



# LEXINGTON

## RFP-12-2026

### Deloitte Consulting, LLP

### Supplier Response

#### Event Information

Number: RFP-12-2026  
Title: Information Technology Consulting and/or Technical Services  
Type: Request For Proposal  
Issue Date: 3/20/2026  
Deadline: 4/20/2026 02:00 PM (ET)

#### Contact Information

Contact: Todd Slatin  
Address: Central Purchasing  
Government Center Building  
Room 338  
200 East Main Street  
Lexington, KY 40507  
Phone: (859) 2583320  
Fax: (859) 2583322  
Email: [tslatin@lexingtonky.gov](mailto:tslatin@lexingtonky.gov)

## Deloitte Consulting, LLP Information

Address: 306 West Main Street

Frankfort, KY 40601

Phone: (614) 364-2187

ONLY ONLINE BIDS WILL BE ACCEPTED! By submitting your response, you certify that you are authorized to represent and bind your company and that you agree to all bid terms and conditions as stated in the attached bid/RFP/RFQ/Quote/Auction documents.

Geoffrey Giancarlo

*Signature*

*Submitted at 4/20/2026 10:51:07 AM (ET)*

[ggiancarlo@deloitte.com](mailto:ggiancarlo@deloitte.com)

*Email*

## Response Attachments

---

**Deloitte - RFP 12-2026 - Information Technology Consulting and or Technical Services.pdf**

Deloitte response to RFP-12-2026.

# Deloitte.



**Deloitte Consulting, LLP  
Response to RFP 12-2026 –  
Information Technology Consulting  
and/or Technical Services**

**TRANSMITTAL LETTER**

April 20, 2026

Todd Slatin  
Central Purchasing, Government Center Building  
200 East Main Street, Room 338  
Lexington, KY 40507

Dear Mr. Slatin,

Deloitte Consulting LLP (“Deloitte<sup>LLP</sup>”) is pleased to submit our response to RFP 12-2026 put forward by the Lexington-Fayette Urban County Government (“LFUCG”) requesting Information Technology (IT) and/or Technical Services.

Deloitte brings an unmatched breadth and depth of public and private sector experience to help address your mission-critical needs and offer innovative solutions. Those experiences make us the ideal partner for such an important strategic initiative.

Consider the following:

**We have unparalleled experience in the public sector.** No other consulting firm has as deep of a knowledge base as Deloitte. Further, no other firm is as committed to helping the public sector solve its most complicated problems; we provide extensive knowledge, frameworks, and methodologies, unparalleled assets and tools, and top-notch staff to augment our clients’ teams.

- We have served US public sector state government clients for **more than 49 years**
- We currently serve **44 of 50 US states** as well as the Commonwealth of Puerto Rico and the District of Columbia
- Deloitte has 3 offices in Kentucky Lexington, Louisville, and Frankfort.
- Deloitte was named the **leader in US State & Local Government Consulting** based on capabilities by Kennedy
- We have over **12,000 practitioners** supporting federal, local, and state government clients and engagements

**We have deep and broad technology consulting capabilities.** Deloitte brings deep technology consulting capabilities to help organizations translate strategy into measurable outcomes while managing complexity and risk. Our integrated approach spans technology strategy and operating model design, governance frameworks that strengthen decision-making and accountability, risk and resilience services that enhance cybersecurity, continuity, and regulatory readiness, project services that improve delivery discipline from planning through execution, and training services that build the workforce capabilities needed to sustain change. By combining strategic insight,

## Response to RFP 12-2026 – Information Technology Consulting and or Technical Services

implementation experience, and practical program leadership, Deloitte helps clients modernize with confidence, improve performance, and create durable value across the enterprise.

**We know the Commonwealth and are committed to the greater Lexington area.** Deloitte is not just a firm that does work in Kentucky, we are part of Team Kentucky. We are proud of the work we have done to help improve the Commonwealth, and uniquely the work we do that helps so many families, children, and vulnerable populations. The Commonwealth has trusted us with the most complex projects and the most challenging problems, and we have been honored to work side by side in achieving great accomplishments.

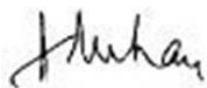
Deloitte has supported the University of Kentucky through both consulting work and a broader institutional relationship, including being selected as a consultant for UK's Project Accelerate and contributing to studies related to governance and curriculum review. Deloitte also brings strong technology consulting capabilities in Kentucky across systems engineering, cloud, enterprise technology, and analytics and AI, and its work with other higher education institutions in the state demonstrates experience relevant to university transformation efforts. In addition, Deloitte maintains a strong talent and recruiting relationship with UK's Gatton College of Business and Economics, where it is recognized as a consistent hiring partner and a major recruiter of MBA graduates.

From our project delivery to our community involvement, our goal is to make Kentucky a better place to live, work, and raise a family. Our more than 250 employees who live in Kentucky are involved in community organizations ranging from the Louisville Orchestra to Junior Achievement. We support the work of civic organizations all around the Commonwealth, from Shaping Our Appalachian Region (SOAR) to the Bowling Green Chamber of Commerce. Deloitte has had a strong footprint in Kentucky for over 50 years based in 4 offices: Lexington, Frankfort, Louisville, and Northern Kentucky/Cincinnati. We are proud to see impacts in all 120 Kentucky counties because for so many of us, Kentucky is our home.

We continue to provide jobs to Kentuckians through our campus recruitment at seven Kentucky universities and are annually one of the top recruiters at the Gatton College of Business at the University of Kentucky. Five years ago, we set up an innovative partnership with Kentucky State University encompassing scholarships and an innovative mentoring program that provides opportunities for Kentuckians of all backgrounds. Our firm and employees are engaged with numerous other charitable endeavors including the Stewart School, Habitat for Humanity, homeless shelters, and many others.

We look forward to continuing to remain engaged with the Commonwealth throughout this process. If you have any questions, please contact me at +1 (919) 264 6925 or [mkumar@deloitte.com](mailto:mkumar@deloitte.com).

Very truly yours,



Mohan Kumar, Managing Director, Deloitte Consulting LLP

# Table of Contents

Executive Summary.....	2
5. Vendor Requirements .....	5
6. Engagement Model & Deliverables.....	38
7. Attachment B – Cost of Services .....	39
8. Company Information .....	41
9. Additional Information and Contract Terms.....	44
Appendix A: Deloitte Standard Contract Draft .....	45
Appendix B: Workforce Analysis Form.....	52
Appendix C: Affidavit .....	53
Appendix D: Equal Opportunity Agreement.....	56
Appendix E: LFUCG MWDBE Participation Forms .....	58

# Executive Summary

## A Firm Committed to Kentucky

Deloitte has a long-standing commitment to Kentucky grounded in work that touches some of the Commonwealth's most important public services. For the state, which includes support around kynect benefits and the broader benefits-delivery ecosystem, where Deloitte works with the Commonwealth not only on the information technology applications but on the training and organizational change management to bring these applications to end users as well as overall project management and strategy services. Our earlier work on kynect likewise helped support integrated eligibility for programs such as Medicaid, SNAP, and TANF—work that matters because it helps connect Kentuckians to critical services with greater consistency and efficiency.

That is the same spirit we will bring to Lexington. We are ready and excited to help the city advance its most important endeavors, whether that means modernizing resident services, improving operations, strengthening data-driven decision-making, or helping complex initiatives move from strategy into execution. Our approach is to work side by side with city leaders and staff, bringing not just ideas, but the implementation discipline, change management, and accountability needed to turn priorities into results.

As a longstanding partner with the Commonwealth, we have an established local talent presence in numerous cities and towns in Kentucky who will be available to support LFUCG with requested engagements. We have offices in the hearts of Lexington, Louisville, and Frankfort where our teams work to deliver measurable impacts for Kentucky. In addition to these distinguished Kentucky team members, Deloitte can and will leverage its nationwide network of professionals based on the expertise and experience needed for the requested engagements from LFUCG.

Most importantly, we would come to Lexington as a true partner. That means listening first, aligning around the city's goals, and building solutions that fit Lexington's realities rather than forcing generic playbooks. We believe the strongest work happens shoulder to shoulder with our clients, and we would welcome the opportunity to help Lexington deliver meaningful results for its residents, workforce, and future growth.

## Helping Kentucky Higher Education Succeed

That commitment extends to Kentucky higher education. The University of Louisville completed Workday HR in 2023 and Workday Finance in 2025 as part of a broader enterprise modernization effort, and Deloitte continues to bring Workday implementation capability in the Louisville market as institutions pursue more connected HR, finance, and reporting environments. At Western Kentucky University, Deloitte's Candidate360 applicant analytics solution used predictive analytics and historical data to generate actionable insights in just 12 weeks, contributing to enrollment growth and increased expected net tuition revenue.

The University of Kentucky is undertaking a broad transformation to expand its reach, strengthen operations, and modernize the way it serves students, faculty, staff, patients, and communities across the Commonwealth. Recent milestones—including the acquisition of King's Daughters and St. Claire, modernization of academic governance, and launch of the Advancing Kentucky Together Network—reflect UK's ambition to extend access,

improve institutional effectiveness, and create a more connected enterprise. Deloitte is supporting UK across these priorities by helping translate strategic vision into executable operating models, enabling technologies, and sustainable organizational change.

A key focus of this work has been supporting the integration of UK King's Daughters and UK St. Claire into the broader UK enterprise. Deloitte is helping bring these organizations onto centralized platforms, including Workday, UKG, Epic, and SailPoint, to improve consistency, strengthen governance, and create a more unified foundation for clinical, workforce, and identity management operations. This work is critical to helping UK realize the full value of these acquisitions while expanding healthcare access in the northern part of the Commonwealth.

Deloitte is also supporting the establishment of Champions Blue LLC, a new entity designed to oversee UK Athletics. Our support includes revamping athletics job architecture, integrating select functions into a shared services model, and deploying Workday and UKG across the enterprise to enable a fully operational Champions Blue by July 2026. In parallel, Deloitte is helping UK advance Integrate Blue, the University's initiative to centralize nearly 20 shared service functions, including support for integrating decentralized IT and MarCom staff by July 2026.

In addition, Deloitte is supporting the design and staffing of the new Beyond Blue entity, which will provide a collaborative framework for UK shared services. Together, these efforts position UK to operate with greater consistency, efficiency, and scalability across academic, administrative, healthcare, and athletics functions. Across each initiative, Deloitte's role is to help UK build an integrated enterprise that can better support growth, improve service delivery, and extend the University's impact throughout Kentucky and beyond.

## **Collaborating for AI Impact**

Deloitte brings the City of Lexington a distinctive combination of AI, Cyber, cloud, and governance capabilities that directly align to the City's modernization priorities. Our approach in the emerging AI space is designed not simply to introduce new technology, but to help public sector organizations improve operational effectiveness, enhance service quality, and establish a scalable foundation for long-term transformation. Through our Government & Public Services practice, we integrate Artificial Intelligence & Data, Cyber, and Trustworthy AI capabilities so that innovation, security, and operational discipline advance together rather than in silos.

Our qualifications in AI are substantial and rooted in delivery at scale. Deloitte executed its first public sector AI project in 2015 and has since implemented more than 120 AI solutions across 30+ states, supported by 20,000+ Government & Public Services professionals and 10,000+ AI specialists. We have also conducted 160+ labs, demos, conferences, and policy discussions across 44 states and delivered 20+ AI and data strategy labs for public sector clients. That scale gives Lexington a partner with the depth to move from vision to implementation while reducing execution risk and accelerating value realization.

Deloitte's eminence is reinforced by market recognition and a strong alliance ecosystem. Deloitte was recognized as the leader in the IDC MarketScape: Worldwide Artificial Intelligence Services 2025 Vendor Assessment and by Gartner as a worldwide leader in data and analytics. Our alliance strength includes 28,000+ Azure and business application certifications and 30 years of experience delivering Microsoft-based mission-critical solutions to government, including more than 240 government projects in the last three years. For

Lexington, that means access to a partner that can combine AI innovation with practical execution across hybrid cloud and Microsoft Azure IaaS environments.

Deloitte's approach is equally differentiated. Our structured Trustworthy AI framework spans Intake and Assess, Develop and Deploy, and Operate and Monitor, with explicit focus on governance, privacy, transparency, bias, accountability, reliability, and security throughout the AI lifecycle. This model is designed to help organizations identify and prioritize use cases, implement risk and control frameworks, and continuously monitor performance, issues, and compliance. For Lexington, that disciplined lifecycle can help improve service quality, reduce downtime and support costs, and create AI-enabled modernization that is supportable, auditable, and resilient from day one.

We translate that framework into practical operating capability through real-time monitoring, automated notifications, workflow routing, approval management, dashboards, and AI risk assessment processes that evaluate safety, privacy, security controls, model design, data used, end-user impacts, and cybersecurity posture. These capabilities are especially relevant to Lexington's goals of improving operational effectiveness and maximizing return on technology investments because they enable the city to standardize oversight, identify risk earlier, and make better decisions about where to scale, improve, or retire technology investments.

Deloitte's prior work for other public sector clients further demonstrates this experience. For an Emergency Management Agency, Deloitte served as AI Governance Project Lead, facilitating a cross-agency AI visioning lab, developing a future-state AI vision and roadmap, and creating an AI guidebook aligned to standards such as NIST and GAO to embed AI governance into existing processes and policies. For a large state Employment & Family Service Agency, Deloitte developed a GenAI use case for intake risk assessment, piloted it across priority use cases, and compiled GenAI usage guidelines to support both governance and workforce adoption. These examples demonstrate Deloitte's ability to help public sector organizations move from concept to governed implementation in a practical, operationally useful way.

Security and resilience are also central to Deloitte's value proposition. Deloitte operates one of the largest cybersecurity practices globally, with deep benches of certified professionals and experience spanning risk assessment, security architecture, and leading cybersecurity frameworks. Deloitte has also been recognized as a global leader in Managed Detection and Response and Cloud Security Services, as well as the No. 1-ranked provider by revenue in Gartner's Security Services report. Combined with our Trustworthy AI capabilities in risk assessment, control implementation, data validation and protection, application risk management, real-time monitoring, and continuous testing, these position Deloitte to help Lexington strengthen the security and resilience of data and systems while modernizing its network, cloud, and endpoint environment.

