Best Practices for Selecting Governance Risk and Compliance Software

By Shannan Layette, Pete McAteer and Buddy Doyle

Shannan Layette and **Pete McAteer** are part of the program management team at Oyster Consulting. **Buddy Doyle** is one of the founders of Oyster Consulting, and leads the Oyster Solutions technology and program management teams for the firm.

Any successful software implementation is dependent upon selecting the right vendor to address your specific business needs, or determining that it is better to build a custom application for your company. The process of selecting Governance, Risk and Compliance ("GRC") software is no different. The best implementations have a disciplined approach with process, people and technology aligned to achieve a common and well-defined goal. We are often asked the question: "What is the best software to help solve our problem?" The answer can only be determined after a reasonable and disciplined analysis.

The famous Benjamin Franklin quotation, "If you fail to plan, you are planning to fail" is never more accurate than when you decide to implement new software. You don't want to spend the time and resources to select and utilize a software solution only to discover that you missed a critical requirement, or adversely impacted stakeholder(s), resulting in an unsatisfactory outcome and lower than expected adoption and return on investment ("ROI").

Many organizations impose a purchase approval process that demonstrates the analysis has been completed, the financial cost/benefit analysis supports the business case, and the software will work within the firm's technology environment. One project at a major wire house may cost more than the entire technology budget at a smaller organization. For large firms, mistakes can cost millions, and deserve a significant investment in the project initiation and planning phases. Your firm's risk may be lower, but following the best practices in selecting software, even in a scaled back approach, will most likely lead to a better implementation.

Engaged Leadership

Time and budget are scarce resources. Developing a fully engaged and supportive executive team will help ensure that your project gets the time and attention needed to be successful. Securing executive sponsorship is the first process you need to master. Ensuring that

the firm's business model(s) and risk management needs are thoughtfully considered will often lead to a commitment to creating more efficient processes, introducing new processes, enhancing capabilities, and solving problems with a software solution.

Start this process by defining what you want to achieve by having this software. There are several approaches that will help your executives evaluate this decision:

- We are not able to comply with new or existing regulations or expectations without additional software;
- We need to replace our existing provider;
- We will lower costs; and/or
- We will mitigate or avoid risk if we implement the new technology.

Once the company is committed to conducting an in-depth analysis and the desired end-state target has been somewhat defined, begin to identify the key stakeholders. It is vitally important that the executive sponsor enlists the leaders whose functions or processes may be directly or indirectly impacted to participate in the process. These leaders are likely to include risk management, legal, compliance, operations, technology, and sales.

Each of these groups should be not just represented, but fully engaged at the outset, as their input will be critical to business case development, developing clear business requirements, and ensuring a successful, targeted vendor request for proposal ("RFP") process. If the business leader delegates the project to someone else, make sure he or she empowers the delegate to speak with the full authority of the leader when decisions are made. Otherwise, if clear requirements cannot be elicited efficiently and are not fully vetted by accountable leaders, re-visiting previously confirmed decisions or requirements will significantly impact scope, schedule, and budget.

The famous Benjamin Franklin quotation, "If you fail to plan, you are planning to fail" is never more accurate than when you decide to implement new software.

Involving the affected leadership team from the beginning will also mitigate future scope creep, help ensure that the implementation will realize the intended benefits, and help to ensure the change will be sustainable. Their direct engagement and contribution into the business case will increase their individual ownership and deepen their commitment.

Assigning an experienced project manager ("PM") or program management office ("PMO") lead is recommended to drive these activities. The PM's role is critical to ensuring the correct requirements are identified and the RFP process is well defined and diligently followed. The PM ensures appropriate representation, is active throughout the critical planning processes, makes certain the requirements are complete, and ensures that any obstacles, risks or issues identified can be captured, tracked and managed efficiently and effectively. There is also tremendous value offered by an objective leader who can facilitate key decisions, manage downstream impacts, identify and resolve potential functional collisions and socialize status among the impacted teams.

