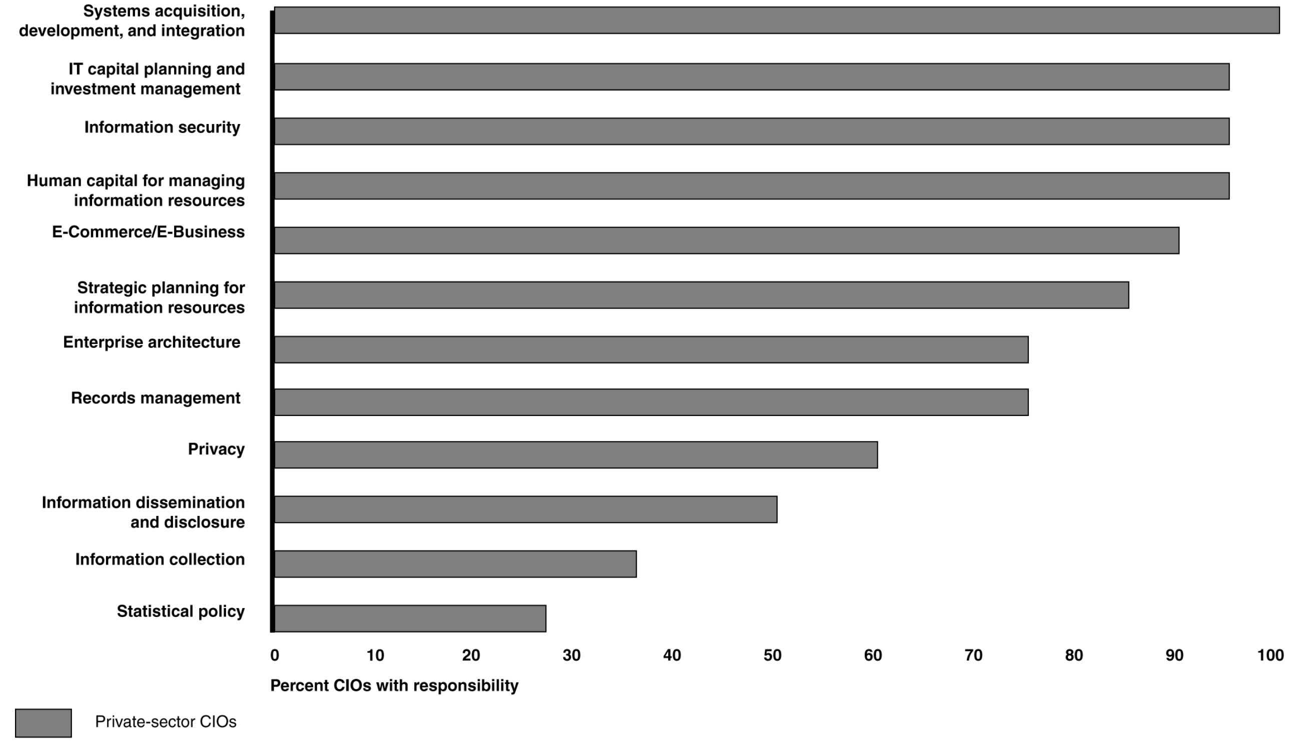
The following chart shows the 12 functional areas covered in this study and the number of the private-sector CIOs who had or shared responsibility for each area.

[1] Shared responsibility refers to CIOs whose responsibility is limited in scope or who provide active support in carrying out the responsibilities for a function even though they may not have primary responsibility.

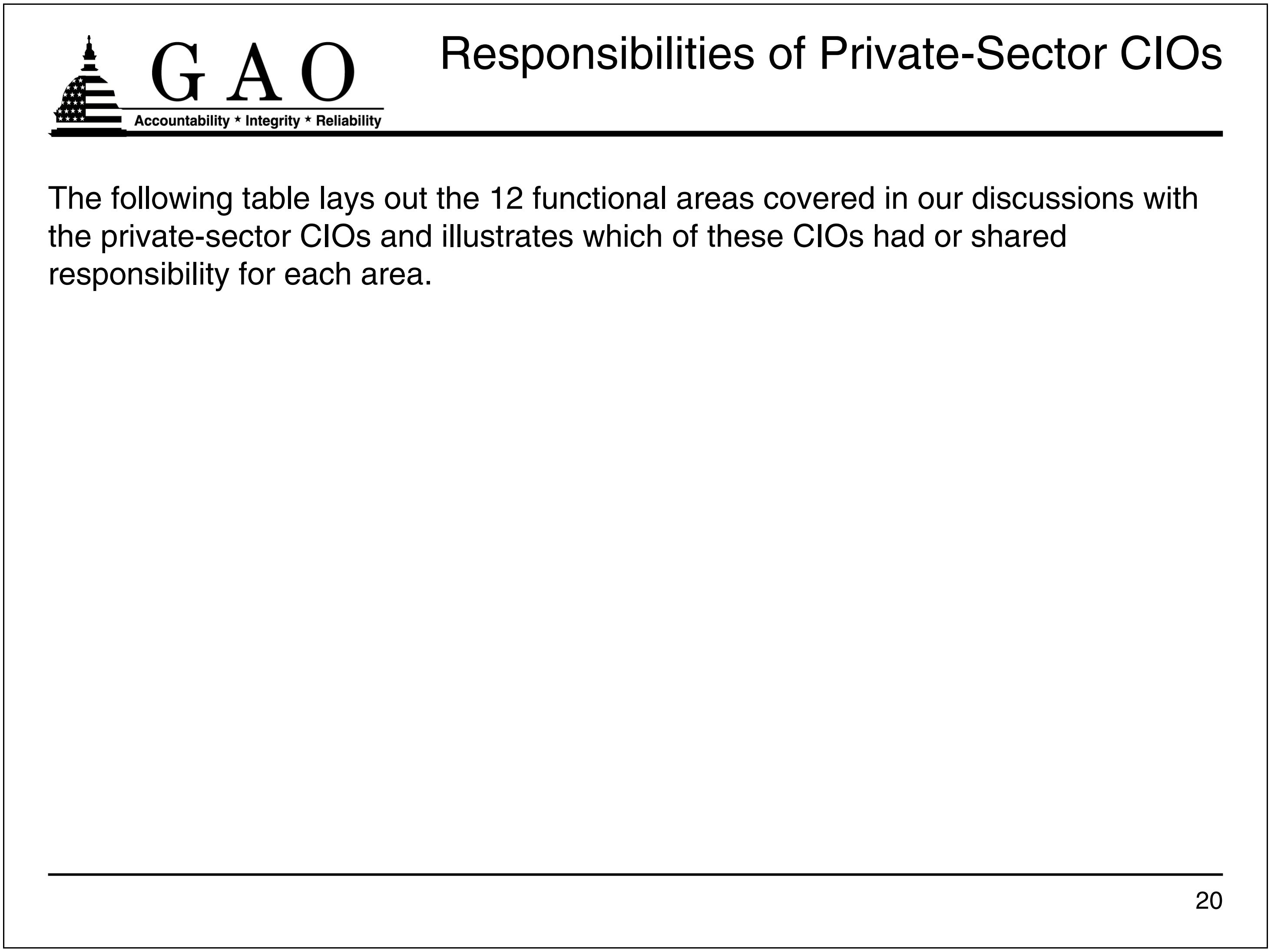
[2] Information dissemination and information disclosure were combined into a single function in the private-sector survey in order to increase the function's relevance for private-sector CIOs.

Responsibilities of Private-Sector CIOs

Percentage of Private-Sector CIOs with Responsibility for Information and Technology Management Areas

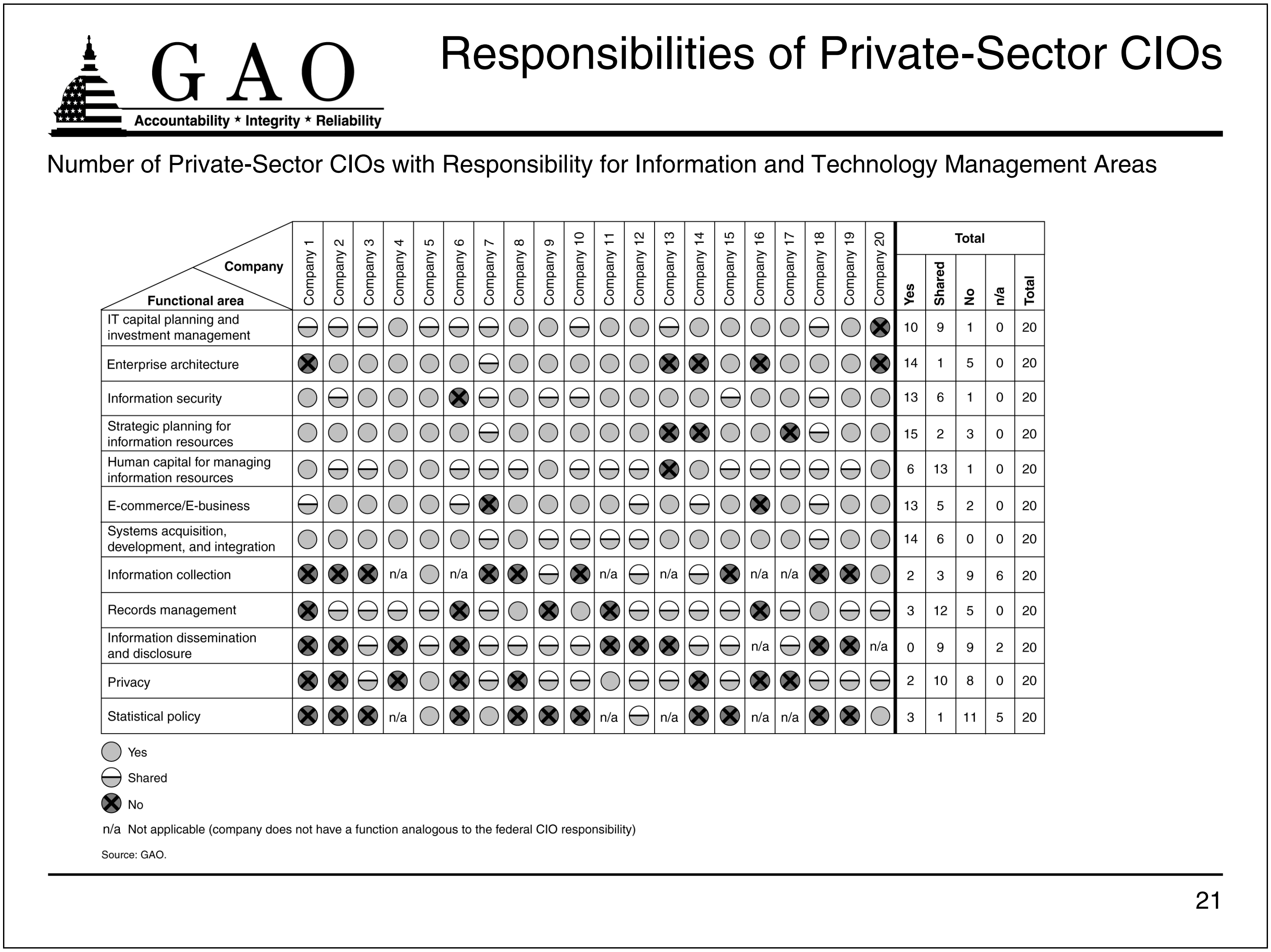


Source: GAO.



Responsibilities of Private-Sector CIOs

The following table lays out the 12 functional areas covered in our discussions with the private-sector CIOs and illustrates which of these CIOs had or shared responsibility for each area.



