DEVONWAY

WHITE PAPER

A General Guide to Contractor Assurance Systems

Abstract: Contractor Assurance Systems (CAS) are the regulatory compliance backbone of any government contractor performing work for the Department of Energy. As policies and procedures evolve, ongoing contractual compliance is critical towards maintaining a healthy relationship with the regulator, whose ultimate responsibility is to ensure that the mission of the contract is carried out with the most cost-effective expenditure of taxpayer funds possible. However, government contractors are not the only professional groups that need to ensure ongoing compliance with contractual obligations. Industries like construction, manufacturing, and energy/utilities companies all use some form of contractor or subcontractor work and require various forms of CAS to support said work. Thanks to the software innovations happening around CAS systems that were previously homebuilt, these activities aren't nearly as tedious. When evaluating a new CAS system, adhering to specific quality and security standards, as well as regulatory, procedural, and process integration best practices will go a long way towards mitigating risk. Future-proofing your CAS system from any issues associated with compliance, will also minimize the amount of costly oversight required.

Audience:

Many examples in this whitepaper come from organizations that perform work under a Department of Energy contract, but the frameworks and best practices discussed can apply to any entity that needs to maintain and prove high levels of quality and compliance to a stakeholder with oversight responsibilities, whether internal or external. In a DOE environment, contractors represent the organization that is doing work for the DOE, with the actual workers being labeled "employees", "subcontractors", or some other variation of the term. In a non-DOE related environment, "contractors" refers to the employees doing the work, and "subcontractors" represent the group of workers who are present for temporal purposes. However, the common denominator is that these contractors have a very specialized skillset and are subject to either regulatory, procedural, or organizational parameters that require some form of oversight and/or work verification.

What is CAS?

According to the United States Department of Energy, a CAS system is “a contractor-designed and utilized system to manage performance consistent with contract requirements. Once implemented, it will be used as a framework that engages the corporate parent to assess performance, provides data to the contractor’s management decision-making process, and allows the contractor to more effectively manage processes, resources, and outcomes. The system provides transparency between the contractor and DOE to ensure alignment across the enterprise to accomplish mission needs, and for DOE to determine the necessary level of Federal oversight.”

For many organizations, particularly organizations that partner with or provide services for government agencies, contractor assurance is a logistical cornerstone that requires just as much attention as operational workflows.

Best Practices

Assessments and Audits

Assessments and/or audits should be digital and linked directly to their requirements, the issues they revealed, and the full results of the activity. This creates superior reportability in easy-to-digest formats that can be easily shared with stakeholders to show the value and results of CAS assessment activities.

Inspections

Because inspections happen often, keeping an easily accessible and informative log of inspections and their respective details is optimal. Linking these logs of inspections to issues management systems will ensure continuity, reduce data duplication, and allow for easier identification and resolution of repeat root causes.

Issues Management

The above best practices don’t work if there is not an accountability system within the organization to ensure that work is being performed at the requisite quality level. A digital system that tracks every issue uncovered during a job or project allows for the above activities to be executed in an auditable way. This approach fosters continuous improvement, improves transparency and accountability, and provides an audit trail if there ever is an unfortunate incident.

Operability and Functionality Reviews

Operability and/or functionality reviews should be digitally triggered as part of the resolution of issues that impact worker safety where structures, systems, or components (SSC) are degraded or need to be modified. Engineers, operators, and others determine if the SSC is operable and what, if any, functional and compensatory measures are to be taken.

Work and Service Requests

Every time a work and/or service request is created, started, or completed, there should be a digitally triggered alert that notifies all stakeholders with whatever is happening during the process. Furthermore, integrating your CAS system with the third-party tools that contractors use to execute their work allows for not only maximum transparency, but increased accountability for auditing and risk mitigation purposes.