Taken together, Deloitte offers Lexington more than AI credentials: we offer an integrated modernization partner. Our AI qualifications, Microsoft and cloud alliances, Cyber depth, and proven governance-led delivery approach position us to help the city improve operational effectiveness and service quality, reduce downtime and support costs, strengthen the resilience and security of systems and data, maximize the return on technology investments, and accelerate modernization through hybrid cloud and Azure-based infrastructure. In short, Deloitte can help Lexington adopt emerging AI in a way that is secure, practical, and tightly aligned to the city's service, operational, and technology objectives.

## 5. Vendor Requirements

### 5.1 Technology Assessment

---

**RFP Reference: 5.1 Technology Assessment**

Proposals must include responses to Attachment A: Technology Capabilities listing applicable technologies and competencies. Vendors should also include additional relevant technologies not listed that could benefit LFUCG.

---

Deloitte is not proposing services for the items listed on Attachment A.

### 5.2 Software Development

---

**RFP Reference: 5.2 Software Development**

If proposing software development services, include:

- Application programming methodology
  - Development life cycle
  - Documentation standards
  - Secure development practices
  - Preferred stacks/frameworks and tooling
- 

Deloitte is not proposing software development services.

### 5.3 Consulting Services

---

**RFP Reference: 5.3 Consulting Services**

If proposing consulting services, provide an overview of each area offered, including:

- Experience
  - Approach
  - Security & Resilience
  - BC/DR
- 

Deloitte brings a long-standing heritage in professional services—rooted in the mid-19th century—and has evolved into a global network that serves complex, highly regulated organizations. That history matters for government and public sector clients because it reflects disciplined delivery, mature governance, and an institutional commitment to quality and integrity. For decades, Deloitte practitioners have supported public missions across federal, state, local, and higher education organizations, helping leaders modernize operations while sustaining public trust and service continuity.

A distinguishing element of Deloitte’s Government & Public Services (GPS) practice is its sustained focus on mission outcomes, not just project outputs. We align strategy, policy, operations, and technology to help agencies improve citizen/customer experience, strengthen program performance, and demonstrate measurable results to oversight bodies. Our teams are accustomed to the realities of public sector work: multi-stakeholder environments, appropriation-driven planning, procurement constraints, transparency expectations, and the need to maintain services during change.

Deloitte differentiates itself through an integrated, end-to-end consulting capability that spans strategy and transformation, program and portfolio management, process and organizational design, data and analytics, digital and cloud-enabled modernization, and cyber risk and resilience. Just as importantly, we bring the ability to connect these capabilities into one coherent approach—so an operating model redesign, for example, is directly translated into measurable performance metrics, enabling technology decisions, workforce impacts, and a practical implementation plan that can stand up to audit and oversight scrutiny.

In the government context, delivery rigor and risk management are often as important as innovation. Deloitte’s approach emphasizes clear governance, disciplined requirements management, proactive risk/issue/dependency management, and transparent reporting that supports leadership decision-making. We use fit-for-purpose delivery methods, whether iterative approaches (e.g., Agile delivery) or stage-gated controls—while maintaining documentation, traceability, and quality assurance practices aligned to public accountability needs. This balance helps agencies move faster where they can, without compromising compliance, security, or operational stability.

Another distinguishing element is Deloitte’s ability to mobilize multi-disciplinary teams that combine domain depth (e.g., health, human services, defense, civilian, transportation, and finance missions) with technical specialization and change leadership. We invest in change management and adoption—communications, training, role design, and frontline enablement—so solutions are used effectively after go-live. When appropriate, we also operate within broader ecosystems, teaming with client stakeholders and partners to bring specialized capabilities while maintaining a single, accountable delivery backbone.

Finally, Deloitte’s reputation is built on enduring client relationships and a culture of stewardship. Bringing candor about tradeoffs, a bias toward sustainable solutions, and a commitment to ethics and quality. Government and public sector leaders face competing priorities—mission urgency, budget constraints, evolving policy, and heightened public expectations. Deloitte differentiates by helping clients make informed choices, execute reliably, and institutionalize capabilities so improvements persist beyond the project—strengthening the agency’s ability to deliver better outcomes for the people and communities it serves.

## **Strategy & Architecture**

### **Approach**

Deloitte’s approach to IT strategy and architecture starts with a simple premise: **technology decisions should be driven by mission outcomes**—not tools, platforms, or point solutions in isolation.

To make this practical and repeatable, we use a structured, end-to-end approach that helps leaders move from **current-state fact base** to **target-state vision** to **executable roadmap**.

<b>Step</b>	<b>What we do</b>
<b>Confirm goals and constraints</b>	Align stakeholders on the outcomes the effort is intended to achieve (e.g., improved service delivery, reduced downtime, stronger security), plus constraints such as budget, procurement timelines, and required standards.
<b>Document the current environment</b>	Create a fact base of the current technology landscape: key systems, integrations, data flows, vendors, operational pain points, and risks.
<b>Define a realistic target state</b>	Describe what the future environment should look like at a practical level, including standards, patterns, and which capabilities should be shared vs. specialized.

Step	What we do
<b>Build an executable roadmap</b>	Translate the target state into a sequenced plan with milestones, dependencies, decision points, and measurable outcomes—designed to stand up to oversight and audit needs.

These principles provide practical guardrails for evaluating options and making consistent decisions across business units and vendors. They are intentionally written in plain language so they can be used in executive discussions as well as in day-to-day planning.

#### Guiding principles we apply

- **Fit-for-purpose hosting:** Place workloads in cloud, hybrid, or on-prem environments based on risk, cost, and performance needs.
- **Standardize where it saves money and reduces risk:** Reduce duplication and simplify the technology footprint.
- **Interoperability:** Use repeatable integration patterns so systems can share information reliably.
- **Security and resilience built-in:** Protect sensitive information and maintain service continuity.
- **Trusted data:** Define ownership and quality expectations so reporting and analytics are reliable.
- **User-centered services:** Design around the experience of residents, employees, and partners.

In addition to principles, the work addresses the full landscape—services and capabilities, information and reporting needs, the systems that enable them, and the underlying platforms they run on, so recommendations are complete and implementable.

#### How we verify the work is complete

- **Structured method:** We use a proven, step-by-step approach to move from current state to target state to roadmap, with clear decision points and documentation.
- **End-to-end coverage:** We consider four viewpoints—**Business** (services and capabilities), **Data** (information and reporting), **Applications** (systems), and **Technology** (infrastructure and platforms).
- **Decision support:** The output is designed to be usable by leadership and delivery teams and to directly support funding, prioritization, procurement, and implementation decisions.

The engagement produces decision-ready outputs that can be used to support funding decisions, inform procurements, and guide implementation. Deliverables are designed to be clear to non-technical stakeholders while still detailed enough for delivery teams to act on.

#### Typical outputs

- **Current-state summary** (systems, integrations, risks, pain points)
- **Business capability map** with priority areas and opportunities
- **Application and platform inventory** with recommendations (retain/modernize/replace/retire)
- **Target-state architecture** (plain-language description plus supporting diagrams as needed)
- **Standards and reusable patterns** (to drive consistency across future procurements and projects)
- **Implementation roadmap** with sequencing, dependencies, and milestones

<b>What we do</b>	<b>What you get</b>	<b>Why it matters</b>
Assess the current environment and pain points	A documented current-state baseline and risk summary	Creates a shared fact base; reduces rework and conflicting assumptions
Define a practical target state and standards	Target-state architecture and reusable standards/patterns	Improves consistency across projects and procurements; reduces fragmentation
Prioritize and sequence modernization	Roadmap with milestones, dependencies, and decision points	Enables phased funding, clearer governance, and a lower-risk implementation path
Embed risk, security, and resilience requirements	Requirements and control considerations aligned to common standards	Supports auditability and reduces compliance surprises late in delivery

**Application portfolio rationalization**

LFUCG’s application landscape can evolve over time into a mix of legacy platforms, overlapping tools, and one-off solutions. We help the city establish a clear, evidence-based view of what to keep, what to modernize, and what to retire—balancing service impact, cost, and risk.

- Identify redundancy, obsolescence, and high-cost/high-risk systems
- Reduce operational complexity by converging on strategic platforms
- Reinvest savings from support and licensing into modernization priorities

**Data as a strategic enterprise asset**

Data becomes most valuable when it is trusted, understood, and governed consistently. We help define practical ownership and rules so reporting and analytics are reliable and departments can share information without creating conflicting definitions or unmanaged risk.

- Define data ownership and stewardship to improve accountability
- Set data quality expectations that support trustworthy reporting
- Establish shared definitions and interoperability requirements to reduce inconsistencies

**Integration architecture**

Modernization efforts often stall when systems cannot share information reliably. We assess the current integration landscape and define repeatable patterns so new solutions connect cleanly, reduce manual workarounds, and are easier to maintain over time.

- Document key interfaces and information exchanges that support critical services
- Define standard integration patterns to reduce one-off connections
- Improve visibility into end-to-end processes and dependencies

**Cloud and infrastructure strategy**

We help LFUCG determine the right hosting approach for different workloads—based on security, reliability, cost, and operational needs—so the city can modernize without increasing operational burden or creating unmanaged exposure.

- Define criteria for cloud vs. hybrid vs. on-prem placement decisions

- Address operating needs early (security, monitoring, cost management, resiliency)
- Verify vendor and service considerations are factored into the roadmap

To keep the target state actionable, we pair the architecture with lightweight governance and a roadmap that makes sequencing and decision points explicit. This helps verify the strategy can be executed through future projects and procurements.

### **Governance: architecture as a governed product**

- Establish governance structures that connect enterprise strategy to solution and program decisions (e.g., architecture review boards, domain authorities)
- Define standards, reusable patterns, and a clear exception process
- Keep governance enabling (decision-focused) rather than bureaucratic
- Align where helpful to established governance disciplines (e.g., COBIT for IT governance; ITIL for service management)

### **Delivery alignment and roadmapping**

- **Connect plans to delivery:** verify architecture decisions are timed to support near-term projects and procurements.
- **Balance speed and control:** avoid overly rigid “big design up front” while preventing inconsistent, one-off solutions.
- **Build an executable roadmap:** dependency-aware waves, major decision points, and measurable milestones.

Because public-sector environments are highly scrutinized, we embed risk, security, and resilience requirements early—so they are addressed through design and procurement, not discovered late in delivery.

### **Built-in risk, security, resilience, and compliance**

- Embed cybersecurity, privacy, continuity, recoverability, third-party risk, and regulatory obligations as **architectural requirements**, not late-stage checkpoints
- Align to widely adopted standards (e.g., NIST-aligned expectations) within reference architectures and engineering patterns
- Reduce rework, accelerate approvals, and scale modernization without increasing operational or cyber exposure

### **Capability transfer and sustainment**

- Governance playbooks, role definitions, and decision-support mechanisms to institutionalize the model
- Reusable templates and training so leaders, architects, engineers, and business stakeholders can apply the approach consistently
- A repeatable way to make better technology decisions after the strategy effort concludes

### **Benefits to LFUCG**

- **Decision-ready documentation:** clear outputs that support evaluation, oversight, and funding decisions

- **Reduced delivery risk:** dependency-aware roadmaps, defined standards, and built-in risk management
- **Improved service reliability:** security and resilience requirements embedded early
- **Better value from spend:** portfolio rationalization and standardization reduce duplication and long-term support costs
- **Stronger transparency:** governance structures and artifacts that make tradeoffs visible and auditable

In summary, our strategy and architecture work is designed to give LFUCG a clear and defensible direction for modernization: a shared understanding of the current environment, a practical description of the future state, and a sequenced roadmap that supports procurement, implementation, and oversight. The result is not just a set of diagrams, but a repeatable way to make better technology investment decisions and reduce long-term complexity and risk.

**Outcome:** A pragmatic target architecture and implementation roadmap that improves investment discipline, reduces fragmentation, and creates a resilient foundation for modernization—making architecture a strategic management tool for delivering measurable value at scale.

## Experience

<b>Client</b>	University of Louisville
<b>Project</b>	Major finance modernization effort combining IT architecture strategy, platform transformation, and operating model standardization to address long-standing fragmentation across the university’s financial environment, leading to implementation of Workday Financials (July 2025) and deployment of Adaptive Planning (fall 2025).

## Work performed

Deloitte helped replace disconnected legacy capabilities with a more unified and scalable environment spanning Workday Financials, Workday HCM, Payroll, existing institutional systems, and reporting assets. The effort required careful alignment across multiple technologies, including PeopleSoft Financials, Campus Solutions, the university data warehouse, JIRA, Smartsheets, HOOVER/ROVER, and Deloitte’s FDM Translation internal asset to support data and process transition. Rather than treating the modernization as a simple system replacement, Deloitte helped shape an enterprise architecture strategy that accounted for upstream and downstream dependencies, reporting requirements, and the varying needs of administrative and academic stakeholders. This allowed the university to move toward a more coherent digital finance landscape while reducing reliance on disconnected tools that had accumulated over time.

A critical part of the strategy was designing the Workday architecture to reflect the university’s institutional complexity. Deloitte helped establish a multi-company structure that could appropriately support the operational distinctions across academic units, athletics, and research while still enabling standardized governance and reporting. At the same time, the team standardized financial approvals, budget checking, and spend controls across the Health Sciences and Academic campuses, reducing inconsistencies in how transactions were reviewed and managed. This balance between enterprise standardization and institutional

nuance was central to the architecture approach: the solution needed to create common processes and controls without disrupting the unique operational realities of different university constituencies.

Deloitte also applied a phased strategy for planning transformation by deploying Adaptive Planning in a way that reflected uneven forecasting maturity across colleges and administrative units. Rather than forcing a uniform rollout, Deloitte tailored the implementation to organizational readiness, which improved adoption and created a more practical path to enterprise planning maturity. The team also provided tailored support to research groups to preserve operational continuity in an area with specialized funding, grant, and compliance considerations. This approach reflects a broader Deloitte IT strategy principle: architecture decisions are most effective when paired with deployment sequencing, stakeholder readiness, and targeted support models that reduce disruption while moving the institution toward a common future state.