GAO

Accountability * Integrity * Reliability

Responsibilities of Private-Sector CIOs

Number of Private-Sector CIOs with Responsibility for Information and Technology Management Areas

Company Functional area	Company 1	Company 2	Company 3	Company 4	Company 5	Company 6	Company 7	Company 8	Company 9	Company 10	Company 11	Company 12	Company 13	Company 14	Company 15	Company 16	Company 17	Company 18	Company 19	Company 20	Total				
																					Yes	Shared	No	n/a	Total
IT capital planning and investment management	⊖	⊖	⊖	●	⊖	⊖	⊖	●	●	⊖	●	●	⊖	●	●	●	●	⊖	●	⊗	10	9	1	0	20
Enterprise architecture	⊗	●	●	●	●	●	⊖	●	●	●	●	●	⊗	⊗	●	⊗	●	●	●	⊗	14	1	5	0	20
Information security	●	⊖	●	●	●	⊗	⊖	●	⊖	⊖	●	●	●	●	⊖	●	●	⊖	●	●	13	6	1	0	20
Strategic planning for information resources	●	●	●	●	●	●	⊖	●	●	●	●	●	⊗	⊗	●	●	⊗	⊖	●	●	15	2	3	0	20
Human capital for managing information resources	●	⊖	⊖	●	●	⊖	⊖	⊖	●	⊖	⊖	⊖	⊗	●	⊖	⊖	⊖	⊖	⊖	●	6	13	1	0	20
E-commerce/E-business	⊖	●	●	●	●	⊖	⊗	●	●	●	●	⊖	●	⊖	●	⊗	●	⊖	●	●	13	5	2	0	20
Systems acquisition, development, and integration	●	●	●	●	●	●	⊖	●	⊖	⊖	⊖	⊖	●	●	●	●	●	⊖	●	●	14	6	0	0	20
Information collection	⊗	⊗	⊗	n/a	●	n/a	⊗	⊗	⊖	⊗	n/a	⊖	n/a	⊖	⊗	n/a	n/a	⊗	⊗	●	2	3	9	6	20
Records management	⊗	⊖	⊖	⊖	⊖	⊗	⊖	●	⊗	●	⊗	⊖	⊖	⊖	⊖	⊗	⊖	●	⊖	⊖	3	12	5	0	20
Information dissemination and disclosure	⊗	⊗	⊖	⊗	⊖	⊗	⊖	⊖	⊖	⊖	⊗	⊗	⊗	⊖	⊖	n/a	⊖	⊗	⊗	n/a	0	9	9	2	20
Privacy	⊗	⊗	⊖	⊗	●	⊗	⊖	⊗	⊖	⊖	●	⊖	⊖	⊗	⊖	⊗	⊗	⊖	⊖	⊖	2	10	8	0	20
Statistical policy	⊗	⊗	⊗	n/a	●	⊗	●	⊗	⊗	⊗	n/a	⊖	n/a	⊗	⊗	n/a	n/a	⊗	⊗	●	3	1	11	5	20

● Yes

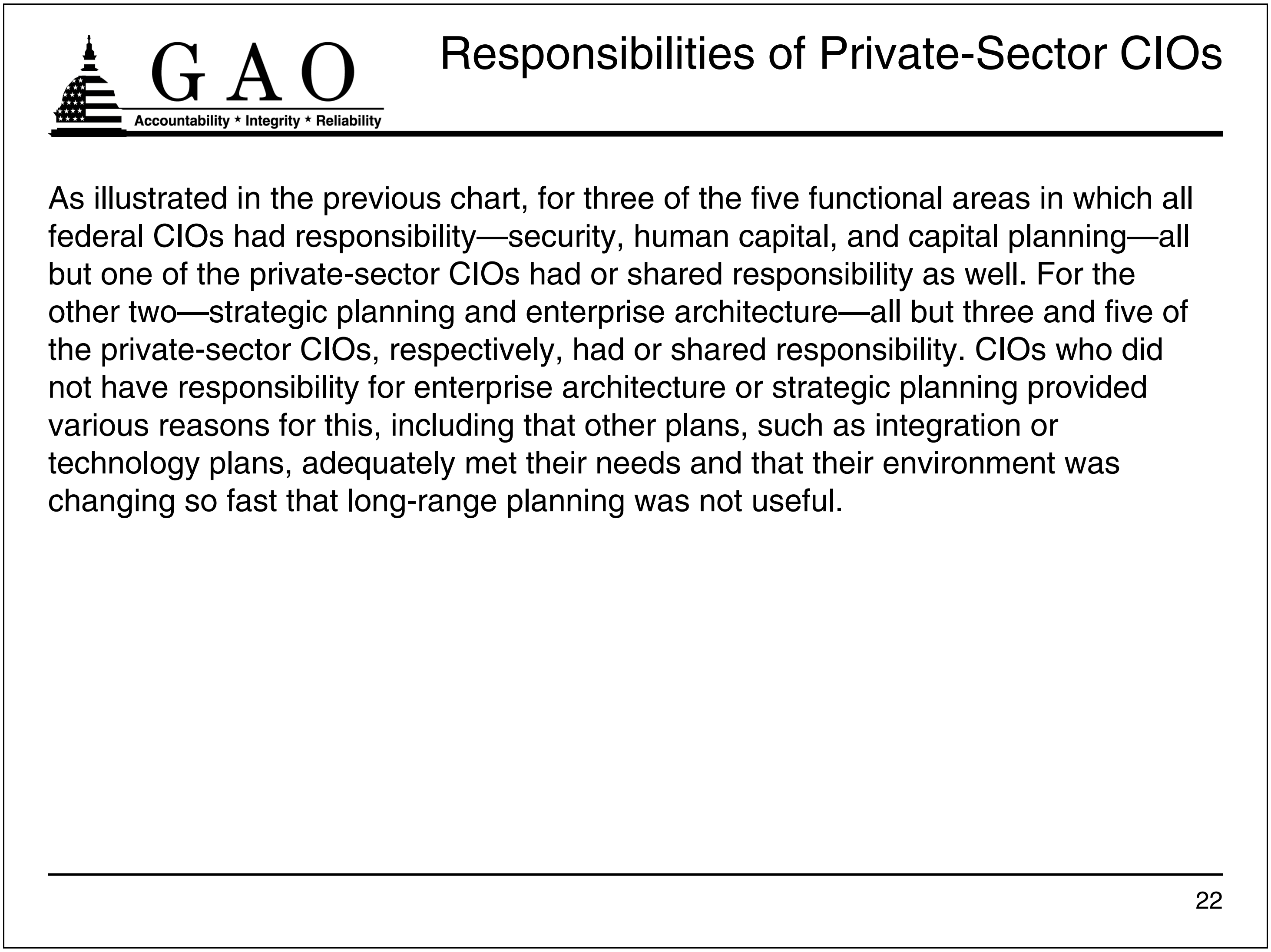
⊖ Shared

⊗ No

n/a Not applicable (company does not have a function analogous to the federal CIO responsibility)

Source: GAO.

21

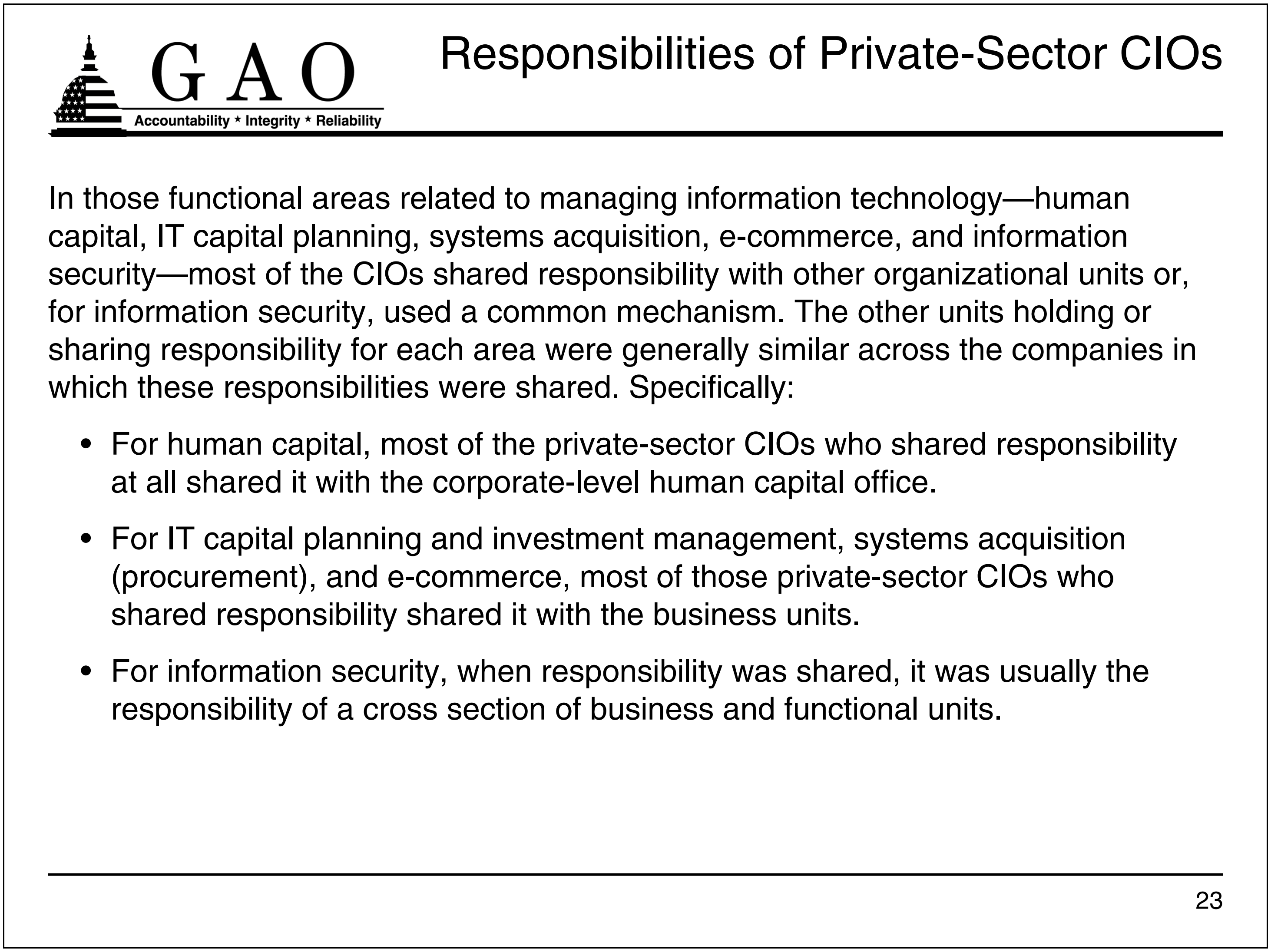


GAO Accountability * Integrity * Reliability

Responsibilities of Private-Sector CIOs

As illustrated in the previous chart, for three of the five functional areas in which all federal CIOs had responsibility—security, human capital, and capital planning—all but one of the private-sector CIOs had or shared responsibility as well. For the other two—strategic planning and enterprise architecture—all but three and five of the private-sector CIOs, respectively, had or shared responsibility. CIOs who did not have responsibility for enterprise architecture or strategic planning provided various reasons for this, including that other plans, such as integration or technology plans, adequately met their needs and that their environment was changing so fast that long-range planning was not useful.

