FEATURE

Accountability for Information Security Roles and Responsibilities, Part 2

Application of the Method

Part 1 of this article proposed a method using ArchiMate to integrate *COBIT® 5 for Information Security* with enterprise architecture (EA) principles, methods and models to properly implement the chief information security officer's (CISO's) role. The next step is to demonstrate how this process works by using a government-owned organization as an example.

An example organization, DemoCorp, a mid-sized government-owned organization, is used to demonstrate this process. DemoCorp has a low level of maturity in information security. This process addresses the problem regarding the challenge of how an organization can implement the CISO's role using *COBIT 5 for Information Security* in ArchiMate. Moreover, the ArchiMate notation was used to demonstrate using EA to implement the CISO's role.

To better address the identified challenge, it is important to focus the as-is analysis on responsibilities of the organization's roles and their respective business functions, information types, processes' outputs and key practices. This assessment of the existent business functions, objects, processes, roles and actors involved allows for a better understanding of the organization's gaps, which will allow an optimal approach to the challenge of implementing the CISO's role using *COBIT 5 for information Security* by leveraging the ArchiMate notation.

Step 1—Model COBIT 5 for Information Security

The first step is to model the types of information that the CISO is responsible for originating. **Figure 1**, based on what is defined in *COBIT 5 for Information Security*,[1] represents the artifact CISO's Business Functions and Information Types viewpoint, which illustrates the business functions and associated information types that the CISO should originate.

Then, following the method, **figure 2** shows the inputs, outputs and roles for which the CISO is responsible in COBIT 5's Evaluate, Direct and Monitor (EDM) process EDM03 *Ensure risk*

Tiago Catarino
Is currently working at the Portfolio and Investment Department at INCM (Portuguese Mint and Official Printing Office). In the scope of his professional activity, he develops specialized activities in the field of information systems architectures, in several transversal projects to the organization. His main academic interests are in the areas of enterprise architecture, enterprise engineering, requirements engineering and enterprise governance, with emphasis on IS architecture and business process engineering.

André Vasconcelos, Ph.D.
Is an assistant professor in the Computer Science and Engineering, Instituto Superior Técnico, University of Lisbon (Portugal) and Researcher at Instituto de Engenharia de Sistemas e Computadores - Investigação e Desenvolvimento (Lisbon, Portugal) (INESC-ID). He has developed strategic advice in the area of information systems and business in several organizations. In the scope of his professional activity, he develops specialized advisory activities in the field of enterprise architecture for several digital transformation projects. He has written more than 80 publications, and he has been involved in several international and national research projects related to enterprise architecture, information systems evaluation and e-government, including several European projects.

Figure 1—CISO's Business Functions and Information Types Viewpoint

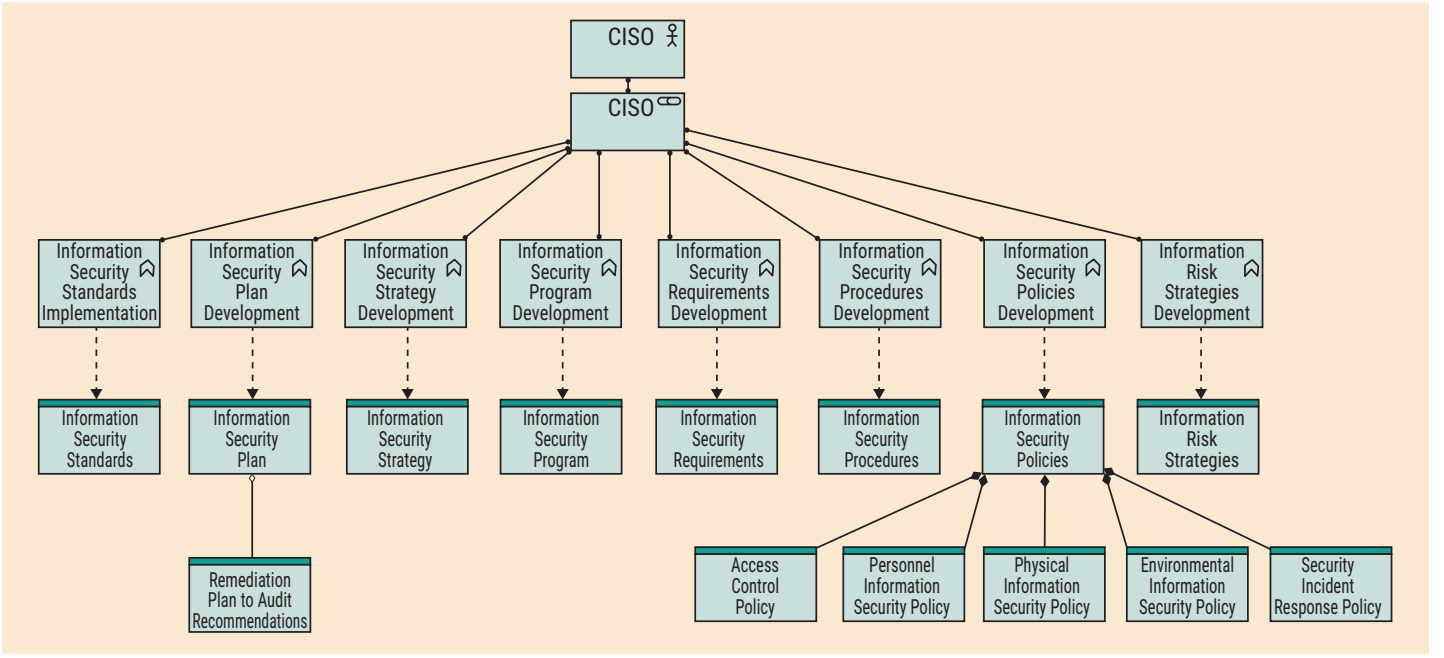
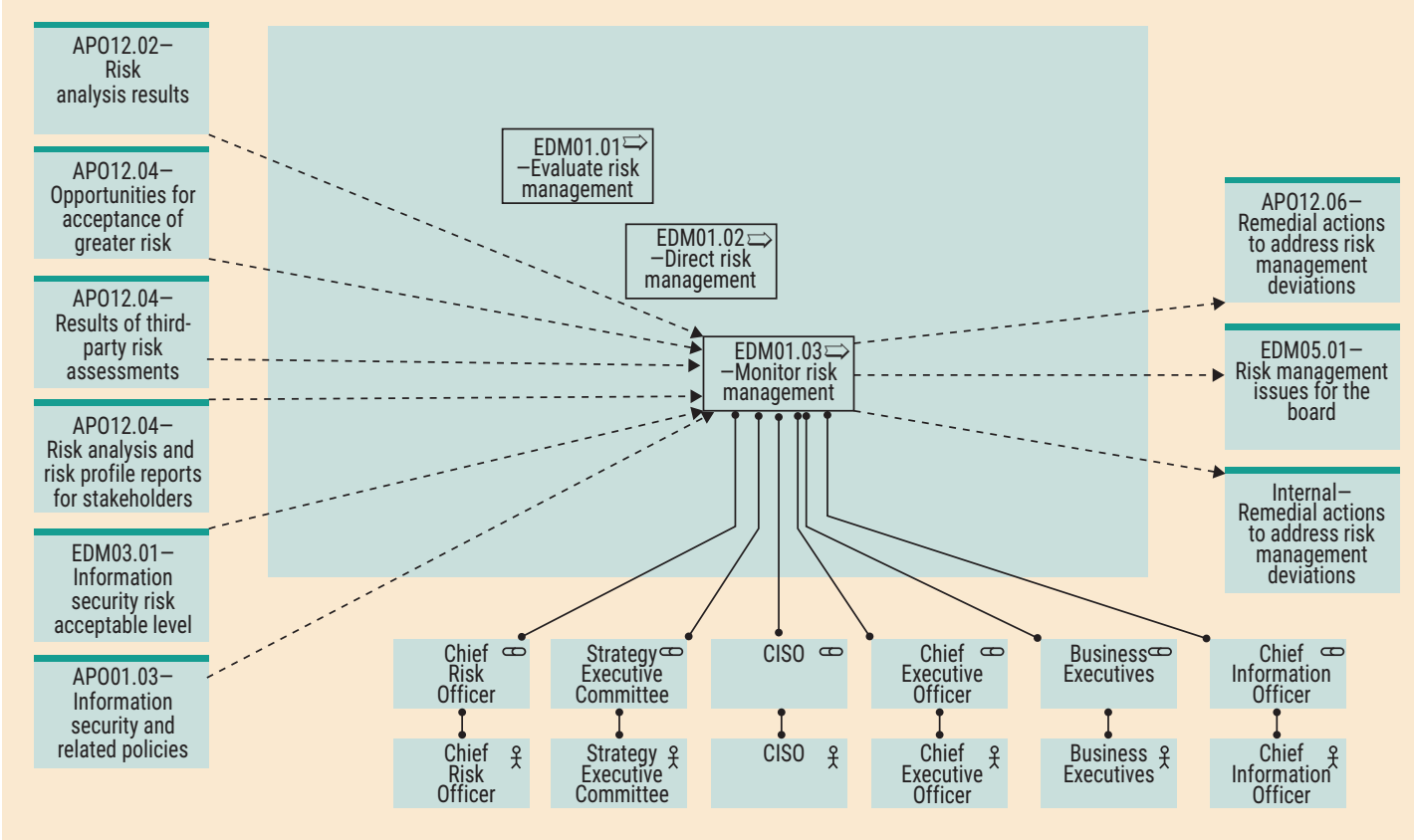


