Editor: **Christof Ebert**
Vector Consulting Services
christof.ebert@vector.com

IT Governance

Christof Ebert, Aurora Vizcaíno, and Antonio Manjavacas

From the Editor

Standards and governance ensure adherence to regulations and laws, mitigate business risks, facilitate global collaboration, and therefore protect society as well as the economy. From a legal perspective, they define the state of the art and thus serve as the basis for transparence, audits, and liability. Authors Aurora Vizcaíno, Antonio Manjavacas, and I show how to practically handle IT governance. We briefly introduce governance and standardization. An overview of tools and an industry case study show how to efficiently handle governance requirements. At this time I specifically invite all readers to participate in our annual industry survey (see "Industry Survey"). —*Christof Ebert*

CORPORATE GOVERNANCE ENCOMPASSES the set of rules, processes, and methods aimed at defining and meeting the strategic objectives of an organization.[1] These objectives normally have long-term repercussions and define the road map of the companies, considering the different entities directly affected by the strategic decisions taken, such as external stakeholders.

IT governance as a subset of corporate governance is of pivotal relevance both in engineering and management. It drives strategic decisions related to IT, considering their impact and repercussions on business value. Business-oriented IT governance should be driven by two main objectives: adding value to the business through information technologies and mitigating the risks associated with them. We can differentiate four key areas in governance[2]:

- *Strategic alignment*: ensuring the connection between IT and business strategies and operations.
- *Value delivery*: ensuring that information technologies generate the expected benefits.
- *Resource management*: optimizing the investments made in IT as well as the correct management of IT resources, from applications to information, infrastructure, and people.
- *Performance measurement*: monitoring the implementation of the IT strategy, evaluating aspects such as the use of resources or the performance of the adopted processes.

IT governance in organizations seeks to ensure that IT investments are made in accordance with the defined strategic objectives. This aligns corporate governance and IT governance, offering monitorable and, therefore, measurable results. At the same time, governance involves practices and commitments focused on the proper management of the organization.[3,4] Thus, governance activities can be

Digital Object Identifier 10.1109/MS.2020.3016099
Date of current version: xxxxxxx

defined as a metamanagement directing of operations toward the objectives set by strategic business levels.

Standards and Governance

International standards and enforced governance ensure legal transparency and, thus, facilitate fair collaboration across companies and countries.[1] They are agreed to at the national and international levels by recognized associations and trade or government organizations. In IT and software development, standards are the basis of the "state of the art," for example, in product liability or in safety and cybersecurity. With the International Organization for Standardization (ISO), the United Nations has deliberately chosen the highest level of standardization to support international cooperation and, thus, world peace.

Often standards are "de facto" accepted and established procedures that facilitate cooperation. In development and IT, many standards have been globally agreed on, for example, for the exchange of data and for component interfaces. Standards facilitate international cooperation and offer reliability in projects and in the use of external components for product development. They are particularly useful in the reliability and security of products and services but also for the finance robustness of companies. For IT and software, there are several standards relevant for governance:

- *ISO/International Electrotechnical Commission [IEC] 38500*: Corporate governance of information technology
- *COBIT5*: Leading IT governance and control framework
- *ITIL*: IT infrastructure library with a focus on IT service management
- *ISO 22301*: Business continuity
- *ISO 330xx*: Process assessments, e.g., ASPICE
- *ISO 20000*: IT service management
- *Prince2 and PMBoK*: Project management
- *ISO 250xx*: Product quality, e.g., performance, portability, reliability, and maintainability
- *ISO 27001*: Information security and risk management
- *IEC 61508 and derived standards, such as ISO 26262 and ISO 25119*: Functional safety
- *ISO 29148 and IREB*: Requirement engineering
- *ISO 29119 and ISTQB*: Software testing.