22

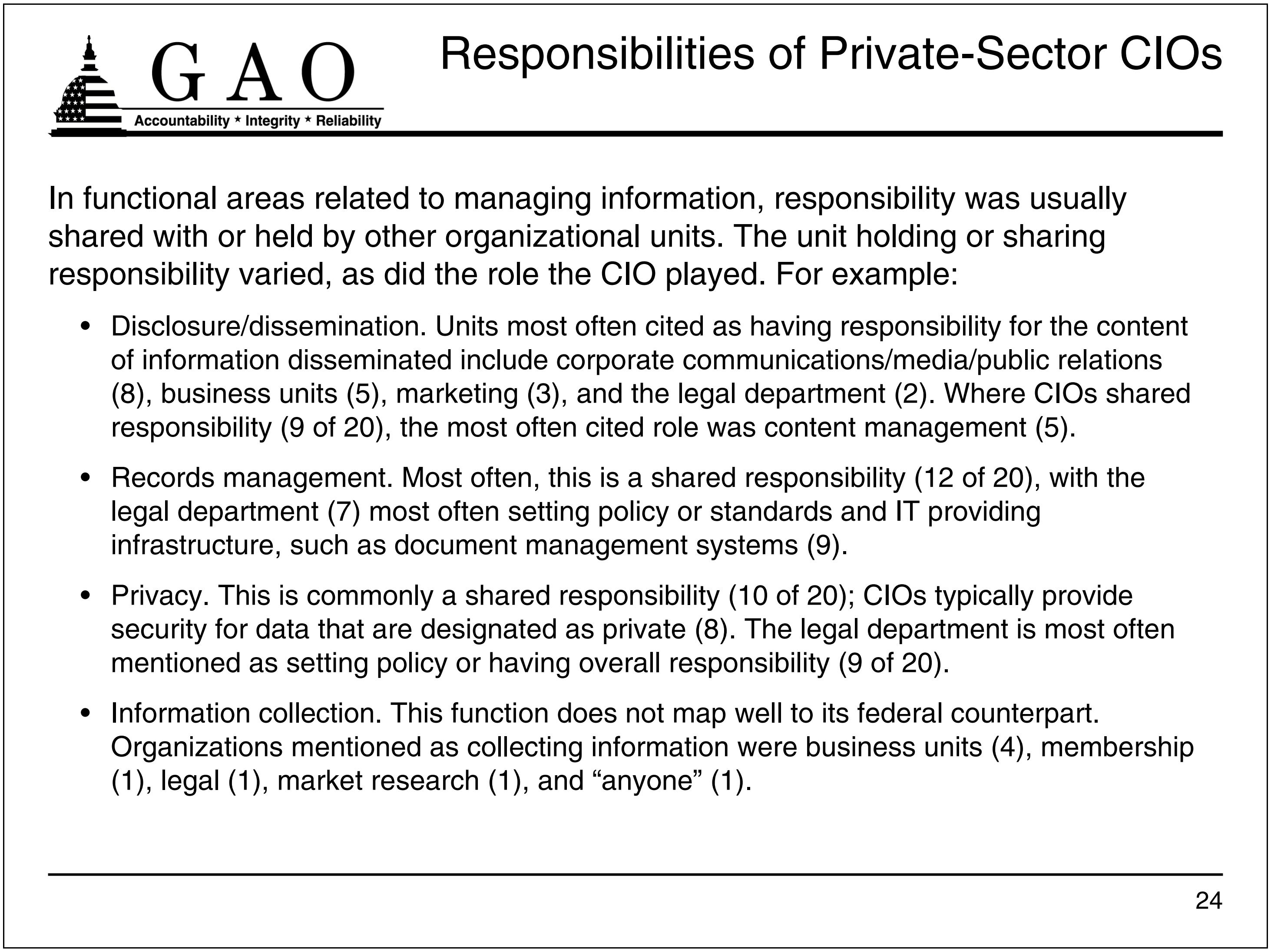


Responsibilities of Private-Sector CIOs

In those functional areas related to managing information technology—human capital, IT capital planning, systems acquisition, e-commerce, and information security—most of the CIOs shared responsibility with other organizational units or, for information security, used a common mechanism. The other units holding or sharing responsibility for each area were generally similar across the companies in which these responsibilities were shared. Specifically:

- For human capital, most of the private-sector CIOs who shared responsibility at all shared it with the corporate-level human capital office.
- For IT capital planning and investment management, systems acquisition (procurement), and e-commerce, most of those private-sector CIOs who shared responsibility shared it with the business units.
- For information security, when responsibility was shared, it was usually the responsibility of a cross section of business and functional units.

23



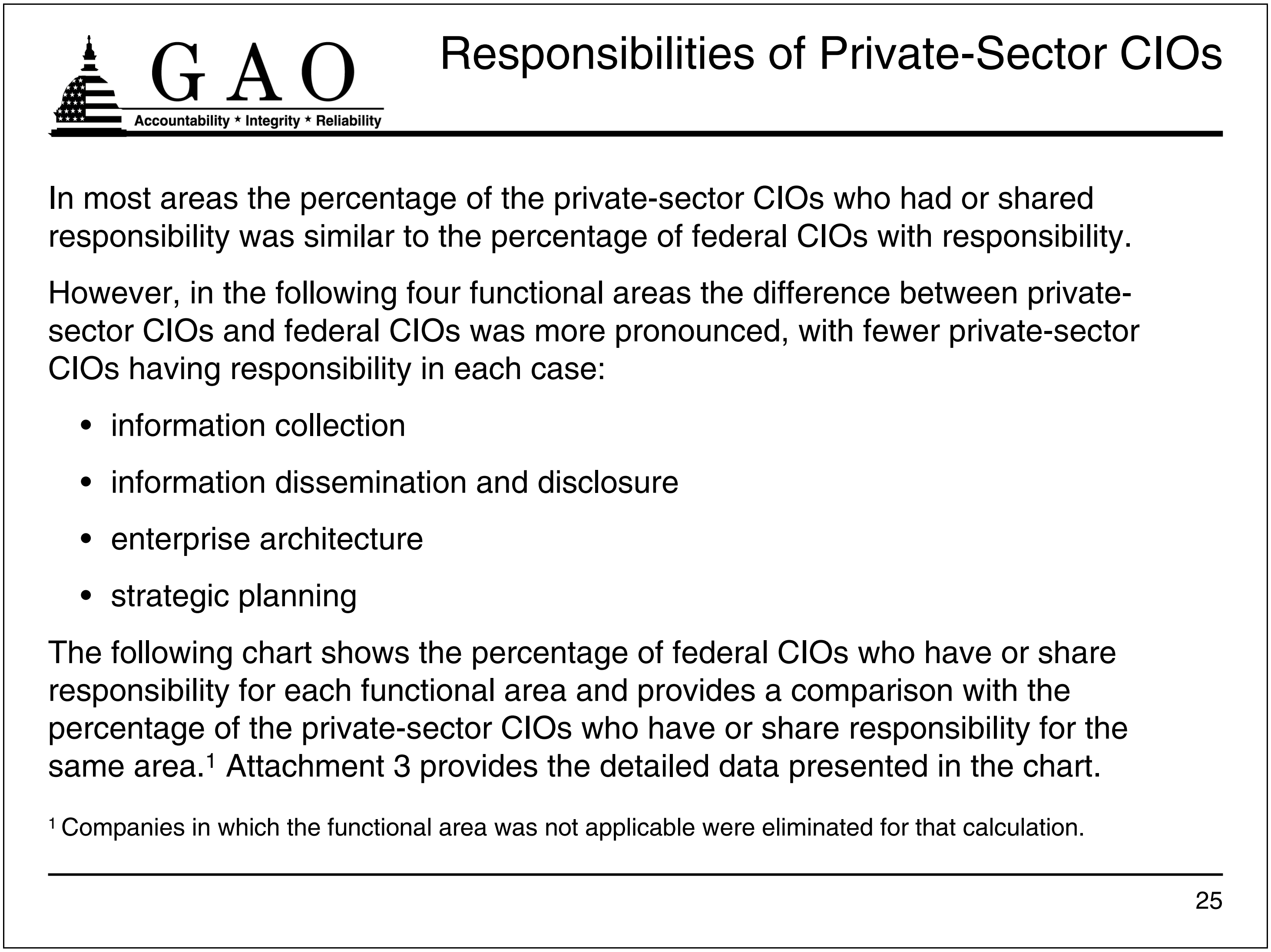
GAO
Accountability * Integrity * Reliability

Responsibilities of Private-Sector CIOs

In functional areas related to managing information, responsibility was usually shared with or held by other organizational units. The unit holding or sharing responsibility varied, as did the role the CIO played. For example:

- Disclosure/dissemination. Units most often cited as having responsibility for the content of information disseminated include corporate communications/media/public relations (8), business units (5), marketing (3), and the legal department (2). Where CIOs shared responsibility (9 of 20), the most often cited role was content management (5).
- Records management. Most often, this is a shared responsibility (12 of 20), with the legal department (7) most often setting policy or standards and IT providing infrastructure, such as document management systems (9).
- Privacy. This is commonly a shared responsibility (10 of 20); CIOs typically provide security for data that are designated as private (8). The legal department is most often mentioned as setting policy or having overall responsibility (9 of 20).
- Information collection. This function does not map well to its federal counterpart. Organizations mentioned as collecting information were business units (4), membership (1), legal (1), market research (1), and “anyone” (1).

24



GAO

Accountability * Integrity * Reliability

Responsibilities of Private-Sector CIOs

In most areas the percentage of the private-sector CIOs who had or shared responsibility was similar to the percentage of federal CIOs with responsibility.

However, in the following four functional areas the difference between private-sector CIOs and federal CIOs was more pronounced, with fewer private-sector CIOs having responsibility in each case:

- information collection
- information dissemination and disclosure
- enterprise architecture
- strategic planning

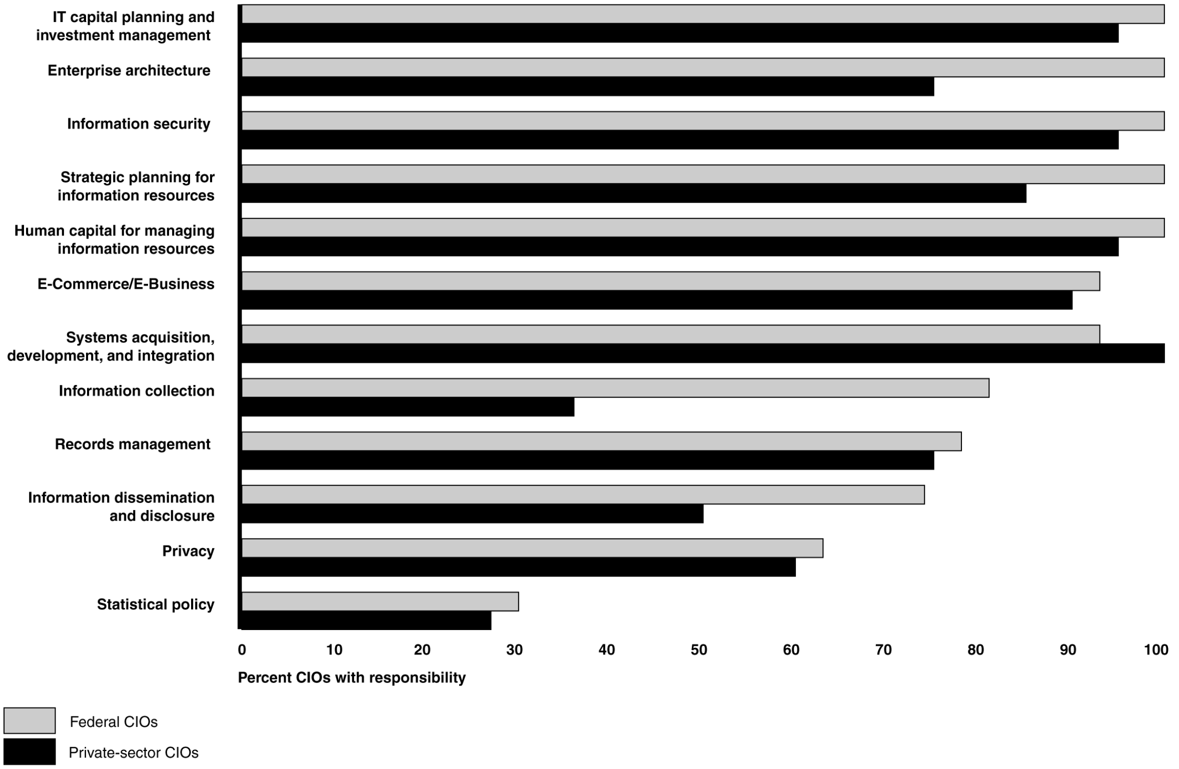
The following chart shows the percentage of federal CIOs who have or share responsibility for each functional area and provides a comparison with the percentage of the private-sector CIOs who have or share responsibility for the same area.[1] Attachment 3 provides the detailed data presented in the chart.

[1] Companies in which the functional area was not applicable were eliminated for that calculation.

