Centralized operations
The future of operating models for Risk, Control and Compliance functions
Contents

Introduction
  What is the future of operating models for Risk, Control and Compliance functions? ........................................ 1

Centralized operating models ........................................ 2

The benefits case .............................................................. 4

The options in new operating models .............................. 7

Transforming your Risk, Controls and Compliance functions ............................................................................. 10

Conclusion
  Don’t underestimate the value of centralized operating models ................................................................. 15
Introduction

What is the future of operating models for Risk, Control and Compliance functions?

In these times of continued global economic uncertainty, cost reduction and effective risk management remain key imperatives. Organizations are required to manage a multitude of challenges. For example:

- Slow growth in mature markets
- Challenges in realizing the full growth potential in emerging markets and managing the risk of operating in these markets
- Commodity price volatility
- The opportunities and threats of new technology and the digital age
- The ever-changing and increasing burden of regulatory compliance

Not surprisingly, back-office functions such as HR, Finance and IT have been required to respond to this cost reduction agenda to ensure they deliver maximum value at minimum cost. One now-standard response has been the use of new, more centralized operating models in the shape of shared services, offshoring (to areas such as India, Eastern Europe and South America), and co-sourcing with and outsourcing to third-party providers.

The need to centralize and reduce the cost of back-office processes and transactions is the standard expectation across businesses today. Historically, Risk, Control and Compliance functions have been less willing to embrace these new, more centralized operating models. Not wanting to disrupt risk, controls and compliance activities and expose an organization to financial loss, compliance failure or reputational damage is the most common reason stated.

However, this is changing. Leading organizations are challenging the status quo of their risk, control and compliance operating models; they are looking at ways in which they too can contribute to cost reduction while enhancing risk management, controls and compliance practices. Transferring activities into a more centralized model through the use of shared services, offshore, co-sourced and outsourced capabilities has been identified as a key enabler to achieve this.

This paper discusses why this is the case; what risk, control and compliance capabilities are being shifted into new centralized operating models (and which are not); and the challenges in making this transition. Specifically, it covers:

- Why organizations are changing their risk, control and compliance operating models, and the nature and scale of benefits to be realized
- What the options are in moving to centralized operating models and what are some of the key decision criteria influencing what to shift (and where) and what to retain within “business as usual”
- How organizations are going about making and embedding these changes and the typical pitfalls to be avoided
Centralized operating models

Different shared service operating models bring different risks and benefits to your organization.

Businesses began to use shared service centers (SSCs) and outsourcing to improve back-office efficiency more than two decades ago. The intention was to move routine, transactional work to specialists who were dedicated to processing it more efficiently and at lower cost. This left the business free to be more agile and focus on its customers. SSCs were the in-house solution, while outsourcing firms provided an external option.

The models used for this vary enormously — by degree of integration, by geographical location, by single versus multiple SSCs, by captive provider versus outsourcing (or a mix of the two), and by governance arrangements — but all share the same core drivers. Cost savings remains a key objective, but now these objectives have extended to include benefits such as, process efficiencies, standardization, additional value, career opportunities for employees; talent sharing across traditional boundaries; innovation and the integration of mergers and acquisitions (M&A) — all resulting in the better use of time and resources for the retained business.

Different centralized operating models exist. A summary of the principal options is given to the right, distinguishing between key decisions on (1) organizational structure to be put in place and (2) where the resources and capability will come from to support the new operating model.
Insights on governance, risk and compliance — Centralized operations

**Offshore**
- Transfer of activities from operating units to a new centralized location
- Location of offshore center independent of operating units — can cover multiple geographies and time zones
- Service-level agreements remain
- Can operate alongside regional shared services

**Hub and spoke**
- Transfer of low-risk and documentation-intensive activities to new centralized location(s)
- Location of offshore center independent of operating units — can cover multiple geographies and time zones
- High-risk activities and those requiring personal interaction

---

**Co-source**
- Third-party providers appointed to support the organization in the undertaking of shared services/offshore center/hub and spoke activities
- Nature of relationship is one of support and joint working
- Responsibility for activities remains with the organization
- SLAs in place between operating units and third party

**Outsource**
- Third-party providers appointed to undertake activities within shared services/offshore center/hub and spoke model
- Responsibility wholly transferred to the third party
- SLAs in place between operating units and third party

---

“The how” — organizational models

“The who” — providers of capability
The benefits case

The core value of moving to a common and optimized set of risk, control and compliance activities can be defined across five key characteristics:

1. Cost to serve
   Minimizing the time and resources devoted to risk, controlling and compliance activities to reduce back-office costs and maximizing those devoted to front-office and market-facing activities.

