



DIGITAL GOVERNANCE SERIES

County Leaders: How to Drive Information Technology Success in Your Organization

As a county leader (Board Supervisor, County Administrator, Department Head, or Manager), do you know what your information technology (IT) department's priorities are, what they are working on, and how satisfied your organization is with the IT services and solutions they deliver? Do you understand the current cyber-risk level you face and the cost and lifecycle of your IT product and solution portfolio, so that you are properly budgeting for its replacement? Well-functioning IT governance delivers all these answers, providing overall IT business alignment and oversight by non-technical county leaders – who pay for and use all the IT products in the first place. Governance comes from the Greek word *Kubernema'n* "to steer a ship: the process of continually orienting and adjusting." It is said that a failure in an IT project is a failure with IT governance. County leadership outside of IT should own and drive effective IT governance.

Selecting, implementing, and managing IT products and solutions has become a major leadership and management issue, strategic element, and an increasing budget demand across all levels of government. Just as with any other county operational area like human resources, fleet management, finance/accounting, etc., information technology management and operations can be well executed, very poorly executed, or just be simply mediocre. Any government organization regardless of size can end up with any of these three options. The level of engagement from top-level county leadership with your county's IT governance drives what IT performance and quality you will have.

Emerging Issues that Require Strong IT Governance Include:

Cybersecurity – This is a growing threat to all counties and IT risk management needs to be a fundamental function across every department and every IT project and product procured. This spans all county service, data, employee, and IT system aspects, from new employee onboarding to vendor contract language and cyber-insurance requirements. The negative operational impacts from a cyber-attack are increasing as well for remediation costs and county services interruption. State and Federal regulatory requirements for criminal justice, health, citizen private information, and credit card transaction data seem to increase annually and come with growing noncompliance fines. The cyber insurance market is quickly maturing to not pay claims if a jurisdiction has not been adequately diligent and proactive in their cybersecurity efforts.

Changes in IT procurement models - For the past 10+ years, the IT industry has been slowly shifting how they price and sell their products from an upfront capital expenditure model where you purchase and own the solution/product, to an annual operational expenditure model where you pay to “use” the solution/product. This is the “cloud” services model and can either decrease or increase total cost of ownership over the long run. This impacts how counties plan and budget for IT investments with more costs shifting to annual operational budgets and with lower one-time capital procurement costs. Counties should have a five-year IT infrastructure replacement plan just like we do for roads and facilities. Enticing short term product cost savings can commonly lead to much larger total cost of ownership in the 5-to-10-year planning horizon in this new IT industry product pricing model.

Consumerization of IT, increasing shadow IT – The availability of cloud-based employee productivity and collaboration tools has exploded. They are user friendly and can be easily procured with a credit card, bypassing formal IT procurement review and recommendation. This is called “shadow IT,” when employees and departments implement their own technology outside of the county established IT procurement processes. While many of these tools are fantastic, some are not, and they all can come with significant risk to the larger county organization and technical/data environment. Many of the tools are not created to address the higher standard needs of a government organization for cybersecurity and regulatory compliance. This creates risk to the county and it is the Board of Supervisors that ultimately pays the 7 figure HIPPA negligent breach fine, not the county department or employee who put sensitive regulated data in an unsecure cloud tool they put in place on their own. These tools can also duplicate functionality and increase costs when your county already has a similar secure solution in place. Lastly, they may not be sustainable for very long, as these tools rely on non-IT individual staff to support and are therefore vulnerable to lose that support during employee transfers or turnover.

Results of Poor Execution, or an Overall Lack, of IT Governance:

- Recurring delays in the delivery of IT projects.
- Increased organizational exposure to unnecessary IT risks.
- IT decisions made without business strategy in mind, which can result in problems.
- Business misalignment or frustrations over not understanding what IT is doing for the business, whether IT is purely operational or strategic, and whether the IT service level is high.
- IT projects that do not solve a business issue.
- Compliance failures from all sides including data protection regulations, software licensing compliance, and State and Federal regulations.