GAO
Accountability * Integrity * Reliability

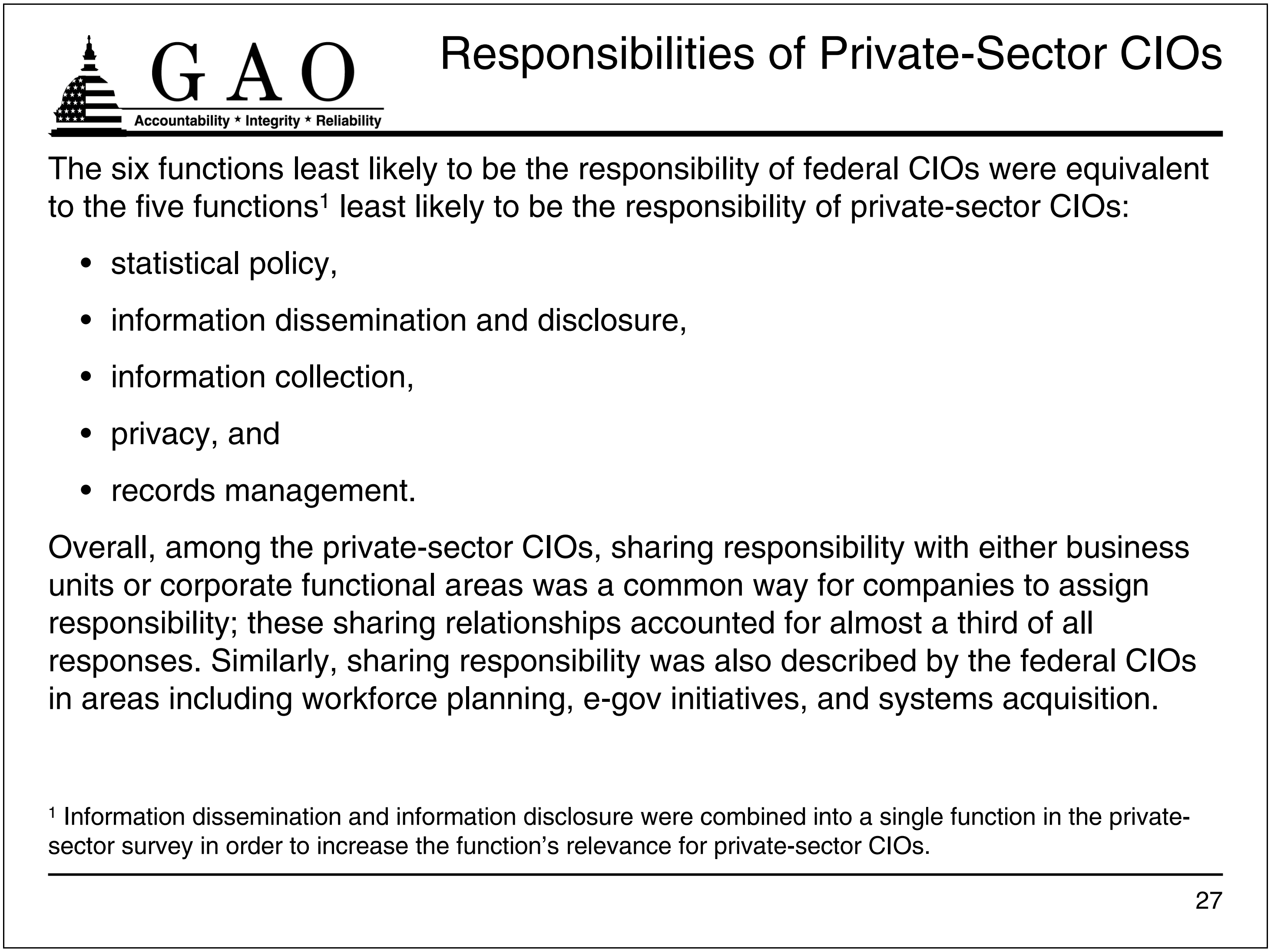
Comparison Chart: Private-Sector Versus Federal CIO Responsibilities

Comparison of the Extent to Which Private-Sector and Federal CIOs Are Responsible for Functional Areas



Source: GAO.

26



GAO
Accountability * Integrity * Reliability

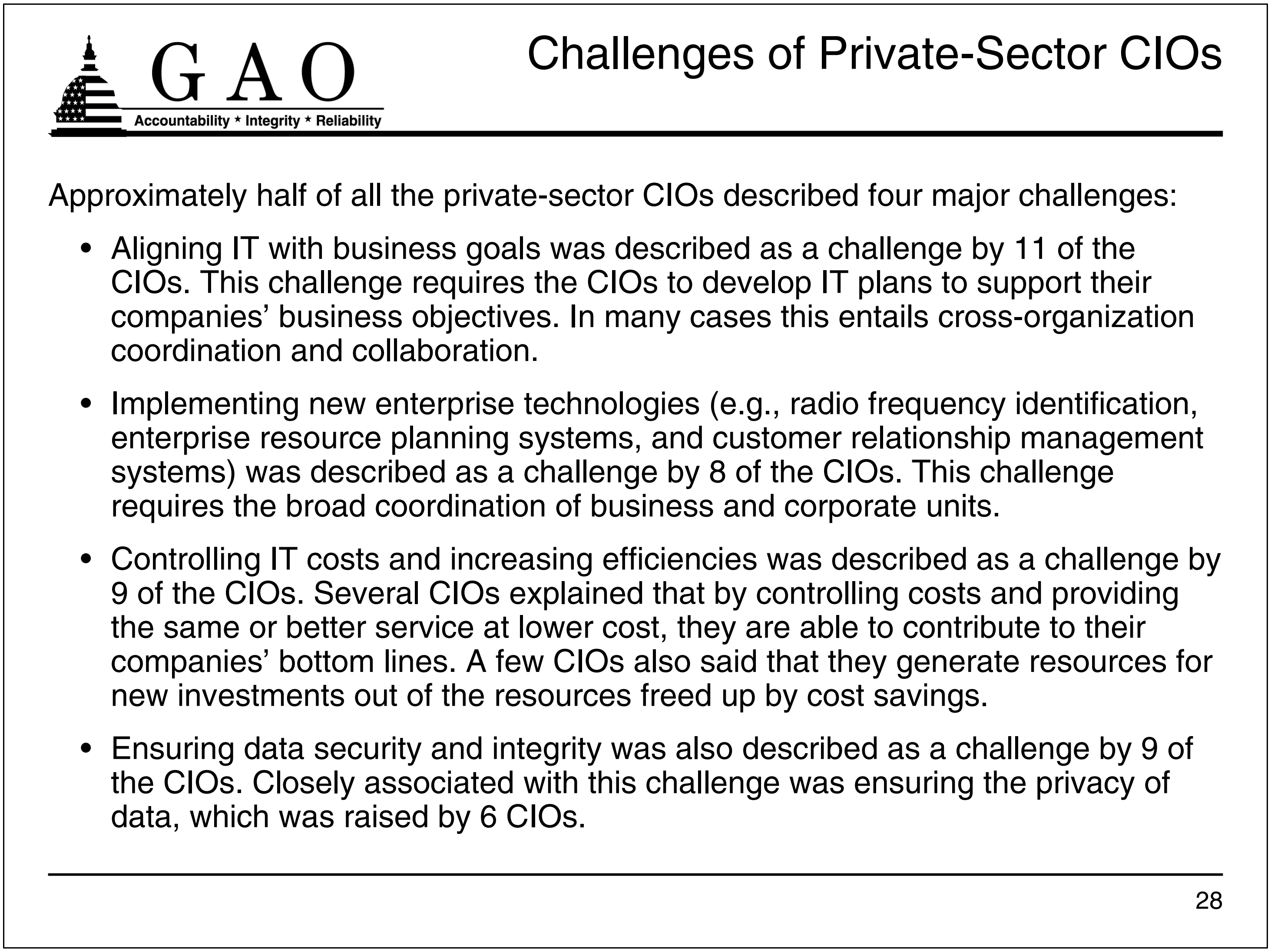
Responsibilities of Private-Sector CIOs

The six functions least likely to be the responsibility of federal CIOs were equivalent to the five functions[1] least likely to be the responsibility of private-sector CIOs:

- statistical policy,
- information dissemination and disclosure,
- information collection,
- privacy, and
- records management.

Overall, among the private-sector CIOs, sharing responsibility with either business units or corporate functional areas was a common way for companies to assign responsibility; these sharing relationships accounted for almost a third of all responses. Similarly, sharing responsibility was also described by the federal CIOs in areas including workforce planning, e-gov initiatives, and systems acquisition.

[1] Information dissemination and information disclosure were combined into a single function in the private-sector survey in order to increase the function's relevance for private-sector CIOs.

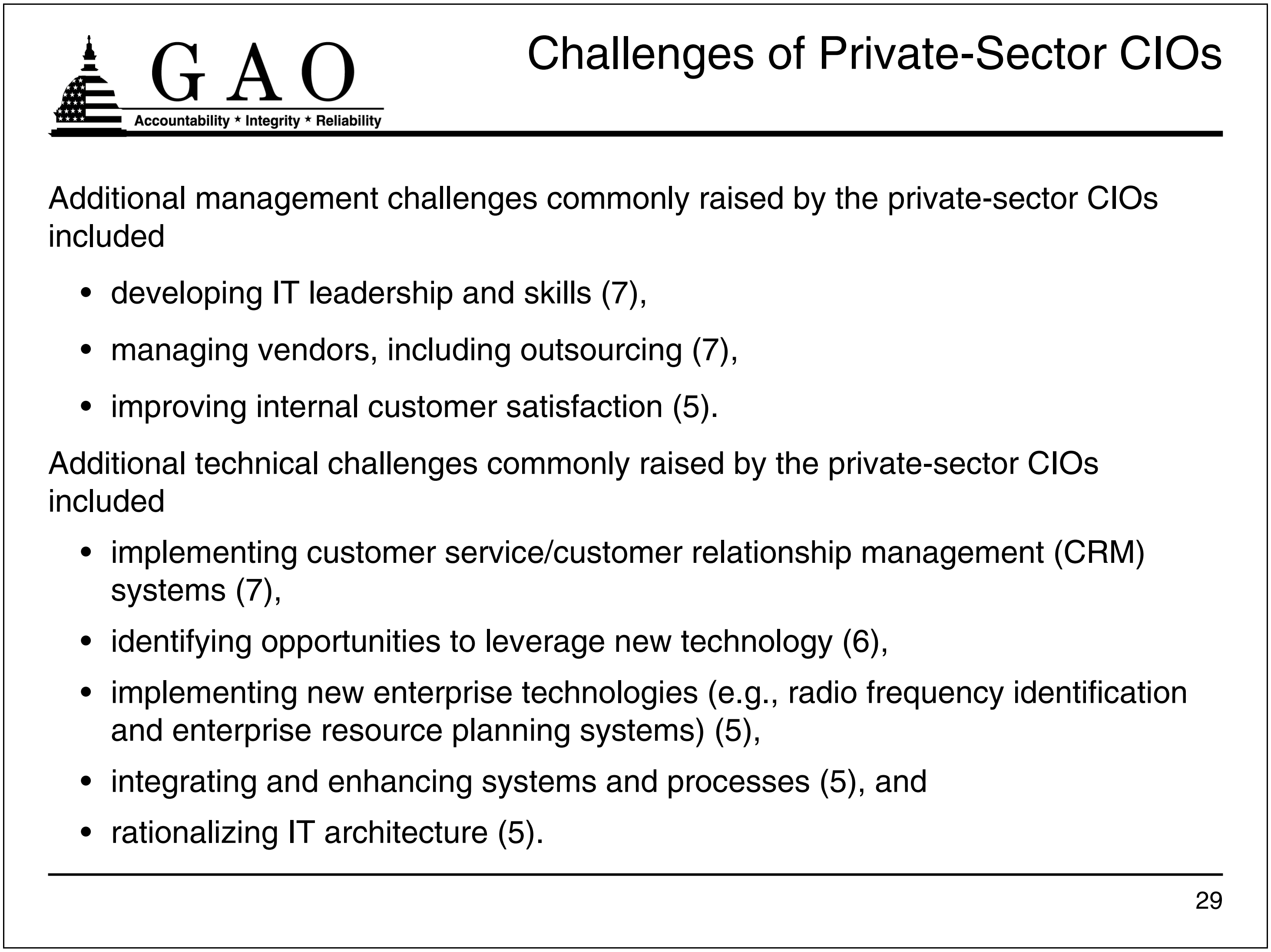


GAO
Accountability * Integrity * Reliability

Challenges of Private-Sector CIOs

Approximately half of all the private-sector CIOs described four major challenges:

- Aligning IT with business goals was described as a challenge by 11 of the CIOs. This challenge requires the CIOs to develop IT plans to support their companies' business objectives. In many cases this entails cross-organization coordination and collaboration.
- Implementing new enterprise technologies (e.g., radio frequency identification, enterprise resource planning systems, and customer relationship management systems) was described as a challenge by 8 of the CIOs. This challenge requires the broad coordination of business and corporate units.
- Controlling IT costs and increasing efficiencies was described as a challenge by 9 of the CIOs. Several CIOs explained that by controlling costs and providing the same or better service at lower cost, they are able to contribute to their companies' bottom lines. A few CIOs also said that they generate resources for new investments out of the resources freed up by cost savings.
- Ensuring data security and integrity was also described as a challenge by 9 of the CIOs. Closely associated with this challenge was ensuring the privacy of data, which was raised by 6 CIOs.



