Aberdeen Group
A Harte-Hanks Company

September 2009

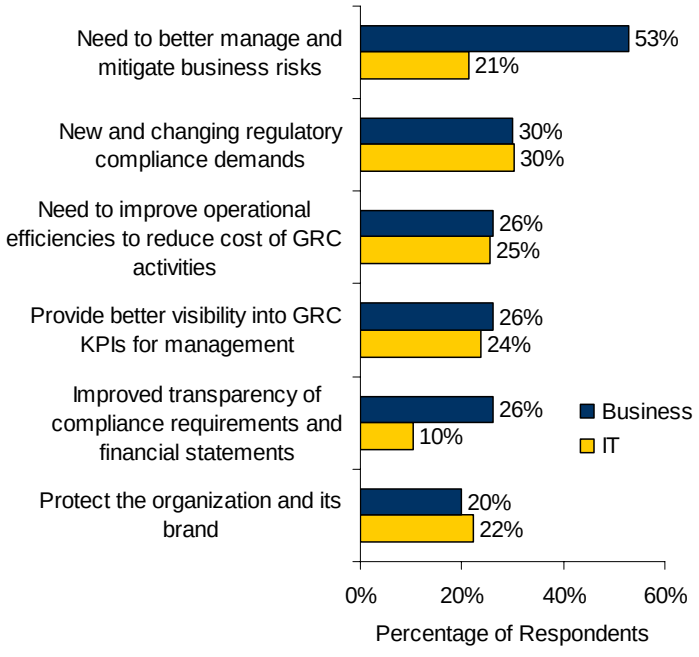
GRC Strategies - Finding the Right Balance of Business and IT

Increased regulatory requirements, the need for transparency, and the desire to better manage and mitigate risks have combined to make Governance, Risk, and Compliance (GRC) top of mind for both business and Information Technology (IT) executives. The rising complexity of business which is undergoing constant change often make executives feel as if they are steering the ship while "fixing" it at the same time. Throw in the accelerating pace of change and that ship becomes a space ship, traveling at warp speed. Corporate stakeholders feel enormous pressure to institute proper segregation of duties (SoD) and access control over key information assets. Business managers and IT security managers must work collaboratively and continuously to control access and authorization, guarding against fraud and mistakes, while providing the clear visibility that is prerequisite for sound corporate oversight to ensure profitability and compliance.

Risk & Compliance Drive Business Transformation

A complicity of pressures drive GRC prompted business transformation.

Figure 1: Top Two Pressures



Source: Aberdeen Group, May 2009

Analyst Insight

Aberdeen's Insights provide the analyst perspective of the research as drawn from an aggregated view of the research surveys, interviews, and data analysis.

Definitions

- √ **Governance** refers to the frameworks, policies, procedures, controls, decision-making hierarchy, etc. which are employed to make decisions and manage the business
- √ **Risk Management** refers to the identification, prioritization and mitigation of risks that could potentially impact the organization
- √ **Compliance** refers to meeting and sustaining requirements for government regulations, industry regulations, and internal policies within the allotted timeframe
- √ **IT GRC** refers to a unified, comprehensive, and inter-connected approach towards Governance, Risk Management, and Compliance as it relates to the organization's use of Information Technology (IT)
- √ **Enterprise Risk Management** refers to the assessment and strategic management of risks across the enterprise

Telephone: 617 854 5200
Fax: 617 723 7897

Business managers and IT often have different perspectives. Figure 1 shows both similarities and differences in how business and IT feel these pressures. While the chart on the previous page displays no single dominant factor from an IT point of view, the need to better manage and mitigate business risks is a clearly dominant factor for business managers. Those business risks typically fall into four high-level categories: *financial*, *strategic*, *operational*, and *other,* and seldom is IT mentioned directly in articulating these risks. Yet IT plays a fundamental, foundational role in addressing many of these key risk factors, and indeed IT is responsible for supporting or enabling numerous aspects of any given company's business. The rise in importance of IT governance, risk management and compliance ("IT GRC") reflects an increasing recognition that the strategic value of IT lies not in the mere technology itself, but in how it is applied and managed most effectively. While Chief Information Officers (CIOs) and IT management in top performing companies are becoming more business-savvy, it is apparent from Figure 1 that many still do not recognize and acknowledge the role they must play in managing and mitigating risk and providing transparency to compliance and financial statements.