Figure 2—EDM03 Ensure Risk Optimization Process Viewpoint



optimization. For the remaining processes for which the CISO is responsible, corresponding viewpoints would have a very similar structure.

Following the first step stated in the solution proposal, **figure 3** presents the key practices for which the CISO could be held responsible.

The definition of the CISO's role, based on *COBIT 5 for Information Security*, is now clear, and it will be the input for the next steps of the proposed method.

Step 2—Model Organization's EA

This step models the as-is state of the organization's EA. Following the method, it is necessary to represent DemoCorp's business functions and information types, which are related to the CISO's role defined in step 1 (**figure 1**).

When looking at the organizational and information types originated by each one of the business functions individually (**figure 4**), it is possible to observe that the CISO is responsible for the development of information security requirements, policies and procedures. Moreover, this role is responsible for the implementation of information security standards.

Then, following this method, model the process that is related to the processes represented in step 1 (**figure 2**), for which the CISO is responsible. **Figure 5** presents the artifact that shows the inputs,

Figure 3—CISO's Key Practices Viewpoint

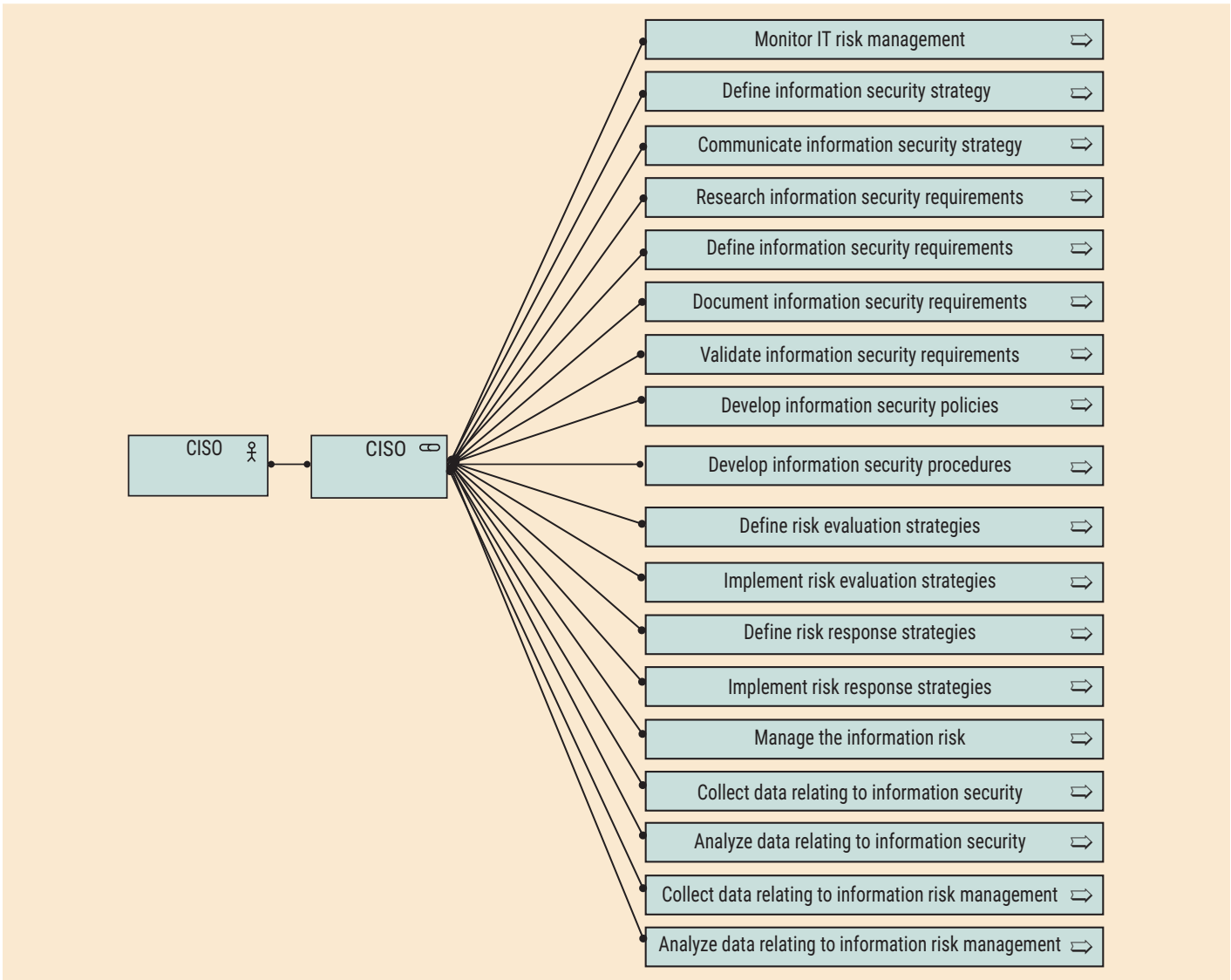


Figure 4—DemoCorp's Business Functions and Information Types Viewpoint

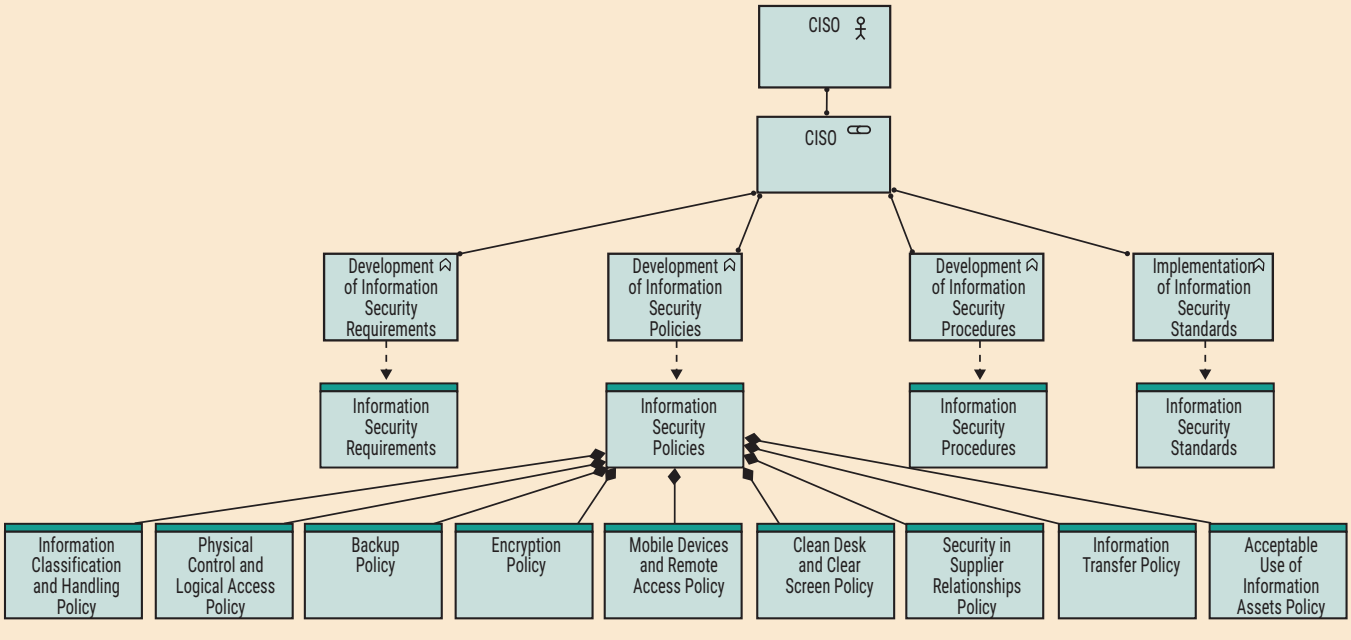
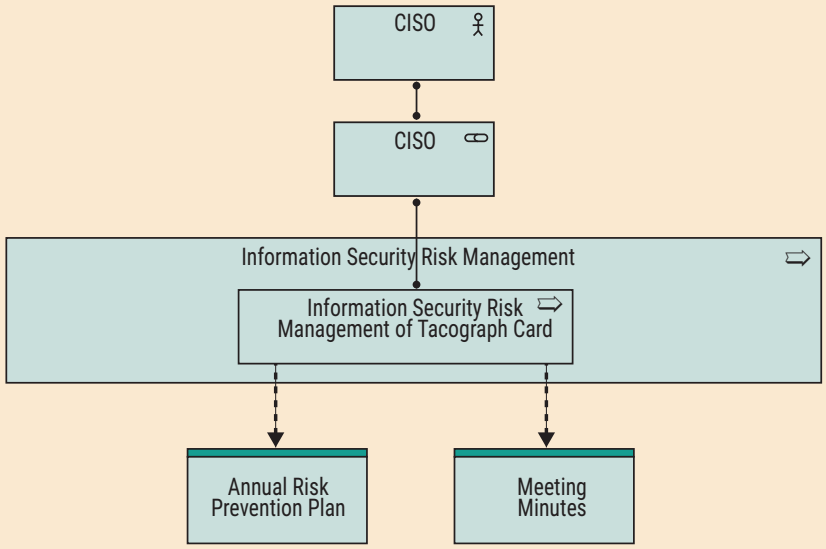


Figure 5—DemoCorp's Information Security Risk Management Process Viewpoint

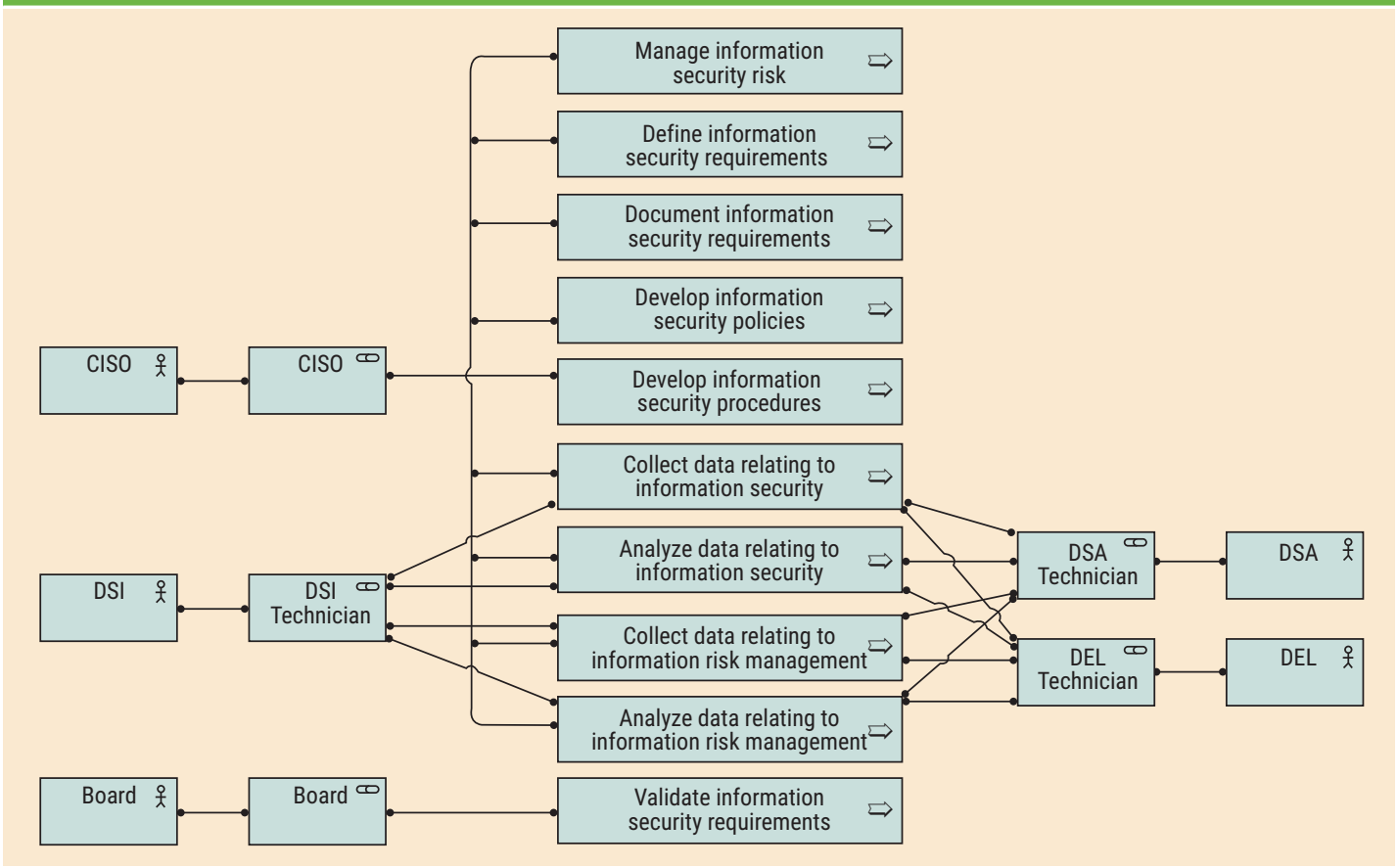


outputs and roles responsible of DemoCorp's information risk management process for which the CISO is responsible.