The impact of a new system implementation that did not include all of the end users' input and requirements could cause the entire project to be scuttled after implementation. If some system functions or business processes were not accounted for, or process change decisions are not articulated on a timely basis, the project can fail, and the project team could also experience some career changes. Strong change control processes, effective communication, and accurate assessments of the project are skills that strong project managers have, and they can make or break a project.

Building the Business Case

Once the project's leadership team is established, it is imperative that all leaders influence the business case and agree that the business problem(s) or opportunities should be addressed with software solutions. Will the functionality clearly serve the firm's needs and address the problem, or will certain functionality or workflows create unintended consequences? Reaching a consensus on the project objective and the problem statement is crucial. This will ensure not only that specific concerns are addressed but also that there is transparency across functional teams.

Functional teams will typically include sales, branch managers, operations support, compliance, trading, risk, and finance departments. These teams all share the same organizational goals to get as much revenue as you can earn honestly, and keep

from plaintiff's counsel, but likely have different requirements and needs. For instance, the branch, district and/or regional managers may want to know how to limit the likelihood of a registered representative missing a breakpoint while efficiently being able to enter orders while the compliance department may want to know how to find customers who have already missed the breakpoint and make sure they are made whole. The trading group wants to make sure the orders are transmitted and settled appropriately, while the finance department wants to make sure commissions are paid efficiently and accurately. One issue with different perspectives and goals makes the organization better when everyone comes together to create a solution.

Dependencies and process handoffs must be apparent and requirements must be assigned to the appropriate business owners so accountability is clearly established. There are certainly areas where shared or secondary interests need to be documented to keep the interests of the entire firm aligned with the project.

Key components of the business case are:

1. A clear problem or opportunity statement
2. Background and supporting data
   - Why does the problem exist?
   - Why is it important or relevant to the business?
   - What are the key factors feeding the issues?
   - What are the current risks and issues facing the firm to be mitigated or resolved?
   - What are the business impacts if these risks are realized or if nothing is done?
   - Are there other ways to achieve the same goals?
3. Options with estimated or "order of magnitude" (OOM) costs and benefits. Parameters to consider for each option include:
   - Cost – High, Medium, Low
   - Advantages – quantify and qualify what will be achieved
   - Disadvantages – what desired results may not be realized
   - Time horizon – Long, Intermediate or Quick
   - Degree of resolution or percent mitigated – How congruent is the option with the problems being targeted?
   - Resources required – sufficient or constrained
   - Evaluating the risks of doing nothing
4. Recommended Next Steps – Set expectations on what you will do next and when to expect updates

The problem statement should clearly define each of the opportunities and pain points being experienced, the potential risks facing the firm and the impacts of not addressing each one. How much pain (or cost) is the firm willing to endure as a result of not addressing the problems? A common process inefficiency is the business unit's dependency on constrained IT resources to change a code within a daily supervisory or complaint tracking report. FINRA is changing the reporting requirements soon. If the technical team is not equipped to make these changes in a timely fashion, there is a financial and regulatory risk to the firm. If you are evaluating a complaint tracking system, an important functional requirement may be "easily configurable parameters and codes by non-technical resources." This additional requirement may be an additional cost, but the flexibility may mitigate potential non-compliance scenarios. There may not be a business or regulatory problem per se; however, the opportunity may be too compelling to pass up. There may be a better way to govern the organization, manage firm-wide risk, and keep the firm in compliance. You can and should also consider that not all efficiencies in GRC software are realized by reducing headcount and direct cost reduction. Increased executive confidence using a robust GRC management program may be difficult to quantify; however, you can point to the experiences of other firms to show a business benefit.

Background considerations include: Has the firm completed a comprehensive risk assessment that considers regulatory, market, reputational, operational, and technology exposure? Are the firm's business models and associated regulatory requirements clearly understood? Are the most impactful threats to the firm, the markets and the clients addressed in the risk management plan? Is the compliance management planning process an ongoing activity and is it in a form that it is flexible enough to meet and/or exceed regulatory scrutiny in a rapidly changing environment?