An important advantage of standards for both producers and consumers is the clearly defined state of the art, which is important not only for engineers as a compendium of applicable knowledge but also for the jurisdiction. Periodic audits are performed, either internally or externally, to check whether a company is complying with this state of the art. Without this proof, liability in the event of damage is typically decided at the expense of the supplier, which has obviously not exercised the necessary care in its processes.

It is becoming increasingly difficult to comply with all applicable standards due to their fast growth. They tend to overlap and exhibit regional characteristics. Standards must be carefully implemented in their complexity to be legally effective and, at the same time, not create overheads. Governance mechanisms should be well synchronized; for instance, cybersecurity should be matched with risk management and, where applicable, functional safety (see "Lean IT Governance in Industry").

INDUSTRY SURVEY

In future issues of *IEEE Software*, the "Software Technology" column will address major challenges in software and IT. As the current fast-changing software and IT landscape adjusts to the COVID-19 pandemic crisis, you are invited to take part in a short survey on industry trends in 2021. Your opinion as a domain expert and decision maker is valuable. Please give us 2 min of your time and answer four brief questions. After the end of the survey, you will exclusively receive its analysis, enriched with experiences and hands-on advice from current projects. With some luck, you will also receive a free copy of the IEEE book *Global Software and IT*. We will not use your personal data any further. Here is the link to the industry survey: www.vector.com/trends-survey.

> IT governance as a subset of corporate governance is of pivotal relevance both in engineering and management.

LEAN IT GOVERNANCE IN INDUSTRY

Currently, many original equipment manufacturers (OEMs) are establishing a transparent software update management system. In the mobility and automotive sector, UNECE has established regulations to achieve safety, security, and transparent functionality. A new regulation will become mandatory in 2022 onward for cybersecurity manage-