Finally, the organization's existent key practices, which are related to the key practices of *COBIT 5 for Information Security* for which the CISO is responsible (**figure 3**), are represented. When looking at the roles and practices assigned (**figure 6**), it can be observed that the CISO is responsible for the development of information security requirements, policies and procedures. Moreover, it can be observed that this role is responsible for some practices, but is not the only role responsible for those practices.

As a result of this step, the as-is state of the organization's EA is modeled, taking into account the definition of the CISO's role. Such representation will be the input to the next steps of the proposed method.

Figure 6—DemoCorp's Key Practices Viewpoint



Step 3—Information Types Mapping

Figure 7 maps the existing DemoCorp information types to the desired *COBIT 5 for Information Security* information types that should be originated by the CISO's role.

When looking at this mapping, it is possible to identify which types of information are being originated and who is responsible for them in the organization. Moreover, this mapping allows for the detection of information security gaps, since some information types are not defined in DemoCorp, such as the information security plan, information risk strategies, information security program and information security strategy.

Step 4—Processes Output Mapping

The fourth step's goal is to map the processes' outputs of DemoCorp to the *COBIT 5 for Information Security* processes for which the CISO is responsible.

Then, the mapping of the processes' outputs of DemoCorp to the desired processes' outputs that the CISO is responsible for producing and/or delivering is required for this step (**figure 8**). With this, it is possible to identify which processes' outputs are missing and who is delivering them to know which role is performing the CISO's job.