GAO

Accountability * Integrity * Reliability

Challenges of Private-Sector CIOs

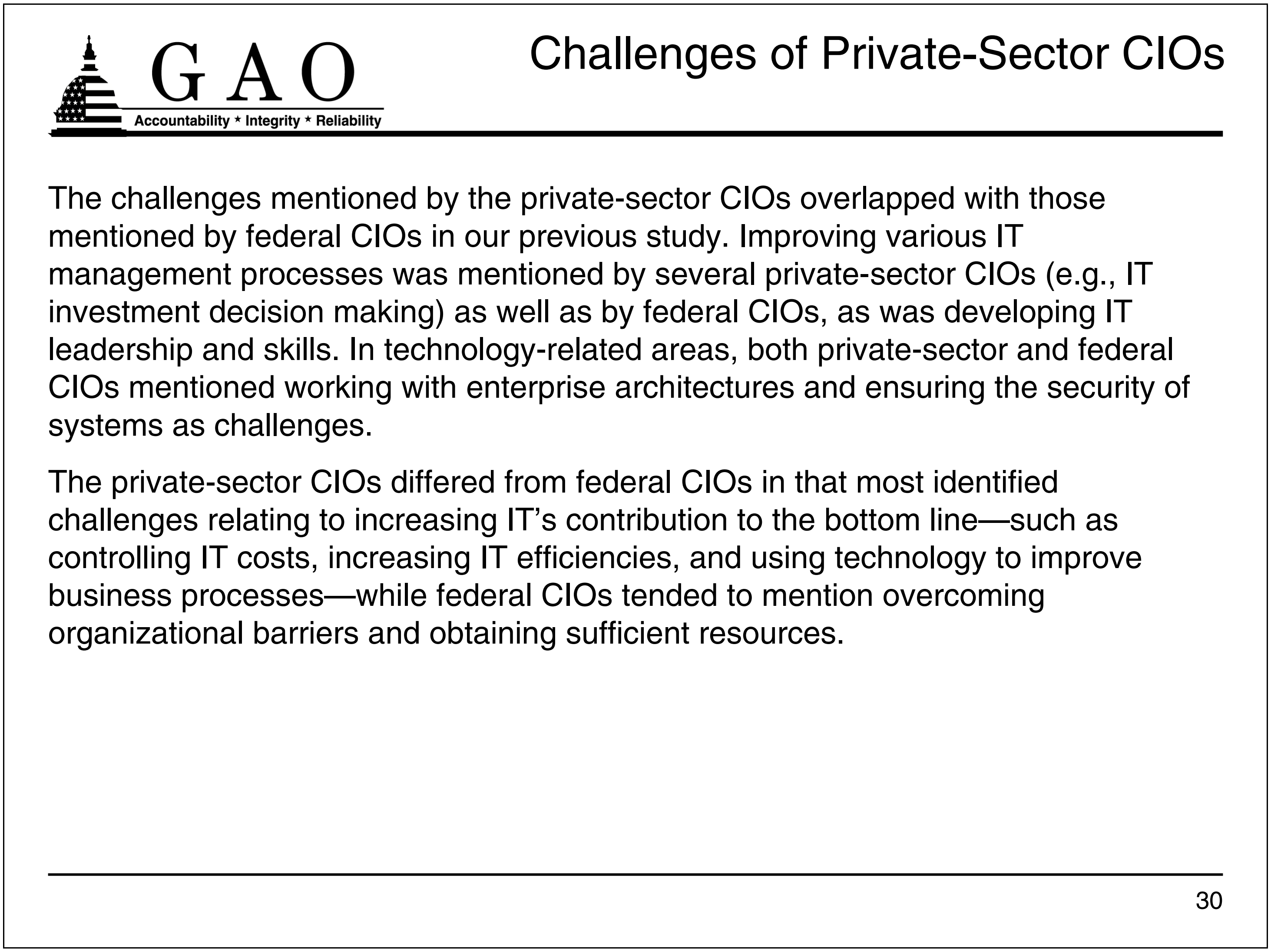
Additional management challenges commonly raised by the private-sector CIOs included

- developing IT leadership and skills (7),
- managing vendors, including outsourcing (7),
- improving internal customer satisfaction (5).

Additional technical challenges commonly raised by the private-sector CIOs included

- implementing customer service/customer relationship management (CRM) systems (7),
- identifying opportunities to leverage new technology (6),
- implementing new enterprise technologies (e.g., radio frequency identification and enterprise resource planning systems) (5),
- integrating and enhancing systems and processes (5), and
- rationalizing IT architecture (5).

29

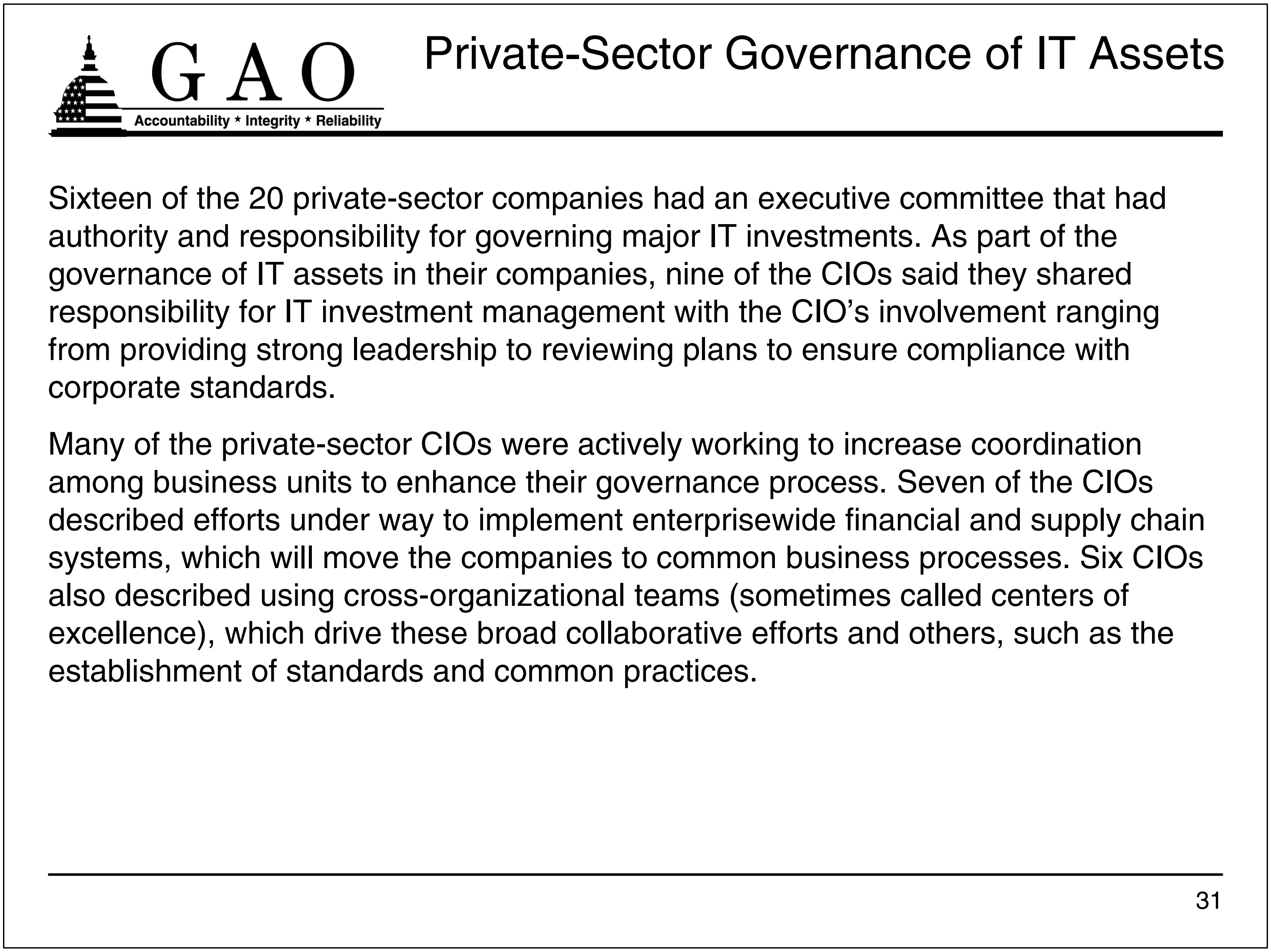


GAO
Accountability * Integrity * Reliability

Challenges of Private-Sector CIOs

The challenges mentioned by the private-sector CIOs overlapped with those mentioned by federal CIOs in our previous study. Improving various IT management processes was mentioned by several private-sector CIOs (e.g., IT investment decision making) as well as by federal CIOs, as was developing IT leadership and skills. In technology-related areas, both private-sector and federal CIOs mentioned working with enterprise architectures and ensuring the security of systems as challenges.

The private-sector CIOs differed from federal CIOs in that most identified challenges relating to increasing IT's contribution to the bottom line—such as controlling IT costs, increasing IT efficiencies, and using technology to improve business processes—while federal CIOs tended to mention overcoming organizational barriers and obtaining sufficient resources.

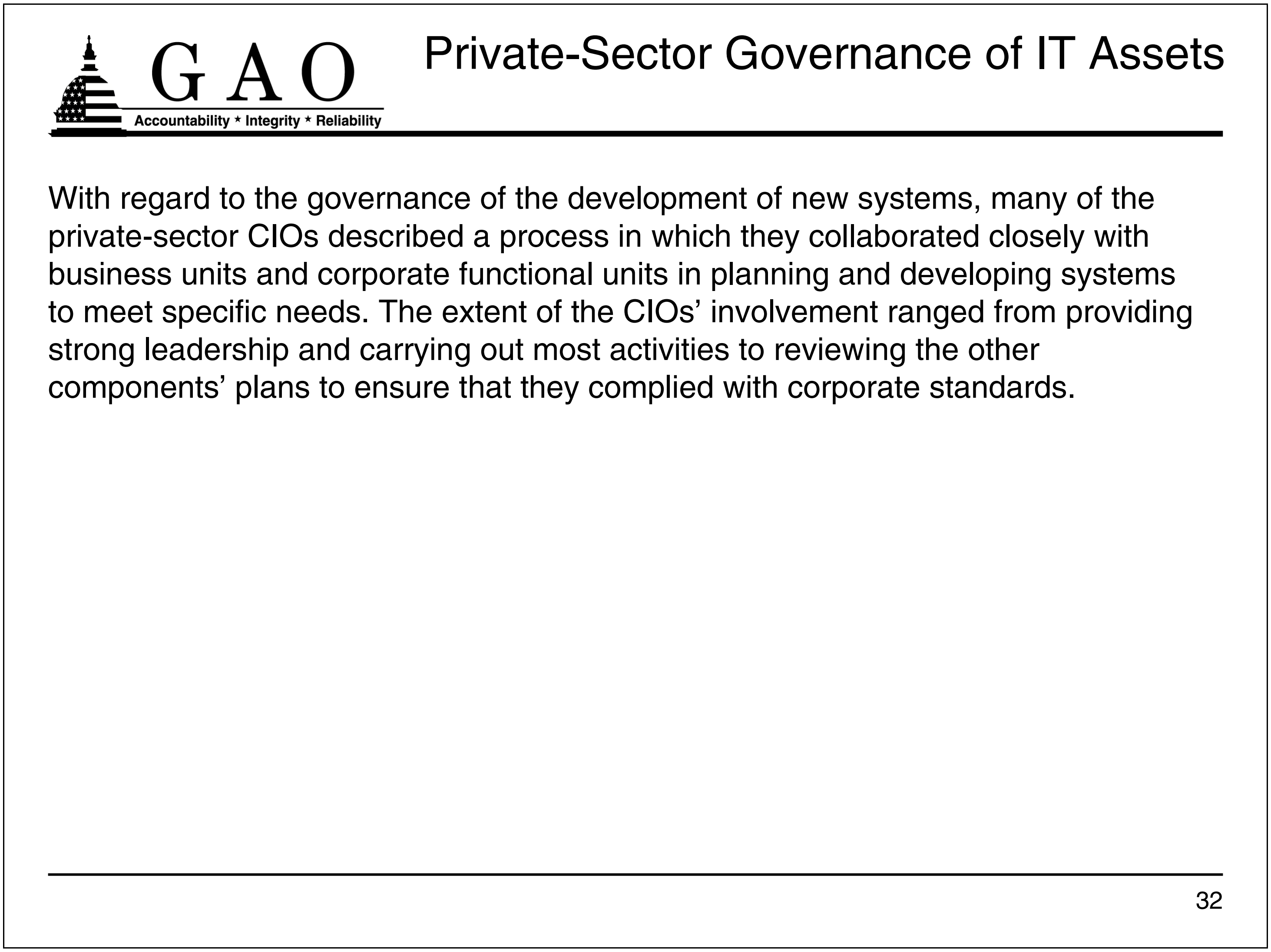


Private-Sector Governance of IT Assets

Sixteen of the 20 private-sector companies had an executive committee that had authority and responsibility for governing major IT investments. As part of the governance of IT assets in their companies, nine of the CIOs said they shared responsibility for IT investment management with the CIO's involvement ranging from providing strong leadership to reviewing plans to ensure compliance with corporate standards.