Actions Taken in Response

While line of business and IT executives may not feel the same pressures (Figure 1), there is a clear convergence in overall strategy in developing a comprehensive 'continuous' compliance infrastructure. However, often the two different constituents do not clearly see the link between the business of GRC and IT's support. Certain characteristics of Best-in-Class companies, including the centralization and automation of processes and controls, point to the fact that the objective is not only to be good at the process of compliance, or governance, or risk management for its own sake – but also to harness IT more effectively in support of achieving business objectives and managing financial, strategic, and operational risks.

Take for example the simple (in concept) process of user provisioning of access to enterprise applications and / or sensitive data contained therein. Often that access is dictated by job role or function. A user may be granted permissions and access to applications and data based on his or her current position. If that same person were to transfer to a different role or department for which the individual no longer needs that same level of access, is there any guarantee it will now be removed? In fact, when employees leave the company, are processes in place to ensure the removal of access to that user? The more automated the provisioning process, the more likely liability will be reduced. Seventy percent (70%) of Best-in-Class companies centrally manage primarily automated controls and procedures, as compared to 22% of all others (not Best-in-Class).

Best-in-Class Criteria

- √ Identification of weaknesses in existing risk management processes
- √ Ability to translate risk assessment data into actionable recommendations
- √ Flexibility to adjust to new or updated regulatory requirements

Attributes Distinguish Top Performers

Effective execution of strategies results in better compliance and improved business transformation. By integrating technology to embed GRC at all

appropriate levels of the organization, cost reductions can be realized both in terms of the cost of operations as well as lower cost of GRC.

Table 1: Competitive Framework for Business & IT GRC

	Best-in-Class	Average	Laggards
Policy & Process	Establish and enforce consistent IT Risk and Compliance management policies and procedures (across geographies and lines of business)		
	72%	49%	45%
	Formal segregation of duties		
	67%	33%	29%
	Adoption of a "continuous improvement" approach to business and IT GRC initiatives		
	55%	28%	24%
Organization	Responsible executive or team with primary ownership of IT GRC initiative		
	85%	55%	49%
	Formal organizational structure to support work flows, risk management and compliance controls and communication channels		
	58%	35%	33%
Monitoring & Measuring	Consistent process prioritization assessments to ensure most important compliance processes are monitored most frequently		
	61%	33%	29%
	Consistent process prioritization assessments to ensure most fiscally relevant risk management processes are monitored most frequently		
	39%	35%	19%
	Consistent monitoring to ensure policy-in and audit-out for technical controls is enabled and accurate		
	55%	24%	20%
	Regular review of output from compliance management, auditing, and reporting solutions		
	58%	31%	29%
	Routine analysis of historic risk management data to identify anomalous activity		
	58%	28%	14%
	Segregation of duties monitoring		
	76%	31%	26%