For the remaining processes for which the CISO is responsible, corresponding viewpoints would have *mutatis mutandis*, a very similar structure.

Step 5—Key Practices Mapping

The fifth step has a mapping of the organizations' practices to key practices for which the CISO should be responsible (**figure 9**).

This mapping allows for the detection of information security gaps regarding information security practices for which the CISO should be held responsible.

Step 6—Roles Mapping

The sixth step's goal is to map the organization's roles to the CISO role to identify who is performing the CISO's job. To that extent, **figure 10** presents the organization's roles that are doing the CISO's job.

Figure 7—Information Types' Mapping Viewpoint

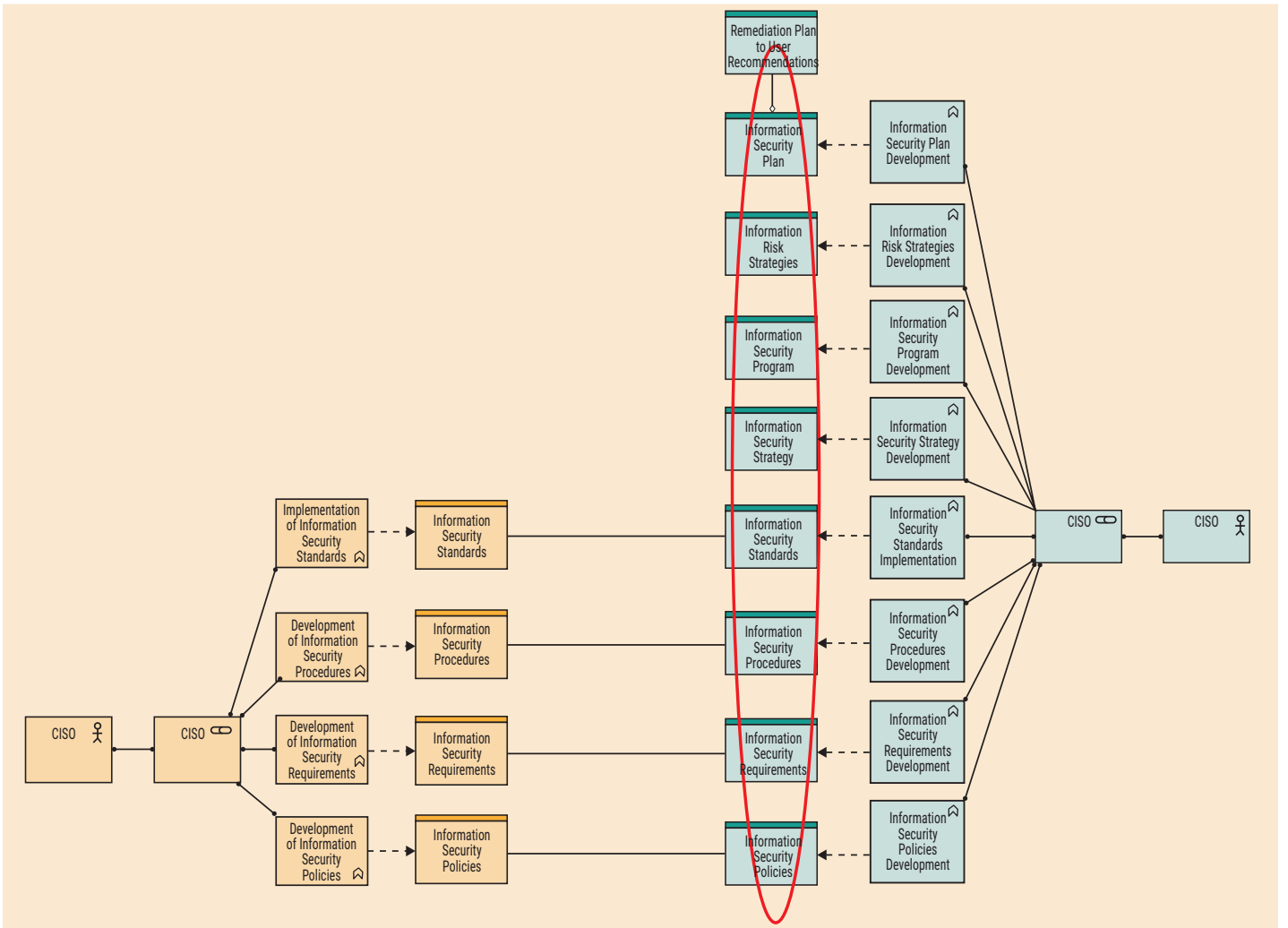


Figure 8—DemoCorp to EDM03 Ensure Risk Optimization Viewpoint

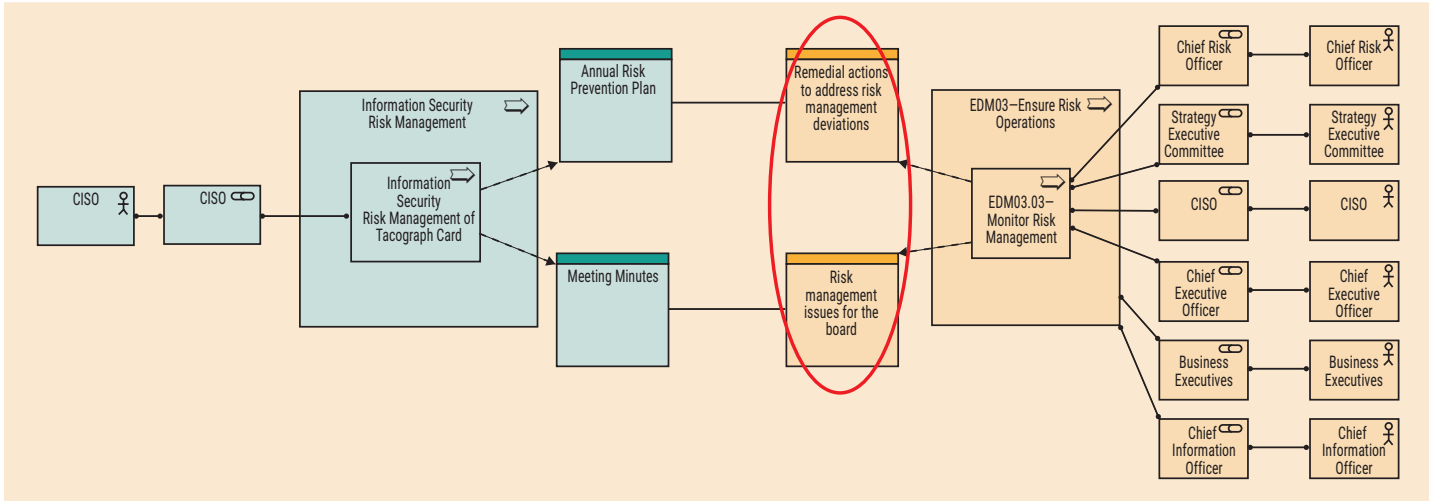


Figure 9—DemoCorp to COBIT 5 for Information Security's Key Practices Viewpoint

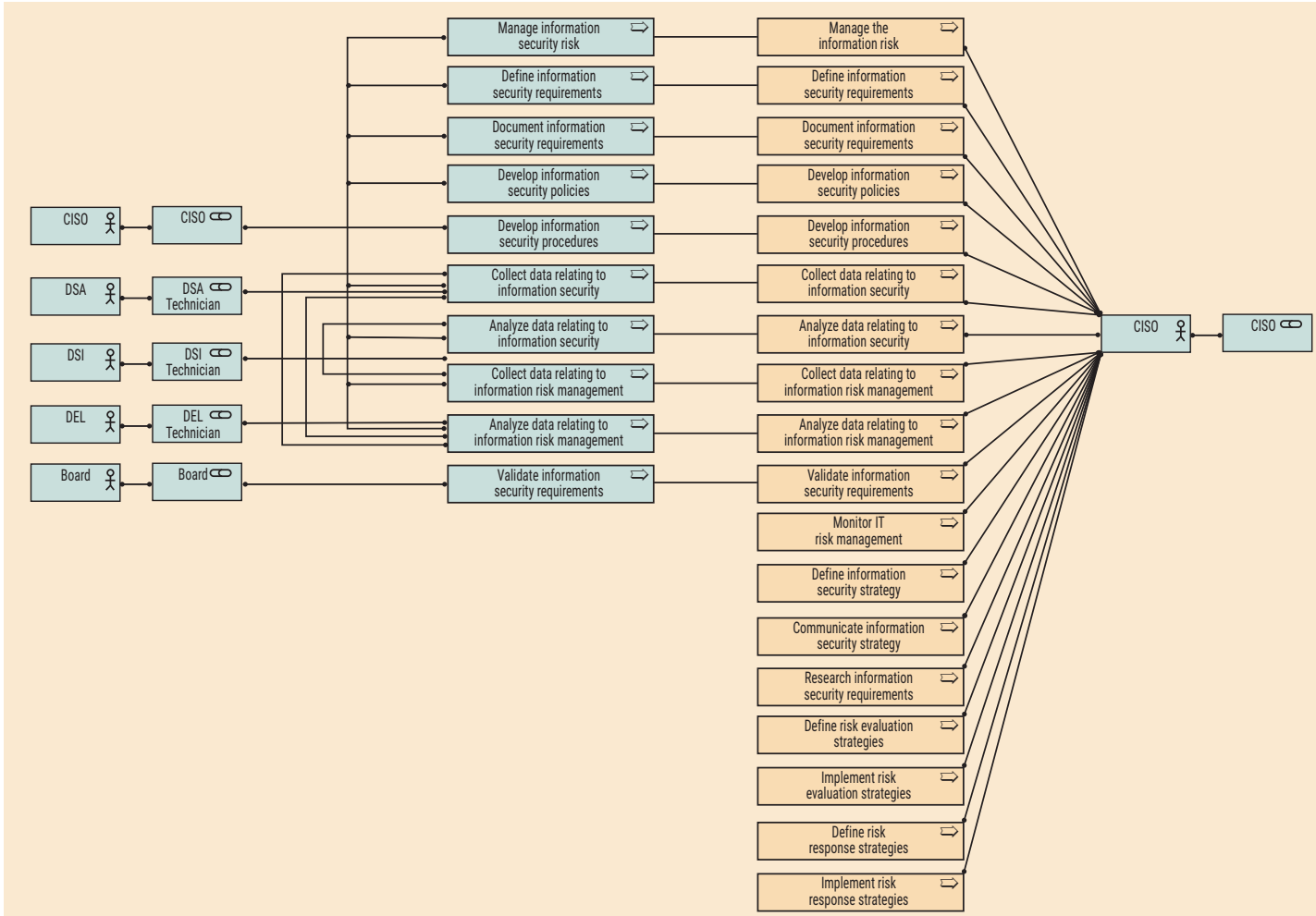
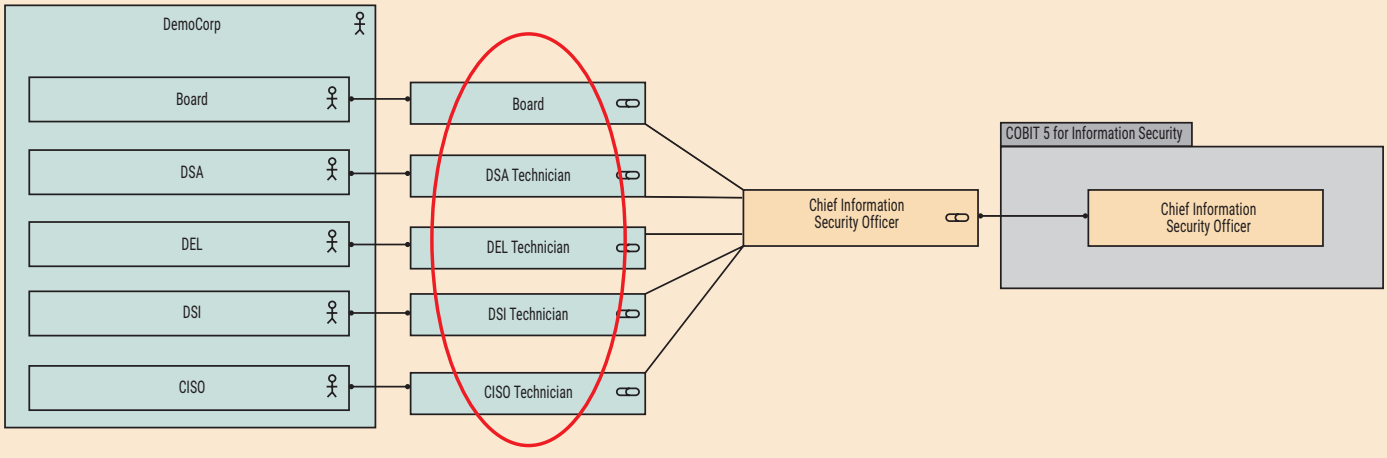


Figure 10—DemoCorp to COBIT 5 for Information Security's Roles Viewpoint



This viewpoint shows four DemoCorp roles that are performing the CISO's role, which are security department (DSA) technician, engineering and laboratories department (DEL) technician, information system department technician and the board.

All of the mappings presented in steps 3, 4, 5 and 6 will be the input for the next step of the proposed method.

Step 7—Analysis and To-Be Design

Some information security gaps were identified, such as missing certain outputs that should have been produced and/or originated by the CISO's role. For example, the development of information security strategy does not have any connection to DemoCorp's information types, which it should, per COBIT® 5.[2] These outputs are essential to any enterprise in which security is an essential part of its business. The absence of these concepts can negatively affect the enterprise (i.e., information security does not create value for the organization).

This step's goal is to design the ideal to-be state of the organization under review. As part of the proposed research method, a set of figures focused on business functions and information types (**figures 11, 12, 13** and **14**) is presented. Furthermore, those figures are required to design the desired organization to-be state. These viewpoints focus on:

- Key practices
- Outputs of the Align, Plan and Organize (APO) process APO01 *Manage the IT management framework*

Figure 11—Information Security Gaps and Recommended Actions of the IT Score