Many of the private-sector CIOs were actively working to increase coordination among business units to enhance their governance process. Seven of the CIOs described efforts under way to implement enterprisewide financial and supply chain systems, which will move the companies to common business processes. Six CIOs also described using cross-organizational teams (sometimes called centers of excellence), which drive these broad collaborative efforts and others, such as the establishment of standards and common practices.

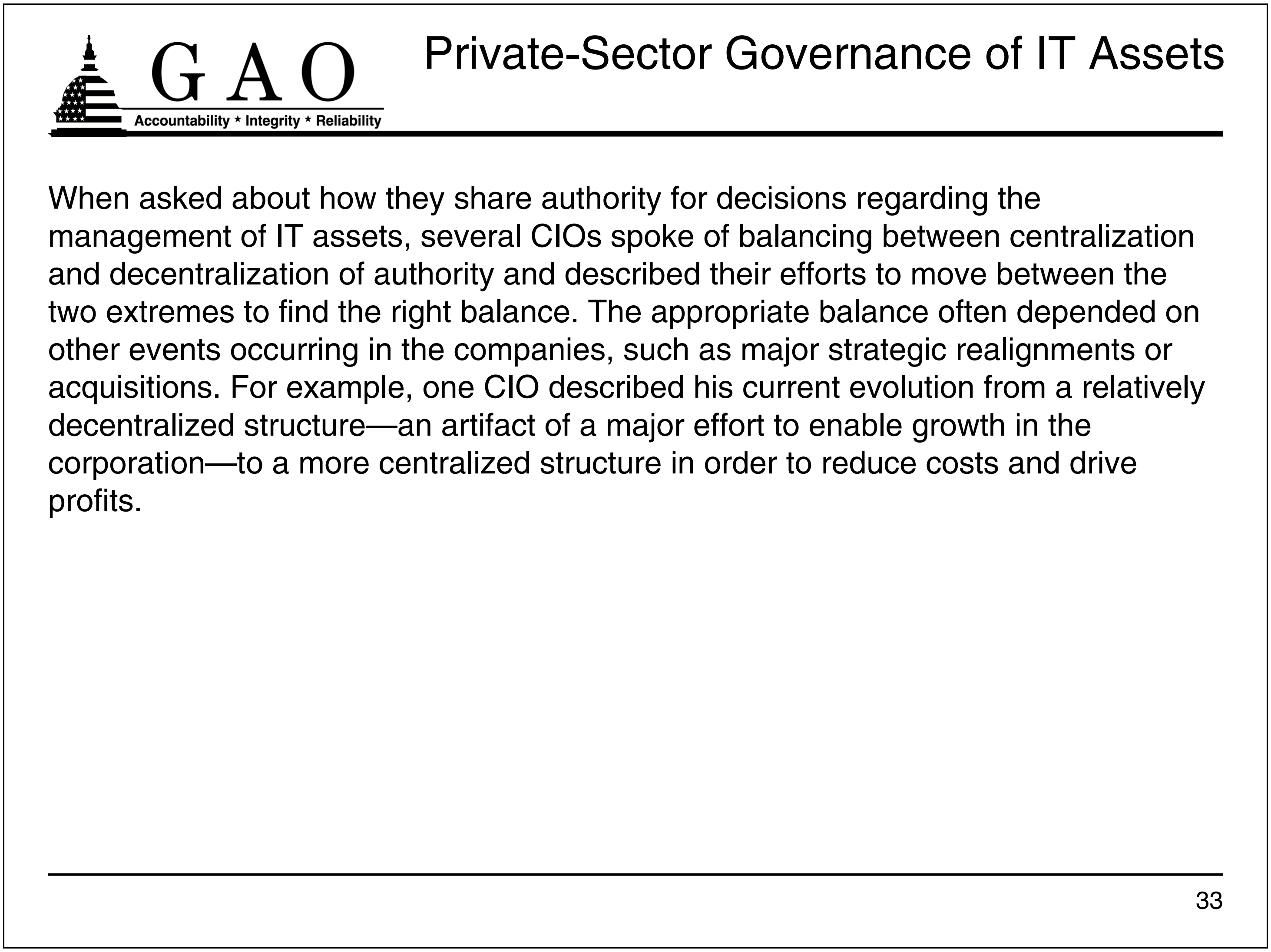
31



Private-Sector Governance of IT Assets

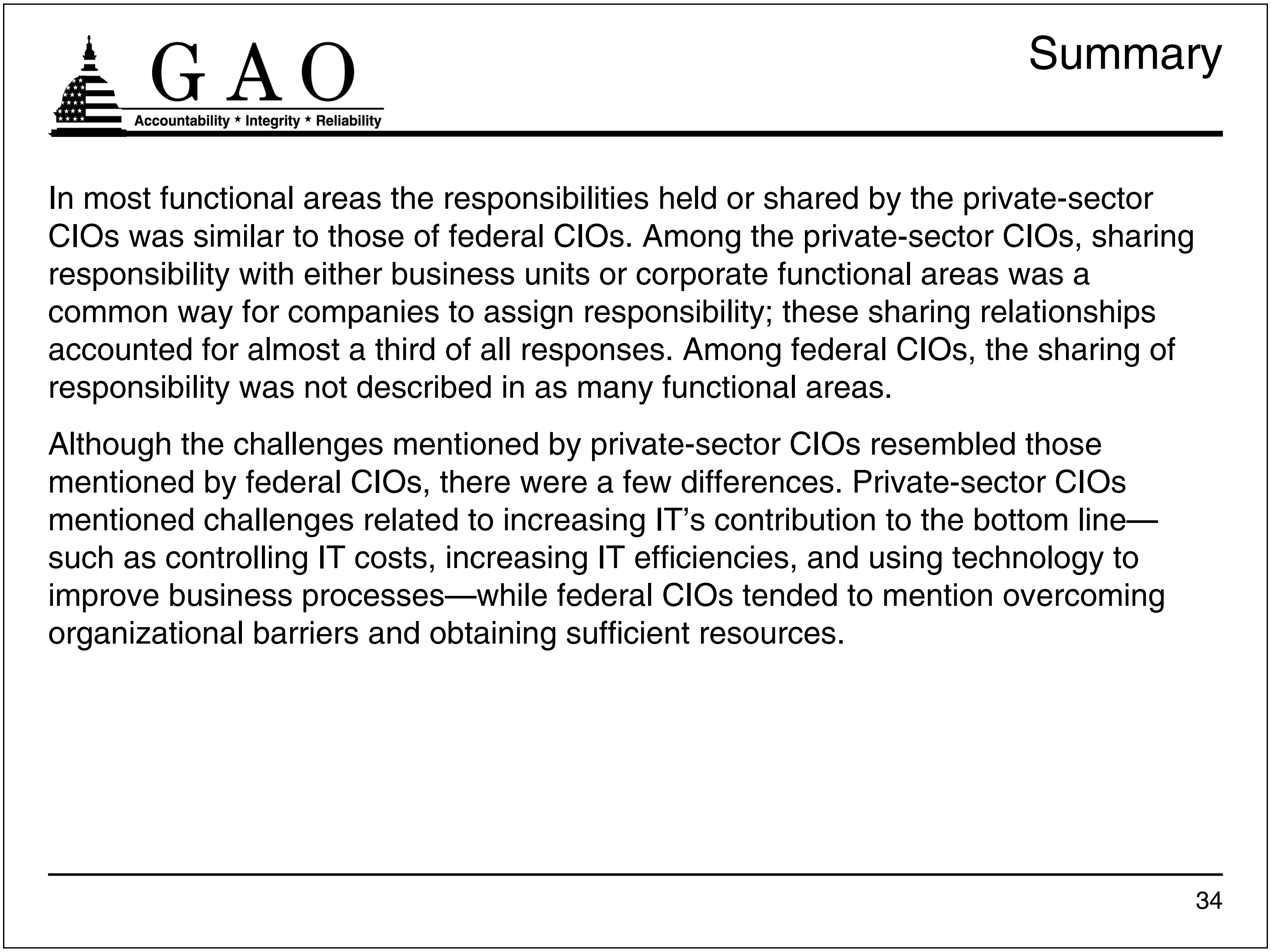
With regard to the governance of the development of new systems, many of the private-sector CIOs described a process in which they collaborated closely with business units and corporate functional units in planning and developing systems to meet specific needs. The extent of the CIOs' involvement ranged from providing strong leadership and carrying out most activities to reviewing the other components' plans to ensure that they complied with corporate standards.

32



Private-Sector Governance of IT Assets

When asked about how they share authority for decisions regarding the management of IT assets, several CIOs spoke of balancing between centralization and decentralization of authority and described their efforts to move between the two extremes to find the right balance. The appropriate balance often depended on other events occurring in the companies, such as major strategic realignments or acquisitions. For example, one CIO described his current evolution from a relatively decentralized structure—an artifact of a major effort to enable growth in the corporation—to a more centralized structure in order to reduce costs and drive profits.



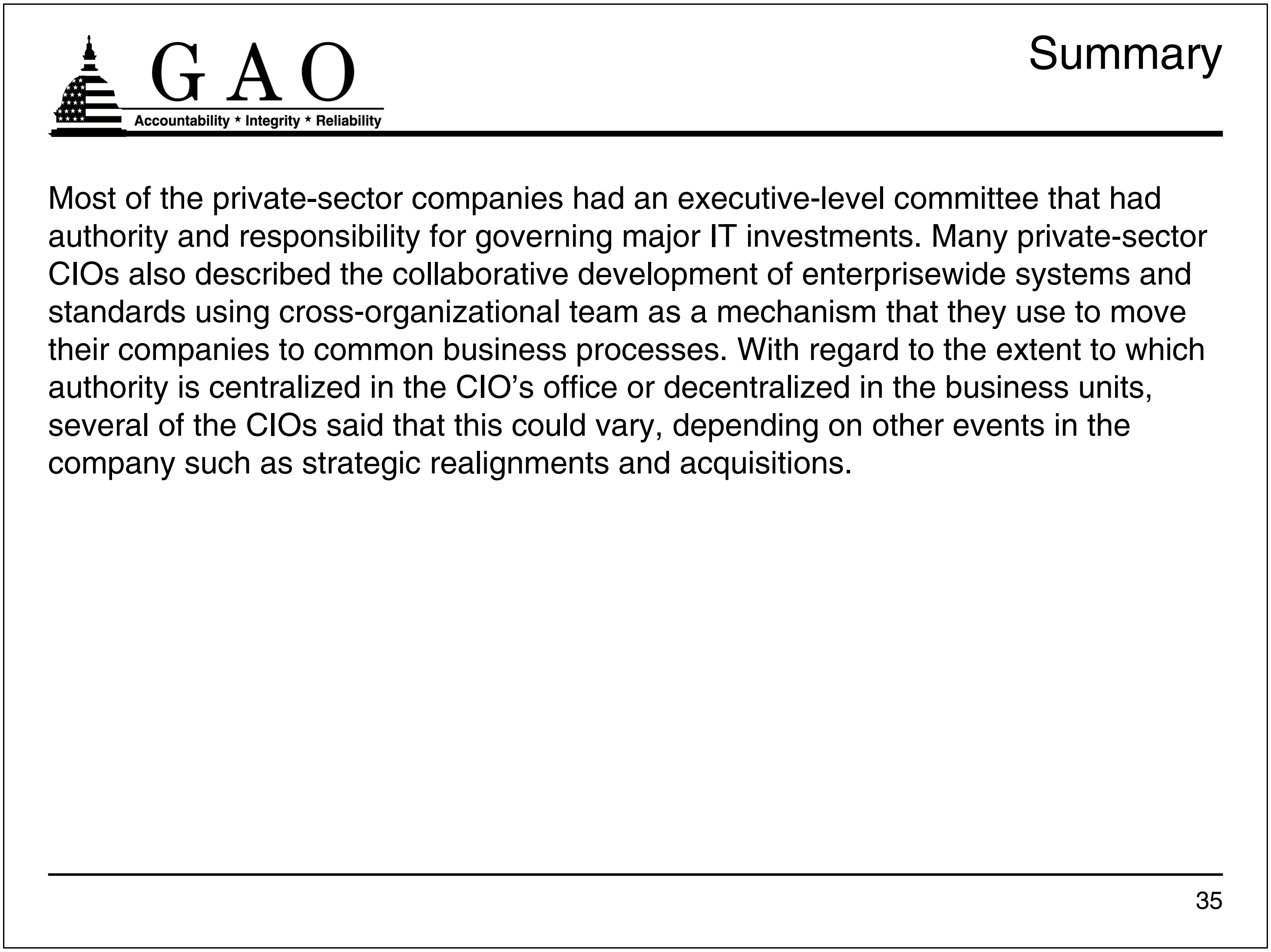
GAO
Accountability * Integrity * Reliability

Summary

In most functional areas the responsibilities held or shared by the private-sector CIOs was similar to those of federal CIOs. Among the private-sector CIOs, sharing responsibility with either business units or corporate functional areas was a common way for companies to assign responsibility; these sharing relationships accounted for almost a third of all responses. Among federal CIOs, the sharing of responsibility was not described in as many functional areas.