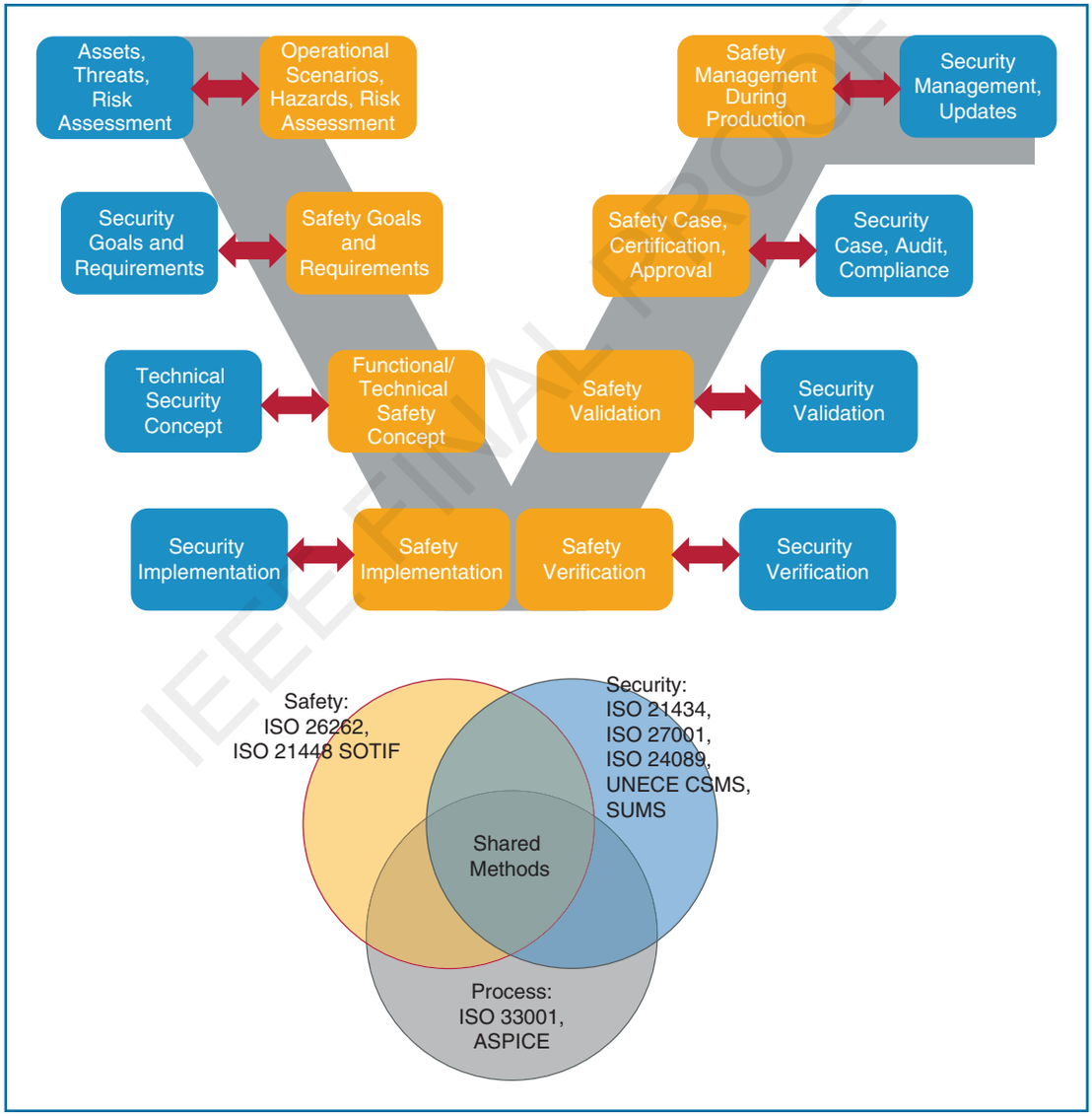

FIGURE S1. Orchestrated lifecycle processes ensure efficiency and consistency. Standards refer to automotive industry, but equally apply to other industries.

(Continued on next page)

LEAN IT GOVERNANCE IN INDUSTRY (CONT.)

ment systems and software update management systems (SUMs). Both target protection against the manipulation of the software in a vehicle.

SUMs require a high level of governance, starting from the OEM IT systems to the cloud services, until each single vehicle and its over-the-air software updates. It requests a continuous transparency of all software versions in the vehicle that are relevant for approval. This starts with the impact analysis of a change or new function at the OEM, and it requires consistency in the development process, documentation of risk assessments, safe transfer to the vehicle and electronic control units, and information for the driver and the approval authority, for example, via infotainment and diagnostic interfaces. Implementation costs are high, especially for vehicles with a lot of variance and functional complexity.

For SUMs we use the existing development processes, which already provide the basics through ASPICE, cybersecurity, and safety. Essential changes are in the impact analysis to the applicable approval requirements as well as the continuous traceability based on regulation × SW identification number (R×SWIN). Safety objectives are derived from the influence and hazard analysis, which are then transformed into requirements and a safety concept. This process is based on ASPICE, because the essential methods, such as system analysis, traceability, and documentation, are anchored there. The security processes, starting with threat and risk analysis, are also directly docked up to delivery and postdeployment updates. For instance, a safety target with a high safety integrity level classification is obviously an asset to be protected from a cybersecurity perspective.

For automatic and autonomous functions, safety of the intended functionality must now be consulted, because the requirements and assumptions for this step are still incomplete. Special analysis methods from SOTIF identify the notorious "unknown unknowns." These are functions and their correlations that can lead to security risks due to ignorance and lack of awareness of this ignorance. This applies to safety (such as a danger from automation) and to security (for example, a misuse case or an abuse case) as a new requirement. The documentation and information with R×SWIN as an anchor point are described in the requirements database. The regression tests can also be directly derived from there so that changes can be immediately secured with the impact analysis on approval specifications.

To ease the IT governance end to end, we have coined, together with major certification bodies, methods that encompass these regulations and can be introduced even to legacy vehicles with partially quite old software systems. Figure S1 shows the underlying standards and how we can simplify their adoption for lean governance by shared methods.