Lessons Learned

Creating a culture and environment where stakeholders can discuss lessons learned after executing the workflows mentioned above ensures that continuous improvement can be achieved and properly documented for training purposes. This will create a virtuous loop of mitigating risk, addressing issues expediently, and then implementing the lessons learned so any identified issues don't happen again.

Risk Management

Finally, using the above processes as inputs into an operational risk management program closes the loop in addressing patterns of issues, whether related to compliance or not. By taking a bird's-eye view of the organization's processes, an effective risk program is critical for enabling continuous improvement.

Quality Standards

Especially when hiring subcontractors to execute a job, ensuring specific quality standards is a must. But if a homegrown system has too many manual processes or inefficient frameworks, it can take a long time to train workers on those quality standards, which ultimately leads to a lower quality of work and difficulties in scaling one's organization. Having a streamlined system that embodies those quality standards can lower the time and cost of performing that ongoing training. To combat administrative issues, many organizations are coming up with a list of "must do's" when starting a job. These rules operate similarly to "quick start" guides in software or video games. The Campbell Institute, a group within the National Safety Council has outlined the following best practices or "must do's" in relation to contractor management:

Set KPI's to Start

While it may seem as simple as assigning "best practice" metrics to your quality goals, one size doesn't necessarily fit all. Best practices are a great place to start, but if you don't know why you're measuring something, what to measure becomes irrelevant. In other words, taking a step back and asking what goal you want your organization to achieve will not only allow it to find the right KPI's, but also what defines a successful outcome. That way, your organization isn't setting itself up for failure by setting unreasonably high goals, or conversely, underperforming by setting unreasonably low goals.

Set Clear Expectations for How Contractor Performances Will Affect KPI's

KPI's at a company and even a departmental level can't be achieved by a single individual or group. An organization's approach with contractors and subcontractors alike should be to set clear expectations by identifying early on how employees' actions and behaviors are measured and how those measurements roll into KPI's. By taking this approach, an organization can prevent cost overruns or errors due to miscommunication or misalignment of expectations.

Managing
CONTRACTOR EXPECTATIONS
24
PERMITS
Phone calls to your contractor should be returned same day.
Emails regarding plans and changes to orders take a few days.
The contractor will be in charge of obtaining needed permits.
Change orders and extra work should be mutually agreed-upon by the client and contractor.

Image Credit: Fix.com

Verify Employee Qualifications and Certifications

This seems obvious, but this principle is a matter of discipline and creating the right structures - particularly when using subcontractors. To use the comparison of building a house, subcontractors are the equivalent of a home's walls - they may not be the foundation, and can be removed as a company expands, but they are still necessary and keep the organization or "house" upright nonetheless. Rushing to hire subcontractors without taking the time to validate qualifications and/or certifications is a strategic misfire. If a subcontractor makes a mistake or goes rogue, having some sort of record keeping system to hold subcontractors accountable is a great way to mitigate risk.

Formalize an Escalation Plan

About risk mitigation, creating a formal escalation structure and process will allow for a clear direction when certain activities don't happen as expected. Not to mention, a formal escalation process will mitigate many potential lawsuits in the future. As a leader, the idea is to empower individual employees to be able to settle most issues amongst themselves, but also create several checks and balances as issues intensify, with appropriate oversight for each level. Striking a balance is key. You don't want to create anarchy by putting all disciplinary power in the hands of your employees and contractors. At the same time, you don't want to micromanage as that unnecessarily wastes time and productivity.

Create a Mitigation Plan

In tandem with a formal escalation structure and process, having a mitigation process for dealing with patterns in escalated issues is key to managing organizational risk. Preferably, each stage of the mitigation process should have an owner that evaluates the plan, determines actions, and serves as the point person for achieving management and organizational buy-in.