Source: Aberdeen Group, May 2009

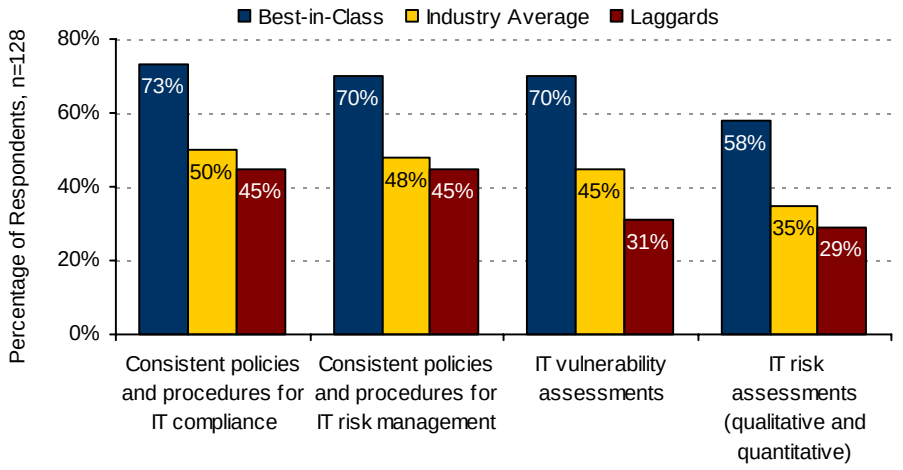
Policy & Process

Consistent policies for compliance and risk management are a foundation for successful GRC strategies. Without them, our executive space ships would be rudderless, hurtling through the galaxy. Formal segregation of duties is at the very heart of these policies, yet requires a firm handle on access control. While assignment of those duties will be a business decision, access to the applications and the underlying data brings IT into the picture. The more automated the authorization process from access request to approval and documentation, the more cost efficiencies can be gained without sacrificing security and control. Consistent policies and procedures, coupled with regular assessments of vulnerability and risk, both qualitative and quantitative, are the hallmark of a Best-in-Class GRC strategy (Figure 2). With Best-in-Class organizations at least twice as likely as Laggards to consistently and routinely assess both, it would appear this is not necessarily an easy task.

"SAP Business Objects Access Control and SAP NetWeaver Identity Manager have helped us save money by automating almost the entire authorization process, from access request to approval and documentation."

~ Reinhard Falke, Director of Business Processes and IT, Vibracoustic GmbH & Co. KG

Figure 2: Consistent Policies; Regular Assessments



Source: Aberdeen Group, May 2009

Organizational

The perceived difficulty in managing vulnerability and risk creates that much more need for establishing primary ownership for these important cross-enterprise initiatives. Aberdeen data consistently confirms the same pattern: management commitment and executive ownership are key Best-in-Class differentiators: 85% of Best-in-Class companies have assigned primary ownership of their IT GRC initiatives to a responsible executive or team. In addition, the typical good news / bad news pattern holds true in terms of investments in end-user training. The good news: the Best-in-Class are 1.7-times more likely than Laggards to invest in communication of corporate policies, practices, and expectations for ethical behavior. The bad news: just two-thirds (64%) of the Best-in-Class currently make such an investment.

In the more successful IT GRC initiatives, organizational structures are "wired" for work flow, problem escalation, and problem resolution (Figure 9). Best-in-Class companies support the responsibility and authority given to individual employees with communication and clarity around what the company views as acceptable parameters of risk. These best practices are arguably even more important for the less centralized, less automated early days of most GRC initiatives, although the research shows that diffused responsibility and poor communications too often go hand-in-hand.

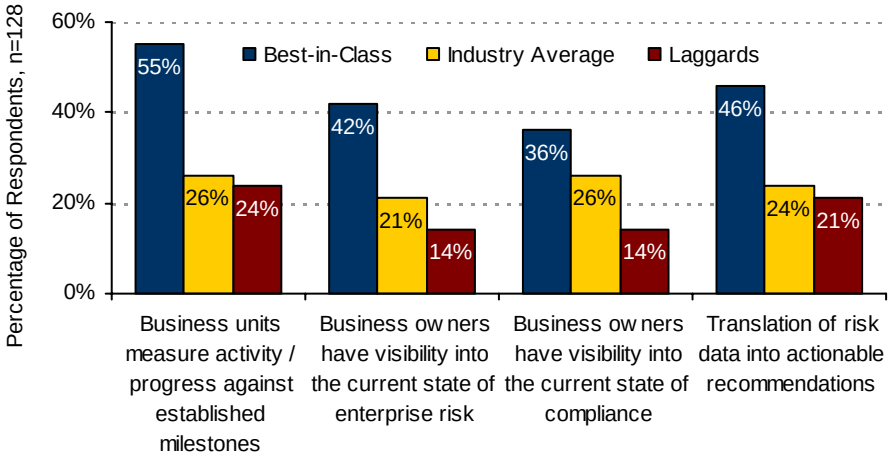
Technology can also be the catalyst that helps bring the organization together. GRC and IT GRC are not two separate problems. By implementing a common platform IT and line of business professionals can read from the same page, speak the same language using the same data and information to help bridge the organizational gap and support collaboration.

Leadership for GRC initiatives tends to be provided by the highest levels of Best-in-Class organizations, i.e., in the majority of top performers the CEO, Chief Compliance Officer, CIO, CFO, CTO, Chief Risk Officer, or COO is identified as either the leader or as a key contributor. For all other respondents, leadership and contributions for GRC initiatives is more widely dispersed. Interestingly, the research shows that budgetary decisions for GRC initiatives are predominantly at the CIO and CEO level – not with the CFO – in Best-in-Class organizations, combining a business and IT perspective at the very highest levels.