IT Governance Solutions

To ease IT governance, tools are necessary that check standards and provide necessary reporting. To conduct the compilation of the main solutions in the market focused on IT governance, an exhaustive search was carried out through dedicated web portals, consultation with domain experts, and specialized publications, resulting in the set of tools reflected in Tables 1 and 2, which address the following points:

- *tool*: the name identifying the tool or solution
- *company*: the company offering the proposed service or tool
- *main features*: the key or more outstanding features of the solution being addressed that identify distinguishing factors and advantages over other solutions.

Industry Domain Applicability

From the point of view of the domains where these governance solutions are most established, Table 2 provides a summary of the main impact areas for each of them.

Practical Recommendations

From our many consulting projects, we derived a set of four major recommendations.

Ensure Compliance—Transparent and Efficient

Recording is rewarding—this old slogan is vital for product liability. Compliance and governance require the consistent application

Table 1. IT governance solutions.

Tool	Main features
ControlCase IT-GRC platform	• Creation of custom compliance programs that incorporate external and internal regulations • Allows implementation of corrective actions • Predefined compliance ControlKits enable compliance with several standards
MetricStream IT-GRC solution	• Integration with multiple-endpoint IT security and infrastructure management tools • Includes data analytics and business intelligence services • Common framework to monitor IT regulations and standards
Modulo GRCi/SAI D360	• Deep integration with Microsoft Business Intelligence solutions • Easy integration with other Module services, GRC platforms, security tools, and so on • Easy generation of high-level reports
ITGRCBond	• Creation of user-configurable workflows • Automatic gap identification and remediation plans • Accuracy and accountability of assessment data through prebuilt prescriptive control content and response audit trail
itmSuite	• Enables the publishing and diffusion of IT governance policies to custom receivers • Offers means to design IT processes and IT enterprise architectures • Allows the assessment of policy maturity by means of real-time reports and dashboards
IBM Open Pages	• Includes data integration from multiple sources through Representational State Transfer (REST) application programming interfaces • Based on the three lines of defense model • Includes artificial intelligence and natural language processing support
Keylight	• Automatically generates audit tasks based on regulatory guidance • Centralizes and connects policies, controls, authoritative guidance, risks and vulnerabilities, IT assets, incidents and issues, third parties, and business continuity plans • Monitors risks against defined key performance indicators (KPIs)
Logic Manager IT: governance, security, and privacy solution	• Allows prioritization of critical IT resources and identification of gaps in risk protection • Helps to track the status of reviews and follow-up actions with automated workflows, notifications, and reminders • Includes a marketplace with featured plugins for frameworks, legal registers, and policies/charters
SAI360: IT risk and cybersecurity solution	• Automated vulnerability management and risks assessment through vulnerability scanning tools • Simple migration of existing policies to a centralized and flexible policy library • Automates vulnerability management with a centralized repository for external data feeds, incidents, risk assessments, and vulnerability scanning tools
Microfocus APM	• Enables IT processes, such as resource budgeting and financing, capacity management, service level agreement management, and customer demand as well as satisfaction management • Ability to produce targeted reporting on demand, at different levels of aggregation, for different end-user classes • Tracking service level availability and performance both on a real-time basis and for offline planning purposes
Aha!	• Creation and sharing of IT road maps • Budgets settlement and costs tracking to make informed investment decisions • Creation of custom workflows to formalize approval processes and streamline review cycles
ServiceNow GRC	• Offers an integrated risk framework that connects business, security, and IT in a single platform • Automatically identifies noncompliant controls, monitors high-risk areas, and manages key risk indicators and KPIs • Automated risk treatment actions across business and IT processes
Alfabet enterprise architecture management (EAM)	• Provides a real-time picture of the enterprise architecture landscape, including applications, technologies, and business processes • Includes out-of-the-box reports, allowing the design of lifecycle graphs, geomaps, business charts, and rankings, including KPI visualization • Allows the categorization of technologies by relevance for supporting business strategy as well as its evaluation

Continued

Table 1. IT governance solutions (cont.).