Well-Functioning IT Governance:

Without the proper ongoing care and feeding, IT governance can fall into a process as just another committee that slows down the organization with little value. While poorly designed and run committees can certainly do that, good governance processes put in place the organizational infrastructure for IT related issues to be discussed, evaluated at all angles, vetted by all stakeholders, and for timely smart IT investment decisions to be made and moved forward.

There are four objectives that a well-functioning IT governance delivers:

1. **Increased County IT Value.** Provides alignment between the IT department, IT investments, and county departments' needs and strategies, including transparency.
2. **Management of IT Performance.** Ensures IT services and products are being delivered to organizational expectations.
3. **Management of IT Risks.** Establishes standards and assigns accountability.
4. **Management of IT Resources.** Develops a comprehensive portfolio of IT assets, investments, and priorities over the lifecycle of IT products and solutions.

Additionally, when an IT project goes to the Board of Supervisors for procurement approval, a well-functioning IT governance will ensure that the following has already been evaluated and addressed:

- The initial required funding and the total cost of ownership and funding over the life of the solution;
- Data and cost sharing, employee access, and business process impacts/optimizations across all affected stakeholders;
- Evaluation for cybersecurity, IT risk, and regulatory and disaster recovery requirements; and
- That the project aligns with county enterprise IT objectives and standards, and complies with county procurement and contract requirements.

IT Governance Roles and Responsibilities Across the Organization

- **Board of Supervisors** – Ensure IT governance is established and functioning. The Board reviews and approves IT contracts and procurements that have been approved by the IT governance committee. Governance will not function optimally without this top-level support and the connection to project/funding approval.

- **County Administrative/Executive Officer** – Functions as the executive sponsor and chair (or designee) of the top-level IT governance committee. The County Administrator works with the IT Director to create and adjust the governance structure and promote organization wide participation. It is the role of the County Administrator to promote an enterprise perspective and priority approach.
- **County IT Director** – Implements, facilitates, and supports the ongoing IT governance framework and committee(s). The County IT Director must actively pursue and support the four IT Governance objectives listed above.
- **County Department Heads** – Actively participate in the governance processes and committee meetings, leading IT committees and project teams. Department heads are responsible for sponsoring and owning their IT projects, products/solutions and initiatives. They must also ensure their Department and employees follow established cybersecurity, project, and product standards.
- **County Managers** – Must understand the IT governance structure and processes, specifically as it relates to IT procurement and contract processes, and employee cybersecurity training requirements. County Managers should work with peers in other departments on data sharing, business process optimization, and cost sharing opportunities.

IT Governance Framework

There is no one size fits all approach to implementing a well-functioning IT governance in your county. In Nevada County, we utilize a three-tier framework.