### **Key outcomes**

- The University of Louisville gained a more integrated finance architecture that improved real-time visibility into financial and operational data, reduced dependence on shadow systems for reporting, and strengthened management of capital projects, grants, gifts, and contracts through unified processes.
- The transformation helped educate the campus community on more disciplined budgeting and operational reporting expectations, reinforcing that technology modernization must be accompanied by changes in how information is used and governed.

### **Relevance to LFUCG**

Deloitte’s work demonstrates an IT architecture and strategy approach that goes beyond platform implementation to include enterprise design, process standardization, deployment planning, and user enablement. The outcome was a modernized financial foundation better positioned to support decision-making, operational control, and future institutional growth.

## **Governance and Process**

### **Approach**

Deloitte’s governance and process approach helps organizations **make decisions faster, execute more consistently, and improve performance**—with documentation and transparency that support leadership oversight.

We treat **governance** (who decides, how decisions are made, and how performance is monitored) and **process** (how work gets done day-to-day) as reinforcing disciplines. When they are aligned, organizations reduce delays, duplication, and rework—and gain clearer accountability.

<b>Step</b>	<b>What we do</b>
<b>Align on outcomes</b>	Confirm what success looks like (e.g., faster decisions, clearer accountability, stronger compliance, improved service levels) and agree how it will be measured.
<b>Diagnose current state</b>	Document how decisions and work currently flow, identify bottlenecks and duplications, and establish a fact base for improvement priorities.

Step	What we do
Design the future state	Define decision rights, forums, operating rhythms; simplify and standardize processes; clarify roles and controls.
Implement and sustain	Create an implementation plan with owners, milestones, and adoption supports, then establish performance monitoring and continuous improvement routines.

We start by working with you to define a few practical principles and measures of success. This provides a shared standard for evaluating tradeoffs and helps keep the governance and process work focused on outcomes rather than reorganizing for its own sake.

### Guiding principles we apply

- **Outcome-focused:** Governance and process changes are tied to measurable results (speed, quality, cost, risk).
- **Right-sized rigor:** “Minimum effective governance” to improve control without unnecessary bureaucracy.
- **Clarity over complexity:** Simple decision pathways, clear ownership, and repeatable operating rhythms.
- **Designed for adoption:** Practical tools, templates, and training so the model can be used on day one.

Next, we document how decisions and work actually flow today, including where approvals stall, where responsibilities are unclear, and where control requirements create friction. This diagnostic gives leadership a fact base to prioritize changes and focus on the issues that most affect speed, quality, and accountability.

### Current-state diagnostic

- Decision rights, approval paths, and escalation routes
- Governance forums (purpose, membership, cadence) and how decisions are prepared
- Policies, controls, and compliance touchpoints
- End-to-end process flows, handoffs, bottlenecks, and rework drivers
- Roles and responsibilities (including where accountability is unclear or duplicated)
- Performance measures and reporting (what leaders can/can’t see today)

### Common diagnostic artifacts

- Stakeholder map; decision inventory; governance calendar and charters
- RACI (who is Responsible/Accountable/Consulted/Informed)
- Process inventory and end-to-end process maps
- Issue and bottleneck themes with root-cause analysis

Based on the diagnostic, we design a governance model that clarifies decision rights and creates a predictable operating rhythm. The goal is to help leaders and teams resolve issues at the right level, quickly, with clear documentation that supports transparency and oversight.

### Governance design

- **Clear decision pathways:** What gets decided where, by whom, and within what timeframes.

## Response to RFP 12-2026 – Information Technology Consulting and or Technical Services

- **Right forums at the right level:** Executive steering vs. operational working groups vs. owner-level decisions.
- **Standard mechanics:** Meeting cadence, agendas, decision packets, and issue escalation thresholds.
- **Traceability:** Decision logs and action tracking that support transparency and oversight.

### Using recognized frameworks

Where helpful, we align governance and process designs to widely recognized practices so they are complete, defensible, and easier to sustain. We tailor the level of formality to LFUCG's needs and avoid adding steps that do not improve control or performance.

- **Control Objectives for Information Related Technologies (COBIT)** (governance and decision rights)
- **Committee of Sponsoring Organizations (COSO)** (internal controls and risk management alignment)
- **Information Technology Infrastructure Library (ITIL)** (service management roles and workflows, where applicable)

With governance clarified, we focus on simplifying day-to-day processes so teams can execute consistently. We look for opportunities to reduce handoffs, eliminate duplicative reviews, and embed control requirements directly into the workflow.

### Process improvement

- **Simplify and standardize** where consistency improves reliability, training, and oversight
- **Preserve flexibility** only where there is a clear service or compliance reason
- **Measure what matters** (cycle time, backlog, quality/error rates, service levels, cost, customer/employee experience)

Depending on the scope and the city's priorities, we apply a focused set of improvement techniques—selected to be practical, time-bounded, and easy for teams to adopt.

### Methods we commonly use

- Lean/continuous improvement techniques to reduce waste and rework
- Practical benchmarking references to validate process coverage and terminology
- Control-point design so compliance requirements are built into the workflow

The work produces implementation-ready outputs: clear decision structures, simplified processes, and the measures needed to sustain performance over time. These deliverables are designed to support procurement, management oversight, and day-to-day execution.

### Typical outputs

- **Current-state assessment summary** (pain points, bottlenecks, and root causes)
- **Decision-rights and governance model** (forums, charters, cadence, escalation paths)
- **Role clarity artifacts** (RACI, role descriptions, accountability maps)
- **Future-state process maps** with defined handoffs, control points, and service expectations
- **Implementation plan** (workstreams, owners, milestones, risks/dependencies)
- **Performance measures** (dashboards/KPIs and review cadence)

The following summary highlights how these activities translate into tangible outputs and benefits for LFUCG.

What we do	What you get	Why it matters
Map decision paths and workflow reality (not just what’s on paper)	A current-state fact base with root causes and improvement priorities	Reduces debate and aligns stakeholders around evidence-based actions
Define governance forums, charters, and escalation thresholds	A right-sized governance model and operating rhythm	Speeds decisions while maintaining transparency and control
Simplify and standardize key processes and controls	Future-state process maps and role/accountability artifacts	Improves consistency, service quality, and compliance performance
Operationalize through implementation planning and measurement	Implementation plan plus KPIs/dashboards and review cadence	Supports sustained improvement and audit-ready visibility over time

**Implementation and sustainment**

- **Make it executable:** Sequenced workstreams, owners, milestones, dependencies, and decision points.
- **Support adoption:** Communications, training, and job aids so teams can work the new way.
- **Monitor performance:** Dashboards, operating reviews, and a continuous improvement backlog.

**Benefits to LFUCG**

- **Faster, clearer decisions:** Defined decision rights and escalation paths reduce delays and ambiguity.
- **Improved transparency:** Decision logs, action tracking, and performance measures support oversight.
- **More consistent execution:** Standardized workflows reduce variation, rework, and “workarounds.”
- **Stronger control and compliance:** Control points embedded into processes improve auditability.
- **Durable improvement:** Measures and operating rhythms that help changes stick over time.

In summary, our governance and process work is designed to help LFUCG operate with greater clarity and consistency: decision rights that are understood and documented, processes that are simplified and measurable, and an implementation approach that supports adoption and sustained performance. The result is a practical operating model that improves transparency for leadership and oversight while helping teams execute day to day with less friction and fewer delays.

**Experience**

<b>Client</b>	Cabinet for Health and Family Services (CHFS) Office of Application Technology Services (OATS)
<b>Project</b>	Develop an organization-specific project and program management framework aligned to the agency’s operating environment, governance needs, and delivery model to address inconsistent project and program management practices across teams supporting approximately 100 applications and platforms.

**Work performed**

Deloitte supported the CHFS Office of Application Technology Services responsible for the design, development, operations, and modernization of approximately 100 applications and platforms serving state staff and residents. With more than 400 personnel across contractors and state employees, the agency faced inconsistent project and program management practices across teams with varying levels of maturity and experience. Differences in terminology, templates, reporting expectations, and documentation approaches limited leadership visibility into status, made it harder to identify and mitigate risks early, and contributed to inefficient resource allocation. While industry standards such as PMBOK provided a useful foundation, the client needed a tailored framework aligned to its operating environment, governance needs, and delivery model.

Deloitte was engaged to develop an organization-specific project and program management framework anchored in practical leading practices and designed for operational adoption. Working closely with client stakeholders, Deloitte established standard templates to guide policy and business rule development, conducted scoping sessions to align on requirements for each policy area, and used an iterative review process to refine content over time. Rather than delivering all materials at once, Deloitte developed and reviewed the policies sequentially, allowing the client to absorb feedback in manageable increments and mature its expectations as the work progressed. Drawing on Deloitte’s experience, established project management methodologies, and practical delivery insights, the team developed 26 tailored policies and more than 100 associated business rules intended to operationalize compliance through the agency’s project and program management platform.

### Key outcomes

- The engagement resulted in tailored policy content spanning 26 critical project and program management domains.
- The final framework gave the client a standardized foundation for more consistent execution, clearer governance, improved reporting discipline, and better visibility into program health across its portfolio.

### Relevance to LFUCG

By translating leading practices into policies and enforceable business rules suited to the client’s environment, Deloitte helped position the agency to improve delivery consistency, strengthen risk management, and support more effective decision-making across a complex technology landscape.

## Risk, Resilience, & Compliance

### Approach

Deloitte’s risk, resilience, and compliance approach starts with a simple question: **what must LFUCG be able to protect and continue delivering**—even during disruption. We focus first on mission outcomes (critical services, data, and public trust), then align controls, governance, and operational practices to what matters most.

Rather than producing a list of technical findings, we translate risk into **decision-ready priorities** and a **practical roadmap** that supports oversight, auditability, and sustained operations.

### How we prioritize

We help stakeholders distinguish between items that are simply “good to do” and issues that materially affect service continuity, compliance exposure, or public trust.

Impact\Likelihood	Lower likelihood	Higher likelihood
Higher impact	<b>Plan and harden:</b> verify recovery plans and compensating controls are in place.	<b>Act now:</b> prioritize remediation and leadership decisions; track to closure.
Lower impact	<b>Monitor:</b> document, set thresholds, and revisit as the environment changes.	<b>Fix efficiently:</b> address through standard work, automation, and routine controls.

### How we work

Our work typically blends assessment, design, implementation planning, and operationalization. We right-size the depth based on the sensitivity of the environment and the level of assurance required, but we maintain a consistent focus on documentation, evidence, and traceability so outputs can withstand oversight.

- **Establish the scope and “crown jewels”:** confirm the services, systems, data sets, and third-party dependencies that are most critical to protect and sustain; clarify in-scope environments (on-prem, cloud, SaaS) and major constraints.
- **Build a fact base:** review policies, prior assessments/audit findings, incidents, architecture standards, and operational procedures; conduct interviews and working sessions with business, IT, security, and risk stakeholders.
- **Assess control design and operating effectiveness:** evaluate whether controls exist, whether they are performed consistently, and whether they produce evidence that can be used for audit and leadership reporting.
- **Define resilience expectations:** identify recovery objectives, minimum service levels, and escalation thresholds for key services; validate plans and test cadence.
- **Prioritize and plan:** translate findings into a risk-based backlog with owners, decision points, sequencing, and measurable outcomes; identify quick wins and foundational improvements.
- **Enable sustainment:** define governance routines, metrics, and operating rhythms so improvements remain active after the engagement concludes.

### What we assess

- **Governance and accountability:** decision rights, risk ownership, escalation paths, and reporting
  - Charters and roles (risk owners, control owners, service owners)
  - Risk acceptance and exception processes (who can approve, how decisions are documented)
  - Operating cadence (reviews, metrics, dashboards, and board/leadership reporting)
- **Policies, controls, and evidence:** whether required controls exist, operate consistently, and can be evidenced for audits
  - Control narratives (what is done, by whom, how often) and evidence expectations
  - Documentation quality, version control, and approval/attestation mechanisms
  - Control testing approach and remediation tracking (including repeat findings)
- **Operational resilience:** change practices, asset/configuration discipline, backup and recovery readiness, incident response coordination
  - Change management rigor and emergency change handling
  - Asset inventory completeness; configuration standards and drift handling

- Backup coverage, restore validation, and monitoring/alerting of failures
- Incident response playbooks, escalation, communications, and after-action reviews
- **Business continuity and disaster recovery:** critical services, recovery objectives, plans/runbooks, and test/exercise results
  - BC/DR scope and ownership; dependencies and single points of failure
  - Recovery objectives (e.g., RTO/RPO) and minimum service levels by service tier
  - Plan quality and practicality (runbooks, contact lists, decision criteria)
  - Exercise design, frequency, lessons learned, and closure tracking
- **Third-party dependencies:** key vendor/service dependencies and how they are monitored and governed
  - Contractual obligations, SLAs, and reporting requirements
  - Access controls for vendors; onboarding/offboarding; privileged access handling
  - Evidence collection from vendors (attestations, test results, incident notifications)
  - Concentration risk and contingency planning for critical suppliers
- **Governance and accountability:** decision rights, risk ownership, escalation paths, and reporting
- **Policies, controls, and evidence:** whether required controls exist, operate consistently, and can be evidenced for audits
- **Operational resilience:** change practices, asset/configuration discipline, backup and recovery readiness, incident response coordination
- **Business continuity and disaster recovery:** critical services, recovery objectives, plans/runbooks, and test/exercise results
- **Third-party dependencies:** key vendor/service dependencies and how they are monitored and governed

### **Evidence and reporting package**

Government stakeholders often need more than recommendations—they need a clear record of how conclusions were reached and how remediation will be tracked. Where appropriate, we provide an evidence and reporting package that can be reused in internal reviews and external oversight contexts.

- **Findings register:** clear issue statements, affected services/systems, root cause themes, risk implications, and recommended actions.
- **Prioritization rationale:** impact and likelihood considerations, criticality tiers, and dependencies that influence sequencing.
- **Remediation tracking:** owners, due dates, decision points, and status (including validation criteria to confirm closure).
- **Control/evidence mapping:** where needed, traceability from obligations (policies/standards/regulations) to controls to evidence artifacts.
- **Leadership-ready dashboards:** a small set of measures that show progress over time (coverage, test results, time-to-close, and repeat findings).

