

Workflow—the Compliance Project Engine

Arnaud Bezancon, Advantys, France

INTRODUCTION

Businesses today are required by law to comply with a vast range of regulations and standards. They have to implement new procedures to ensure full accountability, maintain records of all decisions taken and analyze any deviation through the use of audits.

An organization's ability to manage compliance and governance projects efficiently has become key issue which impacts directly on their business performance.

This chapter highlights a number of processes required by legislation such as Sarbanes Oxley, HIPAA & BASEL 2, IT governance standards such as COBIT, ITIL & ISO 17799, as well as corporate project management.

Automating this type of procedure with the help of a workflow solution is an essential part of any compliance project. Workflow must also be intrinsically linked to the existing IS, as well as a certain number of consultation and audit reports in order to cover all the requirements of the regulations and governance standards.

WORKFLOW – A COMPLIANCE PORTAL

Compliance is largely reliant upon the application and implementation of processes, meaning organizations concerned have to choose between:

- Finding manual hardcopy or electronic solutions,
- Investing in procedure-specific solutions,
- Implementing workflow software covering all the processes via a single Portal.

Manual solutions quickly reveal their limitations in terms of costs and resources.

Specific solutions for each procedure provide short-term answers, but are relatively costly in terms of initial investment, integration and maintenance. Furthermore, end users are regularly required to work with a large number of applications. Ten or more processes are often necessary in a particular IT compliance or governance project.

Using a workflow solution as a compliance portal provides not only financial gains in terms of procedural implementation, but also facilitates support for the changes involved in the project. Users all enter at the same point to initiate requests or perform actions within the compliance procedure, while statistics and other reports allow the various processes to be cross-referenced and compared. Finally, reduced training time means the new procedure will be simpler to deploy.

Speed is also of vital importance—laws and regulations change and so does the way a company is organized. A workflow solution allows for adjustments to be made in the definition of a procedure with far more flexibility than a single, procedure-specific solution, and it provides the company's internal teams with the skills required to make the adjustments within a relatively short timeframe.

Accountability is also a key part of these laws, regulations and standards: auditors often want to know “who did what and when”. Most workflow software pro-

vides a high degree of accountability allowing completed forms and actions implemented at each stage of the process to be traced back.

Using a workflow portal to generate the process part of a compliance project means many technical difficulties encountered when backtracking requests submitted and decisions taken.

SARBANES OXLEY ACT

Complying with SOX is an ongoing process for any business. It implies changes to internal organization and formal guidelines regarding the flow of information and, because the number of processes can rapidly escalate, developing specific measures for each individual process is not viable in terms of time and expense.

In addition, the process workflows need constant updating to integrate internal changes at both organization and IS levels. The SOX workflow is a constant pre-occupation for any business.

Workflow means compliance with the Sarbanes Oxley Act is easier for two main reasons:

- rapid implementation of SOX-related processes,
- compatibility of the workflow solution with the technical constraints imposed by the application of the SOX standard.

Security

- authentication on the workflow portal is fully compliant with the company's security policy,
- access to information depends on the user's profile & access rights,
- forms can include certificate-based electronic signatures meaning information sent and user ID are secure,
- secure access to physical data storage on servers complies with the SOX standard.

Audit trail

- all actions performed during process execution are logged and stored,
- each version of all modified forms can be saved for maximum control,
- files and data circulating in the process can be exported at any point to third-party electronic data management systems.

Availability

- the workflow engine can be integrated into high-availability systems, including Web Farms.
- data and process replication also allows a failure recover plan to be implemented.

HIPAA

HIPAA compliance involves deploying a considerable number of processes and setting up technical safeguards.

The costs generated by HIPAA compliance projects can be dramatically reduced by implementing workflow. Instead of hiring new personnel to perform human-based processes or developing dozens of specific software applications, health care organizations can deploy fully compliant automated processes.

The workflow portal provides real time request follow-up, action tracking and audit trail functions as well as connectors to build gateways with legacy systems like HIS, databases, directories and ERPs.

Administrative safeguards require the implementation of several processes which can be automated using workflow. The administrative safeguards comprise over half the HIPAA processes and are grouped in the following standards:

- Security management process
- Assigned security responsibility
- Workforce security
- Information access management
- Security awareness and training
- Security incident processes
- Contingency plan
- Evaluation
- Business associates contracts and other arrangements

Security management process

This standard requires organizations concerned to "implement policies and processes to prevent, detect, contain and correct security violation".

