



Compliance along with Transformation Effectiveness and Efficiency

Global Presence

North America

Atlanta, Bellevue, Bentonville, Bridgewater, Charlotte, Detroit, Fremont, Hartford, Houston, Lake Forest, Lisle, Monterrey, New York, Phoenix, Plano, Quincy, Reston, Toronto

Europe

Amsterdam, Brno, Brussels, Copenhagen, Dublin, Frankfurt, Geneva, Helsinki, Lodz, London, Milano, Oslo, Paris, Stockholm, Stuttgart, Utrecht, Zurich

Asia Pacific

Bangkok, Beijing, Brisbane, Dubai, Hangzhou, Hong Kong, Manila, Mauritius, Melbourne, Perth, Shanghai, Sharjah, Sydney, Tokyo

India

Bangalore, Bhubaneswar, Chandigarh, Chennai, Gurgaon, Hyderabad, Jaipur, Mangalore, Mumbai, Mysore, New Delhi, Pune, Thiruvananthapuram

For more information, contact askus@infosys.com

About Infosys

Infosys Technologies Ltd. (NASDAQ: INFY) defines, designs and delivers IT-enabled business solutions that help Global 2000 companies win in a flat world. These solutions focus on providing strategic differentiation and operational superiority to clients. Infosys creates these solutions for its clients by leveraging its domain and business expertise along with a complete range of services.

With Infosys, clients are assured of a transparent business partner, world-class processes, speed of execution and the power to stretch their IT budget by leveraging the Global Delivery Model that Infosys pioneered.

Infosys[®]
POWERED BY INTELLECT
DRIVEN BY VALUES

www.infosys.com

Executive Summary

Compliance is an expensive, inevitable and ongoing activity which many companies find hard to cope with. Though SOX has evolved over a period of time and has brought in more clarity to controls documentation and assessment, the corporate world is still groping with the fact that compliance is an expensive activity.

Vladimir Lenin, leader of the Russian Revolution, said: **"Trust is good, but control is better."** But stake holders across the globe are wondering if **"Control is good but trust is better"**. We trust that our employees are executing the control activity as intended. We trust that our auditors are doing a good job of verifying the controls. We trust that the management is keeping a close watch on the day to day activities and will arrest any diversion soon. Trust is inevitable as long as at least a part of the control is executed by human beings. Total automation of controls is a myth and can not yield the results in addition to being disproportionately expensive as compared to the risk that the control is mitigating.

Hence the question arises as to what approach should be adopted by the companies to satisfy their compliance needs? What should be the vision for achieving satisfactory compliance? An organization should have a vision to make its compliance process reliable, effective, holistic, integrated and less expensive as non compliance is not an option. Infosys's "Efficient Compliance"

offering with right mix of people, process and technology helps organizations in achieving their compliance vision. Efficient compliance approach is embedded in large transformation programs and provides a golden opportunity to streamline compliance process for

- Significant savings in cost
- Better visibility and controls
- Quick scale up and extensibility across business units and geographies

Infosys's proactive offering looks beyond the transformation programs and focus on providing steady state compliance assistance to our customers with a declining cost of compliance. A central compliance monitoring cell (CCMC) with alignment of people, process and technology is the answer to company's quest for cost effective, efficient and scalable compliance.

People Right kind of profiles with audit and compliance background, business process understanding and knowledge of SAP

Process Standard compliance operating process and procedures with clear definition for rejection or acceptance

Technology A good technological enabler with features to automate controls, monitor controls and manage compliance program

What are the questions that a compliance steering committee should be asking before embarking on a large transformation project?