Tool	Main features
eQCM IT: governance module	• Allows the consistently following of best practices to initiate IT change requests, assess change impacts, create action plans, obtain approvals, or provide communication throughout all of the stages of the change cycle • Offers the assessment of control objectives based on chosen frameworks, such as COBIT • Integrated with standard enterprise technologies, such as Microsoft, Oracle, and so forth
InvGate service desk	• Logs, manages, resolves, and reports on the IT issues that are affecting business operations. • Provides meaningful financial information on IT activities to assess IT costs as well as capabilities oriented to budget control, forecasting, and chargeback • Includes data analytics mechanisms oriented to monitor efficiency, effectiveness, and value in day-to-day activities as well as to identify trends and improvement opportunities
CMDBuild READY2USE	• Allows the management of the IT asset lifecycle • Implements processes and workflows designed according to the indications of ITIL best practices • Offers multiple interfaces: web GUI, mobile app, and self-service portal as well as REST and SOAP web services
Resolver: IT risk and compliance management software	• Improved IT risk and compliance management through centralization of threats and vulnerabilities, aligning controls to best practice frameworks and regulations • Provides generation of risk trend reports, enabling stakeholders to access executive and operational reports • Guides and instructs users in how to assess risks and controls
RSA Archer: IT and security risk management	• Automated IT assessment, monitoring, and reporting • Implements a consistent process for testing IT controls • Allows the capture of a complete catalogue of business and IT assets for IT risk management purposes • Offers a quantification of the organization's financial risk exposure to IT and cybersecurity events. Also offers a big data approach to identifying and prioritizing high-risk cyberthreats

of standards—and documentation of the results. We often notice with customers that processes are briefly refreshed during audits but get lost in day-to-day business under time pressure and misunderstood agility. Live the standards and demand their use as a rule. If the adaptation of the safety case for a small software change takes too long, it is due to the process. Use semiautomatic technology, such as the techniques described in Tables 1 and 2. Automate processes through modular documentation and (semi)automatic impact analyses.

Use Standards—Smart and Lean

Practically all companies complain about the high costs of implementing the flood of standards. Looking closely, we often find that standards are independently implemented and applied and, thus, are inefficient and complex. Even worse, standards are misused as process instructions, rather than taking their essence into a suitable own process layout. Standards describe goals. They do not describe a method for implementation. This makes standards independent of the environment and timeless. Our clear recommendation is to know and link the relevant standards but never copy them as a process. In addition, we recommend a common architecture of standards and processes in which common methods are specifically developed.

Apply Base Processes—Consistent and Sustainable

Processes and standards help only if they are enforced, periodically checked on their effectiveness and efficiency, and accordingly improved. As consultants, we are called into task forces to safeguard endangered projects. When doing our initial firefighting assessment, we often find out that basic process requirements are not consistently implemented. In many cases, agility is completely misunderstood. Engineers and their managers are misled that agility means they should not follow processes, which is very damaging to companies. They often forget about necessary methods, such as traceability and impact analysis, with the consequence that components cannot be integrated. This becomes especially apparent in supply chains, multichannel sourcing, and the introduction of service-oriented architectures as well as adaptive systems with machine learning and

Table 2. The main domains in IT governance solutions.

	Health care	Finance	Services	Manufacturing	Utilities	Automotive	Government	Education
ControlCase IT-GRC platform	✓	✓	✓	✓	✓			
MetricStream IT-GRC solution	✓	✓	✓	✓	✓			
Modulo GRCi/SAI D360	✓			✓	✓	✓	✓	
ITGRCBond	✓	✓	✓	✓				✓
itmSuite		✓						
IBM Open Pages		✓	✓	✓				
Keylight	✓	✓		✓	✓			✓
Logic Manager IT governance security and privacy solution	✓	✓		✓	✓	✓	✓	✓
SAI360: IT risk and cybersecurity solution	✓	✓	✓	✓	✓			
Microfocus APM	✓	✓						
Aha!								
ServiceNow GRC	✓	✓		✓			✓	✓
Alfabet EAM		✓	✓	✓				
eQCM IT governance module	✓		✓		✓	✓	✓	
InvGate service desk		✓	✓	✓				
CMDBuild READY2USE	✓		✓			✓	✓	✓
Resolver IT risk and compliance management software	✓	✓	✓	✓	✓	✓		
RSA Archer IT and security risk management	✓	✓	✓	✓				