Method's Step(s)	Information Security Gaps	Is it part of the recommended actions for improvement provided by the consulting organization? (Yes/No)
Step 3	Information security plan	Yes
	Information risk strategies	No
	Information security program	Yes
	Information security strategy	Yes
Step 4	Communication on IT objectives	Yes
	Information security training and awareness program	Yes
	Data on the operating environment relating to risk	Yes
	Data on risk events and contributing factors	Yes
	Emerging risk issues and factors	Yes
	Data on information security risk	Yes
	Information security risk mitigation practices	No
	Risk-related root causes	No
Step 5	Monitor IT risk management	Yes
	Define information security strategy	Yes
	Communicate information security strategy	Yes
	Research information security requirements	Yes
	Define risk evaluation strategies	No
	Implement risk evaluation strategies	No
	Define risk response strategies	No
	Implement risk response strategies	No

Figure 12—Mapping of IT Score's Recommended Actions to Information Security Gaps Identified

Recommended Actions for Improvement	Information Security Gaps	Method's Step(s)
Use published information security frameworks, for example, International Organization for Standardization/International Electro technical Commission (ISO/IEC) standards ISO/IEC 27001 and ISO/IEC 27002 to develop a "desired state" vision of the security program, along with associated policies and practices.	Information security program	Step 3
	Information security strategy	
	Define information security strategy	Step 5
	Communicate information security strategy	
Develop a process catalog detailing security practices.	Monitor IT risk management	Step 5
	Define information security strategy	
	Communicate information security strategy	
	Research information security requirements	
Seek formally approved resources, including budget funds and personnel.	Information security plan	Step 3
Begin to formalize processes for cross-organizational communication and collaboration.	Communication on IT objectives	Step 4
	Data on the operating environment relating to risk	
	Data on risk events and contributing factors	
	Emerging risk issues and factors	
	Data on information security risk	
Establish an information security steering committee or working group. This should, preferably, be a high-level policy approval committee, with membership drawn from line-of-business managers.	None	None
Implement an enterprisewide communications program that focuses on ensuring that employees are aware, willing and able to comply with established security policies.	Information security plan	Step 3
	Information security training and awareness program	Step 4