- Do we have a vision for compliance?
 - What do we want to achieve from adopting compliance?
 - > Cost reduction
 - > Efficiency along with effectiveness
 - > Better visibility
 - > Real time reporting of control issues
 - Is there an approach to standardize processes and controls across different countries (80:20 / 70:30 / 60:40)? How flexible or easy is it for the companies to adopt a local process or controls?
 - Is there clarity on the controls owned, defined and executed by the global compliance team and the local compliance team?
 - Are we involving the local countries in the controls definition?
- Do we have clear ownership for compliance of IT enabled controls? Is business responsible or is IT responsible for the same?
 - > Is there a RACI chart for compliance based on nature of controls? Responsibility for
 - Control definition
 - Ownership
 - Execution
 - Monitoring
 - Is there close handshake between the implementation team and compliance team?
 - Have we conducted compliance awareness sessions for our business functional consultants? Do they have a compliance mindset?
 - Are there too many people participating in compliance decision making process?
 - Has the approach for steady state compliance or ongoing compliance monitoring been defined?
 - What all regulations does the company need to comply with (country wise)?

Causes for failure of compliance track during large implementation/transformation

- Delayed start for compliance
- Compliance track not keeping pace with implementation track
- Lack of clear ownership in compliance
- Not having a dedicated compliance manager to take quick decisions and move ahead with a holistic view
- 10 heads for taking decisions on 11 opinions
- Lack of integrated and risk based approach for compliance
- Not using right tool for compliance
- Compliance track in "RED" due to criticality and visibility thereby sending the top management in to panic mode

Are these problems unique to any one company?

"NO"

Is there any one solution to overcome the challenges faced by all companies?

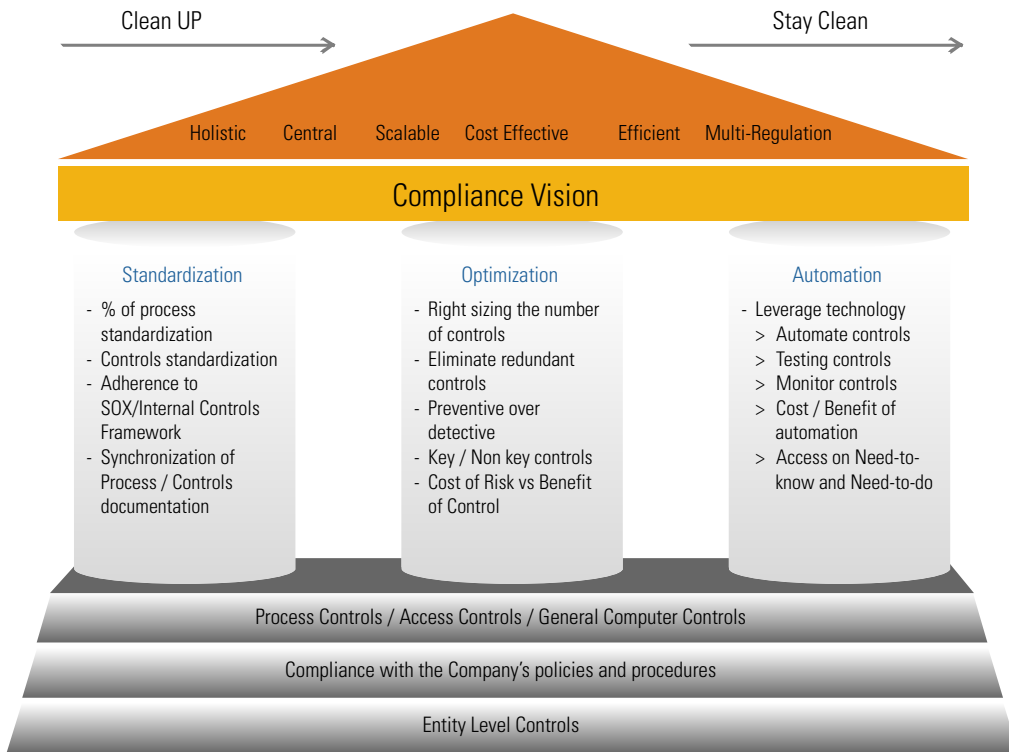
"NO", there is no one solution but there is one good approach that can be adopted by all companies to overcome the challenges faced in compliance track"

Types of Controls	70:30	Definition	Owner	Executioner	Monitor
Configurable controls	70% - Global	Global	Global	Global	Global
	30% - Local	Global & Local	Local	Global	Global
Procedural controls	70% - Global	Global & Local	Global	Local	Global & Local
	30% - Local	Local	Local	Local	Global & Local
Access controls	70% - Global	Global	Global	Global	Global
	30% - Local	Global	Local	Global	Global