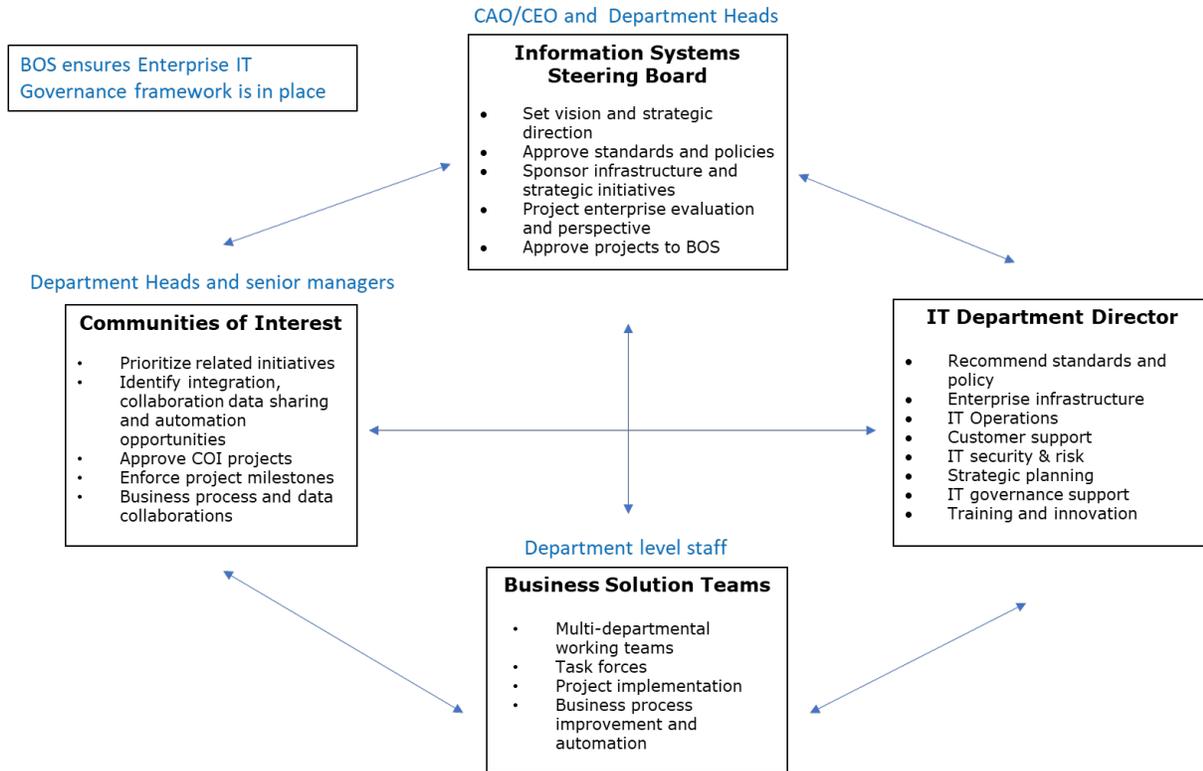
- **Business Solutions Teams (Bottom Tier)** – The bottom tier is made up of Business Solution Teams (BST) that form and dissolve as needed to work on specific projects. BST membership is comprised of staff members who actually work with the technology and data, own the business processes, and who will implement the project.
- **Communities of Interests (Middle Tier)** – The middle tier are four Communities of Interests (COI) committees which are groupings of similar activity departments. Every county department participates in one or more COIs. COIs are chaired by member department heads. As customers, data, and business processes commonly cross departmental borders, new IT solutions should be evaluated and selected with a collaborative perspective to ensure all impacted stakeholders are engaged and issues evaluated. COI's are Justice & Public Safety, Community & Social Services, Internal Services, and Land & Environmental Management. The COI's function is to promote

member collaboration, then to identify, prioritize, and approve COI projects, tracking them through completion.

- **Information Systems Steering Board (Top Tier)** – The top-level tier is the Information Systems Steering Board (ISSB) which is sponsored by the CAO/CEO and chaired by her/him or their designee. COI committee chairs make up the voting membership, thus the entire governance process rest in the hands of the business unit department heads, the users of IT. One role of the ISSB is to evaluate COI project requests on an enterprise perspective and give approval so the procurement request can then go to the Board of Supervisors for their final authorization. **At minimum, small counties should have a top-level active committee that meets regularly, then form specific project teams as needed.**

EXAMPLES: Three-Tiered IT Governance Framework





Next Steps

There are many resources and best practices you can leverage to implement an IT governance solution that works for your county. The most important part is that your county has a well-functioning, active IT governance framework in place and that all county IT projects go through it. IT governance handles business issues and strategies, not the deep technical IT wizardry. As such, they require top level sponsorship and non-IT county leadership’s active participation. Ultimately, any failure with IT is rooted in a failure of IT governance.

AUTHOR



Steve Monaghan is Nevada County’s Chief Information Officer (CIO) responsible for planning, organizing, and directing the county’s overall information technology efforts and investments. His efforts have resulted in significant recognitions and awards for his leadership in the IT industry and, during his tenure, Nevada County has received numerous awards for technology leadership and excellence. In addition, Steve created the CSAC/CCISDA County Technology Executive Credential program, serves on the Advisory Board for the California State University, Chico Cybersecurity for Executives program, and serves as a member of RCRC’s Broadband Advisory Committee. Find additional information about Steve [here](#) and connect with him directly at steve.monaghan@co.nevada.ca.us