The European Union selected COBIT® as one of the three internationally accepted standards¹ to be used to provide information security and control over its agricultural paying agencies.² This brings the question, what are the challenges and benefits of migrating to COBIT® 5³ in the strongly regulated environment of the European Union (EU) agricultural paying agencies? The EU agricultural paying agencies are accredited organizations delegated to execute three main functions in respect of the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD) expenditure:
1. Authorize and control payments to establish that the amount to be paid to a claimant is in conformity with EU community rules.
2. Execute payments to pay the authorized amount to the claimant or, in the case of a rural development, pay the community cofinancing.
3. Account for payments and record all payments in the agency’s separate accounts for EAGF and EAFRD expenditures, in the form of an information system, and prepare periodic summaries of expenditures, including declarations to the European Commission (EC).

Compliance with a set of accreditation criteria is designed to ensure that the paying agency provides sufficient guarantees to:
• Check the eligibility of aid applications before any payment is made
• Keep accurate and exhaustive accounts
• Ensure that required checks by regulation sectors are made
• Make sure all requisite documents are properly kept, accessible and presented in a timely manner

COBIT 5, the latest edition of the ISACA framework, provides EU paying agencies with a great opportunity to rethink their governance and management of enterprise IT (GEIT) while adapting their own information security system and migrating to a new, well-structured and comprehensive standard.

While the International Organization for Standardization (ISO) and British Standards Institution (BSI) standards are specialized “old-style” frameworks that are based on domains, checklists, control objectives and measures, COBIT 5 goes beyond; it focuses not only on the IT function and IT security, but supports the implementation of a comprehensive governance and management system for enterprise IT and information by:
• Enabling IT to be governed and managed in a holistic manner for the entire organization
• Taking in the full end-to-end business and IT functional areas of responsibility
• Considering the IT-related interests of internal and external stakeholders

The main reasons for a paying agency to migrate to COBIT 5 (either from COBIT® 4.1 or from one of the other two guidelines/standards) can be described best by analyzing how the five COBIT 5 principles fit within the paying agency context.

**PRINCIPLE 1: MEETING STAKEHOLDER NEEDS**
One of the most important concerns in a paying agency is managing many stakeholders and actors who play, at different levels, a role in these organizations and have dissimilar (and sometimes conflicting) perspectives and expectations.

A paying agency’s key stakeholders include:
• **Director/top management,** who ensure that:
  – Accounts presented to the EC give a true, complete and accurate view of the expenditure
  – There is a system in place that provides reasonable assurance on the legality and regularity of the underlying transactions, including that the eligibility of demands and, for rural development, the procedure for attributing aid are managed, controlled and documented in conformity with Community rules

---

Giuseppe Arcidiacono, CISA, CISM, CGEIT, PMP, is a computer engineer with more than 10 years of experience. Arcidiacono is the head of the IT department at Agenzia Regione Calabria per le Erogazioni in Agricoltura (ARCEA), a European Commission Accredited Paying Agency (pursuant to Commission Regulation EC No. 885/2006).

---

**Do you have something to say about this article?**
Visit the Journal pages of the ISACA website (www.isaca.org/journal), find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:
• **Internal key users**, mainly from core business departments, who provide aid to make payments correctly, ensure that payments are fully recorded in the accounts, and submit the requested documentation within deadline and in the manners stipulated in EU rules

• **Final claimant**, who should receive claims as soon as possible

• **European Commission**, which accredits, monitors and controls paying agencies. The EC can impose financial corrections on the member state under the conformity clearance procedure.

• **Certification bodies**, which conduct their examination of a paying agency according to internationally accepted auditing standards and taking into account any guidelines on the application of the standards established by the EC

• **Internal auditors**, who have to verify that procedures adopted by the agency are adequate to ensure that compliance with Community rules is verified and the accounts are accurate, complete and timely

It is neither straightforward nor simple in this context to negotiate and decide among different stakeholders’ value interests. It is fundamental to:

• Gather and analyze quantitative and qualitative information to determine whose interests should be addressed

• Identify the interests, expectations and influence of the stakeholders and relate them to the mission of the agency

• Identify stakeholder relationships that can be leveraged to build coalitions and potential partnerships

**PRINCIPLE 2: COVERING THE ENTERPRISE END-TO-END**

A paying agency’s processes are complicated and often cross-departmental. They are regulated by EC laws that establish requirements, rules and specific mandatory steps and require that many roles and responsibilities are set.

All of these processes are IT-related: It is fundamental to integrate GEIT into enterprise governance. In other words, paying agencies have to treat information and related technologies as assets that need to be dealt with, just like any other asset, by everyone in the enterprise.

The EC requires that, at all levels, the daily operations and controls activities of the agency be monitored on an ongoing basis to ensure a sufficiently detailed audit trail.