The following processes defined in this standard can be successfully automated and optimized by using workflow software:

- Risk analysis
- Risk management
- Sanction policy
- Information system activity review

Each process can include the following features:

- e-Form for data entry and management
- Workflow to orchestrate requests and actions
- Connectors to populate e-Forms fields or import/export data during process execution
- If needed, an agent can monitor logs so as to trigger automatic audit processes, for example.

Workforce security

This standard requires organizations concerned to "implement policies and processes to ensure that all members of its workforce have appropriate access to electronic protected health information..."

This particular standard is one of the biggest challenges of the HIPAA in terms of change management.

IT departments are required to delegate access authorization responsibilities to departmental managers without compromising security.

Process examples:

- Authorization and/or supervision
- Workforce clearance processes
- Termination processes

By using workflow software to manage these processes, the costs involved in managing numerous requests every month can be dramatically reduced, while HIPAA traceability and audit requirements are fully complied with.

Workflow software's integration features allows data to be automatically imported from, or exported to your HIS, HR system or directory.

Information access management

This standard requires organizations concerned to "implement policies and processes for authorizing access to electronic health information..."

The following processes can be automated with Workflow:

- Access authorization
- Setting up & modifying access privileges

Security incident processes

This standard requires organizations concerned to "implement policies and processes to address security incidents."

Because implementing this standard is required for HIPAA compliance, health-care organizations must have an effective solution to manage security incidents.

Workflow offers a fast and simple way of managing incident forms and associated workflows such as "response and reporting" processes.

BASEL 2

Published in 2004, the Basel 2 regulation is aimed at European financial institutions and involves implementing a business (credit, markets) and operational risk management system. Compliance involves a whole series of processes.

Workflow offers a fast and simple way of implementing these processes in full compliance with the regulation.

Incident management

This initially involves implementing procedures to collate incidents and providing a permanent log thereof.

Workflow provides an automated procedure facility with logging of requests and actions performed.

Other operations, such as importing or exporting data, can then be performed with the financial institution's other document or data bases and IS applications.

Risk management

Basel 2 also defines procedures for identifying and managing risks. In addition to automating procedures workflow means workflow data can be used with business intelligence software to generate reports and risk monitoring reports.

By optimizing and automating the procedures, workflow reduces the extra work associated with analyzing and monitoring risks generated by the financial institution's business units.

COBIT

COBIT is a standard managed by the IT Governance Institute (ITGI) defining a framework for the implementation of IT Governance.

COBIT defines both operational and control processes for IT departments. COBIT includes nearly 34 controls in four principal fields:

- Planning and Organizing
- Acquisition and Implementation
- Delivery and Support
- Monitoring

Hundreds of corresponding processes must be deployed to implement the various COBIT controls.

Planning and organizing

Who decided what, when and for whom?

Good IT governance relies on a clear definition of responsibilities and the traceability of decisions. Within the COBIT framework the processes to be implemented are particularly strategic. Workflow means the decision-making process can be modeled and implemented with a complete audit trail of actions and decisions taken.

Here are some examples of processes automated by workflow:

- IS strategic planning approval

- Investment management
- Compliance management
- Risk analysis and management
- Quality management
- Human resource management

Acquisition and Implementation

The analysis and implementation of a new IT solution is becoming an increasingly complex process for both purchasing approval and change management.

The large number of projects and people involved makes paper-based or email-based process management almost impossible. Workflow automates these processes and provides genuine productivity gains while integrating the increasingly heavy burden of compliance.

Here are some examples of processes automated by workflow:

- Solution analysis & approval
- Software acquisition and maintenance management
- IT procedure management
- System installation and accreditation management
- Change management

Delivery and support

This is one of the key issues in the new compliance standard, because it incorporates IS security management.

The IT department is required to delegate IT authorization management to the business units (e.g. a complete audit trail of access requests, personnel entry/exit needs to be implemented).

Workflow provides for effective management of these various processes by automating manual tasks that can be sources of errors and productivity losses.

Here are some examples of processes automated by workflow:

- SLA management
- Supplier management
- Performance management
- Authorization management
- Cost management
- Configuration management
- Problem and incident management
- Operation management

Monitoring

Monitoring within compliance projects is very time and resource consuming. Human-based monitoring is not practical because of the volume of data to analyze and the number of processes involved. Workflow software enables the automation of several monitoring processes and control and corrective action tracking.

Connection with the information system means the IT department can issue automatic alerts based on user-defined criteria.

Here are some examples of processes automated by workflow:

- Internal and independent audit management
- Corrective action management

IT INFRASTRUCTURE LIBRARY (ITIL)

The ITIL standard offers guidelines for IT department's governance that are being increasingly implemented by public and private organizations

Based on best practice, this process library comprises eight books:

- Software Asset management
- Service Support
- Service Delivery
- Security management
- Application management
- Infrastructure management
- Business outlook
- Management service implementation schedule

Several processes in each book have to be implemented. Workflow enables a quick and efficient automation of the ITIL processes, while providing compliance with the regulations of the organization's industry.