Measuring & Monitoring

Visibility into the current state of risk and compliance, progress against established strategic milestones and the ability to translate risk data into actionable recommendations (Figure 3) is where real "governance" takes place.

Figure 3: Increased Visibility and Actionable Recommendations



Source: Aberdeen Group, May 2009

Respondents were asked to estimate the degree of change their organization had experienced over the last 12 months across a number of dimensions related to IT governance, risk management, and compliance. Table 2 presents some of the advantages that the GRC initiatives of Best-in-Class organizations are yielding, in comparison to those of their Industry Average and Laggard counterparts in terms of providing better visibility and input to decision-making. High-level conclusions that can be drawn from the findings in Table 2 include the following:

- Best-in-Class organizations are seeing significantly larger gains in their ability to identify, assess and prioritize risks
- Risk management initiatives at Best-in-Class organizations provide management with better access and visibility to current risk status, and better communication of risks to key stakeholders
- Best-in-Class companies have better capabilities to translate risk assessment data into actionable recommendations, enabling faster decision-making
- Best-in-Class organizations are significantly better than other respondents at compliance-related tracking and reporting, and report better flexibility to adjust to new or updated regulatory requirements
- Compliance initiatives at Best-in-Class organizations provide management with better access and visibility to current compliance status, and better communication of compliance status to key stakeholders

Table 2: Average Year-over-Year Changes in Visibility

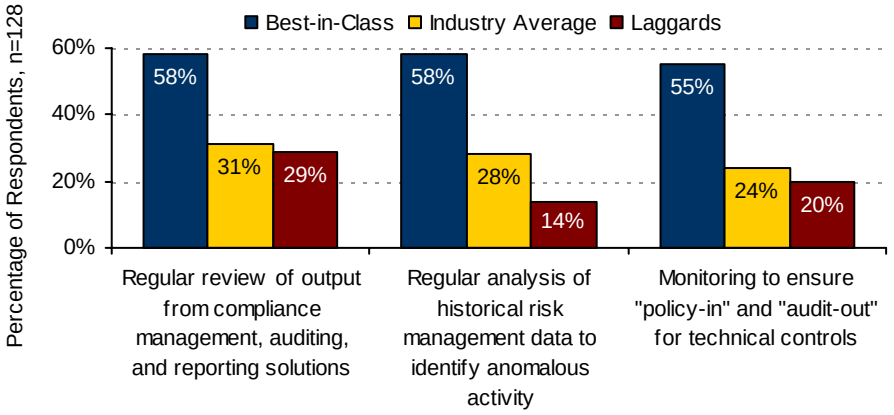
Capabilities in Risk Management and Compliance	Best-in-Class	Average	Laggards
Ability to provide clear, timely communication of risks to shareholders and board of directors	8.9%	4.9%	0.7%
Speed at which business-critical decisions are able to be made based on enhanced visibility into current risk thresholds	9.8%	4.8%	-2.0%
Efficiency of compliance tracking and reporting	12.0%	7.5%	1.9%
Flexibility to adjust to new or updated regulatory requirements	11.5%	4.8%	0.0%
Management's ability to access company's current compliance status	12.2%	5.0%	1.0%
Communication of current compliance status to board of directors and shareholders	9.3%	4.8%	0.1%
Speed at which business-critical decisions	8.9%	4.9%	-0.8%

are able to be made resulting from improved visibility into company's current compliance status			

Source: Aberdeen Group, May 2009

Best-in-Class organizations not only gather the facts, but also are twice as likely as all others to review and analyze the facts they have gathered (Figure 4). About three out of five (58%) Best-in-Class organizations regularly review the auditing and reporting output from their compliance and risk management solutions, compared to less than one-third of all other respondents.

Figure 4: Regular Monitoring, Analysis and Review



Source: Aberdeen Group, May 2009

Technical Capabilities

The need to make well-informed business decisions in the context of governance and compliance and constrained by the organization's appetite for risk ultimately leads to the evaluation, selection and deployment of one or more specific enabling technologies. These choices – along with the policy, planning, process, and organizational elements of implementation – are critical factors in the success of an organization's ability to balance business decisions with IT decisions.