It is critical to fully understand and agree upon the contributing factors to the Governance, Risk and Compliance processes. These are the specific criteria that justify the business case and must be addressed with the software solution. Some of the key contributing factors are regulatory changes, regulatory scrutiny, increasing customer demands/waning customer trust, constrained subject matter experts, business model changes, new product offerings, firm growth, and recordkeeping needs.

Once these are defined, you can begin building a solid business case that is designed to garner executive level support at the outset, and board approvals when needed. A comprehensive, well-defined and agreed upon business case will lay the foundation for all future work, with successful implementation. The primary tenets for building the request for proposal ("RFP") are:

- A clear problem or opportunity statement
- Market, client and regulatory factors influencing the risk environment
- Overall business risk assessment

A thorough, well thought out business case analysis is only the first step. In order to gain executive level support to proceed, it is imperative that we clearly define what is being solved. Creating 'vision-lock' with the executive sponsor(s) will be key in driving any such initiative from the top down. Define the issues and challenges clearly, outline the business groups affected and explain how they are impacted, then identify who will be the key stakeholders for the project.

The process of selecting Governance, Risk and Compliance ("GRC") software is no different. The best implementations have a disciplined approach with process, people and technology aligned to achieve a common and well-defined goal.

Once stakeholders are identified, socialize the overall executive sponsor(s) goals for the project. Gain stakeholder consensus for the business case and how it will be developed and vetted. Accountability for the program can be further secured by gaining each leader's formal approval of the business case.

Finally, present the business case back to the executive sponsor(s), and be sure that you have aligned the business case with the sponsor(s)' initial and current vision.

Preparing for the RFP

A Request for Proposal is a technical component that can be utilized to help solve a business challenge. Prior to creating an RFP, there are many things to consider. Gathering accurate, clear requirements and asking the right questions of your vendor pool will help ensure the selection process identifies the best solution for your firm.

Defining Requirements

Requirements should be categorized as either functional or non-functional. Functional requirements describe specific behaviors of the system, such as a specific need for a business user of the application. Examples of functional requirements might be the ability to track edits to a risk assessment and highlight who made the changes, and what changes were made before the manager or risk owner accepts the change. The system needs this capability to support the user experience you want. A non-functional requirement is what is required to operate a system, such as the need to have the right architecture and appropriate information security controls.

Involve the information technology ("IT") team early in the requirements process. The IT team can help identify the appropriate technical environment for the planned software, ensuring compliance with your organization's IT policies. The IT team can also document system and non-functional requirements such as configuration, data and physical security, privacy, performance specifications, environment compatibility, peripheral equipment interfaces, vendor technical support, and scalability concerns.

Will this solution 'fit' on your current platform and within your organization? The business team will be accountable for defining the current state and predicting the future business model(s) and product(s). The compliance team should be consulted on recent and pending regulatory changes. This will help ensure the solution is configurable and scalable to meet your needs. For example: Does your firm intend to grow through acquisition of another firm? Can your system maintain and process additional transactions without slowing down the system's performance? Will your firm create new products? Can these new products be easily configured and supported?

It is important that all stakeholders are involved in a kickoff meeting to start defining requirements. Make it clear that it is vital that everyone participates, or it may result in missed requirements, scope creep, budget overruns, and delayed

time lines. The initial meeting can include a brainstorming session where key principals and requirements are gathered at a macro level. Once the requirements are documented, they should be circulated for all stakeholders to review and make sure all the high level requirements are covered.

The next session will be more detailed and should be scheduled for a longer period of time; it is common to have this meeting off-site or after hours. At some firms, this can be the most effective way to get all the stakeholders focused on the requirements, without distractions.

Always develop your RFP with existing and future business models in mind. It takes investments of both time and resources to implement change, and having an efficient means of implementing change will save both over the life of your software. Your business will continue to evolve. It will and should be able to evolve as you identify new requirements and opportunities. Will your software solution be able to evolve as well? It takes investments of both time and resources to implement change, and having an efficient means of implementing change will save both over the life of your software. It is important to ensure that the chosen software solution will provide your organization with solutions that not only meet today's requirements but also have the flexibility to meet the requirements of the future of the organization.