2. Risk management and compliance
   The effective management of risks and compliance needs (risks and compliance needs understood, controls in place, risks and compliance monitored) – as defined within an agreed risk appetite.

3. Scalability
   The ability to integrate acquisitions and manage divestments swiftly and cost-effectively through the rapid deployment of a common risk, controls and compliance framework with monitoring capabilities.

4. Agility
   The ability to flex risk and controlling activities and tolerances set as the inherent risks faced by organizational change. This would take into account new risks, as well as the changing profile of existing/known risks.

5. Transparency
   Provision of management information related to risk, controls and compliance that enables decision making through clarity of risk gaps to be addressed, and controls and compliance breaches that require remediation.

Example cost reduction case studies

- A global consumer products organization achieved €30m in savings annually on a total cost of financial control of €100m, which included centralizing and moving controls monitoring to an offshore center.
- The business case for a global software company was based on a 35% cost reduction target for the outsourcing of financial controls and compliance testing.
- A US$30b diversified financial services company saved nearly US$3.5m per annum by moving its 25-member SOX testing team offshore to India.
- A global bank has set up a 40-member control environment center of excellence to remotely test operational and financial controls across the US and Europe, with a savings of US$8 to US$10 million.
- A US healthcare company is setting up a business control testing hub to remotely test all internal control over financial reporting, with a supporting business case of saving US$1.5 to US$2 million.

Cost to serve

When a business is considering the move to a new centralized operating model, the most significant driver is usually one of cost reduction. In EY’s experience, moving risk, control and compliance functions into a centralized operating model (be this shared services, offshoring, co-sourcing or outsourcing arrangements) can typically yield cost savings of 30% to 50%.

Shared service savings are realized through the centralization, standardization, simplification and automation of activities, processes, controls and functions – and associated productivity increases. Offshoring to locations like India, South America and Eastern Europe provides the additional benefits of wage arbitrage. Co-sourcing and outsourcing can also bring cost benefits through, for example, removing the need to manage resourcing peaks and troughs in controls and SOX testing during the financial year.

Cost reduction is, however, not the only source of value to be realized in the move to a new more centralized operating model; it can also bring about benefits in risk management and compliance, scalability, agility and transparency.

Risk management and compliance

To achieve the centralization of risk, control and compliance activities requires a common and clearly articulated set of risks and regulatory requirements for those processes and activities within scope of the new operating model. Without this, it may not be possible to assess if the activities being centralized are appropriate to manage the risks or compliant with the relevant regulations.
As a consequence, a more centralized operating model helps to ensure:

- **Strategic, operational, financial or regulatory risks that need to be managed are formalized, documented and understood.** This will also require clarity and documentation of risk appetite (the extent the organization is prepared to accept the possibility that risks will materialize and regulations will not be met).

- **The need to define the ultimate risk owners.** A centralized operating model drives the need to define who the ultimate risk owners are and to whom the operating center is accountable to.

- **The activities of the operating center manage these risks and compliance needs.** Although this may appear a basic requirement, over time many organizations lose sight of the link between their key risks and compliance needs, and the associated controlling and monitoring activities. The move to new centralized and integrated operating models can provide a timely and valuable review on the alignment or mapping between risk, compliance and assurance activities.

- **Changes in compliance requirements and responses can be handled centrally and globally.**

## Scalability

The centralization of risk, control and compliance activities has the inherent ability to better absorb changes in the organization; for example, acquisitions, mergers or divestments. When working with a centralized capability (be this monitoring, testing or reporting on risk, controls and compliance needs), an organization is able to extend and contract its scale and scope of services for new entities or units swiftly and without a significant increase in associated costs.

## Agility

With the support of governance, risk and compliance (GRC) enabling technology, tolerances for what is deemed to be a risk, control or compliance pass or fail can be flexed and adjusted depending on risk appetite.