Figure 13—Migration Viewpoint: Information Types

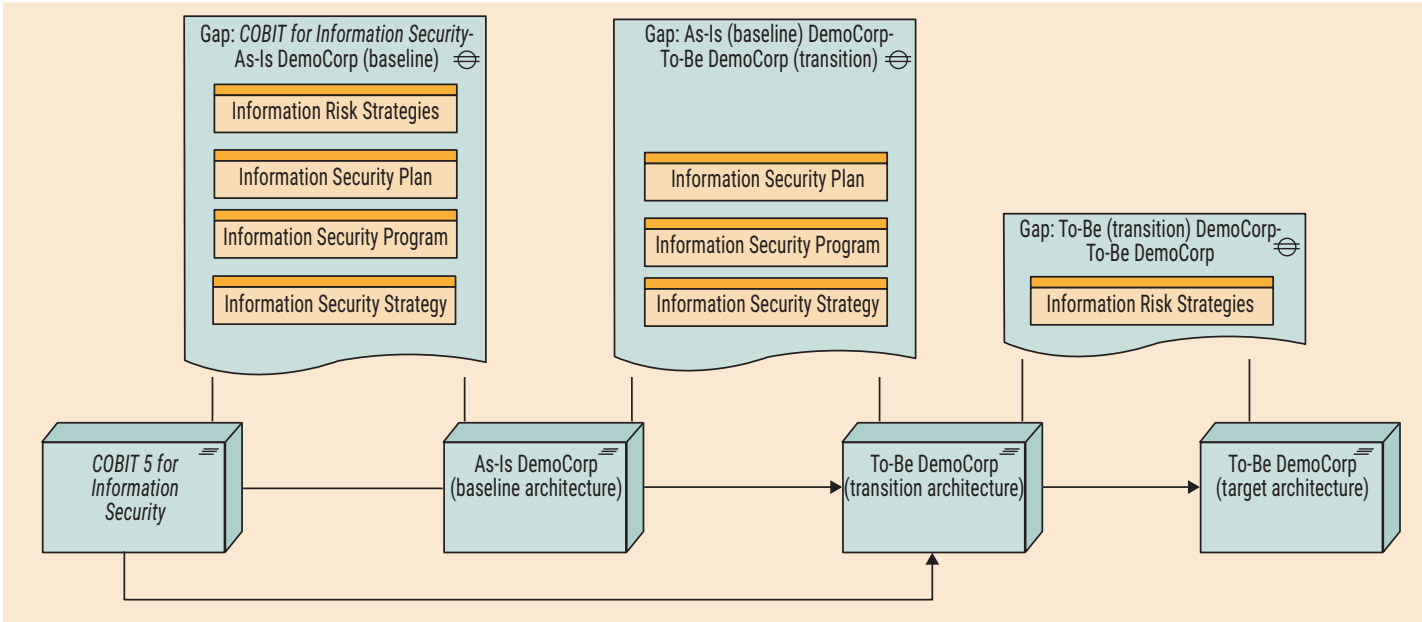
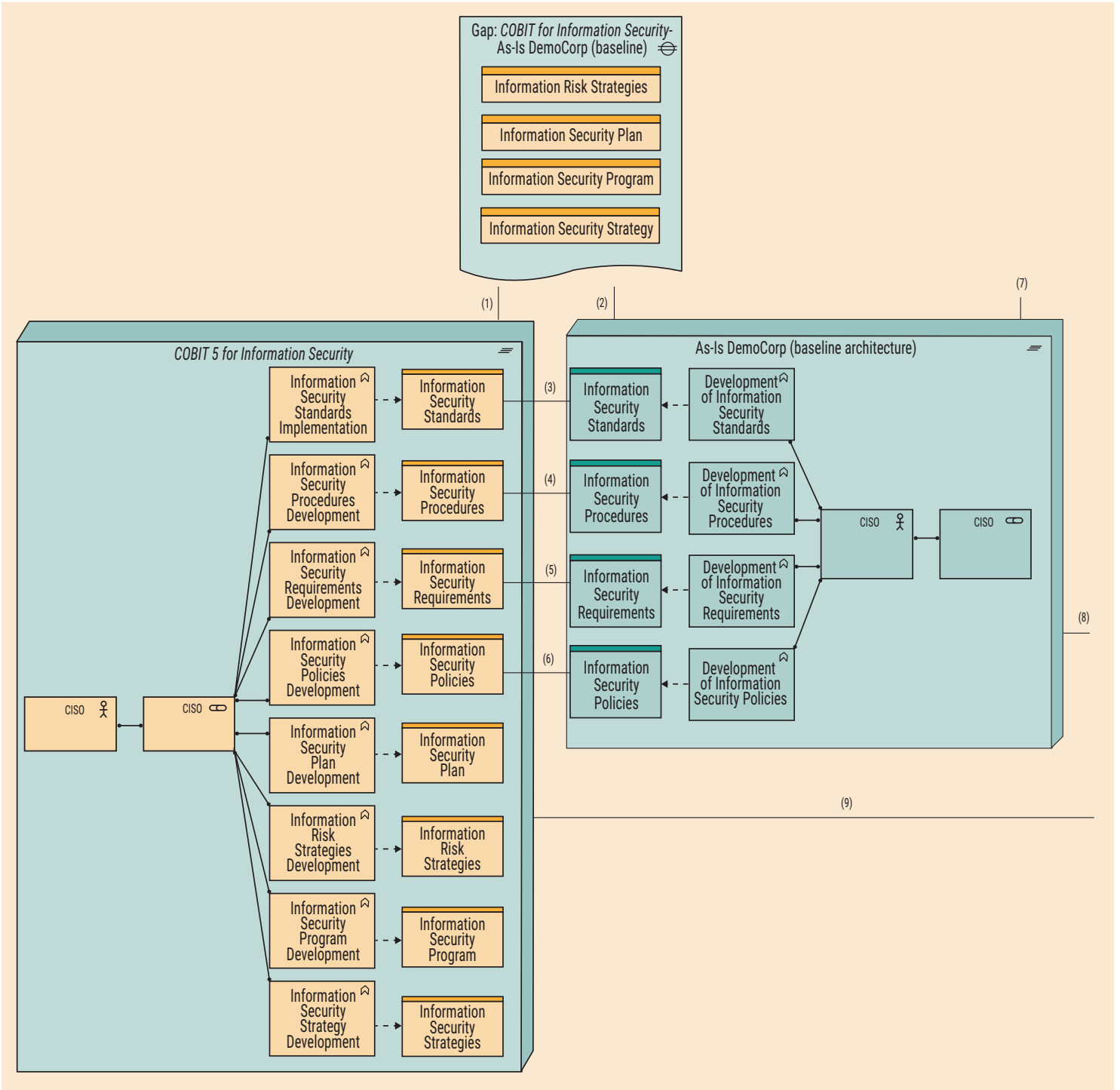


Figure 14—Migration Viewpoint: Information Types (Part 1)



- Outputs of APO12 *Manage risk*
- Outputs of EDM03 *Ensure risk optimization*

In each viewpoint, four plateaus are represented:

1. COBIT 5 for Information Security, taking into account the types of information, key practices and processes' outputs for which the CISO should be responsible (step 1).
2. As-is state of DemoCorp (baseline architecture), taking into account the types of information processes outputs and key practices shown in step 2.
3. To-be status of DemoCorp (transition architecture), which represents the transition architecture of DemoCorp with regard to the role of the CISO in the organization. This architecture

is designed based on the previous two plateaus. In addition, this architecture was designed based on DemoCorp's strategic decision to follow the recommended actions for improvement provided in an INFOSEC IT Score, determined by a consulting organization (figure 11). This information security assessment was made in June 2015.