Key components of the solution and requirements assessment (examples):

- Functionality – What are the tasks that need to be performed by the system?
  Examples:
  - Ability to track investigations of a representative who received a complaint
  - Ability to report complaints to FINRA with preformatted data
- Business Process – What are the current and future states of the business?
  Example:
  - All representatives have unique rep codes which roll up to a branch; however, representatives can change branches. If a representative moves, the complaint should follow the representative and roll up to the new branch location
- Compliance must review all complaints prior to reporting them to FINRA and the sign off should be maintained by the system – What are the rules that need to be followed within the application?
  Examples:
  - Users cannot save a complaint record in the system until it is associated to a rep code and his/her current branch location
  - The system cannot submit the report until the Compliance has performed its review
- Usability – How does the system need to be used, and by whom?
- Scalability – Can the system grow with your company?
- Configurability – Can the system be easily configured by the user to meet the business model and regulatory requirements?
- Ability to stay current ('update-ability') – How does it keep up with the regulatory changes?
- Maintenance costs and support – Can it be efficiently supported?
- Intuitiveness and usability – Will it be readily adopted by the user pool?
- Vendor reliability – Does the company providing the software have sufficient experience, financial stability, and support infrastructure to ensure the success of the software?

Once the requirements are gathered, it is time to prioritize. To assist with this, requirements can be grouped into the following:

- Requirements which must have functionality
- Requirements which should have functionality
- Requirements in which functionality is optional

Also, consider creating a consistent scoring process for the responses, weighting the areas appropriately based on importance. The categories will help prioritize and assist with the vendor selection process. Vendors who can address the majority of your critical categories will be highly ranked. A vendor who cannot address the 'must-have' functionality should quickly be eliminated from the list.

Once all of the requirements have been defined, categorized, and prioritized, all of the stakeholders need to sign off on the document prior to moving to the next step.

Note: After the current and future conditions are modeled, if a software vendor only fits current conditions, you should strongly consider eliminating the vendor from the list.

Research

It is important to do your homework. When you are sending out your RFP, limit your evaluation to the select providers that you are willing to partner with. Identify the leaders and evolving leaders in the industry by talking to your network, reviewing industry journals, and searching vendor websites. Consider attending an industry conference that draws software vendors, to see what is available. When you are ready, reach out to vendors you may be interested in, and request a meeting and demonstration.

Web Meetings/Demos

Each vendor should be able to demonstrate their solution in person or via a web meeting. In these initial meetings, web meetings prove to be a cost-effective and efficient way to meet the team, see the product, and openly communicate with the vendor. Develop your initial reaction to how user-friendly the product appears to be, the quality, and the robustness of the product. The meeting may also give you some insight into their company, how easy the employees are to work with, and if they are customer service oriented.

Ideally, you should send an RFP to at least three but no more than four to six companies, as it can become cumbersome to manage the RFP process effectively. Thorough and targeted vendor research will be important.

What is Included in an RFP?

An RFP is a tool that allows the business to objectively evaluate each of the software vendors. The RFP should clearly outline the following: Background on the Buying Organization, Description of Challenges, Objectives, Guidelines, Key Milestones and Activities, Business and Technical Environment, Requirements, Evaluation Criteria, Testing Processes, Training Processes, Success Factors, Service Level Expectations and Total Project Cost.

Think of all of the ways you can be surprised by service from a vendor and make sure to address the key points. For example, will you be fully supported under your maintenance fees, or will there be a limited amount of support with hourly charges for "out of scope" support? How will upgrades be handled? Is software licensing on a corporate basis, per user, per machine, perpetual or annual?