The ability to bring about this agility in monitoring of risks, controls and compliance needs is enhanced through more centralized operating models; for example:

- The move to a new centralized operating model typically rationalizes, automates and standardizes processes, controls, data and tools so that any subsequent changes in these processes can be implemented and rolled out more effectively and efficiently.

- Training and awareness of the change (its need and impact) can be focused on this more centralized team — as well as those people impacted in the business.

- Assuming technology has been standardized, changes can be implemented once — in contrast to having to amend and upgrade a variety of systems and platforms by business unit or country.

## Transparency

Shared service operating models are invariably underpinned by service-level agreements (SLAs), which will include reference to reporting standards and frequency. As a result, they will deliver more formalized and standardized reporting on risk, control and compliance and identify any activities in need of remediation. With the use of GRC technology, this reporting can be delivered weekly, monthly or quarterly — making the vision of “continuous controls monitoring” a reality. Visibility can be given to diverse risks across disparate emerging and mature markets with speed and integrity embedded.

The Banking, Financial Services and Insurance (BFSI) sector leads the way

The BFSI sector began offshoring of IT-BPO (business process outsourcing) services to low-cost geographies across Asia, Eastern Europe and Latin America in early 2000. Over the last decade nearly all BFSI players have set up SSCs and also leveraged third-party IT-BPO firms based in the above-mentioned geographies for handling their customer relationship management, finance, procurement and other business support services. Key BFSI players such as Bank of America, Citibank, Barclays, HSBC, JP Morgan and American Express have nearly 250k to 300K personnel supporting their global operations from low-cost geographies.

It was therefore natural for the BFSI sector to take the lead in moving operational and financial risk areas (Sarbanes-Oxley, Basel II, Solvency II compliance, etc.) to their offshore locations. The global financial crisis and the wave of new regulations (Dodd-Frank, TARP Basel II, Solvency II, etc.) have accelerated this movement. The high cost of compliance imposed by the above legislation compelled the BFSI sector to reconsider its operating model for financial and operational risk activities, driving greater use of shared services, offshore centers and third parties with critical mass and relevant capabilities in low-cost economies.
Insights on governance, risk and compliance — Centralized operations
The options in new operating models

Establishing the right centralized operating model for risk, control and compliance capabilities starts with defining (a) what are the activities underpinning these capabilities and (b) where within an organization should they reside. The model below provides a summary of these activities and what should be retained within head-office and business functions, and what lends itself to a centralized operating model.

<table>
<thead>
<tr>
<th>Risks</th>
<th>Approach</th>
<th>Risk, controls and compliance coverage</th>
<th>Oversight</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>New product development</td>
<td>Internal controls group</td>
<td>Executive management</td>
</tr>
<tr>
<td></td>
<td>Gain new business</td>
<td></td>
<td>Board</td>
</tr>
<tr>
<td></td>
<td>Procurement</td>
<td>Compliance functions</td>
<td>Audit committee</td>
</tr>
<tr>
<td></td>
<td>Production</td>
<td></td>
<td>Risk committee</td>
</tr>
<tr>
<td></td>
<td>Product delivery</td>
<td>Other risk functions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aftersales support</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**First line of defense: business operations**
- **Key activities**
  - Assesses key risks
  - Defines compliance needs
  - Defines risk owners
  - Defines risk appetite/tolerances
  - Defines common language

**Second line of defense: management assurance**
- **Key activities**
  - Defines controls and compliance activities needed
  - Operates controls and compliance procedures
  - Remedies for control failures/compliance breaches

**Third line of defense: independent assurance**
- **Key activities**
  - Independently assesses controls and compliance procedures
  - Reports on control failures and compliance breaches

**Ownership**
- **Key activities**
  - Assesses key risks
  - Defines compliance needs
  - Defines risk owners
  - Defines risk appetite/tolerances
  - Defines common language

**Low**
- Ownership of defining and assessing risk and compliance requirements should not be delegated
- Operating model can support in provision of reports and data

**Medium**
- Design remains with the business
- Assessment and monitoring of risks, controls and compliance operations can be transferred to centralized operating center
- Plus the provision of reports and data
- however, co-sourcing or outsourcing of internal audit is common

**High**
- Management remains responsible for end-to-end risk, controls and compliance procedures in design and operation
- Centralized operating model can support in provision of reports and data