**PRINCIPLE 3: APPLYING A SINGLE, INTEGRATED FRAMEWORK**

As previously mentioned, paying agencies must comply with a strict baseline defined by Commission Regulation (EC) No. 885/2006.

To be accredited, a paying agency, as defined also in article 6 of Regulation (EC) No. 1290/2005, must have an administrative organization and a system of internal control that comply with the criteria set out in annex I to EC 885/2006 (“accreditation criteria”) regarding:

• Internal environment

• Control activities

• Information and communication

• Monitoring

COBIT 5 helps with compliance because it aligns with other relevant standards and frameworks at a high level (both enterprise- and IT-related) and can, therefore, serve as the overarching framework for GEIT.

Using COBIT 5 makes it easier for a paying agency to comply with accreditation criteria by placing every piece in a cohesive whole and helping stakeholders understand how various frameworks, good practices and standards are positioned (relative to each other) and how they can be used together.

**PRINCIPLE 4: ENABLING A HOLISTIC APPROACH**

The COBIT 5 framework describes seven categories of enablers that individually and collectively influence whether GEIT will work and how they are driven by the goals. The seven enablers are:

• Processes

• Organizational structures

• Culture, ethics and behaviors

• Principles, policies and frameworks

• Information

• Services, infrastructure and applications

• People, skills and competencies

In the paying agencies’ environment, some of these enablers assume a major value, particularly:

• EU regulations require all paying agency activities to be organized in well-structured processes and described by formally adopted manuals. All processes have to achieve certain objectives and produce a set of outputs in support of achieving overall organizational goals.

• The internal organization is one of the most important accreditation criteria for paying agencies. The agency’s organizational structure must provide for clear assignment of authority and responsibility at all operational levels and for separation of the three functions (authorization and control of payments, execution of payments, and accounting). The responsibilities of the three functions are to be defined in an organizational chart and include technical internal audit services.
Information is pervasive throughout paying agencies. Information is required for keeping the agency running and well governed. Although information is not a key product of the agency, European regulations mandate that information security measures be adapted to the administrative structure, staffing and technological environments of each individual paying agency. The financial and technological efforts are to be in proportion to the actual risk incurred.

Paying agencies have to comply with many people-related requirements. They have to respect the following:
- Appropriate human resources must be allocated to carry out the operations, and the technical skills required at different levels of operations must be present.
- The division of duties must be such that no official has responsibility for more than one of the responsibilities for authorizing, paying or accounting of sums charged to funds, and no official can perform one of those tasks without his work coming under the supervision of a second official.
- The responsibilities of each official must be defined in writing.
- Staff training must be appropriate at all levels of operation, and there must be a policy for rotating staff in sensitive positions.
- Appropriate measures must be taken to avoid a conflict of interest.

**PRINCIPLE 5: SEPARATING GOVERNANCE FROM MANAGEMENT**

Paying agencies do not have a board, but the EC requires that they make a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes. Management runs the organization from day to day, while governance sets policy, exercises oversight and strategically guides the organization. The separation of governance and management involves a division of both duties and personnel.

**CONCLUSION**

Migrating to COBIT 5 can bring many benefits to EU accredited paying agencies.

In particular, COBIT 5 could help paying agencies ensure that adequate governance structures are in place and increase the level of capability and adequacy of the relevant IT processes, with the expectation that as the capability of an IT process increases, the associated risk will proportionally decrease and efficiencies and quality will increase.

In addition, the following benefits could be reached:
- Maximizing the realization of activities’ improvements through IT while mitigating IT-related risk to acceptable levels
- Support of the strategic objectives by key investments and optimum returns on those investments, thus aligning IT initiatives and objectives directly with the agency’s mission
- Compliance with EU accreditation criteria
- A consistent approach for measuring and monitoring progress, efficiency and effectiveness as required by the EC
- Lowered cost of IT operations and/or increased IT productivity by accomplishing more work consistently in less time and with fewer resources

**ENDNOTES**

1 The other two guidelines are: ISO/IEC 27002 (www.iso.org/iso/catalogue_detail?csnumber=50297) and Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzhandbuch (the IT Baseline Protection Manual) (https://www.bsi.bund.de/english/publications).
4 Guideline No. 4 on the statement of assurance to be provided by the director of a paying agency pursuant to article 8(1)(c)(iii) of Council Regulation (EC)NO 1290/2005
6 European Commission, Directorate-General for Agriculture and Rural Development, Guidelines for the Certification Audit, Guideline No. 5—Audit Strategy
7 Accreditation criteria cover the four basic areas of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) model.
8 Annex I of Commission Regulation (EC) No. 885/2006 states: “Ongoing monitoring is built into the normal, recurring operating activities of the paying agency.”