Mass-Produced Personal Compliance Guidance

by Matt Cantrell

Compliance guidance that applies to an employee’s real world is, of course, necessary for changing employee behavior to prevent misconduct and shortcuts that circumvent policy. And obviously, compliance teams must update guidance to meet those needs as they evolve.

But the nature of work is not evolving; it’s rolling with upheaval. And compliance simply hasn’t kept pace.

COVID-19 is the most prominent example right now, although it’s not the only one. Since March, 88% of HR executives have advised employees to work from home, and an average of 58% of their workforces have had to use new skills in response to the pandemic.¹

And in the past several years...

• More than 60% of jobs have seen more than 25% of their required skills change.
• Fifty-seven percent of companies have increased geographic dispersion in their workforce.
• Eighty-two percent of employees are encountering new cultural tensions following a significant organizational transition.²

Yet among surveyed compliance leaders ...

• Just 31% provide compliance guidance that contains only components relevant to employees.
• Only 16% have reevaluated guidance in the face of corporate changes.³
Compliance officers should also take advantage of an available tool that they’re likely familiar with as consumers. Consider the evolution of sales, digital marketing and customer service over the last two decades. In the early stages of the internet, digital advertisers relied on mass marketing — the delivery of a single message to a broad audience. That’s a far cry from your Netflix queue today. Netflix can tag components of any given show or film according to the user groups who would enjoy each element. Would this thumbnail appeal to a teenage boy? Would this description intrigue a sci-fi aficionado? The company also tracks significant amounts of data about customer interests. What types of movies did you watch last year? Which ones did you turn off after five minutes? After mapping the program’s tags to your interests, Netflix can deliver a selection that feels handcrafted to your taste, even though it came from an algorithm, not a human curator.

The revolution wrought by this type of mass-produced personal experience can extend to training and guidance — it is the compliance team’s turn.

**Relief for an Unsustainable Situation**

Most compliance programs work to make their employee guidance applicable by creating custom-made guidance to address top employee needs as they arise. That works, but it’s not scalable. It only addresses one need at a time, it has high ongoing costs and you have to start from scratch when needs change. Compliance executives tell us they don’t have the time or money to do that, particularly in less regulated industries where there might not even be one FTE on the team for every 1,000 corporate employees. Even if that workforce were static (which it isn’t), it would still typically be spread through scores of countries (with a variety of languages) and an even greater mix of responsibilities (which are constantly changing).

The answer is configuration — creating a modular form of compliance that can be assembled many different ways. Since employees receive only what applies individually to them, the compliance guidance feels fully customized, even though it’s been selected from an existing library.

Configuration simultaneously addresses many employee needs, has low ongoing costs after the initial investment and is easy to build upon when needs change.

Below are the four steps to configuration, followed by a walk-through of how QBE North America, a division of the QBE Insurance Group, applied each of the steps.

- **Step 1: Review (and Prioritize) Guidance Library**
- **Step 2: Unpack Component Parts**
- **Step 3: Classify Component Parts by Audience**
- **Step 4: Deliver Tailored Content to Employee Groups**

**Figure 1. Identification of First-Priority Policies**

<table>
<thead>
<tr>
<th><strong>Phase 1: Corporate Policies</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Code of Ethics and Conduct</td>
</tr>
<tr>
<td>• Whistleblowing Policy</td>
</tr>
<tr>
<td>• Conflicts of Interest</td>
</tr>
<tr>
<td>• Privacy and Information Security Policies</td>
</tr>
<tr>
<td>• Gifts and Entertainment Policies</td>
</tr>
<tr>
<td>• Records Management</td>
</tr>
<tr>
<td>• Sanctions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Phase 2: Departmental Policy Sets</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Based on your risk assessment results, high-risk departmental policy sets</td>
</tr>
<tr>
<td>• Medium-risk departmental policy sets</td>
</tr>
</tbody>
</table>

**Take a Top-Down Approach**

Start with the corporate policies and procedures that apply to your entire employee population.

**Factors to Prioritize:**

1. Content that applies broadly, as this presents the greatest opportunity
2. Departmental policy sets that align with your highest areas of risk
3. Additional (medium- and lower-risk) departmental policy sets
Step 1: Review (and Prioritize) Guidance Library

The first step is deciding which parts of the guidance library to start with. For most compliance functions, time and resource constraints will require a narrow initial scope for a configuration project. One approach is to begin configuration with the highest-priority compliance guidance for this year. (For example, our polling shows that the top policies updated in response to COVID-19 as of 9 April 2020 were information security; recognizing and reporting misconduct; environmental; health and safety; and data privacy.) Another path to configuration is to apply it gradually as a part of all future guidance refreshes (e.g., updates to policies and training modules).

QBE started with its internal policies and procedures. As shown in Figure 1, the compliance team prioritized the policies and procedures that apply broadly to the entire employee population and moved on to departmental policy sets prioritized by risk.

Figure 2. Identification of Requirements Within a Policy

Sample Compliance Policy (Required actions highlighted)

Sample Requirements for All Employees
- Handle confidential information with care.

Sample Requirements for Some Employees
- Log into a VPN when using public Wi-Fi.
- Do not contact customers using personal devices or accounts.
- Ensure direct reports are properly trained before handling confidential information.

Source: Adapted From QBE

Mass-Produced Personal Compliance Guidance
Step 2: Unpack Component Parts

The next step is to break down the selections into the discrete employee obligations they contain (see Figure 2).

QBE analyzed 15 policies and identified 432 distinct obligations contained within. Without eliminating any requirements from the policies, the compliance staff was able to convert the 432 distinct obligations into 22 “simplified” all-employee obligations. The team used a system to winnow the number, applying one of three distinct “methods” to each obligation:4

Method 1: Consolidating obligations (e.g., broadening the scope of an obligation, presenting lists within an embedded hyperlink)

Method 2: Disregarding obligations (e.g., if they are duplicates, if they aren’t actionable)

Method 3: Simplifying obligations at the source (e.g., modifying an underlying policy, procedure or process design).