4. To-be state of DemoCorp (target architecture), which represents the target of DemoCorp's architecture based on *COBIT 5 for Information Security.*

Three gaps are represented in **figures 11, 12, 13** and **14** as well:

1. Gaps between COBIT 5 for Information Security and the as-is state of DemoCorp (baseline architecture), which identify what types of information, key practices and processes outputs are not defined in the organization and, according to COBIT 5 for Information Security, are part of the CISO's responsibilities in an organization.
2. Gaps between the as-is and to-be states of DemoCorp (baseline and transition architecture), which identify which information types, key practices and processes' outputs will be part of DemoCorp's transition architecture. This selection was made based on a strategic decision of the organization.
3. Gaps between the plateaus to-be DemoCorp transition architecture and to-be DemoCorp target architecture that identify which information types, key practices and processes' outputs were not treated in transition architecture due to the strategic decision, but will be treated in DemoCorp's target architecture.

According to the IT score determined by the consulting organization, DemoCorp has a lower maturity level than average government organizations (DemoCorp had 2.5 vs. average government organizations had 2.8). Furthermore, the DemoCorp business focus suggests a maturity target similar to financial services organizations (level 3).

EA should be adapted to the organization and not the other way around. As such, the design of the transition architecture must be in accordance with the organization's business needs. As can be seen in **figure 11**, not all the gaps identified are treated in the design of DemoCorp's transition architecture because the organization decided that it only had to follow the recommendations of the IT score. These recommendations aim to enable the organization to achieve an information security maturity level of 3 to have a maturity level similar to that of financial services organizations. The information security maturity level, which ranges from 1 to 5, is measured according to:

- Security governance
- Planning and budgeting
- Organization
- Controls framework
- Architecture and engineering
- Process and operations
- Communications and awareness
- Event detection and response
- Threat and vulnerability management
- Risk and controls assessment

As can be seen in **figure 12**, there are six recommended actions that DemoCorp should take to reach an information security maturity level of 3. To follow the strategic decision made by DemoCorp, in which the definition of the CISO's role should follow these recommended actions, they have been mapped with the information security gaps identified in steps 3, 4 and 5.

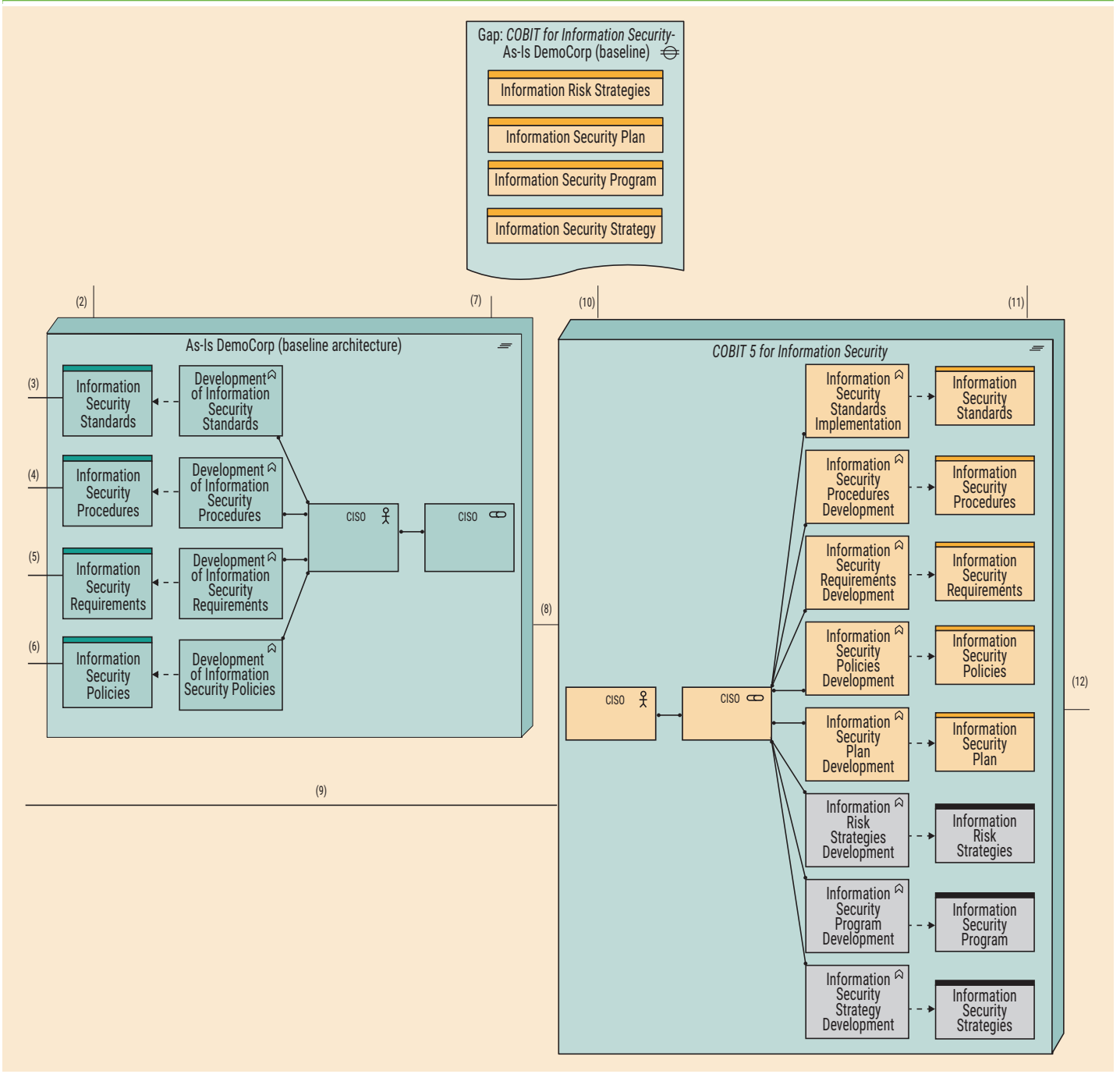
Considering this information, **figures 13**, **14**, **15** and **16** represent DemoCorp's transition and target architecture, regarding the business functions and information types for which the CISO is responsible for originating.

Figure 13 represents the as-is state of DemoCorp, represented by the plateau "As-is DemoCorp (baseline architecture)." This viewpoint presents the organization's information types and the types of information for which the CISO should be responsible for originating, represented in the plateau *COBIT 5 for Information Security*.

In addition to this mapping between the as-is state of the organization's architecture and *COBIT 5 for Information Security*, this viewpoint also represents the information security gaps identified regarding the information types.

Based on what has been described previously (**figures 11** and **12**), it was possible to exhibit DemoCorp's transition architecture, represented in the plateau "to-be DemoCorp (transition architecture)." As can be seen in the "Gap: As-is DemoCorp (baseline)—To-be DemoCorp

Figure 15—Migration Viewpoint: Information Types (Part 2)



(transition)," only the information security gaps information security plan, information security program and information security strategy were considered for the transition architecture, according to the strategic decision made by the organization.