A variety of tools come into play in providing technical sustenance to GRC initiatives. Top of mind are security, process control and access control. But analytic and business intelligence capabilities also play a key role in providing transparent information to the business about the current state of compliance and the current status of various risk parameters. The more automated the controls to monitor and verify that requirements of internal policies and external regulations are achieved, the more cost savings can be realized.

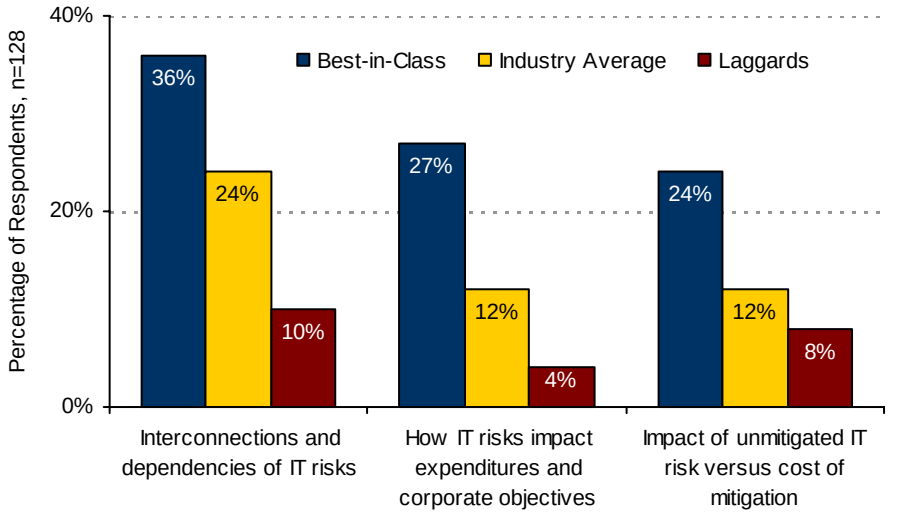
Modeling the interconnections and dependencies between IT risks, understanding how they impact budgets and corporate objectives, and the

"Our earliest IT governance meetings were extremely time-intensive, based primarily on manually prepared information. And the discussions were basically subjective, such as the relative importance of an SAP project to close the books more quickly in our Japanese subsidiary versus a secure Web portal project to streamline transactions with our value-added resellers. But we were successful in getting the company's business leaders to think and work together in terms of strategy, financials, operations, compliance, and risk. That has been and remains the real win for IT GRC."

~ CIO,
Mid-Size High Tech Company

ability to conduct "what-if" analysis regarding the costs and benefits of mitigation are newly emerging capabilities, but their use is significantly higher among the companies with top results (Figure 5). In individual interviews with select survey respondents, for most companies this is currently an area of open-ended discussion, intuition and ultimately judgment calls by the decision-making body, though all were quick to acknowledge the appeal of a more analytical approach.

Figure 5: Modeling Risks, Dependencies, Cost and Objectives



Source: Aberdeen Group, May 2009

The use of a corporate repository of all applicable compliance laws and regulations with controls and established procedures to respond to amended regulations is beyond the "emerging" stage with 58% of top performers claiming this technical capability, but this cream of the crop is head an shoulders compared to 34% of those not Best-in-Class. Similarly, 55% of Best-in-Class have a central repository for all risks and risk-related information, compared to 26% of all others. Yet we see a wider differentiation in observing that the majority (76%) of Best-in-Class are able to readily produce retrievable audit trail records to support analysis, audit, reporting or investigation, more than twice as likely as a combination of Average and Laggards.

Yet often in order to obtain a clear, accurate and complete picture, it is necessary to aggregate disparate compliance data into an integrated view or executive dashboard that is customizable by role. While Best-in-Class are still more than twice as likely to have this capability, there is still much room for improvement, with only 30% of top performers having invested in this capability.

Case in Point: Valero Energy Corporation

Valero Energy Corporation is a Fortune 500 company based in San Antonio, Texas. Valero has an extensive refining system with a throughput capacity of approximately 3 million barrels per day. The company's geographically diverse refineries in the United States, Canada and Aruba are supported by a mid-stream logistics system of pipelines and terminals. Valero also has a network of about 5,800 retail and wholesale branded outlets. Valero has approximately 22,000 employees and total assets of $37 billion. The largest refiner in North America, Valero's current annual revenues have grown through acquisitions from approximately $5 billion in 1997 to over $110 billion in 2008.