Common Mistakes

- Attempting 100% standardization which is a ideal scenario and may not work in most of the situation
- Attempting standardization without considering the nature of controls
- Not utilizing the existing applications to automate the controls to the extent possible which will not enable remote accessing or testing of controls
- Not choosing appropriate enabler for efficient compliance – too many or stand alone compliance automation applications may not provide the required efficiency as compared to integrated compliance management software
- Not offshoring the controls management to specialized group of consultants – cost of consulting may not come down as expected
- Inappropriate centralization or decentralization of controls monitoring (geography / nature of controls)

What is a typical compliance vision of an organization?



The first step to be taken in the compliance track for any implementation/transformation project is to set the vision. Typical compliance vision of an organization is to achieve holistic, central, scalable, cost effective and efficient compliance. This vision stands on the pillar of standardization, optimization and automation. The Compliance Vision as depicted in the above picture describes the objective of compliance unit in a company.

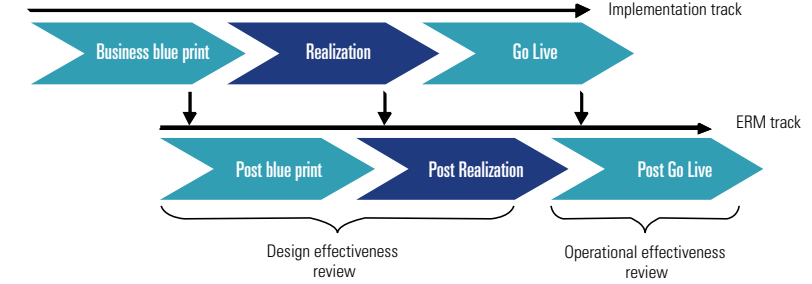
The vision should be designed to convert the challenges faced by the company during transformation into opportunity to

- Increase process efficiency and control effectiveness
- Reduction in cost of compliance in the long run
- Increase share holders confidence

- Increase brand value/market image thereby help in becoming market leader
- Be prepared to take up the upcoming/new challenges

Large Transformation program is an opportunity for you to clean up and stay clean

Compliance during SAP implementation/transformation



<ul style="list-style-type: none"> > Understand processes from blueprint > Review existing SOX documentation including global templates > Realigning existing controls to new processes ensuring control adequacy > Validation from all stakeholders > Recommendations incorporated in design document 	<ul style="list-style-type: none"> > Reviewing test plans for application controls > Review the master configuration in new system > Review the role profile matrix > Identifying Key and compensating controls and recommendation for control optimization and automation 	<ul style="list-style-type: none"> > Review of General IT controls surrounding the new application > Documenting Evidence of controls tested > Conclude on operational effectiveness
--	--	--



How can organizations realize their vision for compliance during large transformation programs?

Infosys offers compliance track as an integrated service offering along with SAP implementation to ensure proactive compliance. Infosys approach to ensure compliance during SAP implementation or functional upgrade gives enterprise not only an opportunity for a detailed review and realignment of its internal controls along with improved or changed business processes, keeping industry best practices in consideration, but also reduce its year on year cost of compliance by bringing in optimization and automation of controls.

Figure above depicts a three phased approach to Efficient Compliance during SAP implementation and beyond. The three phases post blueprint, post realization and post Go-live period. The activities performed in each part have been explained in detail below.

Post blueprint is a phase when To-be business blueprint documents are reviewed to analyze process as well as controls standardization, optimization and automation. This is the most critical activity as this phase lays foundation for efficient compliance.

Output of this phase is the final list of redesigned controls which are approved by the key stakeholders. This effort is usually coordinated by the Unit Compliance Managers who will be required to ensure that there is no resistance to critical controls and at the same time business requirements are not compromised.