### **Typical Outputs**

- **Risk and control assessment report (plain-language):** findings written in business terms, including affected services/systems, root-cause themes, and clear remediation actions.
- **Prioritized remediation backlog:** ranked recommendations aligned to impact/likelihood, service criticality, and dependencies, including quick wins and longer-term foundational improvements.
- **Framework mapping (as needed):** traceability to commonly used expectations (e.g., NIST/COSO/COBIT) to support defensibility and oversight—tailored to LFUCG’s environment.
- **Resilience targets and service tiers:** proposed recovery objectives, minimum service levels, escalation thresholds, and a recommended test cadence for critical services.
- **BC/DR updates and exercise plan:** updates to plans/runbooks where needed and an exercise plan (tabletop and/or technical test options), including lessons-learned capture and closure tracking.
- **Governance and reporting artifacts:** decision rights/roles, meeting cadence, dashboards, and templates for ongoing risk and resilience management.
- **Roadmap and implementation plan:** sequencing, milestones, owners, and decision points that align remediation to procurement and delivery realities.

**Benefits to LFUCG**

- Improved audit readiness through clearer evidence of control design and operation
- Reduced likelihood and impact of disruptive events through targeted, prioritized improvements
- More predictable response and recovery supported by practiced procedures and clear ownership
- Better transparency for leadership and oversight through practical metrics and reporting routines
- A repeatable way to manage risk over time (not a one-time assessment)

In summary, our goal is to help LFUCG move from generalized risk discussions to a practical, defensible posture: clear accountability, controls that operate consistently, continuity plans that can be executed, and a prioritized roadmap that improves resilience over time without adding unnecessary bureaucracy.

**Experience**

<b>Client</b>	Commonwealth of Kentucky
<b>Project</b>	Design, implement, and enhance RSA Archer solutions to build an enterprise-enabling governance, risk, and compliance (GRC) capability supporting compliance obligations, security oversight, operational efficiency, and risk-based decision-making.

**Work performed**

Over the past decade, our Archer support for the Commonwealth of Kentucky has grown from targeted solution delivery into a broader effort to build an enterprise-enabling governance, risk, and compliance (GRC) capability. Since 2016, we have helped design, implement, and enhance Archer solutions that enable the Commonwealth to manage compliance obligations, strengthen security oversight, improve operational efficiency, and make more informed risk-based decisions. What began as focused platform support has evolved into a sustained program to create a more connected, scalable, and business-aligned GRC ecosystem.

Our work has included implementation of a customized Weakness and POA&M management solution for IEES, later expanded to Medicaid IT and HIPAA teams through workflows tailored to their operational processes. We have also continuously maintained and updated control frameworks to align with evolving requirements across CMS, NIST, MARS-E, and ARC AMPE. This ongoing alignment has helped verify the Commonwealth’s compliance content remains current, structured, and responsive to changing regulatory expectations.

In addition, we have developed custom Archer applications to support software inventory governance, vulnerability monitoring through API integration with the NIST National Vulnerability Database, security incident lifecycle management, and biannual reviews of agency data sharing agreements. We also enhanced executive visibility through vulnerability trend dashboards, implemented Archer single sign-on to improve user access and experience, and expanded third-party risk capabilities through Archer Engage integrations, including supply chain risk management and HIPAA assessments that replaced manual, spreadsheet-based processes.

As a result, Archer now serves as a more centralized and strategic repository for GRC-related activities across weaknesses, risks, vulnerabilities, incidents, software, assessments, policies and procedures, and supporting compliance processes. This has helped the Commonwealth move away from fragmented, manual methods toward more structured, transparent, and sustainable operations. It has also strengthened the Commonwealth’s ability to meet the expectations of federal and state oversight bodies, including CMS, IRS, SSA, and other regulatory stakeholders, through more consistent documentation, monitoring, and evidence management.

**Key outcomes**

- From a leadership perspective, this work has improved compliance readiness, increased visibility into risk and remediation activities, strengthened accountability through better lifecycle tracking and auditability, and reduced administrative burden through workflow automation and integration.
- It has also enhanced reporting and decision-making by giving stakeholders clearer insight into vulnerability trends, incident management, vendor risk, and assessment outcomes.
- Most importantly, it has positioned Archer not simply as a technology platform, but as a foundational capability supporting the Commonwealth’s broader goals for security, compliance, operational discipline, and enterprise risk management.

**Relevance to LFUCG**

This has helped the Commonwealth move away from fragmented, manual methods toward more structured, transparent, and sustainable operations. It has also strengthened the Commonwealth’s ability to meet the expectations of federal and state oversight bodies, including CMS, IRS, SSA, and other regulatory stakeholders, through more consistent documentation, monitoring, and evidence management.

**Program & Project Services**

**Approach**

Deloitte’s program and project services help LFUCG translate priorities into reliable execution—especially when work spans multiple departments, vendors, and oversight stakeholders.

Our focus is to establish **decision-ready visibility** (so leaders can act early) and a **delivery rhythm** that reduces surprises while keeping administrative overhead proportionate to the size and risk of the effort.

<b>Project Management Office capability</b>	<b>What it provides to LFUCG</b>
<b>Integrated planning</b>	A single view of scope, milestones, dependencies, and decision points across teams and vendors.
<b>Status and decision support</b>	Clear reporting that highlights what’s on track, what’s at risk, and what decisions are needed.

Project Management Office capability	What it provides to LFUCG
RAID management	Active tracking and escalation of risks, assumptions, issues, and dependencies with accountable owners.
Scope and change control	A practical way to evaluate change requests and prevent unmanaged scope growth.
Vendor coordination	Defined touchpoints, deliverable tracking, and interface management across third parties.
Quality and readiness	Evidence-based go/no-go checkpoints (testing progress, operational readiness, training readiness).

### Core disciplines we bring

Program and project services are most effective when they combine integrated planning with day-to-day operational discipline. In addition to the project management office (PMO) capabilities above, we commonly provide the following detailed support areas—tailored to the size and risk profile of each effort.

- **Governance cadence and decision management:** Define the forums (executive, program, workstream), cadence, and decision packet structure; maintain a decision log so approvals, tradeoffs, and rationale remain traceable.
- **Dependency and integration management:** Maintain cross-team dependency maps (technical, business, vendor), identify critical path risks, and coordinate resolution options before they become schedule impacts.
- **Quality management and delivery standards:** Define what “done” means for key deliverables; establish review checklists and evidence expectations for approvals.
- **Issue escalation with options:** Escalate early with clear alternatives (cost/schedule/scope impacts) so leadership can make timely decisions.
- **Readiness and cutover planning:** Coordinate go-live readiness (testing completeness, training readiness, support model readiness, communications) and execute cutover rehearsal activities where needed.
- **Documentation and auditability:** Maintain structured logs and artifacts (RAID, actions, decisions, approvals) so program history is retrievable and defensible.

### How we engage

We tailor structure and rigor to the program’s complexity, keeping it lightweight for smaller efforts and scaling up only when risk, visibility, or vendor coordination require it.

- Confirm outcomes, constraints, and success measures
- Stand up governance forums and predictable operating rhythm (cadence, agendas, decision logs)
- Create an integrated plan and dependency view; keep it current
- Provide decision-ready reporting; escalate issues early with options
- Support transition to operations (cutover readiness, support model, and knowledge transfer)

### Common artifacts and templates

To reduce overhead, we use repeatable templates and keep them consistent across workstreams. Examples include:

- **Integrated master schedule** with milestone definitions, dependency links, and approval gates
- **RAID log** with severity criteria, escalation triggers, and resolution validation
- **Decision packets** with context, options, recommendation, impacts, and required approvers
- **Status dashboard** with schedule, scope, risks/issues, actions, resourcing, and—when applicable—budget burn
- **Change request intake** with impact assessment and approval routing
- **Vendor deliverable tracker** and interface/handshake log
- **Readiness checklist** and go/no-go criteria for major releases
- **Communications calendar** and stakeholder engagement plan (where needed)

### **Typical outputs**

Outputs are scaled to the engagement, but we typically provide a consistent set of planning, reporting, and control artifacts that support predictable execution.

- **Integrated workplan** with milestones, dependencies, and decision points
  - Includes milestone definitions, owners, and a maintained critical path view
- **Status reporting package** aligned to leadership needs
  - Highlights what’s on track, what’s at risk, and which decisions are needed (with options)
- **RAID log and action log** with owners and due dates
  - Includes severity/priority criteria and escalation triggers
- **Governance artifacts** (charters, cadence, agendas, decision log templates)
  - Defines meeting purpose, attendees, inputs/outputs, and decision authorities
- **Readiness checkpoints** and go/no-go criteria for major milestones
  - Testing progress, training readiness, operational readiness, and cutover readiness
- **Transition and knowledge transfer materials** (as applicable)
  - Support model definition, runbooks, ownership handoffs, and lessons learned

### **Benefits to LFUCG**

Earlier issue visibility and faster decisions; clearer accountability across teams and vendors; improved audit-ready documentation of delivery decisions; and fewer surprises at go-live through evidence-based readiness checks.

In summary, our program and project services provide LFUCG with a practical delivery backbone: the minimum structure needed to coordinate work, manage risk, and support leadership decisions—without turning execution into unnecessary paperwork.

## Experience

<b>Client</b>	Cabinet for Health and Family Services – Integrated Eligibility and Enrollment System (IEES)
<b>Project</b>	Provide project and program management office support to coordinate a large, complex delivery environment requiring disciplined execution, transparent governance, and audit-ready operational rigor.

### Work performed

For over 10 years, Deloitte has provided project and program management office support for Kentucky's Integrated Eligibility and Enrollment System, helping coordinate a large, complex delivery environment that demands disciplined execution, transparent governance, and audit-ready operational rigor. Supporting a team of hundreds, Deloitte has served as a central integrator across workstreams, aligning day-to-day execution with strategic objectives, client direction, and program priorities. Our role has combined enterprise-level program coordination with the tactical PMO disciplines required to keep a large, fast-moving delivery organization operating effectively and in compliance with established controls.

A core component of Deloitte's support has been change management, including coordinating and driving to completion tens of thousands of hours of work to enhance and improve the IEES platform through a rigorous process designed to withstand regular audits. Deloitte has helped verify that changes are properly documented, reviewed, tracked, and advanced through established governance and approval channels so that improvements to the system are delivered in a controlled and compliant manner. This disciplined approach has enabled the program to balance the need for continuous enhancement with the accountability and traceability required in a highly scrutinized environment.

Deloitte has also provided comprehensive resource management to keep a large, multifaceted team integrated and aligned. This has included maintaining visibility into resource structure and allocation, supporting leadership with regular reporting on team composition and deployment, and managing tactical workforce coordination activities such as onboarding, offboarding, access provisioning, and required documentation. By combining strategic resource oversight with operational workforce management, Deloitte has helped the program maintain continuity, reduce administrative friction, and verify that personnel are positioned to support evolving delivery needs.

In parallel, Deloitte has led robust RAID management processes to strengthen visibility, accountability, and issue resolution across the program. Our team has comprehensively documented and escalated risks and issues through standard governance channels so that leadership and cross-functional teams remain informed of emerging concerns and potential impacts. Deloitte has also managed hundreds of discrete action items through active follow-up, maintenance of logs, and coordination with owners to drive closure. In addition, Deloitte has supported decision management by capturing key program decisions in a standardized, searchable format, creating an accessible record to support governance, traceability, and future reference.

### Key outcomes

- Deloitte's PMO support has further included regular status reporting tailored to the visibility needs of both leadership and cross-functional delivery teams.
- Through structured reporting, the program has been able to monitor progress, surface issues, and maintain a common understanding of priorities and delivery health.
- Our team has also supported schedule management through the development and maintenance of integrated work plans, monitoring progress against milestones, and analyzing critical path performance to identify potential delays or dependencies requiring intervention.

### Relevance to LFUCG

Together, these capabilities have enabled Deloitte to provide Kentucky IEES with a disciplined PMO function that enhances coordination, supports informed decision-making, and helps drive predictable program execution across a complex and highly governed environment.

## Training & Administrative

### Approach

Deloitte’s training and administrative services help organizations build capability and keep operations running smoothly during change. We design training and administrative support around **practical performance outcomes**, what people need to do differently and what services must become more reliable.

Our approach emphasizes role clarity, usable materials, and routines that make improvements sustainable after the engagement concludes.

Enable	Practice	Support	Sustain
Define audiences, outcomes, and what “ready” means.	Deliver role-based training and hands-on scenarios.	Provide job aids, office hours, and admin workflows to reduce friction.	Transfer ownership with playbooks, measures, and refresh routines.

### Training approach details

Training is most effective when it is designed around the work people must perform and reinforced through practical application. We tailor the depth and modality (instructor-led, virtual, self-paced, job aids) based on role criticality and the complexity of the change.

- **Training needs analysis:** Identify audiences, roles, tasks, and proficiency targets; confirm what “ready” means for each role.
- **Curriculum and content design:** Develop role-based learning paths, lesson plans, facilitator guides, participant guides, and exercises aligned to real scenarios.
- **Delivery planning:** Determine delivery methods, scheduling, enrollment/roster management, and accommodations; coordinate with project milestones and go-live waves.
- **Hands-on practice:** Use scenarios, simulations, or practice transactions to build confidence; provide “day in the life” exercises where appropriate.
- **Readiness measurement:** Track completion and—when appropriate—use knowledge checks, practical assessments, and feedback to identify where additional support is required.
- **Reinforcement:** Office hours, job aids, quick reference guides, FAQs, and targeted refreshers to reduce post-go-live support burden.

### Training services

We design training so it is role-based, practical, and timed to when staff will use it—so completion translates into real readiness.

- **Needs assessment and segmentation:** audiences, roles, and skill gaps
  - Role/task matrices and readiness criteria per audience
  - Training plan aligned to program milestones and release waves
- **Role-based learning paths:** concise curricula, facilitator materials, and participant guides
  - Instructor-led and virtual options; self-paced modules where appropriate

- Scenario-based exercises and “day in the life” walkthroughs
- **Training operations:** scheduling, rosters, attendance tracking, and communications
  - Coordination with business calendars and coverage needs
  - Logistics and enablement for trainers and participants
- **Reinforcement tools:** job aids, quick reference guides, FAQs, and targeted refreshers
  - Office hours and coaching to reduce post-go-live support burden
  - Targeted communications for recurring issues and updates
- **Readiness tracking:** completion, feedback loops, and (when appropriate) knowledge checks
  - Identifies roles/units needing additional support prior to go-live
- **Train-the-trainer and sustainment:** enable LFUCG to continue training over time
  - Facilitator guides, lesson plans, and content maintenance routines
  - Content ownership transfer and refresh cadence recommendations

### **Administrative services**

Administrative services are often where delays, backlogs, and inconsistent service are felt most acutely. We help stabilize operations through clearer workflows, defined service expectations, and lightweight performance routines.