artificial intelligence. In such adaptive software and IT systems, ensure under all circumstances effective basic processes, especially project management, configuration management, and requirements engineering.

Integrate Expertise and Knowledge—Usable and Useful

Many teams work well on their specific functional requirements but overlook the standards to be applied. Reworking later is very time consuming, as our above example of cybersecurity in key management and real-time performance shows. Agile teams can hardly build up the necessary competencies. Isolated ivory towers with governance experts are too far away from project pressure. We therefore recommend agile feature teams in which the minimum necessary basic expertise on and responsibility for governance are explicitly named for one person who, in turn, is networked with colleagues and subject matter experts. Agile push and pull ensures effective governance more than rigid specifications. External reviews are pivotal as they facilitate fast corrective cycles. For many of our customers, we use virtual governance managers as a

single contact person for the project, thus ensuring consistency and continuity.

To conclude on governance in software and IT, we recommend staying pragmatic and balancing cost and risk. Too often, we see shadow organizations that dogmatically fight for formal rules without understanding the business tradeoff. Not all standards are of the same relevance, and not all rules are necessary in practice. Examples are privacy regulations, which, during the recent pandemic crisis, were treated as more relevant than health in some European countries. The famous German philosopher Hegel, whose 250th birthday we currently commemorate, underlined the very necessity of such a balance: "the fear of error is the error itself." Innovation must not be constrained by too many rules. As engineers, we should follow critical rules but also allow error and learn from it—to move forward and not administrate the past.

Acknowledgment

The work of A. Vizcaino and A. Manjavacas has been funded by the G3SOFT project (Consejería de Educación de la Junta de Comunidades de Castilla La Mancha) and BIZDEVOPS-GLOBAL project (Ministerio de Ciencia).

References

1. C. Ebert, *Global Software and IT: A Guide to Distributed Development, Projects, and Outsourcing*. Hoboken, NJ: Wiley, 2012.
2. "COBIT 2019 framework. Introduction and methodology," ISACA, Rolling Meadows, IL, 2018. [Online.] Available: https://www.isaca.org/bookstore/bookstore-cobit_19-print/cb19fim
3. P. L. Bannerman, "Software development governance: A meta-management perspective," in *Proc. ICSE Workshop Software Development Governance*, May 2009, pp. 3–8. doi: 10.1109/SDG.2009.5071329.
4. A. Manjavacas, A. Vizcaíno, F. Ruiz, and M. Piattini, "Global software development governance: Challenges and solutions," *J. Softw. Evol. Process*, to be published. doi: 10.1002/smr.2266.

ABOUT THE AUTHORS

CHRISTOF EBERT is the managing director of Vector Consulting Services. He serves on the editorial board of IEEE Software and is a Senior Member of IEEE. Further information about him can be found at https://twitter.com/christofebert. Contact him at christof.ebert@vector.com.

AURORA VIZCAÍNO is a professor and researcher at the Alarcos research group, Escuela Superior de Informática, University of Castilla–La Mancha, Spain. Her research interests include global software development and knowledge management. Contact her at aurora.vizcaino@uclm.es.

ANTONIO MANJAVACAS is a research assistant at the Alarcos research group, Escuela Superior de Informática, University of Castilla–La Mancha, Spain. His research interests include artificial intelligence and sociotechnical congruence. Contact him at antonio.manjavacas@uclm.es.

Recording is rewarding—this old slogan is vital for product liability.