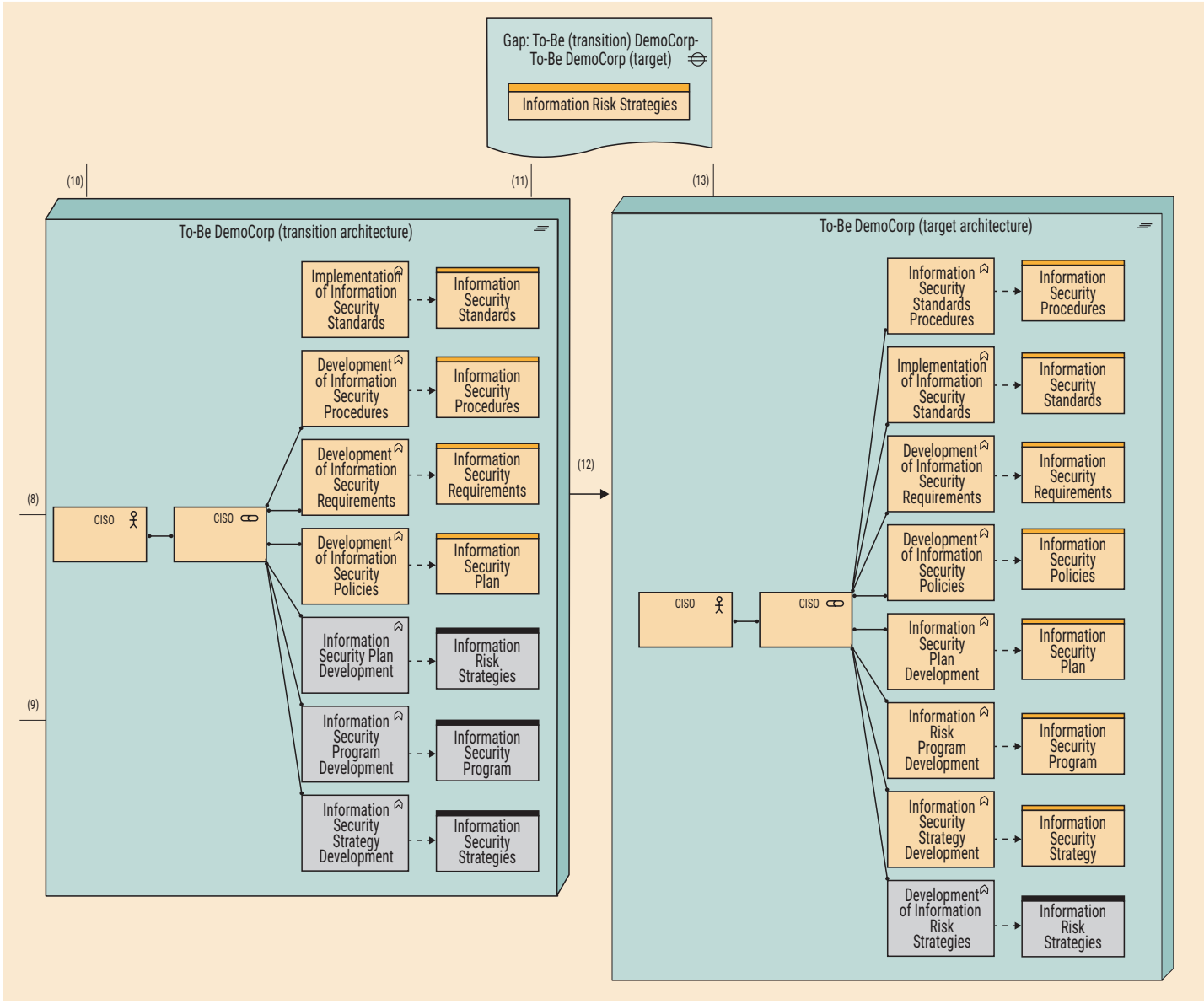
Finally, DemoCorp's target architecture will consider the type of information "information risk strategies," which the CISO is responsible for developing.

Figure 13 only presents the gaps between each one of the plateaus. For a better understanding of what is represented in each one of the four plateaus, see **figures 14**, **15** and **16**, in which the mapping between DemoCorp's as-is state and *COBIT 5 for Information Security*'s definition of the CISO's role is represented and, also, the design of DemoCorp's to-be state (transition and target architecture).

When interpreting the figures, it is important to note that:

- The blue color represents what is defined in DemoCorp.
- The yellow color represents what *COBIT 5 for Information Security* defines as what should be the responsibilities of the CISO.

Figure 16—Migration Viewpoint: Information Types (Part 3)



- The gray color represents what is new (i.e., what will be defined according to the identified gaps).

Figure 14 shows that only the information types information security standards, information security procedures, information security requirements and information security policies are defined in DemoCorp, and the CISO is responsible for originating them.

The remaining information types are not defined in the organization, as can be seen by the absence of the relation "association" between the business objects of plateaus "*COBIT 5 for Information Security*" and "as-is DemoCorp (baseline architecture)." Taking into account the absence of this relation, four gaps have been identified between the two plateaus previously described. Those gaps are information risk strategies, information security plan, information security program and information security strategy.

Figure 15 shows the plateaus "as-is DemoCorp (baseline architecture)" and "to-be DemoCorp (transition architecture)" and the gaps between them. As can be seen, between the baseline and transition architecture, three gaps were identified: information security plan, information security program and information security strategy.

On the plateau of the transition architecture, new responsibilities were added to the CISO's role in DemoCorp, i.e., the CISO will be responsible for originating the information security plan, information security program and information security strategy based on the strategic decision stated previously.

> IN TIMES WHEN COST AND VALUE GENERATION ARE IMPORTANT DRIVERS, INFORMATION SECURITY, MORE THAN EVER, SHOULD DELIVER VALUE AND MAKE ORGANIZATIONS MORE EFFECTIVE AND EFFICIENT.

It is important to note that the design of the plateau "to-be DemoCorp (transition architecture)" is based on the analysis of plateaus *COBIT 5 for Information Security* and "as-is DemoCorp (baseline architecture)."

Figure 16 shows the transition and target architectures of DemoCorp regarding the definition of the CISO's role. Between these plateaus, one gap was identified, since DemoCorp decided that the CISO should be responsible for originating information risk strategies, so the responsibilities of the DemoCorp CISO will be aligned with the responsibilities defined in *COBIT 5 for Information Security*.

Moreover, the corresponding viewpoints for remaining processes and key practices for which the CISO's role is responsible would have *mutatis mutandis*, a very similar structure.

Discussion

It can be assumed that given the proposed method for defining the CISO's role in organizations, the solution that should address this problem is complex and organization-specific. Should organizations adopt *COBIT 5 for Information Security* to define the CISO's role using ArchiMate notation?

The proposed method can be applied in an organization that aims to implement the CISO's role, based on *COBIT 5 for Information Security*. As can be seen from the viewpoints modeled using ArchiMate, the number of gaps regarding the information types that the CISO should be responsible for originating between the as-is state and the to-be state of DemoCorp decreased.

Moreover, new responsibilities were added to the CISO's role in DemoCorp, considering the gaps identified between the DemoCorp's as-is state and *COBIT 5 for Information Security*.

Based on the outcomes of this work, the following are opportunities for related future work:

- Developing a solutions proposal that addresses the inconsistencies detected, allowing stakeholders to establish an accurate connection between the guidance in *COBIT® 5 Enabling Processes*[3] and *COBIT 5 for Information Security* to enable IT governance for different organizations, the goal being to deliver more value to the organization
- Demonstrating and evaluating the method in more government-owned organizations
- Demonstrating and evaluating the method in private-sector organizations, eventually comparing the results with those obtained in the public-sector domain
- Customizing the proposed method by industry/type of organization (e.g., small and medium enterprises [SME] and banking)
- Extending the research proposal to comprise other architectural levels (application and technology layers)
- Extending the proposal to connect the governance and management of information security
- Proposing a framework to guide researchers in analyzing documents and standards of IT governance, and identifying inconsistencies and developing a definition and conceptualization of inconsistencies (e.g., How are they defined and what levels of inconsistencies might exist?)

Conclusion

Organizations that adopt information security governance invest in frameworks to address assignments involved in the action of IT governance. Simultaneously, roles and assigned responsibilities are defined in the COBIT 5 framework.

COBIT 5 should be seen as a framework to support management and governance that provides a "thinking approach and structure" with very useful examples. Furthermore, it is important that stakeholders are critical when using the material to ensure the correct use of the COBIT 5 framework.

This is an effective solution that addresses the research problem and enables the information security implementation, particularly the CISO's role. This solution is based on *COBIT 5 for Information Security*.

In times when cost and value generation are important drivers, information security, more than ever, should deliver value and make organizations more effective and efficient. EA does not reveal how the CISO's role should be defined and implemented, and *COBIT 5 for Information Security* does not provide implementation guidance. But the guidance presented herein provides one method that integrates the EA and COBIT 5 approaches, with distinct organizational structures, that have much more to gain from aligning together instead of diverging.

Endnotes

1 ISACA®, *COBIT® 5 for Information Security*, USA, 2012, *www.isaca.org/COBIT/Pages/Information-Security-Product-Page.aspx*
2 ISACA, COBIT® 5, USA, 2012, *www.isaca.org/COBIT/Pages/COBIT-5.aspx*
3 ISACA, *COBIT® 5: Enabling Processes*, USA, 2012, *www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Processes-product-page.aspx*