**Oversight**
- **Key activities**
  - Ultimate accountability for risks, controls and compliance
  - Reviews and approves overall risk and compliance needs
  - Receives risk, controls and compliance reporting

**Low**
- Accountability for risk, control and compliance cannot be delegated
- Operating model can support in the provision of reports and data
In general, it is those processes and activities that are mechanistic in nature and/or repetitive that are most appropriate to be delivered remotely from the business. From a risk, control and compliance perspective this typically represents the activities of monitoring, testing and reporting. If we apply a “lines of defense” model, it lends itself most strongly to the second and third lines of defense across management assurance and independent assurance (i.e., internal audit) activities.

**Risk ownership and oversight**

Ownership and oversight of risks (strategic, operational and financial) and compliance needs are rarely delegated. It would be inappropriate to shift responsibility for these activities into centralized operating model functions because of:

1. The business critical nature of decisions being taken
2. The authority needed to drive changes in risk, control and compliance practices across an organization when required

These activities in the vast majority of cases remain the responsibility of the executive management team, the board, and risk and audit committees.

**Business operations (first line of defense)**

Business units or operations typically define the day-to-day controls and compliance activities needed to manage the above risks and are held accountable for their operation. They are also typically accountable for fixing or remediating control failures or compliance breaches. Again, in EY’s experience, this accountability is rarely delegated outside of the business unit.

**Management assurance (second line of defense) and independent assurance (third line of defense)**

Activities associated with management assurance (the business assuring itself that it is compliant with internal needs and external regulations) and with independent assurance (independent assessment of risk management through internal audit or external audit) lend themselves to centralized operating models. Management assurance has been leading the trend, particularly in sectors such as finance, health care and utilities, which have all been subject to the upheaval of new and stringent regulations.

It is recognized that internal audit, in many cases, adopts a centralized model – given its inherent need to be independent of the business – and the adoption of co-sourcing or outsourcing is relatively common.
The underlying activities associated with the second and third lines of defense have the following characteristics:

- **Repetitive** — they tend to take place on a monthly, quarterly or annual basis (e.g., testing for controls operating effectiveness).
- **Routine** — it is usually possible to define criteria that determine if a risk has been managed or a control operated in line with internal procedures or external compliance regulations.
- **Collaborative** — bringing an organizational or group perspective to these testing and monitoring activities. Good practice from one region or business unit can be shared with others. Trends can be picked up across the organization that may not be apparent when considered locally; for example, stock in transit being identified as an issue across key emerging markets due to loss (accidental and theft) or damage due to poor transport links.

Typical activities that have been moved to new and centralized operating models include:

- **Banking, financial services and insurance**: AML (Anti-Money Laundering), KYC (Know Your Customer), Basel II, Sarbanes-Oxley (SOX), FACTA (Fair and Accurate Credit Transactions Act), Volcker rule, Solvency II; Fair Credit Regulation (FCRA) reporting, and vendor monitoring as required by the Consumer Financial Protection Bureau (CFPB)
- **Health care**: Health Insurance Portability and Accountability Act (HIPAA), HITECH, affordable care, claim integrity, fraud and abuse
- **Telecom**: revenue assurance and controls compliance
- **Technology and software**: channel partner compliance, royalty payments and FCPA compliance across the channel
- **Consumer products**: financial controls compliance (including Sarbanes-Oxley), plus global provision of systems access and reporting of segregation of duty breaches

The power of technology

Technology is a key enabler for realizing and managing new risk, control and compliance operating models. Recent trends in technology supporting this include:

- **Global ERP** — Deployment of global ERP has ensured that underlying processes and data are available centrally and can be accessed remotely from any location. Those reviewing and giving assurance over controls do not need to be on-site to understand the process flow and access/test underlying data.
- **eGRC** — eGRC tools provide a standardized platform and work-flow engine to capture all the activities undertaken by risk, control and compliance teams across the globe. This facilitates offshoring of work by allowing the teams the flexibility to operate from any geography.
- **Analytics** — Companies are moving toward continuous control monitoring, designing algorithms to obtain and test data in real time from ERP. Tools such as SAP Approva help configure algorithms to detect design and operational effectiveness gaps across the process cycle; for example, procurement process algorithms are being used to identify duplicate invoices, invoices without purchase orders, open orders, etc.