Create a Formal Assessment Framework

Typically, misalignment with contractor work comes during the expectation setting stage of the project. Often, organizations set unreasonable, inconsistent, or unsustainable expectations for their contractor or project groups. This sets up contractors to fail before a job even starts. To eliminate any inconsistencies and set up a project for success, organizations should create a formal assessment framework that can be shared with contractors prior to the start of the job. Beyond being a good management technique, this framework is also an investment in the future as consistent standards will allow more tenured contractors to train newer ones. DOE contractors do this by creating an assessment schedule – defined times where contractors are audited against NQA-1 standards. Industries can create similar assessment schedules that will eventually become a part of the quality standards for all incoming contractors and/or subcontractors.

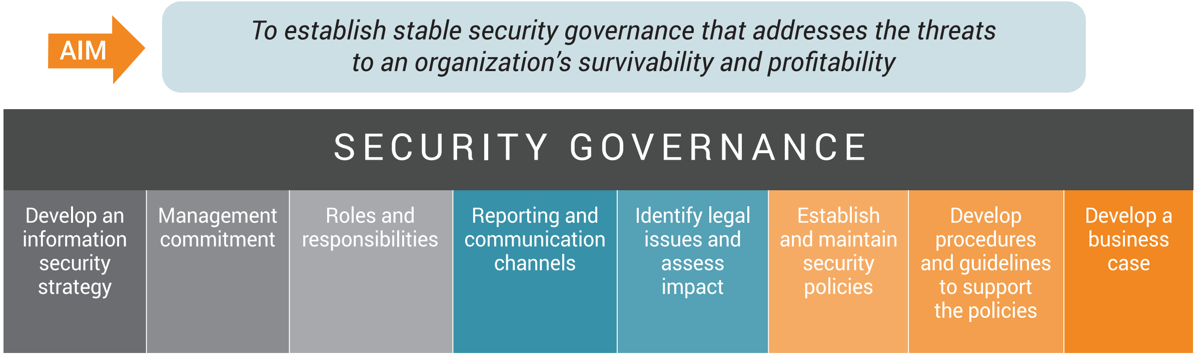
Commit to Continuous Improvement and Training

Ultimately, ensuring policies are adhered to involves leaders in the organization committing to continuous improvement and training. Subcontractors and employees alike will come and go. But by hosting frequent training and re-training sessions, you'll be able to ensure that your employee base not only knows policies and procedures, but also that your organization has a culture that values improvement. This will allow longer tenured employees to easily support and train employees with less tenure. Particularly with subcontractors, this approach will create a culture where they can easily integrate themselves into commonly framed projects.

Help Subcontractors Understand "Why"

Getting your organization, and subcontractors specifically to adhere to your culture can be as simple as honestly answering the question "why". Often, policies and procedures are interpreted as nothing more than rules that employees must follow. By constantly reinforcing "why" employees and subcontractors are engaging in certain practices, not only do you allow for those practices to be mapped directly to internal KPIs, but you also help encourage intrinsic motivation within your less connected employee base.

Security Standards



AIM

To establish stable security governance that addresses the threats to an organization's survivability and profitability

SECURITY GOVERNANCE

Develop an information security strategy	Management commitment	Roles and responsibilities	Reporting and communication channels	Identify legal issues and assess impact	Establish and maintain security policies	Develop procedures and guidelines to support the policies	Develop a business case

Image Credit: http://informationsecurityichigen.blogspot.com

Create Clear Governance Roles

While "governance" may be one of the most overused terms among corporate security professionals, when working with subcontractors especially, a clear governance structure is needed. Most organizations use a 3-tiered system (owner, admin, user), but if your workflows encompass multiple stakeholders or departments that have varying levels of access during the workflow process, a 3-tiered system may be too simplistic and broad. However, an organization can experience organizational simplicity, while still creating tight security control over their workflows. By following a 3-tiered system, but matching access levels to the stage of the workflow, organizations can still maintain tight security measures, but remain adaptable as the business grows.