In addition to these all-employee obligations, others applied only to certain employee groups. To ensure that simplifying doesn’t lead to increased noncompliance — the opposite of its intended effect — QBE implemented controls such as an audit trail maintained within the register that indicates the basis for the consolidation. That makes it very easy to undo or be challenged at a later time by another assurance function. Further, the final obligations always link back to the source records for convenient verification.

Figure 3. Classify Component Parts by Audience

<table>
<thead>
<tr>
<th>Sample Obligations</th>
<th>Employee Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Managers</td>
</tr>
<tr>
<td>Handle confidential information with care.</td>
<td>✓</td>
</tr>
<tr>
<td>Log into a VPN when using public Wi-Fi.</td>
<td></td>
</tr>
<tr>
<td>Do not contact customers using personal devices or accounts.</td>
<td></td>
</tr>
<tr>
<td>Ensure direct reports are properly trained before handling confidential information.</td>
<td>✓</td>
</tr>
</tbody>
</table>

Total Obligations:

|           | 15 | 5 | 8 | 3 | 6 |

Source: Adapted From QBE
Step 3: Classify Component Parts by Audience

Next, map the obligations to the employee groups they apply to. QBE maps obligations using job code data and other role identifiers — for instance, employees who engage directly with customers are mapped to certain job titles within certain departments. The key here is to bring in the right stakeholders. If you gather the relevant subject matter experts and policy owners in a room, unpacking and classifying obligations is a lot faster and easier than it sounds.

QBE includes two measures in this step:

- Policy owners sign off on the employee groups their obligations apply to.
- Compliance maintains an audit trail of how obligations are defined, simplified and sorted.

QBE then identifies the aggregate number of obligations applicable to each employee group (see Figure 3).

Generally, policies tend to be written broadly and in overly general terms, which makes it inherently difficult for employees to understand how policies impact their individual role. QBE found a new means for delivering compliance to the first line when the audience became only those with a “need to know.”

**Note:** Alternative ways to classify employee groups exist for compliance programs that don’t have access to robust HR management data or similar data sources. For example, employees can self-select into groups through a simple activity questionnaire, or managers can make this selection for their teams.

---

**Figure 4. Methods for Providing Content Specific to Employee Groups**

- **John Smith**  
  Sr. Manager, Sales  
  USA — New York

  **Click to see your obligations:**
  - For All QBE Employees [-]
  - For QBE People Leaders [+]
  - For Staff With Customer Contact [+]

  If you have a potential conflict of interest as defined by [these guidelines](#), inform your manager and disclose the conflict using [our reporting platform](#).

- **Jane Doe**  
  Sr. Manager, Finance  
  USA — Wisconsin

  **Click to see your obligations:**
  - For All QBE Employees [+]
  - For QBE People Leaders [+]  
  - For Staff With Access to PII [+]  
  - For Staff Who Travel Internationally [+]  
  - For Staff Who Engage With Regulators [+]

Source: Adapted From QBE

---

Excerpt from Gartner Business Quarterly 3Q20
Step 4: Deliver Tailored Content to Employee Groups

QBE is developing a policy map where employees would see all the obligations that relate to their individual role based on their role profile. In the example in Figure 4, John and Jane both belong to the “QBE People Leaders” group, but the rest of their groups are different. So, they both receive guidance for people leaders, but the other guidance they receive is different. Embedded links provide employees with access to all the information needed to fulfill each requirement and can link back to the full policy detail.

Simplifying employee obligations and mapping their applicability to specific roles created an opportunity for QBE to break away from the old policy-centric way of communicating compliance information. Policies remained intact, but employees now have an alternative means for accessing what they need to know that is both user-friendly and far more effective, clarifying expectations and responsibilities.

The shift to modular compliance creates a whole new ecosystem that can be expanded over time as needs change. Joseph Sherno, chief compliance officer for QBE North America, told us in an interview that the benefits are clear: The move encouraged “innovation within compliance as a function” and improved “first-line accountability and ownership.”

---

1 Gartner COVID-19 Crisis Benchmarking Against Your Peers Webinar Poll (2 April 2020)
2 2019 Gartner for HR Leaders Research
3 2020 Gartner Compliance Guidance Imperatives Survey for Legal and Compliance Leaders
4 See “Case Study: Configurable Compliance Guidance (QBE North America)” for more detail on the company’s simplification methodology.
Gartner Business Quarterly is exclusively for clients logged into gartner.com. Others can access complimentary resources at gtnr.it/gartner-business-quarterly.

About Gartner Business Quarterly

Gartner Business Quarterly provides business executives with insights from best practices research and the real-world experience of practitioners. The journal’s insights especially equip executives to tackle challenges that cut across the C-suite and affect multiple executive teams. Writers, contributors and data analysts are members of Gartner Research & Advisory (R&A) whose teams are led by Executive VP Mike Harris. The Gartner Business Quarterly publication is led by Editor-in-Chief Judy Pasternak with executive sponsorship by Group VP Scott Christofferson.

About Gartner

Gartner, Inc. is the world’s leading research and advisory company and a member of the S&P 500. We equip business leaders with indispensable insights, advice and tools to achieve their mission-critical priorities today and build the successful organizations of tomorrow.

Our unmatched combination of expert-led, practitioner-sourced and data-driven research steers clients toward the right decisions on the issues that matter most. We are a trusted advisor and an objective resource for more than 14,000 enterprises in more than 100 countries — across all major functions, in every industry and enterprise size.

© 2020 Gartner, Inc. and/or its affiliates. All rights reserved.