The combination of ERP, eGRC and analytics has enabled organizations to move toward location-agnostic risk, control and compliance models.
Transforming your Risk, Controls and Compliance functions

In this section we consider three key aspects of transitioning to a centralized operating model:

1. To “shift and lift” or “lift and shift”?
2. Defining the right operating model for risk, control and compliance
3. Challenges and risks of moving to a new centralized operating model

1. To “shift and lift” or “lift and shift”?

One of the first considerations in transitioning to a centralized operating model is the decision on whether to:

- **“Shift and lift”** – move existing processes, activities, reporting, technologies, etc, as currently performed, and then standardize these within the new operating center over time.
  
- **“Lift and shift”** – in transitioning to the new operating center, the organization standardizes the processes, activities, reporting and technology, so the new ways of working are embedded from day one.

Both models have their advantages and disadvantages (see opposite page). Each transition plan needs to be assessed on its own merits to arrive at the right conclusion. It is noted, however, that our experience indicates that business case realization in the longer term is higher when adopting the “lift and shift” approach.
**“Shift and lift”**

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Speed of transition</strong> – ability to move activities swiftly to a new centralized operating model</td>
<td><strong>Complexity</strong> – the need for the centralized operating center to manage the complexity of the different practices and procedures per operating unit/region</td>
</tr>
<tr>
<td><strong>Benefits case realization</strong> – wage arbitrage cost savings are realized sooner</td>
<td><strong>Productivity</strong> – linked to the above, the benefits case associated with standardization is deferred</td>
</tr>
<tr>
<td><strong>Business acceptance</strong> – by following existing practices and procedures, business acceptance is likely to be greater (in the short term)</td>
<td><strong>Change fatigue</strong> – the business will have to manage two transitions: 1. The switch of activities to new operating center 2. Subsequent standardization of activities in the monitoring, testing and reporting on risks, controls and compliance</td>
</tr>
<tr>
<td><strong>Commitment</strong> – demonstrates early commitment to the new operating model (“we need to and will do this”)</td>
<td></td>
</tr>
</tbody>
</table>

**Advantages Disadvantages**

<table>
<thead>
<tr>
<th>“Lift and shift”</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Productivity</strong> – the new centralized operating model is based on new standardized ways of working from day one. This increases the productivity and benefits case of the new operating center – once it is established (see “Speed of transition”).</td>
<td><strong>Speed of transition</strong> – given the potential scale of change to the business and the centralized operating center (processes, controls, systems, roles and responsibilities) the move will take longer to design and implement when compared to “shift and lift.”</td>
</tr>
<tr>
<td><strong>Business impact</strong> – the business and operating units will experience a single, albeit more fundamental, change. This needs to be managed carefully to ensure success in transition, but it significantly reduces the time spent in managing multiple transitions and frees the business to focus on other initiatives and priorities.</td>
<td><strong>Business acceptance</strong> – the switching of activities to a more remote, centralized location (e.g., reliance on controls monitoring from an offshore center in India versus people who used to reside in the same office) and the standardization of activities (e.g., a common controls framework definition and standardization in risk, control and compliance reporting) will, if not well managed, lead to business resistance and push back. Ultimately this can adversely impact the speed to transition, the scope of transition and the overall benefits case of the new operating model.</td>
</tr>
</tbody>
</table>
When assessing the right operating model for risk, control and compliance, an organization will need to consider a number of key aspects. Each model has its own set of merits, and it is critical that the operating model for risk, control and compliance must be aligned with organization strategy.

Also, it is imperative that organizations have a long-term view of the model being chosen as it is likely to have a significant impact on both cost and performance. For example, outsourcing helps avoid investments on costly system upgrades and provides greater flexibility of turning fixed cost into variable cost. However, managing a third-party outsourcing vendor requires a well-defined vendor management framework, including performance monitoring and adherence to defined performance levels.

An organization may also be reluctant about sharing confidential data with a third-party vendor. With the shared service model there is an increasing trend for adoption of a “hub and spoke” model. Typically under such a model, teams are strategically divided between onshore and offshore centers: low-risk and documentation-intensive sub-processes are handled by offshore teams, whereas onshore teams are mainly involved in handling front-end risk, control and compliance roles. This model gives more comfort to organizations seeking a balance between cost and quality; it can be classified as a natural extension of the finance and administration outsourced setup, with less critical and more labor-intensive work products being managed offshore. The model has gained momentum in the recent past with regional spokes coming up in countries like India, the Philippines and Argentina.