Create Subcontractor Specific Security Protocols

This approach may seem unnecessary given governance controls based on user level but creating a separate role for subcontractors within your governance system or creating subcontractor level access with a standard user governance role can save a significant amount of time and frustration. Typically, subcontractor responsibilities are fixed, either at the departmental or company level. Despite this reality, many companies find themselves scrambling to grant proper access to a subcontractor when onboarding or offboarding for a project. This usually points to the company having institutional knowledge, but not codifying said knowledge in such a way that the project onboarding and/or offboarding process is smooth. By asking yourself what facets of the internal systems you want subcontractors to have access to and what their level of control will be, upon making these decisions, your company's IT team can automate those requirements in a way where adding or removing a subcontractor is as easy as a few mouse or keyboard strokes.

Manage Your Employee Ease Through Digital ID's

The above best practices about governance and security will get unwieldy at scale if there is not a consistent labeling convention for employees. Implementing a digital ID system for ALL employees makes the most sense. It still allows you to keep track of the number of employees with an ordinal level of organization. But digital IDs become most powerful when implemented into a directory system. The most common and widely used directory approach is known as Lightweight Directory Access Protocol (LDAP for short). Most commonly used as a part of Microsoft's Active Directory tool, LDAP is a server protocol for storing username information and passwords. Without getting too technical, this approach centers around relational databases, or databases that are tied together by a particular database attribute. This is where digital IDs tied to specific employees becomes helpful in managing and auditing employees assigned to certain projects. By implementing a digital ID system for all employees, it becomes easier to provision user roles for governance purposes, onboard and offboard employees, and create an audit trail to mitigate risk or improve on previous mistakes.

The above best practices and standards suggest the cultural infrastructure and organizational mindset to support an optimal work environment for subcontractors and permanent employees alike. The below tips will center around what day to day workflows, tools, and processes are needed when managing contract work.

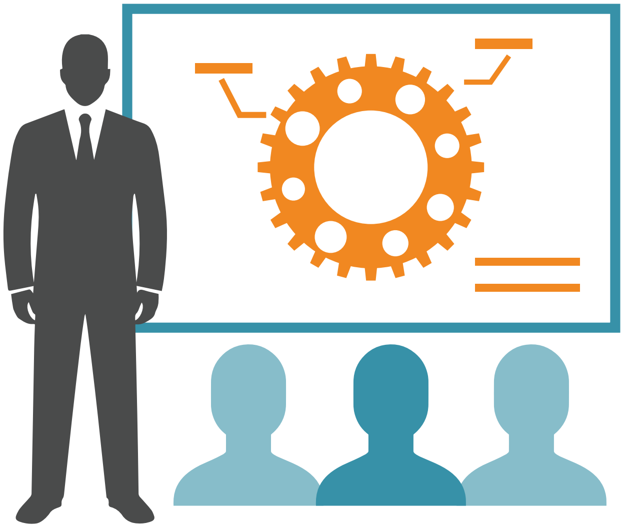


Image Credit: Safety Resources

Regulatory Integration

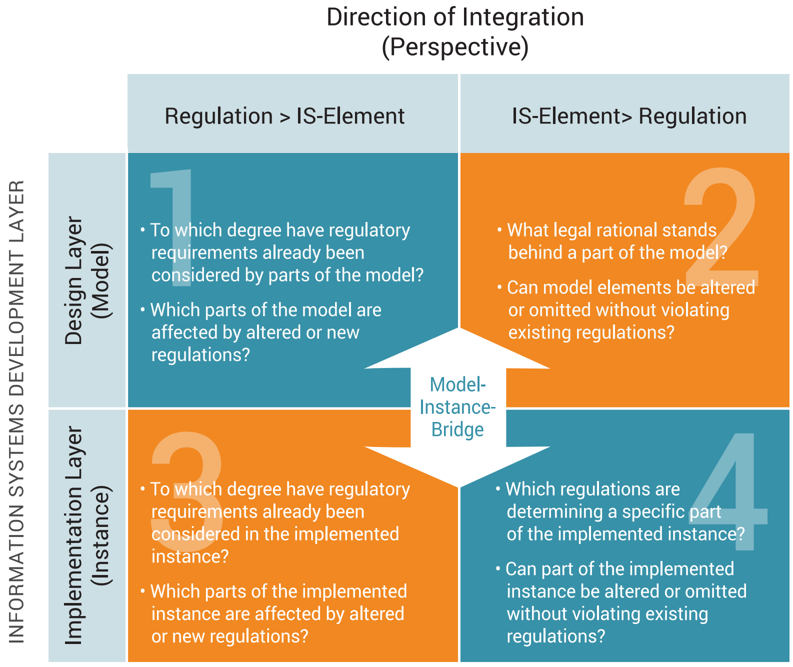
Design Your Organizational Workflows Around Your Industry's Respective Regulatory Agency