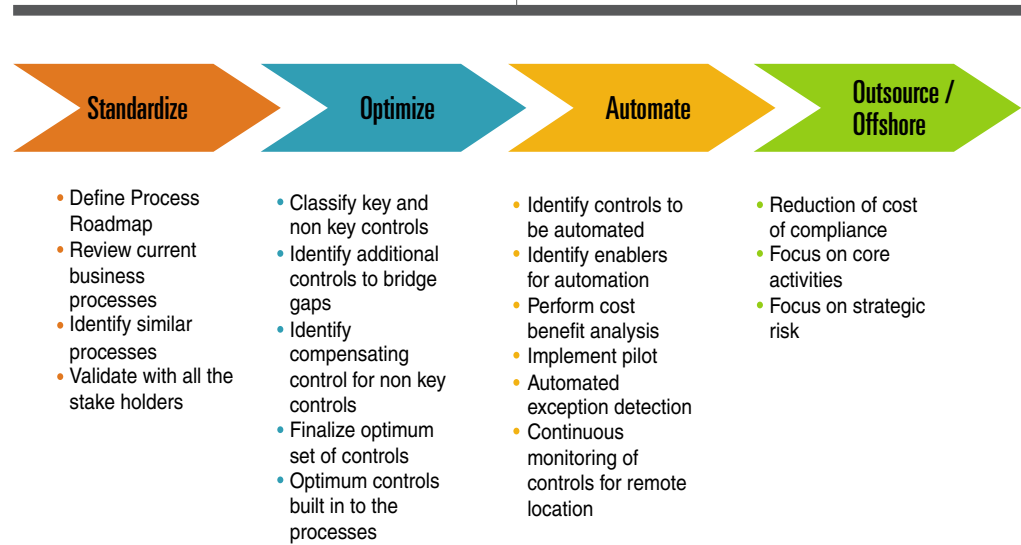
Finalized list of controls are then validated with the external auditors and this is the most critical piece of work because once the controls are finalized and approved by external auditors, the same will be rolled out to the respective units. There will not be any scope for change post this stage. Any further change post this approval will prove to be a costly affair.

Post Realization is the phase when a basic structure of controls in various processes is ready to be configured in the golden client. Based on the inputs in the final business blue print document, configurations are made in the development system by the implementation team. Parallel to configuration, enhancements are done for any control that can not be configured in SAP. Once the configuration in development system is complete, unit testing of the same will be done by the implementation team.

It is advisable that automated (e.g. 3-way match, in SAP) and IT dependent (e.g. controls on reports) SOX controls are also tested at the same time and in the same unit test scripts with different sets of evidences as the objective of testing will be different. These evidences are tracked separately and book marked with specific reference to business blue print document, process number, activity number, unit test plan or SOX documentation of the company. This would enable easy trace back of any controls documentation.

with the stakeholders including process owners and internal compliance officers.

Standardization of process assumes more importance in the blueprint phase of SAP implementation / upgrade. This ensures that processes are standardized from the beginning rather than rationalizing it after they been in operation.



The 4 pillars of efficient compliance for process controls

Standardization of controls begins with the standardization of processes. Processes for standardizing are selected based on certain criteria as it is not advisable to attempt 100% standardization in the first year, which may never be achieved owing to complexity of organization or multi country operation or local legal requirements. (E.g.- unit wise / process wise / location wise. E.g. – Finance and HR process will be standardized in the first year).

As a first step a Compliance consultant, needs to review the existing process documents. He would then identify similar processes in different entities or geographies. The next important part is to come up with a standard process after rationalizing the process and controls. This needs to be validated

Standardization of process results in multiple benefits:

- Reduced efforts - Standardized process leads to reduced efforts in documentation and testing of controls.
- Easier maintenance - Changes to the processes need not be made to all the documents. Similarly test plans may be altered once, instead of at multiple places

Standardization of controls leads to **optimization** since linking control activity to standard control objectives helps in identifying overlapping controls and reducing the number of controls. Identification of key controls is the key to optimization.

The objective of optimization of control is to have just the right number of controls to ensure process effectiveness and enable compliance. Since regulations are silent about the number and nature of controls, internal compliance team along with steering committee decide on the optimum controls. Optimum number of control is a relative term and each company has to do a cost benefit analysis of controls in the process. More number of controls does not mean more security.