Where appropriate, we treat administrative work like a service: define intake channels, clarify priority rules, make the backlog visible, and create a predictable operating rhythm for triage, approvals, and completion.

- **Workflow mapping and simplification:** intake, triage, handoffs, approvals, and escalation
  - Clarify “front door” intake and reduce unnecessary handoffs and rework loops
  - Define exception paths and escalation thresholds for time-sensitive items
- **Role clarity:** ownership for decisions, quality checks, and exceptions
  - Define who can approve, who can make changes, and how decisions are documented
  - Crosstrain for coverage and continuity in critical administrative functions
- **Service management basics:** service levels, queue/backlog visibility, and operating reviews
  - Define service expectations (e.g., response and completion targets) by request type
  - Implement basic dashboards for volume, aging, backlog, and throughput
- **Controls and compliance touchpoints:** embed required checks into the workflow
  - Reduce “end of process” surprises by building controls into standard work
  - Maintain an evidence trail for approvals and exceptions where needed
- **Continuous improvement:** maintain a small improvement backlog and revisit metrics regularly
  - Use trend data to address recurring drivers (policy ambiguity, handoff friction, tooling gaps)

Where appropriate, Deloitte incorporates hands-on and reinforcement-based methods to improve retention and transfer to the job. These may include scenario-based exercises, facilitated discussions, system simulations, practice transactions, role plays, job aids, quick reference guides, office hours, and knowledge checks. These elements help learners move from awareness to application, which is often the difference between training

that is completed and training that actually changes behavior. We also use assessments selectively to confirm readiness and identify where additional support is needed before go-live or transition.

**Benefits to LFUCG**

- Improved readiness and adoption through role-based, job-relevant training
- Reduced administrative friction and backlog through clearer workflows and operating routines
- More consistent service delivery supported by measurable expectations
- Sustained capability through playbooks, templates, and ownership transfer

In summary, our training and administrative services are designed to help LFUCG implement change without overloading staff: build the skills people need, simplify the supporting work behind the scenes, and establish practical routines that help keep performance on track over time.

**Experience**

---

<b>Client</b>	Louisville Metro Government (LMG)
<b>Project</b>	Organizational assessment to improve the effectiveness of talent acquisition and related administrative processes, including recruiting, hiring, onboarding, and retention practices.

---

**Work performed**

Deloitte supported Louisville Metro Government (LMG) with a targeted organizational assessment focused on improving the effectiveness of its talent acquisition and related administrative processes. LMG sought to strengthen recruiting, hiring, onboarding, and retention practices so it could better attract, support, and retain a qualified and motivated workforce serving the Louisville community. At the outset of the engagement, the organization was facing challenges across several human resources functions, including recruitment efficiency, time-to-hire, compensation policy constraints, HR staffing capacity, internal communication, and employee training. Deloitte’s role was to assess the current state, identify root causes across the talent lifecycle, and develop actionable recommendations to improve both workforce experience and administrative performance.

Deloitte executed the work through a three-phased approach designed to generate practical, implementation-ready recommendations. During the Discovery phase, the team collected and reviewed 20 recruiting, hiring, and onboarding documents to understand existing processes, policies, and operational constraints. Deloitte also researched leading practices across 11 comparable and diverse government organizations to benchmark LMG’s approach against peer institutions. To capture stakeholder perspectives, Deloitte conducted 24 interviews with HR leaders, Deputy Mayors, HR representatives, and department directors across 13 departments, including Public Works, Corrections, the Zoo, and Public Health. In addition, the team facilitated four focus groups with new staff members to assess the end-to-end experience from application through onboarding.

These activities enabled Deloitte to develop a detailed current-state analysis of LMG’s recruiting, hiring, onboarding, and retention environment, including a clearer understanding of how challenges varied across stakeholder groups and departments. Building on that foundation, Deloitte moved into the Design phase by synthesizing key themes from document review, interviews, and focus groups and then facilitating an in-person Transformation Workshop with 25 LMG stakeholders. The workshop was used to validate findings, review relevant leading practices, and prioritize opportunities based on feasibility, stakeholder interest, and likely organizational impact. This collaborative design process helped verify that recommendations were grounded in operational realities and had support from both HR and business leadership.

In the Delivery phase, Deloitte translated the assessment findings into 43 actionable recommendations aligned to eight core discovery themes. These recommendations were organized into quick wins and longer-term

initiatives to help LMG sequence improvements in a manageable and strategic way. The recommendations addressed key administrative and workforce priorities such as reducing time-to-hire, improving communication and transparency throughout the hiring process, strengthening onboarding, addressing compensation-related barriers, and enhancing coordination across HR functions. Deloitte also provided implementation roadmaps outlining suggested next steps for the highest-impact opportunities, giving LMG a practical path forward rather than a high-level assessment alone.

**Key outcomes**

- Establish a stronger foundation for improving both employee enablement and administrative service delivery.
- Deloitte’s recommendations supported more efficient and transparent talent acquisition operations, identified opportunities to strengthen internal communication and onboarding effectiveness, and highlighted ways to improve the employee experience from first contact through early tenure.
- The work also fostered stronger alignment between LMG leadership and the HR function, which is critical for implementing process changes that require both operational ownership and executive support.

**Relevance to LFUCG**

Overall, Deloitte provided LMG with a structured roadmap to improve the administration of talent processes, enhance workforce readiness and engagement, and position the organization to become a more competitive and effective employer over time.

## 5.4 Security & Compliance

**RFP Reference: 5.4 Security & Compliance**

All proposals should demonstrate capability to design, implement, and operate security aligned with recognized frameworks and public-sector practices, including:

- Identity & Access
- Endpoint Security
- Network Security
- Monitoring & Response
- Data Protection
- Vulnerability & Configuration Management
- Compliance Alignment
- Documentation

### Identity & Access

Typical outputs	Evidence / measures
IAM current-state assessment and prioritized backlog	Coverage metrics; orphaned account counts; privileged account inventory; remediation tracking
Target-state IAM capability model and phased roadmap	Milestones, owners, decision points; measurable control improvements over time
Access review / attestation process and supporting templates	Attestation completion rates; exception logs; audit-ready review artifacts

Typical outputs	Evidence / measures
PAM design and operating procedures (where applicable)	Admin access approvals; session logging; break-glass usage monitoring

Deloitte’s approach to Identity and Access Management (IAM) positions identity as the primary control plane for the modern enterprise, integrating security and compliance into every digital touchpoint. While our technological framework remains consistent across Citizen and Workforce initiatives, we customize the user experience and service delivery to address the unique requirements of each ecosystem. We focus on governing who can access specific resources, from which locations, and under what conditions, providing the defensible evidence necessary to withstand rigorous audits. By aligning IAM scope with strategic business and regulatory drivers—such as data protection, fraud prevention, and cloud transformation—we drive towards target outcomes that include least privilege, robust authentication, and streamlined provisioning and deprovisioning.

A common first step is an IAM maturity and risk assessment across people, process, and technology: identity lifecycle (joiner/mover/leaver), authentication and credential hygiene, privileged access, third-party access, access request/approval flows, and monitoring. We map risks to control requirements and define a prioritized backlog—often focusing early on high-impact gaps like orphaned accounts, excessive privileges, weak administrator controls, inconsistent identity proofing, and lack of attestation evidence. The output is a target-state IAM architecture and phased roadmap that balances quick wins with foundational modernization.

From an architectural standpoint, Deloitte helps clients design and implement integrated capabilities across identity governance and administration (IGA) [provisioning, access requests, policy, certifications/attestations, segregation of duties (SoD)], access management (AM) [single sign-on (SSO), passwordless, federation, conditional access, multi-factor authentication (MFA)], and privileged access management (PAM) (vaulting, session management, just-in-time access, break-glass controls). We also address directory services, cloud identity patterns, API/service identities, and machine identities where they materially affect risk and compliance. Reference architectures and standards are used to drive consistency across applications, cloud platforms, and environments. Furthermore, we have experience with most advanced areas like Identity Proofing (how to validate a user in real-time), Identity Fraud Analytics (how to prevent fraudulent account creation, how to prevent fraudulent transactions and account take over, and how to detect dormant fraudulent accounts), and the integration with mobile devices where a user can more easily interact with the county using a secure, single application.

For compliance, Deloitte emphasizes control design + operating effectiveness—not just tool deployment. We help define role models and entitlement cataloging, implement least-privilege patterns, standardize approvals, and establish recurring access reviews with defensible evidence trails. Where relevant, we align IAM controls to widely used control frameworks (for example, mapping to NIST-aligned control objectives and audit requirements) for logging and monitoring support detection and response, including integration with security operations (e.g., centralized logging and alerting on anomalous access).

Operationalization is a major focus: Deloitte helps define IAM operating models (roles, responsibilities, runbooks), service levels, and governance (policies, exceptions, KPIs/KRIs). This includes integrating IAM into HR, IT service management, and DevSecOps pipelines so identity controls keep pace with organizational change and application delivery. We also plan for resilience—high availability for critical identity services, tested recovery procedures, and continuity plans—because IAM outages can become enterprise-wide outages.

Finally, Deloitte’s IAM capabilities typically include program leadership, solution architecture, implementation support, and change enablement—covering requirements, design, build, test, cutover, and adoption. We place particular emphasis on reducing “identity debt” (manual processes, duplicated identities, inconsistent

entitlements) while helping improve user experience through automation and SSO, which helps security and compliance goals stick.

The work described above is based on our 26+ years of having a dedicated IAM practice where we have supported the complete continuum of the life cycle, from client strategy to operating some of the most strategic and mission critical IAM systems.



**Benefits to LFUCG**

- **Reduced access risk:** stronger joiner/mover/leaver controls, MFA, and least-privilege patterns reduce unauthorized access and account misuse.
- **Improved audit readiness:** repeatable access reviews, role models, and evidence trails support public-sector oversight and compliance requirements.
- **Faster onboarding and service delivery:** streamlined provisioning and SSO reduce delays for employees, vendors, and partners.

**Endpoint Security**

Control layers	Operational practices
Secure configuration baselines and drift management	Defined ownership; change control; automated remediation where feasible
Threat prevention and detection (AV/EDR)	Tuning; alert triage workflows; integration into monitoring/response
Vulnerability and patch management	Patch SLAs; exception governance; reporting for coverage and aging
Encryption and application/device control	Policy enforcement; evidence capture; periodic compliance review

Deloitte’s approach to endpoint security (workstations, laptops, servers, and increasingly mobile and specialized devices) frames endpoints as both a primary attack surface and a critical source of security telemetry for compliance and incident response. We start by aligning endpoint security objectives to business and regulatory needs—protecting sensitive data, enhancing availability, meeting control requirements, and enabling a productive user experience—and then define measurable outcomes such as risk reduction, faster detection/containment, and audit-ready evidence of control operation.

A typical engagement begins with an endpoint posture and maturity assessment across inventory and coverage, configuration baselines, patch/vulnerability management, endpoint detection and response (EDR) effectiveness, encryption, application control, local admin/privilege use, logging/telemetry, and operational processes. We identify exposure drivers like unmanaged assets, inconsistent builds, delayed patching, tool overlap, and gaps in monitoring. The output is a prioritized roadmap that balances quick containment actions (e.g., hardening and coverage) with longer-term modernization (e.g., unified management and automated controls).

From a capability standpoint, Deloitte helps clients design and implement layered endpoint controls: secure configuration (baseline hardening and drift management), threat prevention and detection (next-generation antivirus and EDR with tuned policies), vulnerability and patch management, device encryption and data loss protections, and application/device control (allow/deny listing, peripheral control). We also address endpoint

identity and access controls (e.g., reducing local admin, just-in-time elevation, strong authentication) and integrate endpoint signals into broader security operations for correlation and response.

For compliance, Deloitte focuses on translating regulatory and internal control requirements into repeatable, testable endpoint controls with clear ownership and evidence. This typically includes standardized build images, policy-as-code or centrally managed configuration, patch SLAs, exception handling, and continuous compliance reporting (coverage, baseline adherence, encryption status, EDR health, vulnerability remediation). Where appropriate, we align endpoint control objectives to recognized security control expectations (e.g., NIST-aligned practices) so that audit artifacts can be produced consistently without unnecessary manual effort.

Operationalization is treated as essential: Deloitte helps define the endpoint security operating model (governance, roles, runbooks, escalation, change control), tooling integrations, and performance management. We emphasize automation—self-healing agents, automated remediation for drift, prioritized patching based on exploitability and asset criticality, and streamlined exception workflows—to reduce operational toil. We also address resilience considerations such as endpoint tool reliability, update ring strategies, rollback plans, and continuity of endpoint management services during disruptions.

Finally, Deloitte supports transformation delivery end-to-end: helping select and rationalize endpoint security tools, implementing configuration standards, onboarding endpoints at scale, migrating from legacy agents, and training IT and security teams on steady-state operations. We help clients measure outcomes through dashboards and key indicators (coverage, mean time to contain, vulnerability aging, policy compliance) to prove risk reduction and compliance performance over time.

The work described above is based on our 30+ years of Cyber experience where we have supported the complete continuum of the life cycle, from client strategy to operating some of the mission critical IAM infrastructure.

### Benefits to LFUCG

- **Reduced ransomware and malware exposure:** Hardened baselines and disciplined patching reduce common attack paths on endpoints.
- **Audit-ready endpoint control evidence:** Measurable compliance reporting for encryption, baseline adherence, and vulnerability aging.
- **Lower operational burden:** Automation and standardized workflows reduce manual remediation and improve consistency at scale.