Below is a partial list of some of the DOE-specific regulations that businesses are required to adhere to when performing daily work:

- 10 CFR 830 - Nuclear Safety Management
- 10 CFR 851 - Worker Safety and Health Program
- DOE O 226.1B - Implementation of DOE Oversight Policy
- DOE O 227.1A - Independent Oversight Program
- NQA-1-2008 and 1a-2009 - Requirement 16, Corrective Actions
- NQA-1-2008 and 1a-2009 - Requirement 18, Audits
- NQA-1-2008 and 1a-2009 - Requirement 2, Quality Assurance Program

When integrating your organizational workflows with the above or similar regulations, simply trying to exactly match your workflows to each regulation not only is shortsighted but doesn't set your organization up for growth. Additionally, when expecting employees or subcontractors to adhere to these regulations out in the field, it doesn't make sense to expect them to memorize a series of regulations, no matter how experienced they are. Therefore, a framework designed around the best practices of your organization's regulatory requirements allows your organization to adhere to them, while remaining prepared for any changes in the future.

A group of researchers from the University of Muenster and University of Hildesheim did a study on Integrating Regulatory Requirements into Information Systems Design and Implementation. Their study led them to creating the following chart, which outlines some of the key considerations an organization has to ask itself in order to measure its degree of regulatory compliance. An important area to highlight is that it is equally crucial to test how an organization's policies affect a regulation as it is to test a regulation against an organization's policies – and to do both as early as possible in the process, i.e. during the design phase. This not only helps with the implementation of digital systems that confront immediate regulatory requirements, but also opens space to address future ones.



1
- To which degree have regulatory requirements already been considered by parts of the model?
- Which parts of the model are affected by altered or new regulations?

2
- What legal rational stands behind a part of the model?
- Can model elements be altered or omitted without violating existing regulations?

3
- To which degree have regulatory requirements already been considered in the implemented instance?
- Which parts of the implemented instance are affected by altered or new regulations?

4
- Which regulations are determining a specific part of the implemented instance?
- Can part of the implemented instance be altered or omitted without violating existing regulations?

Whatever the framework, adopting and adhering to a specific approach frees up the organization to create a digital "rulebook" of sorts that employees can refer to. When combined with a system that also digitizes best practice workflows that adhere to internal quality standards, an organization has a digital platform that subcontractors can use in the field as a reference point, and as a tool to complete their work.

Be Proactive, Not Reactive

When arming your workers in the field with the information they need to do their jobs, it's best to be proactive instead of reactive. Typically, organizations attempt to train their workers immediately after something goes wrong, whether it be internally or on the news. However, this approach has two main drawbacks:

1. It's shortsighted in nature and doesn't typically solve the root cause of any said issue
2. It's counterintuitive to true behavioral change – contractors will make sure to memorize any rule based on a scare tactic, but without adequate training will not be as vigilant with other equally important regulations

Instead, organizations should be more proactive about regulatory adherence. We have mentioned training approaches in a previous section, but another proactive activity would be to invest in software-based tools that make it easier to mitigate issues before they begin – for example, by reminding workers of regulatory requirements in the same system they use to execute work, such as a Pre-job Brief with specific instructions included in a Work Package.