Although the challenges mentioned by private-sector CIOs resembled those mentioned by federal CIOs, there were a few differences. Private-sector CIOs mentioned challenges related to increasing IT's contribution to the bottom line—such as controlling IT costs, increasing IT efficiencies, and using technology to improve business processes—while federal CIOs tended to mention overcoming organizational barriers and obtaining sufficient resources.

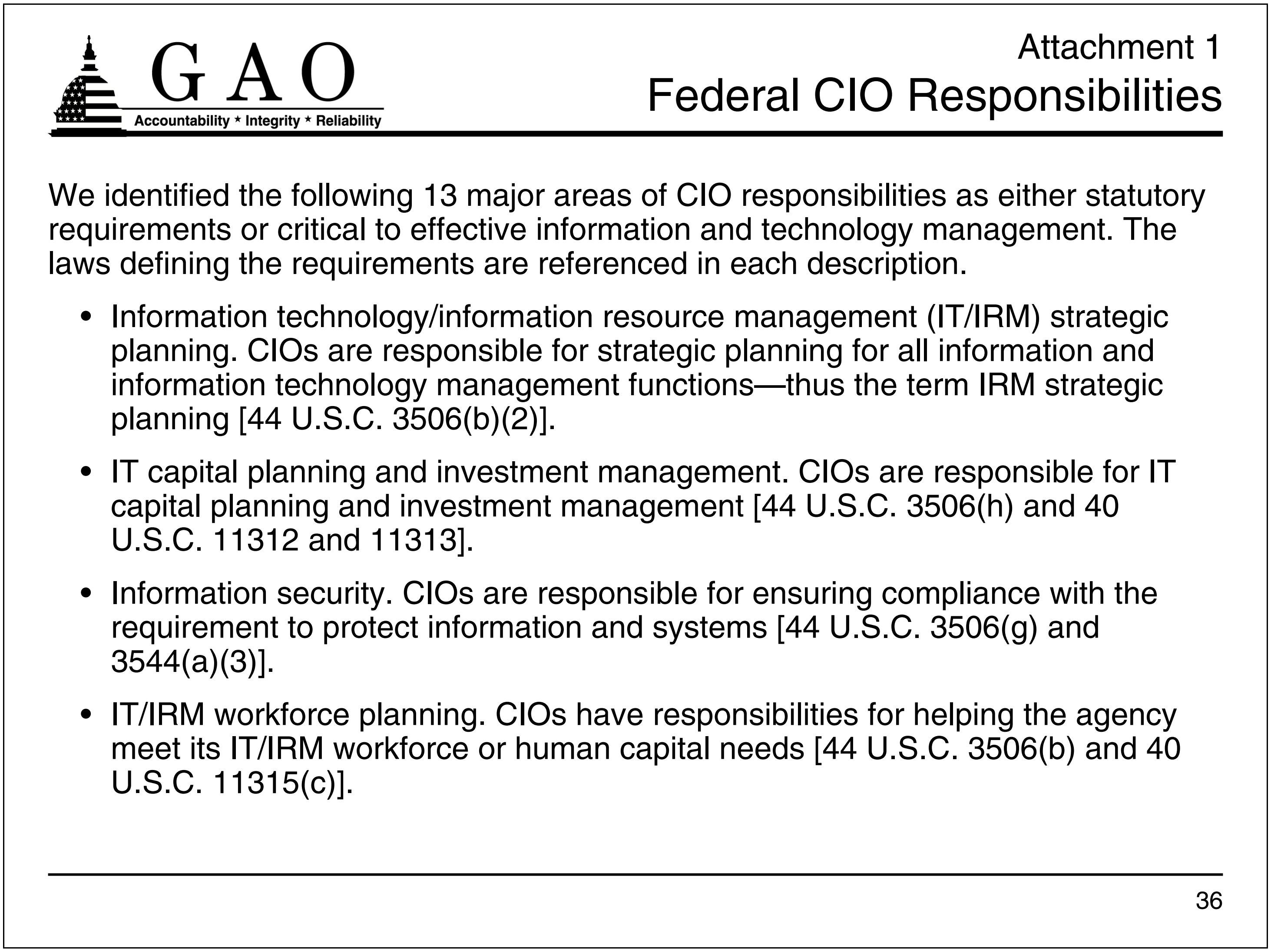
34



GAO
Accountability * Integrity * Reliability

Summary

Most of the private-sector companies had an executive-level committee that had authority and responsibility for governing major IT investments. Many private-sector CIOs also described the collaborative development of enterprisewide systems and standards using cross-organizational team as a mechanism that they use to move their companies to common business processes. With regard to the extent to which authority is centralized in the CIO’s office or decentralized in the business units, several of the CIOs said that this could vary, depending on other events in the company such as strategic realignments and acquisitions.



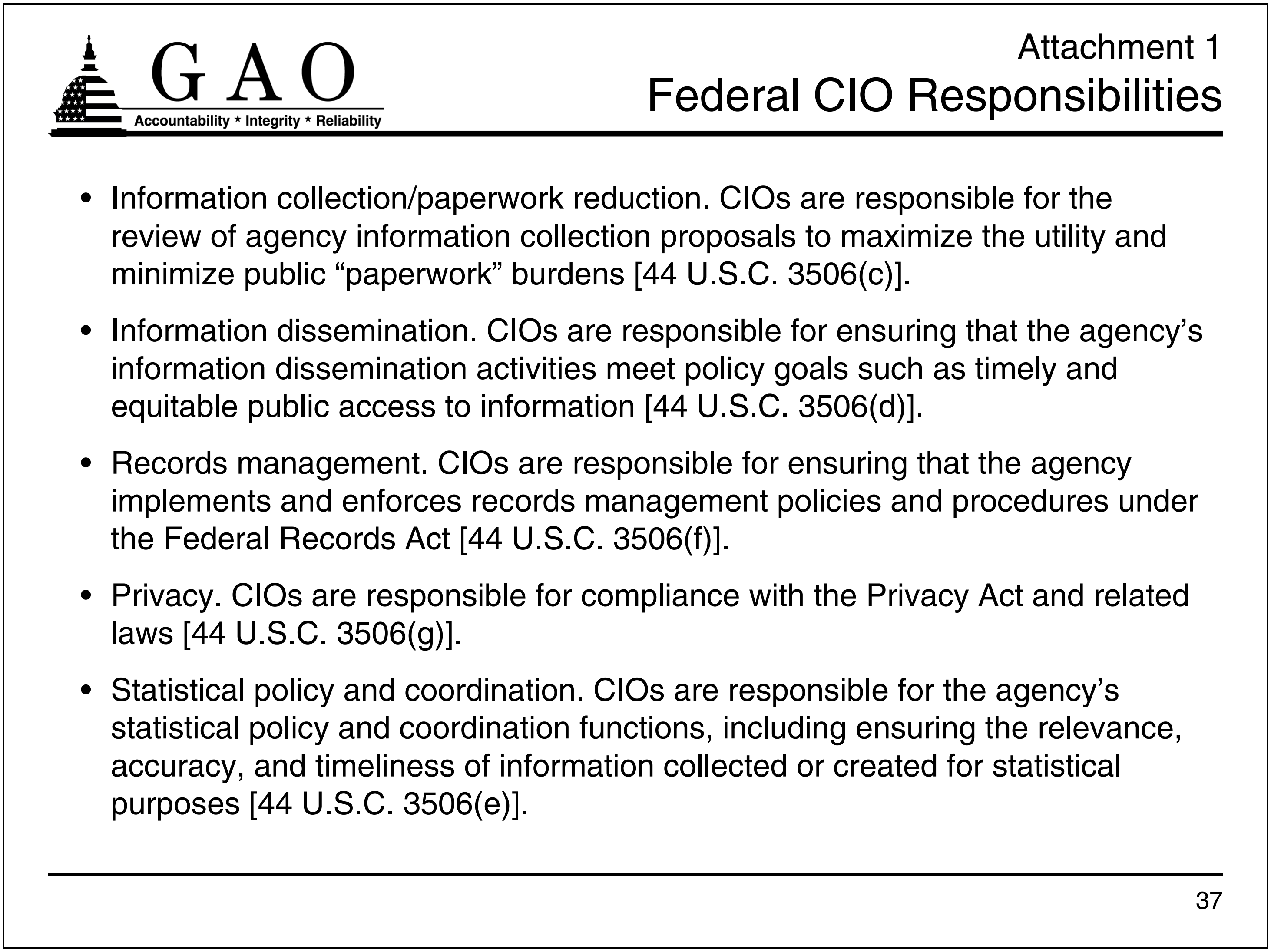
GAO
Accountability * Integrity * Reliability

Attachment 1

Federal CIO Responsibilities

We identified the following 13 major areas of CIO responsibilities as either statutory requirements or critical to effective information and technology management. The laws defining the requirements are referenced in each description.

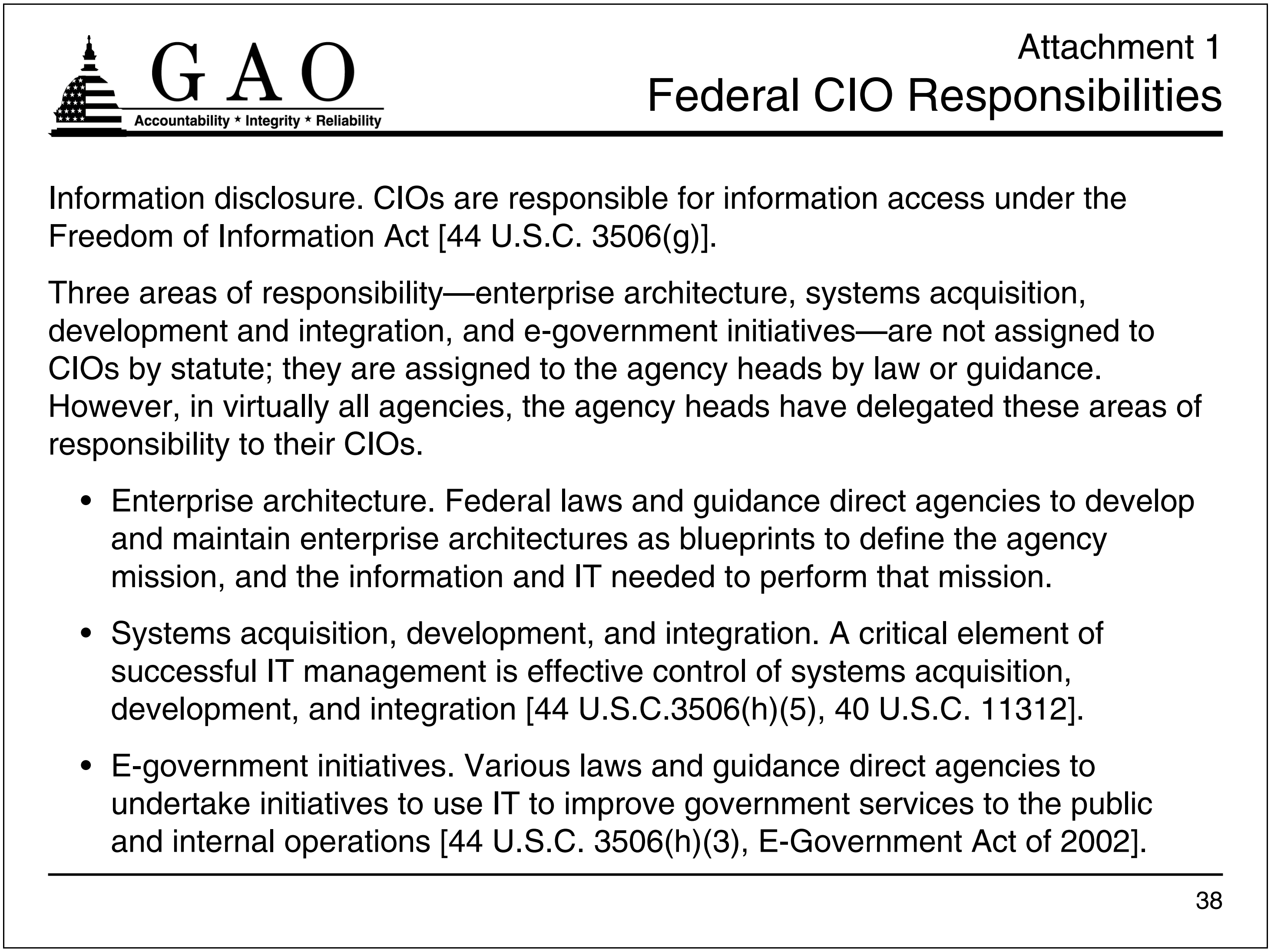
- Information technology/information resource management (IT/IRM) strategic planning. CIOs are responsible for strategic planning for all information and information technology management functions—thus the term IRM strategic planning [44 U.S.C. 3506(b)(2)].
- IT capital planning and investment management. CIOs are responsible for IT capital planning and investment management [44 U.S.C. 3506(h) and 40 U.S.C. 11312 and 11313].
- Information security. CIOs are responsible for ensuring compliance with the requirement to protect information and systems [44 U.S.C. 3506(g) and 3544(a)(3)].
- IT/IRM workforce planning. CIOs have responsibilities for helping the agency meet its IT/IRM workforce or human capital needs [44 U.S.C. 3506(b) and 40 U.S.C. 11315(c)].