Bill Weber is Valero's SAP Manager responsible for SAP financial applications and GRC. He and Jack Ligon, Vice President of Sarbanes-Oxley Compliance have worked together since their current SAP GRC applications were implemented, beginning with a project initiated to address segregation of duties (SoD) issues identified during Valero's roll out of its SOX 404 internal controls program. "We suspect our issues were not very different from many companies. Employees had joined the company and were given access to data and functions. As they settled in and grew, they needed more access. Then they might transfer to another role in the company. In some cases, they kept their existing levels of access and layered on new ones. Ultimately some wound up having access they no longer needed, including some transactions that conflicted with each other… hence the SoD issues," according to Ligon.

As Valero started to get its arms around the issue, it considered various alternatives. "We considered developing our own SoD matrix, but we realized the effort would have been extensive and it would have been fairly easy to miss something," said Webber. "Instead we chose to implement SAP Business Objects Access Control."

"I don't think anyone should consider this a 'once and done' deal. The business evolves."

~ Jack Ligon, VP of SOX Compliance, Valero Energy Corporation

Ligon goes on to explain, "Using Access Control and other SAP tools, we analyzed user access requirements and designed completely new SAP roles that greatly reduced or eliminated SoD conflicts. Existing access capabilities were eliminated for all users and replaced with the newly designed roles. Mitigating controls were identified to address most remaining SoD conflicts, and our external auditors agreed that the residual conflicts at year-end were not material. Eventually all conflicts were eliminated or mitigated, and we now run daily Access Control reports to demonstrate that we have no unmitigated SoD conflicts."

Valero started with the SoD rule sets delivered by SAP. "These provided a good start," said Weber. "They were more comprehensive than we could have created ourselves. But in the end, our SoD rule sets needed to be Valero specific. So we have evolved and adapted by disabling SoD rules that we consider to be low-risk for Valero. In addition, we evaluate all new Access Control SoD rule set updates for Valero relevance. For example, we recently disabled new SoD rules related to transaction codes for Brazilian banks because we don't do business in Brazil."

Valero has also implemented other modules of Access Control for user provisioning enabling Valero to evaluate whether new user access requests will result in SoD conflicts before SAP security changes are made. Other modules allow for approval and monitoring of temporary elevated access that may be required for system maintenance. Valero is also beginning to use SAP NetWeaver Identity Management.

Key Takeaways

Best-in-Class organizations are making greater strides in balancing the business and IT perspectives of GRC initiatives, which translate to strategic and operational benefits that include:

- Significantly larger year-over-year improvements in their ability to identify, assess and prioritize risks
- Better access and visibility for business owners regarding current risk status
- Better communication of risks and compliance status to key stakeholders
- Better capabilities to translate risk assessment data into actionable recommendations, enabling faster decision-making
- Significantly greater year-over-year improvements in compliance-related tracking and reporting
- Better flexibility to adjust to new or updated regulatory requirements

Aberdeen's current research demonstrates that both business and IT GRC initiatives are continuing to grow in relevance, as a direct result of their ability to apply and manage IT more effectively and thereby to maximize its strategic value to the organization. Some key recommendations for all companies seeking to transform business processes to reduce costs, improve governance and compliance, while mitigating and managing risk:

- Take a continuous improvement approach to GRC.
- Operating standards should be consistent and enforced across the enterprise. Apply same level of diligence and control to IT process as you do to financial controls.
- Confirm security and access control is being effectively managed and maintained. Effectively monitor and control the provisioning of users and more importantly the removal of access when employees change positions or roles or when they leave the company. The more automated these processes, the more likely security hazards are minimized, making more cost savings possible.

- Make effective use of analytic and BI tools to measure and monitor, providing clear visibility to the state of governance, risk and compliance.

For more information on this or other research topics, please visit www.aberdeen.com.

Related Research	
IT GRC: Managing Risk, Improving Visibility, and Reducing Operating Costs; May 2009 *Are CFOs Ready for Unified GRC Solutions?* April 2008	*Is Your GRC Strategy Intelligent? Incorporating Analytics to Empower Accurate, Real Tine Visibility and Decision-making*; July 2008 *SAP's Unified GRC: A Holistic Answer in Troubling Times*; March 2009

Author: Cindy Jutras, Vice President, Research Development & Research Fellow (cindy.jutras@aberdeen.com)