## Network Security

Control areas	Evidence / artifacts
Segmentation and trust boundaries	Network zoning diagrams; approved rule sets; validation/test results
Perimeter and internal enforcement	Firewall/IDPS standards; change approvals; exception logs
Monitoring and detection	Key log sources; alert use cases; tuning notes; coverage metrics
Remote and third-party connectivity	Remote access standards; third-party connection inventory; access reviews

Deloitte's approach to network security treats as both a critical control layer (segmentation, enforcement, visibility) and a high-value telemetry source for detection, response, and compliance. We start by aligning to business and regulatory drivers—protecting sensitive data, enhancing service availability, enabling cloud and remote work—and translating those into measurable objectives (e.g., reduced attack surface, faster containment, auditable control operation). This includes defining a target-state architecture and operating model that fits the client's environments (data center, cloud, campus, branch, operational technology (OT) where applicable).

We typically begin with a current-state assessment across network architecture, asset and traffic visibility, segmentation, perimeter and internal controls, remote access, third-party connectivity, and monitoring/response processes. Common findings include flat networks, inconsistent rule management, limited east-west visibility, unmanaged legacy protocols, and tool sprawl. The output is a prioritized roadmap that balances quick risk reduction (hardening and visibility) with longer-term modernization (segmentation, policy automation, and cloud-native controls).

From a capabilities perspective, Deloitte supports design and implementation of layered controls including next-generation firewalls (NGFW), intrusion detection and prevention systems (IDPS), web and domain controls, distributed denial-of-service (DDoS) protections, secure remote access, and network detection and response (NDR). We also help clients implement segmentation and micro-segmentation strategies (by application, environment, and sensitivity), standardize rule and policy management, and embed secure patterns for cloud connectivity and hybrid networking. Where clients are modernizing, we incorporate secure access service edge (SASE) and software-defined wide area network (SD-WAN) designs with clear security guardrails.

For compliance, Deloitte focuses on converting requirements into testable, repeatable network controls with defensible evidence. This commonly includes documented zoning and trust boundaries, controlled ingress/egress, standardized configuration baselines, change control and approvals for rule updates, periodic rule recertification, and continuous validation of segmentation effectiveness. We map these controls to widely used security and risk frameworks (for example, NIST-aligned control expectations and broader governance models such as COBIT where relevant) for monitoring/logging supports audit needs and incident investigations.

Operationalization is central: Deloitte helps define governance, roles and responsibilities, runbooks, escalation paths, and metrics (coverage, policy compliance, rule aging, mean time to detect/contain). We also integrate network telemetry into security information and event management (SIEM) and security operations workflows, tune detections to reduce noise, and establish a sustainable lifecycle for policy management, exceptions, and continuous improvement. The goal is a network security program that is not only well-architected, but operable at scale—reducing risk while enabling business change.

The work described above is based on our 30+ years of Cyber experience where we have supported the complete continuum of the life cycle, from client strategy to operating some of the mission critical IAM infrastructure.

### Benefits to LFUCG

- **Reduced attack surface:** Segmentation, standardized policy management, and controlled remote/third-party access limit lateral movement.
- **Stronger visibility for investigations:** Improved telemetry and tuned detections reduce blind spots across on-prem, cloud, and remote connectivity.

- **More defensible controls:** Documented trust boundaries, rule approvals, and recertification artifacts support oversight and compliance requirements.

## Monitoring & Response

What we measure	Why it matters
MTTD / MTTR by severity	Shows how quickly threats are detected and contained
Coverage of critical log sources	Reduces blind spots that delay investigations
Alert fidelity (false-positive rate)	Improves analyst efficiency and response quality
Backlog and case documentation quality	Supports sustained operations and audit defensibility

Deloitte’s approach to security monitoring and response is to build an outcomes-driven capability that can detect, triage, contain, and recover quickly—while producing audit-ready evidence that controls are operating effectively. We typically align the monitoring strategy to business risk, crown-jewel assets, and compliance obligations, then define what “good” looks like in measurable terms (e.g., mean time to detect (MTTD), mean time to respond (MTTR), alert fidelity, and coverage across critical systems).

We often start with a current-state assessment of the security operations center (SOC) (or equivalent function): visibility and telemetry coverage, use cases and detection logic, alert volumes and false positives, incident handling workflows, skills and staffing model, and third-party/provider dependencies. This includes validating whether key log sources are present and usable (cloud, identity, endpoint, network, application, data), and whether investigations can reliably answer “what happened, what was impacted, and what do we do next.” The output is a prioritized roadmap that balances quick wins (coverage gaps, high-noise tuning) with longer-term modernization (automation, advanced detections, and operating model improvements).

On the technology side, Deloitte helps clients design and integrate a monitoring stack centered on security information and event management (SIEM), often complemented by security orchestration, automation, and response (SOAR), endpoint detection and response (EDR), and—where needed—network detection and response (NDR) and user and entity behavior analytics (UEBA). The emphasis is on engineering reliable data pipelines (normalization, enrichment, time sync, retention) and detection content that maps to real threats, frequently using frameworks like MITRE ATT&CK to structure use cases and coverage. We also help rationalize tools to reduce overlap, improve signal quality, and lower operational burden.

For response, Deloitte typically strengthens incident response (IR) by defining severity models, decision rights, escalation paths, and playbooks that teams can execute under pressure. We align procedures to recognized guidance (e.g., National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide (SP 800-61) and/or ISO/IEC 27035) for evidence handling, containment steps, communications, and recovery activities are documented and rehearsed. Where relevant, we integrate response with legal, privacy, risk, and business continuity so that incidents are managed end-to-end, not just technically contained.

Operationalization is a core focus: Deloitte helps establish an operating rhythm (daily triage, weekly tuning, monthly metrics reviews), quality management (case documentation standards, peer review), and continuous improvement loops based on incident learnings and threat intelligence. We commonly implement automation for repeatable tasks—alert enrichment, ticket creation, containment actions, and notifications—so analysts spend more time on high-value investigations. Success is tracked through pragmatic metrics: detection coverage for critical assets, alert-to-incident conversion rate, false-positive rate, MTTD/MTTR by severity, and backlog health.

Finally, Deloitte supports compliance and defensibility by confirming monitoring and response controls are testable and evidenced—log retention policies, access controls on monitoring systems, change control for detection content, and repeatable reporting for auditors and leadership. This includes producing clear, decision-ready dashboards and executive incident reporting that links security operations performance to business risk reduction

The work described above is based on our 30+ years of Cyber experience where we have supported the complete continuum of the life cycle, from client strategy to operating some of the mission critical Cyber and Fusion operation centers.

### Benefits to LFUCG

- **Faster detection and containment:** Improved log coverage, higher-fidelity alerts, and defined playbooks reduce MTTD/MTTR for high-severity events.
- **Better operational efficiency:** Automation and tuning reduce false positives and analyst backlog.
- **Stronger audit defensibility:** Repeatable evidence for monitoring controls, case documentation standards, and retention/change controls.

## Data Protection

Our approach to data protection is designed to help the County reduce enterprise risk, protect resident, workforce, and business partner information, improve operational continuity, and align cybersecurity practices with applicable regulatory frameworks and standards. County governments face an increasingly complex threat environment driven by ransomware, phishing, legacy infrastructure, third-party dependencies, adversarial artificial intelligence (AI), and growing volumes of sensitive data. Quantum cyber readiness is another area of data protection State and local governments must be prepared for as current encryption standards will not be sufficient to withstand quantum computing capability to avoid unauthorized decryption of sensitive data. Threat actors are harvesting organization's data now to be able to decrypt that data in the future when quantum computing capability is available to them to decrypt the data.

We start our approach with discovering and classifying data, where we define what data matters most, where it lives, and how it should be handled—then turning that into enforceable controls with real-time monitoring and audit-ready evidence. We typically anchor on a data risk lens (confidentiality, integrity, availability) and compliance obligations, identifying “crown jewel” datasets, key business processes, and the most likely loss paths (email, cloud sharing, endpoints, third parties, APIs, and misconfigured storage).

A common first step is to conduct a data protection posture assessment covering data discovery, classification/labeling, retention, access patterns, encryption, data movement, and monitoring. We validate whether the organization can answer practical questions auditors and responders ask: *What sensitive data do we have and where does it reside? Who can access it? How is it protected in storage and transit? Can we prove controls are operating (and exceptions are governed)?* The output is a prioritized roadmap that sequences foundational steps (inventory, classification, access governance) alongside targeted risk reduction (high-risk repositories, critical workflows).

Deloitte helps clients implement layered controls across the data lifecycle: data discovery and classification, encryption and key management, tokenization/masking for analytics and non-production use, data loss prevention (DLP), and data flow monitoring of both structured and unstructured data to prevent exfiltration via email, endpoints, web, and cloud services. In cloud-heavy environments, this often includes cloud access security broker (CASB)-style controls and cloud-native guardrails to manage sharing, risky applications, and

misconfigurations. We also address secure collaboration patterns and information rights controls where clients need persistent protection beyond the perimeter.

For compliance, Deloitte focuses on translating requirements into repeatable, testable controls—policy, technical enforcement, and operating procedures. This typically includes retention and disposal rules, defensible exception processes, evidence capture (logs, reports, attestations), and control mapping to internal risk frameworks and external expectations. Where privacy requirements apply, we align protection controls to privacy-by-design needs (purpose limitation, minimization, lawful processing support) while confirming that security controls do not break business operations.

Operationalization is central: Deloitte helps define the data protection operating model—data owners/stewards, decision rights, escalation paths, and a steady cadence for policy updates, exception reviews, and control tuning. We also integrate data protection signals into security monitoring and response, so events like anomalous access, mass downloads, or sensitive-data sharing trigger meaningful investigations and containment. Data protection and data flow monitoring are key inputs to the overall incident response capability when potential security events are detected based on detected anomalies of data access and data flows. Our depth and breadth of experience with data protection methods combined with data protection software and tools that facilitate achieving the goal of sustained reduction in data exposure risk, improved user experience through clear handling rules, and stronger compliance defensibility.

In summary, we have vast experience and demonstrated capability from an advise, implement, and operate capacity for data protection services. Our data protection approach and services will better position the County to:

- Protect sensitive data and critical public services
- Reduce ransomware and breach risk through stronger preventive and recovery controls
- Address current and future risks based on the advent of artificial intelligence and quantum computing
- Improve governance and executive visibility into cyber risk
- Support compliance obligations for sensitive and regulated data
- Increase the maturity level of the data pillar if endeavoring to achieve a zero trust architecture (ZTA)
- Prioritize investments based on risk, feasibility, and service impact
- Strengthen public trust through improved resilience and stewardship of County data

#### **Benefits to LFUCG**

- **Reduced sensitive-data exposure:** Discovery, classification, and enforceable handling controls limit loss paths (email, cloud sharing, endpoints, third parties).
- **Improved response readiness:** Monitored data flows and clear ownership help investigate and contain suspected exfiltration more quickly.
- **Stronger compliance support:** Repeatable evidence for encryption, retention, exceptions, and DLP/CASB-style controls improves audit outcomes.

## Vulnerability & Configuration Management

Prioritization input	How it is used
Vulnerability severity	Starting point for triage and remediation targets
Asset criticality	Focuses effort on systems supporting critical services/data
Exploitability and exposure context	Helps prioritize issues more likely to be used in real attacks
Exception and compensating controls	Make deviations are time-boxed, approved, and evidenced

Deloitte’s approach to vulnerability and configuration management is to run them as a single, risk-driven control system: continuously finding exposure, prioritizing what matters, fixing it through repeatable engineering and operations, and proving control effectiveness for audits. We typically align the program to business risk and compliance obligations, then set clear outcomes (asset coverage, remediation speed by severity/criticality, baseline compliance, and measurable reduction in exploitable exposure).

A common first step is a posture and maturity assessment across asset inventory, scanning coverage, credentialed scanning quality, cloud and container visibility, configuration baselines, patching processes, exception handling, and reporting. We validate whether the organization can reliably answer: *What do we own? What’s vulnerable/misconfigured? What’s the business impact? Are fixes happening within defined timelines—and can we evidence that?* The output is a prioritized roadmap that typically sequences foundational fixes (inventory/coverage, standards, workflow) before advanced optimization (risk-based prioritization and automation).

On core capabilities, Deloitte helps clients implement risk-based vulnerability management (RBVM)—combining vulnerability severity with asset criticality, exploitability signals, and exposure context—to drive focused remediation rather than “scan-and-report.” This includes establishing remediation service levels, integrating findings into IT service management workflows, coordinating patching with change control, and building repeatable paths for common fix types (OS patches, third-party software, firmware/network devices, cloud services, containers, and code dependencies where in scope).

For configuration management (CM), Deloitte typically emphasizes hardened, standardized baselines [often informed by industry benchmarks like Center for Internet Security (CIS)] and continuous drift detection/remediation. We help define “gold” builds, policy enforcement, and automated configuration-as-code patterns (especially in cloud) so controls are consistent across environments. Where relevant, we integrate cloud posture controls [e.g., cloud security posture management (CSPM) patterns] to address misconfigurations that drive a large share of modern incidents.

For compliance and defensibility, Deloitte focuses on control design + operating effectiveness: documented standards, measurable remediation timelines, governed exceptions with compensating controls, and evidence capture (scan results, remediation records, baseline compliance reports, change tickets). We also help define metrics that leadership and auditors care about—coverage of critical assets, vulnerability aging by risk tier, patch compliance, baseline adherence, and repeat exception drivers—so the program is measurable and sustainable.

Operationalization is a major component: Deloitte helps establish the operating model (roles, decision rights, cadences), a pragmatic intake-to-fix workflow across infrastructure and application owners, and automation to reduce toil (auto-ticketing, prioritized remediation queues, maintenance windows, drift auto-remediation). The goal is a program that not only identifies issues but reliably reduces exposure over time without overwhelming delivery teams.

The work described above is based on our 30+ years of Cyber experience where we have supported the complete continuum of the life cycle, from client strategy to operating mission critical applications hosted on premises as well as major cloud platforms for state and local governments as well as higher education institutions.

**Benefits to LFUCG**

- **Lower exploitable exposure:** Risk-based prioritization focuses remediation on the vulnerabilities most likely to impact critical services.
- **More consistent configuration control:** Hardened baselines and drift detection reduce misconfiguration-driven incidents.
- **Clear, reportable SLAs and evidence:** Measurable timelines, governed exceptions, and remediation records support oversight and audits.