Attachment 1

Federal CIO Responsibilities

- Information collection/paperwork reduction. CIOs are responsible for the review of agency information collection proposals to maximize the utility and minimize public “paperwork” burdens [44 U.S.C. 3506(c)].
- Information dissemination. CIOs are responsible for ensuring that the agency’s information dissemination activities meet policy goals such as timely and equitable public access to information [44 U.S.C. 3506(d)].
- Records management. CIOs are responsible for ensuring that the agency implements and enforces records management policies and procedures under the Federal Records Act [44 U.S.C. 3506(f)].
- Privacy. CIOs are responsible for compliance with the Privacy Act and related laws [44 U.S.C. 3506(g)].
- Statistical policy and coordination. CIOs are responsible for the agency’s statistical policy and coordination functions, including ensuring the relevance, accuracy, and timeliness of information collected or created for statistical purposes [44 U.S.C. 3506(e)].



GAO
Accountability * Integrity * Reliability

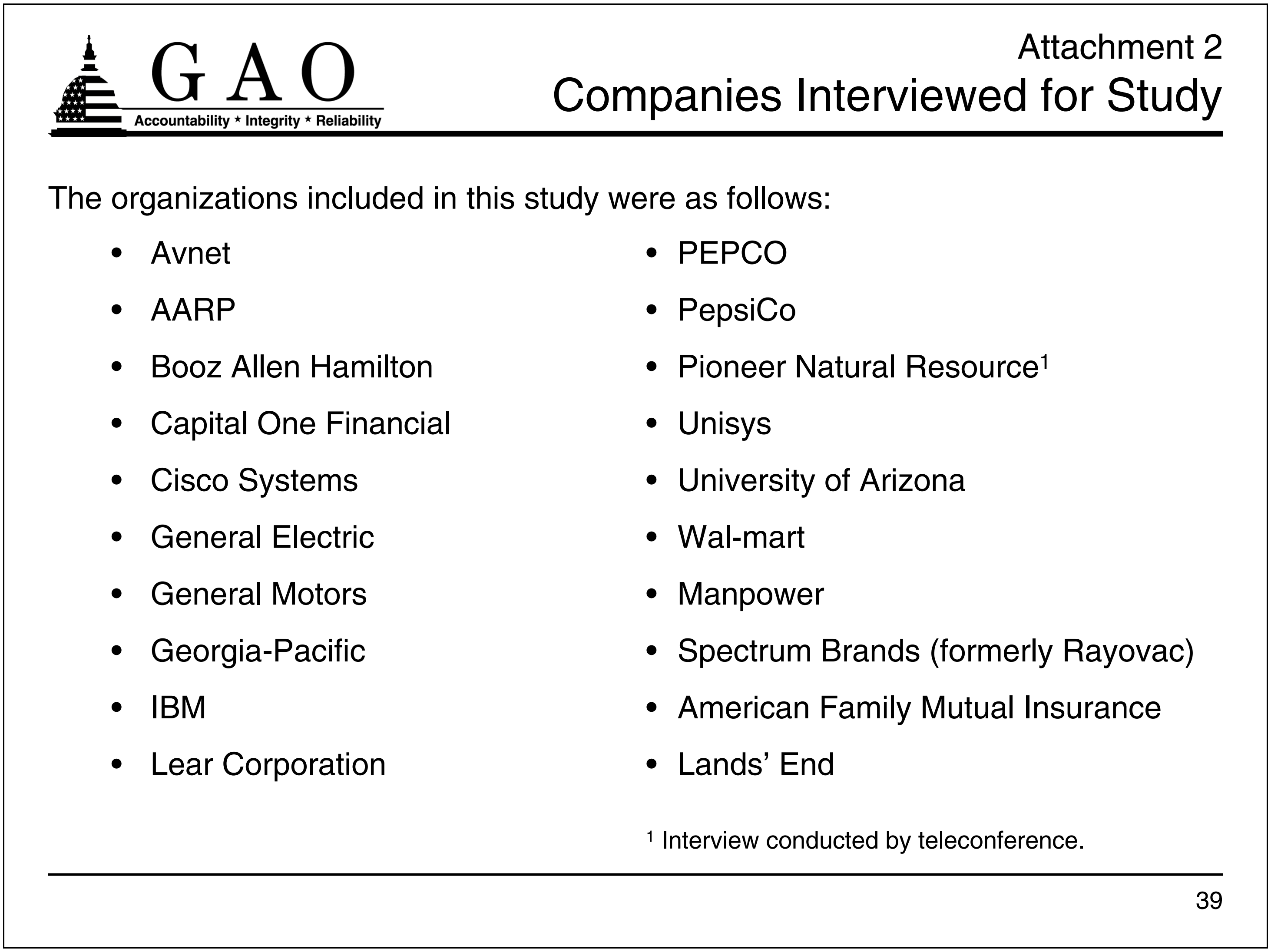
Attachment 1
Federal CIO Responsibilities

Information disclosure. CIOs are responsible for information access under the Freedom of Information Act [44 U.S.C. 3506(g)].

Three areas of responsibility—enterprise architecture, systems acquisition, development and integration, and e-government initiatives—are not assigned to CIOs by statute; they are assigned to the agency heads by law or guidance. However, in virtually all agencies, the agency heads have delegated these areas of responsibility to their CIOs.

- Enterprise architecture. Federal laws and guidance direct agencies to develop and maintain enterprise architectures as blueprints to define the agency mission, and the information and IT needed to perform that mission.
- Systems acquisition, development, and integration. A critical element of successful IT management is effective control of systems acquisition, development, and integration [44 U.S.C.3506(h)(5), 40 U.S.C. 11312].
- E-government initiatives. Various laws and guidance direct agencies to undertake initiatives to use IT to improve government services to the public and internal operations [44 U.S.C. 3506(h)(3), E-Government Act of 2002].

38



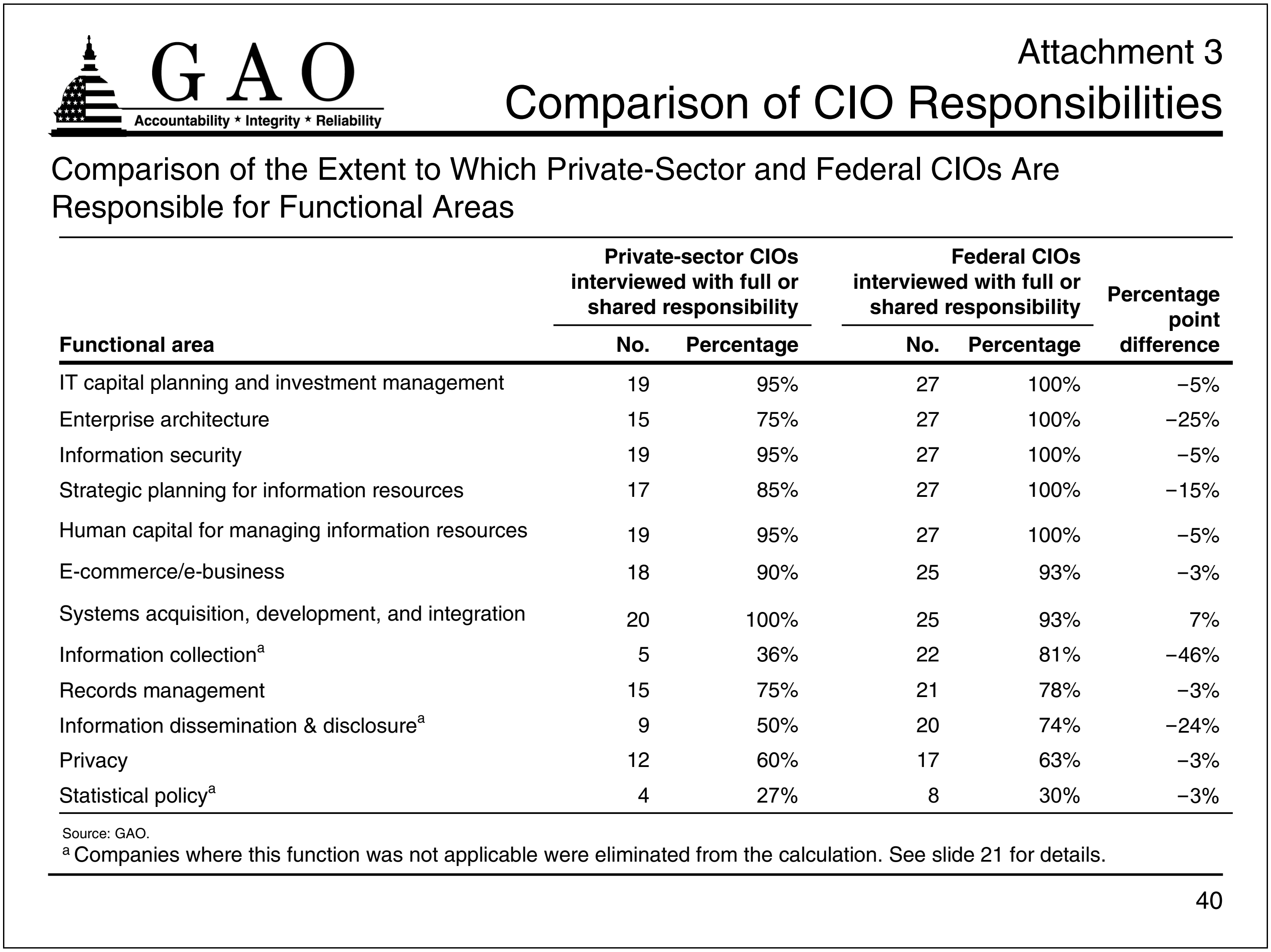
Attachment 2

Companies Interviewed for Study

The organizations included in this study were as follows:

- Avnet
- AARP
- Booz Allen Hamilton
- Capital One Financial
- Cisco Systems
- General Electric
- General Motors
- Georgia-Pacific
- IBM
- Lear Corporation
- PEPCO
- PepsiCo
- Pioneer Natural Resource[1]
- Unisys
- University of Arizona
- Wal-mart
- Manpower
- Spectrum Brands (formerly Rayovac)
- American Family Mutual Insurance
- Lands’ End

[1] Interview conducted by teleconference.



Attachment 3

Comparison of CIO Responsibilities

Comparison of the Extent to Which Private-Sector and Federal CIOs Are Responsible for Functional Areas

	Private-sector CIOs interviewed with full or shared responsibility		Federal CIOs interviewed with full or shared responsibility		Percentage point difference
Functional area	No.	Percentage	No.	Percentage	
IT capital planning and investment management	19	95%	27	100%	–5%
Enterprise architecture	15	75%	27	100%	–25%
Information security	19	95%	27	100%	–5%
Strategic planning for information resources	17	85%	27	100%	–15%
Human capital for managing information resources	19	95%	27	100%	–5%
E-commerce/e-business	18	90%	25	93%	–3%
Systems acquisition, development, and integration	20	100%	25	93%	7%
Information collection[a]	5	36%	22	81%	–46%
Records management	15	75%	21	78%	–3%
Information dissemination & disclosure[a]	9	50%	20	74%	–24%
Privacy	12	60%	17	63%	–3%
Statistical policy[a]	4	27%	8	30%	–3%

Source: GAO.

[a] Companies where this function was not applicable were eliminated from the calculation. See slide 21 for details.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON ♻ RECYCLED PAPER