Getting **LESS** from **MORE**

*What’s wrong with current approaches to compliance – and what to do about it!*
First – what is ‘Compliance’?

Compliance —

“Adhering to the requirements of laws, industry and organizational standards and codes, principles of good governance and accepted community and ethical standards.” AS 3806-2006

Legal compliance (due diligence) —

“Effective control of legal risks in order to ensure that the law is complied with.” HB133—1999
Let’s think about the origins of compliance

Legal & regulatory compliance tends to be imposed when….

1. **Minimum community expectations** need to be met
2. **Reliable outcomes** need to be assured
3. To ensure **protection of the vulnerable**
4. To guide or **control markets**
5. **Transparency** is needed
6. **Stakeholder confidence** needs to be maintained
Compliance is about risk management

Legislated risk management in order to achieve societal objectives.
The Compliance Formula

S x C x P > E_S

S – Strategy
C – Culture
P - Process

E_S - Societal Expectations
The 3 focus areas

Strategy

Culture

Process
1. STRATEGY
The compliance burden is immense

Compliance repeatedly ranks amongst the top Strategic Risks for organisations today

...impacting costs, productivity, effectiveness...

and it’s increasing.

- Ernst & Young Strategic Business Risk Reports
- SAI Global Report: Risk and Compliance in Australia
- Productivity Commission
- Australian Chamber of Commerce and Industry (ACCI)
- Independent Regulatory and Pricing Tribunal (IPART)
- WEF rankings going backwards – attributable to ‘red tape
- Deloitte estimate $294Bn
- IPA says in 2014 alone 4,607 pages of new legislation were passed by the federal parliament
Why is Compliance so Difficult?

- Too many requirements to manage easily
- Maintaining ‘line of sight’ to regulations
- Integrating obligations into work processes
- Difficult to establish internal controls
- COST
Compliance differs from Risk

<table>
<thead>
<tr>
<th>ORGANISATIONAL RISK (ISO 31000)</th>
<th>COMPLIANCE (AS 3806 / ISO 19600)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determined by the organisation</td>
<td>Externally imposed</td>
</tr>
<tr>
<td>Balance loss with opportunity</td>
<td>Must be addressed</td>
</tr>
<tr>
<td>Consequences for noncompliance</td>
<td>Penalties often apply for noncompliance</td>
</tr>
<tr>
<td>Require internal controls</td>
<td>Require internal controls</td>
</tr>
</tbody>
</table>
2. CULTURE
Hi all,

As an input to your internal Legal discussions relating to notification, below is a summary of a discussion we had within (deleted).

Our intention is not to avoid notifying consumers of the change, allowing time for them to tidy up their credit information before it forms part of their credit file.

What I want us to resolve is whether the driver for this is legislative or because we want to. Reason being that the type of notification would be quite different depending on what the view is.

As such I think this is the first step towards understanding how we approach the topic.

Happy to discuss further,

Thanks

(Withheld)
Culture drives behaviour

The corporate regulator says it is considering the need for criminal sanctions and pushing for heavy fines for poor cultures in the financial services sector.

The Australian Securities and Investments Commission's chairman Greg Medcraft told a Senate Estimates hearing that he wants to be able to charge banks and their directors when company culture has allowed for misconduct by employees.

Reference: “ASIC considers criminal sanctions for poor financial company culture” mobile.abc.net.au, 3 June 2015
1. Commitment that permeates the organisation
2. Policy aligned to strategy and objectives
3. Compliance program is adequately resourced
4. Compliance objectives & strategy is endorsed by Management
5. Compliance obligations are identified & assessed
6. Responsibility is clearly articulated and assigned
7. Competence & training needs are addressed
8. Behavioural expectations are expressed and applied
9. Controls are in place to manage compliance and achieve desired behaviours
10. Performance of the compliance program is monitored, measured and reported
11. The organisation is able to demonstrate its compliance program through both documentation and practice
12. The compliance program is regularly reviewed and continuously improved
3. PROCESS
Compliance responses

1. Do nothing!
2. Attestations
3. Compliance overlay
4. Financial trade-off
5. Integrative approach
An Automated, Preventive approach is best

Low productivity
High cost
Low effectiveness
Poor governance visibility

Best productivity
Lowest cost
Highly effective
Transparent governance

Automated controls
---------
Detective approach

Manual controls
---------
Preventive approach

Automated controls
---------
Preventive approach

Manual controls
---------
Detective approach

© RelianSys Pty Ltd 2015
Approaches to integration

1. Scanning
OK for simple compliance environments.
But in complex environments

- High cost, low productivity
- Difficult to deploy
- Difficult to assure outcomes
- Individuals control their own risk - maybe
- Reporting is impossible
Approaches to integration

2. Update service

This is really ‘half’ a solution. It solves the scanning problem for a sector or common regulations.

But...

- Still have to work out the detail
- Still difficult to assure outcomes
- Still difficult to deploy
- Less reliance on individuals to control risk
- Reporting is restricted - and costly
Approaches to integration

3. Managed content with automation:
Delivers against all governance compliance needs

- Content is collated and condensed
- Control responsibility is transferable
- Easy to deploy
- High reporting capability
- Maximises productivity outcomes
To Summarise – How to get **MORE** from **LESS**?

Strategy x Culture x Process
> Societal Expectations

- Compliance is a strategic risk

- Cultural alignment with a total governance approach is essential

- Preventive approach utilising outsourced update services and automation is essential
Helping Organisations -

- to get MORE from LESS