To summarize, the following key factors should be considered for organizations to assess the right operating model:

- **Cost** – There are several cost components that need to be looked into. SSC setup costs must be compared with the cost of transitioning to an outsourced vendor. There could be hidden costs due to poor service delivery performance, particularly in an outsourced setup. Technology and infrastructure investment also must be factored in the overall cost benefit computation.

- **Talent availability** – This factor is determined by the location chosen for the new operating center and has a potentially significant impact on the overall commercial viability of the entire model. Choosing a location with an adequate talent pool of the necessary skill set is critical, and this also includes having the requisite language skills required.

- **Market stability** – The location must not be politically unstable or exposed to significant market or currency risk.

- **Process vulnerability** – It is important that the process being transitioned to a SSC, or outsourced to a third-party vendor, continues to operate within the prescribed risk appetite of the parent organization. While the organization needs to have clarity of reason for choosing a centralized operating model, process-specific risk dynamics must be evaluated to ensure that the transition has not resulted in a significant dip in quality of service delivery due to cost or other associated benefits.
The transition from the “old world” to the “new world” is very carefully managed.

- Hand-over
  The learning curve of people within the new operating center is explicitly managed as they become increasingly familiar with their role.
- Customers of the new operating model are absolutely clear on what they need to do, what they will receive, and when they will receive it.

These challenges and risks faced when moving to a new centralized operating model can be categorized as (i) getting the design right and (ii) managing the transition.

### Key risks to be managed – in design

- **Use of shifts**
  In a new centralized operating model there can be a failure to make full use of shifts within a shared/offshore service center to maximize productivity and global coverage.

- **Service-level agreements**
  With SLAs, there can be a lack of clarity on what is required from the centralized operating unit to fully support the business in managing risk, controls and compliance. Deterioration in the effectiveness of the second and third lines of defense leads to potential financial loss, reporting error or fraud.

- **Roles and responsibilities**
  With new roles and responsibilities there can be a lack of clarity in roles and responsibilities – and hand-over points – between group, business units and central operating unit. Deterioration in the effectiveness of the second and third lines of defense leading to potential financial loss, reporting error or fraud.

- **Number of centers**
  The use of one center challenges the ability to provide global coverage and represents a single point of failure due to operational, social or political challenges.

- **Exchange risk, inflation risk, telecommunication costs**
  There can be a failure to take into account the offshore risks and costs that will influence how well the operating center is deemed to be performing and related SLA measures.

### Key risks to be managed – in transition

- **Ramp up**
  When ramping up, there is the possibility of failure to understand and manage expectations on how long it takes to recruit into an SSC – especially when dealing with offshore countries such as India and Poland. This will either delay “go live” or incur costs to accelerate ramp up (e.g., through the use of third parties).

- **Transition**
  Things often go wrong in transition periods and will need to be rectified. Difficulties typically include delays in reporting, incorrect reporting due to data issues, limited business understanding of those in the operating center frustrating the business (see below), and technical and telecommunication failures and interruptions.

- **Knowledge transfer**
  There is a need for a transfer of knowledge to those people within the operating center having insufficient knowledge of the business at a group and business unit level. There is a risk of having a limited understanding and awareness of the day-to-day risks, controls and compliance needs of the business.

These risks, if realized, can seriously undermine the value and confidence in the move to the new operating model. In many (but not all) cases they come back to people and trust:

- Customers of the new operating model are absolutely clear on what they need to do to, what they will receive, and when they will receive it.
- The learning curve of people within the new operating center is explicitly managed as they become increasingly familiar with their role. Examples used in practice to support this include:
  - Training on leading risk and compliance products such as ACTIMIZE and databases such as World-Check, COSIMA and Dun & Bradstreet. Internal trainings on regulatory requirements around Sarbanes-Oxley, Dodd-Frank, Consumer Financial Protection Bureau, Fair Credit Regulation Act (FCRA), Health Insurance Portability and Accountability Act (HIPAA) and Volcker rules.
  - Hand-over points between the business and operating center are clarified.
- The transition from the “old world” to the “new world” is very carefully managed.
Conclusion

Don’t underestimate the value of centralized operating models

The use of shared services, offshore, co-sourced and outsourced models is common (verging on standard) in Finance, IT and HR but Risk, Controls and Compliance functions are increasingly realizing the value that such centralized operating models can bring to their activities and capabilities.