How to Evaluate Vendors - Scoring

It is important to create an evaluation system for each response. This list should match all details listed within the RFP, and they should be prioritized, weighted and ranked per vendor. A simple sample of how to organize the scoring is listed below:

Table 1

Detailed Functional Requirement	Explanation of Functional Requirement	Priority	Vendor 1 Score (1-10)	Vendor 2 Score (1-10)	Vendor 3 Score (1-10)

A firm also needs to identify deal breakers, which are the criteria that will immediately eliminate a vendor. This must include security and privacy needs. For example, if a vendor is not able to encrypt and secure your data behind appropriate authentication controls, it should be eliminated from the list. Some deal breaker questions to ask are:

- Does the vendor have adequate disaster recovery programs that meet your objectives and tolerance for risk?
- What kind of background checks do they run on their employees and vendors?
- Do they have adequate physical security controls at their offices and data centers?
- How will they communicate and implement changes?
- Do they have a balance sheet and income statement that shows they will be able to support you, or can you own and manage the code if the business fails?
- If you run Oracle throughout your firm and they only run on Microsoft, will the cost to switch be prohibitive for your IT team, as they will have to support multiple database platforms?

Note: When requesting and evaluating pricing, the comprehensive Total Cost of Ownership ("TCO") should be considered. This includes the initial expense of the product and the ongoing expenses, which include maintenance, upgrades, service and support, networking, security, training, and software licensing. It is highly recommended to involve your finance and accounting partner(s) in the RFP preparation, scoring, and final evaluation processes.

All scores need to be shared with all the stakeholders, and they must sign an agreement of who are the top vendors.

Once you have identified the top vendors, it is now time to visit the vendors on-site.

On-site Review of a Vendor

Always do an on-site visit with the vendor. This will allow you to see a lot about their business that cannot be ascertained via a conference call, computer screen, or on a piece of paper. You need to understand their corporate culture, in addition to evaluating how they are developing their product. Do they have developers that are employees or are they offshoring their development? Do they have enough resources available to give you the support you need during an implementation or are their resources stretched too thin? Does the office look like they have been and intend to be in business for a long time? Is your vendor investing in their products or has the innovation stopped?

If the cost of travel makes on-site visits prohibitive, another option is hosting an evaluation day. This is when the top tier vendors visit your site, and each vendor is given a specific block of time to give a presentation to all the stakeholders at once.

It is important to include a procurement or third party contract management ("TPM") resource at these meetings; they are going to play an important role as the vendor is selected and contract terms are discussed.

Things to Keep in Mind

- Executive Sponsorship: Organize your thoughts to start the process and obtain key executive buy-in.
- Key Stakeholders & Performers: Gather your core team that can get you through the selection process with the right input, including generating, challenging, and prioritizing requirements.
- Clear Requirements: Define your requirements via a thorough and disciplined process that leads to clarity and executive buy-in.
- Do your Homework: Research potential vendors on the web, at conferences, and by reaching out to your network within the industry.
- Benchmark: What are others using? Leverage your industry network.
- Financial Stability: Ask the company to provide references where the company implemented a similar project.
- Build a Strong Project Team: Determine what skill sets and experience this effort requires.
- Interview resources. Have they done similar work before?
- Reliable References: Ask the vendor to provide references where they have implemented their software to similar competitors.
- Data Security: Understand how the vendor secures your data, and how it ensures that you can get it when you need it.
- Know the vendor team that you will be working with on the project, and make sure they have implemented this type of project in the past.
- Critically Assess Your Budget: Make sure that internal and vendor resource availability and costs are fully understood.
- Buy or Build: Make sure that internal and vendor resource availability and cost are fully understood. Differentiate between out-of-the-box functionality and functionality that can be built.
- Cost of Customization: Make sure that you believe the custom functionality can and will be built within the timeframe of your implementation, and have real incentives for the vendor to meet your deadlines and expectations.
- Privacy: Understand how your data may be used from a privacy and information sharing perspective.
- Manage Project Risks: Ensure all of the above are being managed and monitored throughout the project effort.

Conclusion

It is important to make a confident decision when selecting a software vendor. Mistakes can cost time, money, and can even end careers. Making the right decision can lead to efficiency, effectiveness, and recognition for a job well done, but there is more to a successful implementation than just selecting the right vendor. Carrying on the discipline that you used in the initiation and planning phases of the project by using a thorough testing process and a thoughtful communication and training plan will help eliminate problems in the execution phase.