**Compliance Alignment**

Convert obligations into...	So LFUCG can produce...
A normalized control catalog with clear ownership and frequency	Consistent evidence of control operation across standards
Requirements-to-controls traceability	Audit-ready mapping without duplicative rework
Controls embedded in operational workflows	Repeatable artifacts from day-to-day execution (not a scramble)

Deloitte’s approach to security compliance alignment is to convert regulatory and contractual obligations into a single, risk-based security control system that is practical to operate and straightforward to evidence. We begin by confirming the compliance scope across entities, environments [on-premises, cloud, and software as a service (SaaS)], and data types, then rationalize applicable requirements into a unified view of “what must be true” to meet both audit expectations and real-world threat conditions. This upfront alignment avoids duplicative effort across overlapping standards and makes the program focus on the controls that most directly reduce security risk and audit exposure.

We translate requirements into clear, testable controls by building a normalized control catalog and requirements-to-controls traceability that supports multiple frameworks without rewriting the program for each assessment. Controls are defined in an audit-ready manner—including ownership, frequency, operating procedure, and evidence expectations—so design and operating effectiveness can be assessed consistently. Deloitte then evaluates current-state maturity and identifies gaps across core security domains such as identity and access management (IAM), logging and monitoring, vulnerability and configuration management, incident response, data protection, and third-party risk. Findings are prioritized based on business impact, exploitability, and audit materiality to produce a remediation roadmap that balances quick wins with durable control improvements.

Deloitte’s capabilities emphasize embedding compliance into day-to-day security and IT operations, so compliance becomes a byproduct of execution rather than a periodic evidence scramble. We integrate controls into operational workflows (e.g., access requests, change management, patching, incident handling, and vendor onboarding) and improve evidence quality through repeatable reporting, standardized artifacts, and automated collection where feasible. We also help establish sustainable governance—decision rights,

escalation paths, control health metrics, and a pragmatic operating cadence—so control performance is continuously managed and exceptions are time-boxed, risk-accepted, and traceable. Throughout delivery, we maintain traceability from obligation to control to evidence, enabling faster audits, fewer surprises, and measurable reduction in security exposure.

The work described above is based on our 30+ years of Cyber experience where we have helped our clients remain compliant with many regulations and governing bodies like NIST, CMS, IRS, SSA, CJIS to name a few.

### Benefits to LFUCG

- **Reduced audit effort and rework:** One normalized control catalog supports multiple standards without duplicative mapping.
- **Clear ownership and sustainable operations:** Defined control owners, frequencies, and operating procedures improve consistency over time.
- **Better risk prioritization:** Remediation is sequenced by business impact, exploitability, and audit materiality.

### Documentation

Deloitte's approach to security documentation is to create a coherent, audit-ready documentation set that is accurate, usable by operators, and directly traceable to security requirements and controls. We begin by confirming documentation scope and audiences—security leadership, IT operations, risk and compliance, internal audit, and external assessors—then inventory existing artifacts to identify overlaps, gaps, and inconsistencies. This enables a rationalized documentation architecture that standardizes structure, terminology, and ownership so documentation is easy to maintain and consistently applied across business units and environments [on-premises, cloud, and software as a service (SaaS)].

We develop and/or refine core documents such as security policies, standards, and procedures, writing each with clear intent, measurable requirements, and practical implementation guidance. Deloitte emphasizes operational usability by aligning documentation to real workflows—identity and access management (IAM), change management, vulnerability and configuration management, logging and monitoring, incident response, data protection, and third-party risk—so teams can execute consistently and produce reliable evidence. Where needed, we create supporting runbooks, playbooks, and control narratives that define roles, frequencies, triggers, handoffs, and escalation paths, helping reduce ambiguity and minimize control failures that too often result from unclear instructions.

To support compliance and assurance, Deloitte designs documentation for defensibility: traceability from obligations to controls to procedures to evidence, clearly defined exceptions and compensating controls, and version-controlled approvals that demonstrate governance. We also establish a sustainable documentation operating model—document owners, review cadences, change control, and quality checks—so the documentation set remains current as systems, threats, and regulations evolve. The result is a streamlined, maintainable security documentation library that helps improve day-to-day execution, accelerate audits, and strengthen the organization's overall security posture.

The work described above is based on our 30+ years of Cyber experience where we have documented our work and kept our clients compliant with many regulations and governing bodies like NIST, CMS, IRS, SSA, CJIS to name a few.

**Benefits to LFUCG**

- **More consistent execution:** Clear policies, standards, and runbooks reduce ambiguity and control failures.
- **Faster audits and easier evidence collection:** Traceability from obligations to controls to procedures to evidence improves defensibility.
- **Sustainable maintenance:** Defined ownership, review cadence, and change control keep documentation current as systems and requirements evolve.

# 6. Engagement Model & Deliverables

**RFP Reference: 6. Engagement Model & Deliverables**

For each engagement initiated under the contract awarded, vendors may be asked to provide:

- Scope of Work (SOW)
- Project Plan
- Architecture & Design
- Implementation
- Knowledge Transfer
- Operational Readiness
- Closeout

As part of each engagement with our clients, Deloitte develops a statement of work (SOW) that defines background and context, the scope of services to be provided, the timeline of activities and milestones, a high-level description of our approach to deliver services, the project team, and constraints and assumptions that underlie our work. The SOW lays out the expected timeline and scope of knowledge transfer from Deloitte to our clients at the end of the engagement. The SOW defines the process for defining operational readiness of the services delivered, and how project closeout will be executed. Below is a sample table of contents from our typical SOW template that we leverage for our engagements.

As part of our submitted SOWs for requested engagements by LFUCG, we will include the proposed project team. This proposal will include their credentials, experience with similar projects, as well as the overall team structure with track leads, engagement directors and team members clearly delineated in an organizational chart. Deloitte is uniquely positioned to bring to bear a mix of local Kentucky resources who have experience both with past Kentucky government engagements as well as fresh perspectives coming from their status as Kentuckians themselves. Given the nature of Deloitte’s project staffing approach, we are able to rapidly stand-up teams to respond to the needs of LFUCG for potentially “short-notice” engagements.

<b>Table of Contents</b>	
<b>Section #</b>	<b>Section Name</b>
<b>1</b>	<b>Background and Purpose</b>
1.1	Program Overview
1.2	Client Desired Benefits
<b>2</b>	<b>Scope of Service</b>
2.1	Approach
2.2	Functional Scope
2.3	Organizational Change Management and Training Scope
2.4	Out-of-Scope
<b>3</b>	<b>Other Considerations</b>
3.1	Impacts and Dependencies with Other Systems and Processes
3.2	Infrastructure and Software/Licensing Considerations
3.3	Security Considerations
3.4	Recommended Client Resources
<b>4</b>	<b>Timeline</b>
<b>5</b>	<b>Project Organizational Chart</b>
<b>6</b>	<b>Project Constraints</b>
<b>7</b>	<b>Fees and Fee Schedule</b>
7.1	Acceptance of Deliverables
<b>8</b>	<b>Knowledge Transfer &amp; Closeout</b>
<b>9</b>	<b>Signatures</b>

# 7. Attachment B – Cost of Services

**RFP Reference: 7. Cost of Services (Attachment B)**

Include the following in your proposal:

- Fee schedule – Hourly rates for employee classes or categories
- Pricing Model
- Additional Charges

Deloitte proposes providing for the “Consulting Services” section of Attachment B with the below details. These are proposed as Not-to-Exceed rates and will be finalized upon scope of work approval.

Service	Experience & Resources	Ceiling Hourly Rate
Disaster Recovery & Business Continuity Planning	Deloitte’s Consulting Services business has existed for over 30 years in its current structure in the US and employs over 20,000 professionals in the government and public sector consulting space.	\$200
Technical Requirements Gathering		\$175
IT Strategic Planning & Roadmaps		\$200
IT Governance & Compliance		\$175
IT Project Management (Agile, PMI)		\$200
Certified Project Management (PMP)		\$200
Enterprise Architecture & Cloud Strategy		\$200
PeopleSoft HCM & FCSM Consulting		\$200
ESRI ArcGIS Enterprise Portal Design & Implementation		\$175

## Pricing Model

When responding to requests for project scopes of work (SOWs), Deloitte will provide pricing based on the requested structure of the opportunity (for example, fixed-fee, or deliverables based).

## **Additional Charges**

Deloitte's proposed pricing for project scopes of work (SOWs) will be inclusive of all relevant charges such as travel.

## 8. Company Information

### RFP Reference: 8. Company Information

Provide:

- Company Name and Address
- Business Partnerships
- Years in Business
- References

### Company Name and Address

Deloitte Consulting LLP operates in Kentucky from three offices, listed below:

#### Louisville

220 West Main Street, Suite 2100

Louisville, KY 40202

#### Lexington

250 West Main Street, 25<sup>th</sup> Floor

Lexington, KY 40507

#### Frankfort

306 West Main Street, Suite 302

Frankfort, KY 40601

### Business Partnerships

Deloitte brings to clients a powerful combination of local market presence, deep public sector experience, and one of the broadest technology alliance ecosystems in the industry. Throughout the Commonwealth, Deloitte maintains strong relationships with organizations such as the City of Louisville, the Cabinet for Health and Family Services, the University of Kentucky, the University of Louisville, and many others. These relationships are reinforced by Deloitte GPS's national alliance network, which spans leading technology providers including AWS, Google Cloud, Oracle, Salesforce, Microsoft, ServiceNow, SAP, Workday, Databricks, and other priority platforms. Together, these alliances enable Deloitte to deliver end-to-end support across cloud strategy and migration, cybersecurity, enterprise resource planning, workflow modernization, customer and constituent engagement, data modernization, and AI-enabled transformation. For clients, this means access not only to leading technologies, but also to implementation experience, accelerators, governance models, and specialized talent needed to deploy them effectively in complex and highly regulated environments.

Deloitte's alliance strategy is designed to translate platform relationships into measurable client outcomes. Rather than approaching modernization as a set of disconnected technology projects, Deloitte helps clients bring together front-, middle-, and back-office capabilities into an integrated transformation agenda. Through its hyperscaler and enterprise platform alliances, Deloitte can support everything from cloud adoption and application modernization to cyber resilience, intelligent automation, ERP transformation, digital experience,

and managed services. This ecosystem-based model helps clients move faster, reduce delivery risk, improve interoperability across the enterprise, and gain access to proven capabilities that have been shaped through joint investment, innovation, and sector-specific solution development.

The breadth of Deloitte’s alliance-enabled offerings is especially evident across its work with major cloud and enterprise platforms. With Google Cloud, Deloitte provides cloud transformation and managed services, AI and data analytics capabilities, secure cloud modernization, and public sector solutions focused on constituent engagement, geospatial planning, and mission insights. With Oracle, Deloitte helps clients accelerate enterprise AI and analytics adoption through the Oracle AI Data Platform, supported by more than 50 industry AI and analytics use cases and a global network of more than 1,000 Oracle analytics and AI professionals <sup>8</sup>. Across CRM and digital engagement, Deloitte’s Salesforce alliance strengthens its ability to deliver next-generation constituent, customer, and case management solutions, including emerging agentic AI capabilities such as Agentforce-enabled offerings in life sciences. Deloitte’s alliances with Microsoft, ServiceNow, SAP, Workday, and Databricks further extend this value by supporting modern workplace transformation, workflow orchestration, ERP and HCM modernization, advanced analytics, and enterprise data platforms.

Deloitte’s alliance credentials are also validated by significant recognition across the technology ecosystem. At AWS re:Invent 2024, Deloitte was recognized as the EMEA Industry Partner of the Year for Healthcare and Life Sciences and as the Global Consulting Winner for GenAI. At Google Cloud Next, Deloitte earned 2025 Partner of the Year recognitions for Artificial Intelligence – Global Sales & Services, Industry Solutions – Government, Security – Global, and Security – EMEA, following multiple 2024 awards that included Global Industry Solution – Services and Social Impact. In the Oracle ecosystem, Deloitte received the 2025 AI Innovation Award and the 2024 Oracle Innovation Partner of the Year – Global Service Partner Cloud/Tech Customer Success. Deloitte Digital also received Salesforce Partner Innovation Awards in Public Sector in 2024 and Life Sciences in 2025. These recognitions are important not simply as credentials, but because they demonstrate Deloitte’s ability to convert alliance relationships into real-world innovation, platform fluency, and delivery excellence for clients.

For clients, the result is a partner that can bring more than software implementation. Deloitte offers the ability to align business strategy, mission priorities, technology platforms, and delivery execution in a unified transformation model. Its alliances provide clients with earlier access to emerging capabilities, stronger alignment to platform roadmaps, reusable accelerators, and teams that understand how to tailor commercial technologies to public sector needs. Whether the objective is to modernize legacy systems, improve service delivery, strengthen cyber posture, enhance workforce productivity, deploy responsible AI, or create a more connected enterprise, Deloitte’s alliance ecosystem gives clients access to a proven, scalable, and future-oriented set of capabilities designed to deliver durable value.

## Years in Business

Deloitte was founded as part of the merger of Deloitte and Haskins & Sells in 1845 and has been in business for 181 years.

## References

## Response to RFP 12-2026 – Information Technology Consulting and or Technical Services

Deloitte is proud to present the following distinguished points of contact for references from around the Commonwealth who can attest to our history of delivering impactful results through our consulting services work.