Major task in optimization involves classifying the controls as key/non-key and redundant controls. A key control can have following characteristics:

- a control that mitigates more than one risk; or
- a control that is of paramount importance in a process; failure of that control would render the whole process ineffective.

Benefits from Control optimization

1. Increase process efficiencies

More controls in a process take more time to complete a task. By weeding out redundant controls, process would more efficient.

2. Focus on Key controls

Auditors can focus more on key controls where the impact of failure is high

3. Reduced number of controls

This leads to reduced effort for implementing and testing controls and thereby reducing cost of controls.

Case Study

Minimizing Residual financial risk Large Systems and Network Security Solutions Company in US

The major challenges in this assignment were revenue accounting and compliance to SOP 97-2 with several manual reviews and back end excel based adjustments. Infosys's solution minimized its financial reporting risk by standardizing, optimizing and automating its controls. Some of the highlights are:

- Vendor specific objective evidence analysis and compliance for Enterprise Business (35% of total business) ensuring significantly greater compliance to SOP 97-2,
- Automated or eliminated 80% of manual steps involved. The dollar value of month-end manual accounting entries reduced by 96%
- Worldwide consolidation closed and ready for reporting within 9-12 working days from close of business.
- Actionable Decision Support Information based on SAP BW with near real-time reporting capability across multiple dimensions

After classifying controls as key or non-key, the compliance consultant would identify redundant controls. Redundant controls are eliminated from the process in such a way that the process efficiency is improved and security is not compromised. Redundant controls can be addressed by key controls or other controls in a process. Classifying controls as key or non-key helps in prioritizing the testing. Key controls can be tested more frequently than other controls.

Once controls are standardized and optimized, an attempt should be made to **automate** them to the extent possible. A right balance of Automated Vs Manual and Preventive Vs Detective should be achieved by choosing right set of controls based on company's environment. In case of high risk areas, both preventive and detective controls can be used e.g. an error log in system and a warning message for same is an automated preventive control in itself. However, in case of critical applications like uploading exchange rates, a monthly or quarterly review by superior of person responsible for uploading can be a detective manual control.

Decision to automate the control would be decided based on the criticality of the risk that the control will mitigate and the cost of automation. Cost of enhancement should be considered for controls that can not be directly configured in the system. Only such controls should be automated who's benefit will out weight the cost of automation.

Cost of an automated control is sum of cost of implementation and cost of maintenance for 'x' number of years. Initially, cost of automation would invariably be high due to high implementation cost. However, over a period of time, cost of automated control would come down.

As for the manual controls, the cost could vary depending on various factors such as knowledge transfer, increase in sample size due to an exception etc. In most of the automated control, the auditor or tester needs to select only one sample as compared to 20-25 in case of manual controls. And in case of an exception, the number of manual controls could be doubled based on testing methodology followed by the auditor.

Benefits of automation include:

1. Reduction in cost of compliance

As mentioned above, in the long run benefits of automation out weigh the costs

2. Better compliance management

Compliance tools like SAP GRC help in managing compliance program effectively. Companies can move from spreadsheet based documentation to system based.

3. Enables preventive control

Preventive controls are better than detective controls.

SAP has various in built controls that can be configured without developing or implementing any add-ons. Compliance consultant can help companies to use as many configurable controls as possible (Example: Purchase order value-wise authorization).

Automation of controls evaluation or testing enables remote testing / monitoring of controls and SAP GRC is a good tool meet that requirement. Compliance program management in addition to automating the controls, eliminates the problems of version management, duplication of efforts and reporting issues.

How do we identify key controls?

Risk based approach should be followed involving re-scoping and re-assessing on controls that are key controls. For this, a process of mapping controls to control objectives and financial statement assertions related to significant financial statement accounts should be followed. A key control is a control which is indispensable to meet the control objective.

Preventive controls are considered more strong and easier to test than detective controls, however certain situations may allow for reliance on good detective controls, for example, in case of reconciliations.