Using CAS To Develop and Refine Procedures

Most high reliability organizations use written procedures or checklists to perform maintenance work and other operational activities. Applying outputs from elements of a CAS program, such as QA audits, surveillances, readiness assessments, management observations, issues management, and more, to the development and refinement of procedures, can markedly improve the quality and effectiveness of your work execution.

In parallel, the ability to feed data gathered from your procedure execution process back into your CAS system can shorten the feedback loop necessary to identify and resolve issues, especially those related to procedure adherence, which in many organizations is a significant portion of incidents.

Non-CAS Process Integration

Ultimately, while the frameworks above help make the structuring and planning of contractor-related work a lot more integrated and seamless, work still needs to be done to be sure that CAS is a part of a holistic approach to operational excellence. The following areas can typically be implemented quickly, with minimal structural changes.

Operability and Functionality Reviews

These should be triggered as part of issue resolution to help resolve issues that impact worker safety where structures, systems, or components (SSC) are degraded or need to be modified. Engineers, operators, or other knowledgeable personnel determine if the SSC is operable and what, if any, functional and compensatory measures are to be taken.

Work and Service Requests

Should be triggered as part of assessment completion or issue resolution. For example, Maintenance Work Requests should be easily generated and linked to the related issue or assessment. Integration with existing systems can provide two-way updates between a CAS system, any external systems, and a fast and simple employee user interface in order to address and resolve issues.

Inspections

Regular inspections, inventories, drill exercises, and similar activities are an important part of good operating procedure and a safety-conscious work environment. In a digitally based CAS system, these activities should link to an issues management tool for easy documentation and resolution of issues identified by these activities.

Action Tracking

The best approach is to create a simple way for managers and organizations to create, manage, track, and report on general actions and agendas. This tool should also have a weighting system for important actions that may not rise to the level of "issues" that relate to safety, health, quality, or emergency management. This app can be linked to issues or assessments if desired.

Special Communications

Special communications in an optimal CAS system should be built for many specialized scenarios, such as spill notifications, safety bulletins, operating experiences, and more. Communications should enable fast, easy input of relevant information for a site-customized email notification. Communications should also be linked to issues management to automatically create an issue when the notification is sent or approved or vice versa. Custom distributions can be built on-the-fly or site-managed distributions can be used.

Conclusion

Whether you're performing work as a contractor, or managing your own contractors or subcontractors, having an effective process framework and digital system for ensuring that work is performed efficiently, safely, and in compliance with your contractual obligations is critical to maintaining a long-term, healthy relationship with your customers. Even if you have many CAS elements already in place, we hope that the preceding guide has given you some ideas on ways to further maximize their potential.

Appendix

https://www.nsc.org/Portals/0/Documents/CambpellInstituteandAwardDocuments/WP-BestPractices-ContractorMgmt.pdf

https://federalnewsnetwork.com/commentary/2019/05/security-awareness-training-dont-exclude-contract-workers/

https://everifile.com/blog/5-vendor-security-best-practices-18-ss1/

https://www.dol.gov/ofccp/TAguides/sbguide.htm

http://diligent.com/wp-content/uploads/2016/10/WP0018_UK_Five-Best-Practices-for-Information-Security-Governance.pdf

http://www.wifcon.com/discussion/index.php?/blogs/entry/3446-cybersecurity-best-practices-for-small-business-contractors-%E2%80%93-part-2/

https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html

https://people.apache.org/~elecharny/ldapcon/Andrew%20Findlay-paper.pdf

https://pdfs.semanticscholar.org/977f/d7ca0da48fa9ed72e990b3bc19a3d4dfd316.pdf

https://pdfs.semanticscholar.org/73bb/a46d5b66b74f08e5ba295e2b925430f38b2f.pdf

DEVONWAY

devonway.com
1.888.DevonWay