They can support cost reduction initiatives, adapt to changing risk profiles, and provide real insight into the management of risks, controls and compliance needs globally and locally. They can also drive fresh thinking on key risks and compliance needs, what this means for a “fit for purpose” controls framework, and how best to use existing and new technologies.

New centralized operating models represent a fundamental opportunity for Risk, Controls and Compliance functions to align with the rest of the business, manage risk more effectively and drive down cost. The financial services industry has been leading the way with other sectors now beginning to catch up. While recognizing that there are challenges in defining the right operating model and in transition, the tide is definitely turning. Risk, Control and Compliance functions are increasingly asking “when and how” they make this move – not “if.”

<table>
<thead>
<tr>
<th>Key questions</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has your risk, control and compliance operating model kept pace with the rest of your business?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are your risk, control and compliance resources and capabilities residing in the right function and location to minimize their cost while maximizing compliance, scalability, agility and transparency?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you understand the capacity and capabilities that exist in lower-cost countries that support risk, control and compliance activities that other organizations are already tapping into?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you know what your current cost of risk, control and compliance is today – and the operational opportunities to reduce it?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is your risk, control and compliance operating model aligned to your long-term business strategy?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If one of these questions has been answered with “no,” it is time for you to take action as soon as possible.

Yes

No
Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our Insights on governance, risk and compliance series at www.ey.com/GRCinsights

Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our Insights on governance, risk and compliance series at www.ey.com/GRCinsights

Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our Insights on governance, risk and compliance series at www.ey.com/GRCinsights

Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our Insights on governance, risk and compliance series at www.ey.com/GRCinsights

Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our Insights on governance, risk and compliance series at www.ey.com/GRCinsights

Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our Insights on governance, risk and compliance series at www.ey.com/GRCinsights
At EY, we have an integrated perspective on all aspects of organizational and IT risk. We are the market leaders in internal audit, financial risk and controls, and information security. We continue to expand our capabilities in other areas of risk, including governance, risk and compliance, as well as enterprise risk management.

We innovate in areas such as risk consulting, risk analytics and risk technologies to stay ahead of our competition. We draw on in-depth industry-leading technical and IT-related risk management knowledge to deliver services focused on the design, implementation and rationalization of controls that can potentially reduce the risks in our clients’ applications, infrastructure and data.
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2014 EYGM Limited.
All Rights Reserved.

EYG no. AU2150
ED none

In line with EY’s commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com/GRCinsights

About EY’s Advisory Services

Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or more specifically on achieving growth, optimizing or protecting your business, having the right advisors on your side can make all the difference.

Our 30,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

To find out more about our IT Risk Advisory services could help your organization, speak to your local EY professional, or a member of our team.

The leaders of our RISK practice are:

<table>
<thead>
<tr>
<th>Global RISK Leader</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Paul van Kessel</td>
<td>+31 88 40 71271</td>
<td><a href="mailto:paul.van.kessel@nl.ey.com">paul.van.kessel@nl.ey.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Area RISK Leaders</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jay Layman</td>
<td>+1 312 879 5071</td>
<td><a href="mailto:jay.layman@ey.com">jay.layman@ey.com</a></td>
</tr>
<tr>
<td>EMEIA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jonathan Blackmore</td>
<td>+971 4 7010921</td>
<td><a href="mailto:jonathan.blackmore@ae.ey.com">jonathan.blackmore@ae.ey.com</a></td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Iain Burnet</td>
<td>+61 8 9429 2486</td>
<td><a href="mailto:iain.burnet@au.ey.com">iain.burnet@au.ey.com</a></td>
</tr>
<tr>
<td>Japan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yoshihiro Azuma</td>
<td>+81 3 3503 1100</td>
<td><a href="mailto:azuma-yshhr@shinnihon.or.jp">azuma-yshhr@shinnihon.or.jp</a></td>
</tr>
</tbody>
</table>