Efficient compliance approach to design effective access controls

In addition to ensuring the design effectiveness of business process controls, it is very important to ensure that users are granted access to the SAP system on "need to know and need to do basis only". Such an approach ensures that users get access to the system depending on the role played by them in the organization. This can be achieved by building and implementing effective access control mechanism during implementation and beyond. Security design approach adopted by the organization should facilitate the following:

1. Meet the business needs

2. Satisfy the audit and compliance needs
3. Ensure efficiency of future maintenance

It is important to ensure appropriate access is granted at the beginning as otherwise insufficient / extra access given to the system may be misused. If more access is granted to the users in order to make them accept the new system as fast as possible without hampering their daily work, withdrawing the same at a later stage would amount to a huge problem. This is so because users tend to associate more access in the system to having more power in the organization.

Access Security design approach for a large transformation project should include assessment and design of

- Global roles – for activities that will be performed by users in all countries
- Country specific roles – for activities that will be required for users in specific countries and
- User specific roles – for activities that will be performed by a user only

This way, a user can at any point of time have a minimum of one role and maximum of three roles. (Example: Purchase Manager XYZ in US will have PM Global role + PM US role + xyz role)

Before assigning any of the above mentioned roles, they should be analyzed for:

- SOD violation at inter and intra role level
- Access to critical transactions and
- Access to critical authorization objects with values

In instances where SOD violations risks can not be completely mitigated, appropriate mitigating controls will have to be designed.

Mitigating Controls – Best Practices

- Mitigating controls should be ideally designed at the user level after the role level conflicts are resolved
- Mitigating controls should be defined only for very few high risks as they are cost intensive in designing, executing and monitoring
- Mitigating controls should be designed along with the group SOX team to ascertain the sufficiency of controls

Off-shoring of ongoing compliance monitoring

Self Assessment Questions

1. How much time are we spending on compliance initiative?
2. What is the percentage of spend on compliance as compared to total IT spend?
3. How do you rate our self on a scale of 1 to 5 (1 being the best) in terms of efficient compliance?

General Computer Controls

Efficient compliance approach defines the general computer controls that need to be followed during the project phase such as

- Data migration
- System Development Life Cycle

General Computer controls defined for the steady state compliance ensure that changes to IT systems and security around IT systems are sufficiently covered:

- Change management
- Data centre and physical access controls

"Entirely automated application controls are generally not subject to breakdowns due to human failure" Auditing Standard 5 of PCAOB. PCAOB allows the auditors to adopt bench marking strategy for the evaluation of automated controls if the change management controls are operating effectively.

Continuous monitoring of controls:

Once the production system stabilises, unit compliance team should move the control monitoring to a remote location in order to reap the benefits of efficient compliance. Since most of the controls would be automated, access to these systems / controls from remote locations would not be difficult. A compliance team would classify the controls as automated / manual and prepare assessment project plan for periodic testing. Periodic testing plan may include details such as processes to be tested, controls to be tested, prioritisation of controls etc. A small team of consultants would visit the respective locations to assess the operational effectiveness of manual controls periodically and automated controls can be monitored continuously by either a dedicated compliance team or a compliance team working on shared service model.

Infosys has developed a governance framework for ensuring steady state compliance. The framework can be tailored to suit the needs of the customers. This framework can serve as the basis for ongoing compliance monitoring in the steady state through a central compliance monitoring cell. Such a cell would address the compliance requirements on proactive, detective and corrective basis.

In a transformation program, as and when any country goes live, it can be added to the fold of CCMC steady state compliance track. Shadow support for compliance (for both access and process controls) will be provided during the hyper care / intensive care period. Central compliance team acts as a goal keeper for all compliance related issues and will be the single decision making body for deciding all compliance related matters.

In summary

Achieving compliance in large SAP transformation projects is a challenge that all companies will have to live with. Central Compliance Monitoring Cell (CCMC) with right set of people, process and technology will help the company in achieving a cost effective compliance not only during implementation but also in Steady phase. Having a centralized CCMC offers many advantages rather than having many regional teams and helps in reducing the cost of compliance during implementation and ongoing compliance.