Workflow—the ITIL project accelerator

Thanks to fast deployment and powerful features, workflow dramatically reduces the implementation costs of the ITIL processes. The lack of time and resources often holds back ITIL project implementation. Yet ITIL processes do improve a company's agility by offering a better IT service to internal users, and provide a further step towards IT system governance and compliance with industry regulations.

Workflow provides a quick ROI while ensuring compliance with the regulations through the traceability and logging of actions and decisions. Workflow also integrates ITIL processes with existing applications (ERPs, databases, directories, etc).

Here are some examples of ITIL processes which can be incorporated into the workflow portal:

- Support management (Helpdesk)
- Incident management
- Configuration management
- Change management
- Update management
- Problem management
- SLA management
- Availability management
- Capacity management
- Service continuity management

ISO 17799

The ISO 17799 standard is a good example of today's laws and regulations on IS security and implementation is an excellent way of preparing for the compliance project.

ISO 17799 includes the following sets of standards:

- Risk appraisal & management
- Security Policy
- Information security organization
- Asset management
- Personnel Security
- Communications and Operations Management
- Access Control

- IS Acquisition, Development & Maintenance
- Information security related incident management
- Business Continuity Management
- Compliance

In addition to the technical actions, a large number of processes must be implemented. Using workflow facilitates ISO 17799 certification by automating the processes with the required level of audit trails.

Examples of ISO 17799 processes

ISO 17799 provides guidelines to implement IS security management in an enterprise, including risk management, definition of security policy, system access control, incident management and audit management.

Here are some examples of processes automated by the workflow portal:

- Analysis and risk management
- Definition of security policy

Personnel security:

- Definition of roles and responsibilities
- Clearance process at point of recruitment
- New employee
- Employee status change
- Employee termination
- Sanction management

Incident management:

- Incident report
- Analysis and management of an incident
- Corrective action management

PROJECT MANAGEMENT

In today's environment project management becomes a key activity for the enterprises. A product launch, the deployment of a new information system or aligning business activities with the market's demands are examples of complex projects that often have to be resolved simultaneously.

Project management is now standardized and structured in several processes ensuring a greater quality and traceability of operations. Compliance with new legislation also requires a greater rigor in project management. Automating processes via workflow is now a prerequisite to delivering projects on time and in line with the company's governance policy. Backers, project managers, project teams, task managers, clients, partners and vendors all play a role in project management workflows.

Defining the project

Good project definition and approval are the keys to successful corporate projects, and an increasing number of players are involved in this initial phase. The traceability of decisions and the use of check lists are examples of features offered by workflow for the automation of project management processes

Here are some examples of processes that can be automated by workflow:

- Project submission
- Project charter approval
- Statement of work approval
- Responsibility matrix approval
- Communication plan approval

Project scheduling

At this stage of the project the traceability of the decisions is critical especially regarding the risk management. Workflow provides a complete audit trail of the decisions made and can syndicate the risks identified in a knowledge base.

Here are some examples of processes that can be automated by workflow:

- Risk analysis and management
- Work Breakdown Structure (WBS) approval
- Schedule approval

Controlling the project

Project management now fully encompasses change management. Competition or new technologies can directly impact ongoing projects. Workflow enables the automation and improvement of change management and problem resolution, and decisions can be logged and stored in knowledge bases for later use.

Here are some examples:

- Problem analysis & management
- Task assignment
- Project status approval
- Change management
- Configuration management
- Closure report approval

Integration with the legacy IS

Automated project management processes can be seamlessly integrated with legacy databases, content bases or third-party project management applications. Project management process automation enables a quick and efficient automation of the project management processes while providing the compliance with the regulations of your organization's industry and significant productivity gains.

CONCLUSION

The new regulations on compliance and governance have forced businesses to speed up the changes in working methods and move to a more process-oriented organizational system.

As such, a huge quantity of messages currently sent via email are set to be turned into a workflow, structuring the continuity of actions and defining roles while providing full accountability and control.

The workflow portal will play a central role in any business's virtual office.

Workflow project management becomes particularly strategic where compliance and governance are concerned and there are many instances today where senior management and IT departments are involved in this type of project. The difficulty resides in the complexity of solutions based on separate business units (compliance with standard appraisal), organizational elements (change management modeling) and technical issues (implementation & integration with the legacy IS).

We have seen that workflow is the driving force behind these new projects and a tool which, once mastered, can generate a new source of added value for any company.