### **Dana Mayton**

Louisville Metro Deputy Mayor for Operations and Budget

- Email: [Dana.Mayton@louisvilleky.gov](mailto:Dana.Mayton@louisvilleky.gov)

### **Jay Blanton**

Vice President for University Relations, Chief Communications Officer, University of Kentucky

- Email: [jay.blanton@uky.edu](mailto:jay.blanton@uky.edu)

### **Jennifer Harp**

Executive Director, Office of Application Technology Services, Cabinet for Health and Family Services

- Email: [Jennifer.Harp@ky.gov](mailto:Jennifer.Harp@ky.gov)

### **Brian Lykins**

Information Security Architect, Office of Application Technology Services, Cabinet for Health and Family Services

- Email: [Brian.Lykins@ky.gov](mailto:Brian.Lykins@ky.gov)

### **Kelvin Brooks**

Application Architect, Office of Application Technology Services, Cabinet for Health and Family Services

- Email: [Kelvin.Brooks@ky.gov](mailto:Kelvin.Brooks@ky.gov)

## 9. Additional Information and Contract Terms

---

**RFP Reference: 9. Additional Information & Contract Terms**

- Evaluation: LFUCG employees and representatives of relevant user groups will evaluate proposals.
  - Awards: LFUCG intends to award contracts to multiple vendors to establish a list of firms to provide services as needed. LFUCG reserves the right to award this contract in its best interest.
  - Term: The contract will be three (3) years with the option to renew for two (2) additional one-year terms.
  - Standard Contracts: If your firm requires execution of a standard contract, include a draft with your response.
  - Ownership & Rights; All materials developed, data collected, or reports prepared under the project agreement become the property of LFUCG. LFUCG reserves non-exclusive rights to copy, publish, disseminate, and use materials developed under the agreement, in print or electronically.
  - Public Sector Considerations: Proposers should acknowledge public records obligations, auditability, and operational resiliency requirements typical of government environments.
- 

Deloitte acknowledges and agrees to the following.

- Evaluation: LFUCG employees and representatives of relevant user groups will evaluate proposals.
- Awards: LFUCG intends to award contracts to multiple vendors to establish a list of firms to provide services as needed. LFUCG reserves the right to award this contract in its best interest.
- Term: The contract term will be three (3) years with the option to renew for two (2) additional one-year terms.
- Standard Contracts: If your firm requires execution of a standard contract, include a draft with your response. Deloitte has included a draft of this contract in Appendix A of this proposal.
- Ownership & Rights: All materials developed and reports prepared on behalf of LFUCG under the project agreement become the property of LFUCG. LFUCG reserves non-exclusive rights to copy, publish, disseminate, and use such materials developed under the agreement, in print or electronically.
- Public Sector Considerations: Proposers should acknowledge public records obligations, auditability, and operational resiliency requirements typical of government environments.

## Appendix A: Deloitte Standard Contract Draft

Deloitte Consulting LLP (“Deloitte Consulting”) is pleased to submit this proposal (the “Response”) to the Lexington-Fayette Urban County Government (“County) for **Information Technology Consulting and/or Technical Services**, in response to Request for Proposal #: 12-2026 (the “RFP”). Our working relationship with the Commonwealth of Kentucky (and its various agencies) has proven that, almost without exception, we have been successful in expeditiously working together through important engagement requirements and provisions such as the ones we take exception to herein (i.e., indemnification, limitation of liability, intellectual property, insurance, etc.). Thus, in the event that we are selected for award, please trust that Deloitte Consulting is open and ready to promptly negotiate mutually agreeable terms in a collaborative and expeditious manner – similar to how the parties have successfully negotiated and executed previous complex engagements. Most notably the Commonwealth and Deloitte Consulting have executed the following contracts: Kentucky Unemployment Insurance Portal, MA 758 24000000505 dated 5/21/2024, Integrated Eligibility and Enrollment System, MA 758 2300001488 dated 1/1/2024, and BARS Budget, Accounting, and Reporting System, MA 758 2300000311 dated 9/27/2022.

As set out in our Response, Deloitte Consulting is qualified and prepared to provide the requested services to the County. In this regard, enclosed are our general business terms that we believe are appropriate for this type of engagement (as requested on page 34 of the RFP). We look forward to working with the County on this opportunity as our Response is submitted subject to the condition that Deloitte Consulting and the County reach mutual agreement.

### GENERAL BUSINESS TERMS

**1. Services.** The engagement letter to which these terms are attached (the “Engagement Letter”) describes the services to be performed thereunder (the “Services”) by Deloitte Consulting LLP (“Deloitte Consulting”). For purposes of these terms and the Engagement Letter, “Client” shall mean the entity to which the Engagement Letter is addressed.

**2. Compensation.**

Client shall compensate Deloitte Consulting for all Services performed and expenses incurred in connection with this engagement. Client shall be responsible for any taxes imposed on the Services or on this engagement, other than taxes imposed by employment withholding for Deloitte Consulting’s personnel or on Deloitte Consulting’s income or property. Client shall pay each invoice within thirty days of its receipt thereof. If payment is not received within such period (i) such invoice shall accrue a late charge equal to the lesser of (a) 1½% per month or (b) the highest rate allowable by law, in each case compounded monthly to the extent allowable by law, and (ii) Deloitte Consulting may also suspend or terminate the Services upon five days written notice to Client.

**3. Term.** Unless terminated sooner as set forth below, this engagement shall terminate upon the completion of the Services. Either party may terminate this engagement by giving thirty days prior written notice to the other party. In the event of any termination for breach, the breaching party shall have the right to cure the breach within the notice period. Deloitte Consulting may terminate this engagement upon written

notice to Client, if Deloitte Consulting determines that the performance of any part of the Services would be in conflict with law, or independence or professional rules.

**4. Ownership.**

a) For purposes of these terms (i) “IP” means works of authorship, materials, information and other intellectual property; (ii) “Deloitte Consulting IP” means all IP created prior to or independently of the performance of the Services, or created by Deloitte Consulting or its subcontractors as a tool for their use in performing the Services, plus any modifications or enhancements thereto and derivative works based thereon; and (iii) “Deliverables” means all IP that Deloitte Consulting or its subcontractors create for delivery to Client as a result of the Services.

b) Upon full payment to Deloitte Consulting hereunder, and subject to the terms herein, Deloitte Consulting hereby (i) assigns to Client all rights in and to the Deliverables, other than any Deloitte Consulting IP included therein; and (ii) grants to Client the right to use, for Client’s internal business purposes, any Deloitte Consulting IP included in the Deliverables in connection with its use of the Deliverables. Except for such license grant, Deloitte Consulting or its licensors retain all rights in and to all Deloitte Consulting IP.

c) To the extent any Deloitte Consulting IP provided to Client in connection with the Services constitutes inventory within the meaning of section 471 of the Internal Revenue Code, such Deloitte Consulting IP is licensed to Client by Deloitte Consulting as agent for its product company subsidiary on the terms contained herein. The rights granted in this Section do not apply to any IP that is licensed to Client under a separate agreement.

**5. Warranties.** This is a services engagement. Deloitte Consulting warrants that it shall perform the Services in good faith and in a professional manner. **DELOITTE CONSULTING DISCLAIMS ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.**

**6. Limitation on Damages.** Each party, its affiliates and subcontractors, and their respective personnel shall not be liable to the other party for any claims, liabilities, or expenses relating to or in connection with this engagement (“Claims”) for an aggregate amount in excess of the fees paid by Client to Deloitte Consulting pursuant to this engagement, except (i) to the extent resulting from their recklessness, bad faith or intentional misconduct, or (ii) for payment for fees and expenses due under the Engagement Letter. In no event shall either party, its affiliates or subcontractors, or their respective personnel be liable to the other party for any loss of use, data, goodwill, revenues or profits (whether or not deemed to constitute a direct Claim), or any consequential, special, indirect, incidental, punitive, or exemplary loss, damage, or expense, relating to or in connection with this engagement. The terms of this Section shall not apply to any Claim for which one party has an express indemnification obligation under these terms or the Engagement Letter. In circumstances where any limitations or exculpations set forth herein are unavailable, the aggregate liability of each party, its affiliates and subcontractors, and their respective personnel for any Claim shall not exceed an amount that is proportional to the relative fault that their conduct bears to all other conduct giving rise to such Claim.

**7. Relationship and Responsibilities.**

## **Response to RFP 12-2026 – Information Technology Consulting and or Technical Services**

a) Each party is an independent contractor, and neither is, nor shall be considered to be, nor shall purport to act as, the other's agent, partner, fiduciary, joint venturer, or representative.

b) In addition to Client's responsibilities as set forth in the Engagement Letter, Client shall cooperate with Deloitte Consulting in the performance of the Services, including providing Deloitte Consulting with adequate working space, equipment and facilities and timely access to data, information, and personnel of Client. With respect to the data and information provided by Client to Deloitte Consulting or its subcontractors for the performance of the Services, Client shall have all rights required to provide such data and information and shall do so only in accordance with applicable law and with any procedures agreed upon in writing. If Deloitte Consulting is provided with access to or use of Client's facilities outside the United States for the purpose of performing the Services, such facilities will not be dedicated solely for Deloitte Consulting's use and Deloitte Consulting will not be deemed a tenant of Client with respect to such facilities.

c) Client shall be solely responsible for, among other things (i) the performance of its personnel and agents; (ii) the accuracy and completeness of all data and information provided to Deloitte Consulting for purposes of the performance of the Services; (iii) making all management decisions, performing all management functions, and assuming all management responsibilities; (iv) designating a competent management member to oversee the Services; (v) evaluating the adequacy and results of the Services; and (vi) establishing and maintaining internal controls, including monitoring ongoing activities.

d) The Services may include advice and recommendations, but Deloitte Consulting will not make any decisions on behalf of Client in connection with the implementation of such advice and recommendations. Deloitte Consulting's performance is dependent upon Client's (i) timely and effective satisfaction of its responsibilities under these terms and the Engagement Letter, and (ii) timely decisions and approvals in connection with the Services, upon which Deloitte Consulting shall be entitled to rely.

e) Deloitte Consulting shall use diligent efforts to meet performance dates set forth in the Engagement Letter and shall notify Client promptly if Deloitte Consulting encounters significant delays in completing the Services. Notwithstanding the foregoing, all performance dates contained in the Engagement Letter shall be regarded only as estimates.

### **8. Confidentiality and Internal Use.**

a) To the extent that, in connection with this engagement, either party (each, the "receiving party") comes into possession of any confidential information of the other (the "disclosing party"), it will not disclose such information to any third party without the disclosing party's consent, using at least the same degree of care as it employs in maintaining in confidence its own confidential information of a similar nature, but in no event less than a reasonable degree of care. The disclosing party hereby consents to the disclosure of such information (i) as expressly set forth in the Engagement Letter; (ii) to the receiving party and its affiliates, subcontractors and contractors for use in connection with this engagement or the provision of administrative, infrastructure and other support services to the receiving party and its affiliates, in each case, whether located within or outside of the United States, provided that they have agreed to be bound by confidentiality obligations similar to those in this sub-Section; (iii) as may be required by law or regulation, or to respond to

governmental inquiries, or in accordance with applicable professional standards or rules, or in connection with litigation pertaining hereto; or (iv) to the extent such information (A) is or becomes publicly available other than as the result of a disclosure in breach hereof, (B) becomes available to the receiving party on a nonconfidential basis from a source that the receiving party believes is not prohibited from disclosing such information to the receiving party, (C) is already known by the receiving party without any obligation of confidentiality with respect thereto, or (D) is developed by the receiving party independently of any disclosures made to the receiving party hereunder.

b) All Services and Deliverables shall be solely for Client's benefit and are not intended to be relied upon by any person or entity other than Client. Client shall not disclose the Services or Deliverables, or refer to the Services or Deliverables in any communication, to any person or entity other than Client except (i) as expressly set forth in the Engagement Letter, (ii) to Client's contractors solely for the purpose of their providing services to Client relating to the subject matter of the Engagement Letter, provided that they comply with the restrictions on disclosure set forth in this sentence, or (iii) to the extent included within Client-created materials that do not in any way, expressly or by implication, attribute such materials to Deloitte Consulting or its subcontractors. Client agrees to indemnify and hold harmless Deloitte Consulting, its affiliates and subcontractors, and their respective personnel from all Claims attributable to claims of third parties relating to the use or disclosure of the Services or Deliverables.

**9. Indemnification.**

a) Each party agrees to indemnify, defend and hold harmless the other party, its subcontractors and their respective personnel from all Claims attributable to claims of third parties solely for bodily injury, death or physical damage to real or tangible personal property occurring while Deloitte Consulting is performing the Services, to the extent directly and proximately caused by the negligence or intentional misconduct of the indemnifying party and that does not arise from the indemnifying party's performance obligations under this engagement.

b) Deloitte Consulting agrees to indemnify, defend and hold harmless Client and its personnel from all Claims attributable to claims of third parties for infringement by a Deliverable of any U.S. patent existing at the time of delivery or copyright or any unauthorized use of any trade secret, except to the extent that such infringement or unauthorized use arises from (i) modification of the Deliverable other than by Deloitte Consulting or its subcontractors, or use thereof in a manner not contemplated by the Engagement Letter, (ii) the failure of the indemnified party to use any corrections or modifications made available by Deloitte Consulting, (iii) information, materials, instructions, specifications, requirements or designs provided by or on behalf of the indemnified party, or (iv) the use of the Deliverable in combination with any platform, product, network or data not provided by Deloitte Consulting. If Client's use of any such Deliverable, or any portion thereof, is or is likely to be enjoined by order of a court of competent jurisdiction as such an infringement or unauthorized use, Deloitte Consulting, at its option and expense, shall have the right to (x) procure for Client the continued use of such Deliverable, (y) replace such Deliverable with a non-infringing Deliverable, or (z) modify such Deliverable so it becomes non-infringing; provided that, if (y) or (z) is the option chosen by Deloitte Consulting, the replacement or modified Deliverable is capable of performing substantially the same function. In the event Deloitte Consulting cannot reasonably procure, replace or modify such Deliverable in

accordance with the immediately preceding sentence, Deloitte Consulting may require Client to cease use of such Deliverable and refund the professional fees paid to Deloitte Consulting with respect to the Services giving rise to such Deliverable. The foregoing provisions of this sub-Section constitute the sole and exclusive remedy of the indemnified parties, and the sole and exclusive obligation of Deloitte Consulting, relating to a claim that any of Deloitte Consulting's Deliverables infringes any patent, copyright or other intellectual property rights of a third party.

c) The indemnified party shall provide the indemnifying party with prompt written notice of any claim, liability, or expense for which indemnification is sought hereunder (an "Indemnity Claim"), cooperate in all reasonable respects with the indemnifying party in connection with any such Indemnity Claim, and use reasonable efforts to mitigate any Indemnity Claim; provided, however, that the indemnified party's failure to comply with the foregoing obligations shall not relieve the indemnifying party of its indemnification obligations, except to the extent the indemnifying party has been actually prejudiced by such failure. The indemnifying party shall be entitled to defend and control the handling of any such Indemnity Claim, with counsel of its own choosing that is reasonably satisfactory to the indemnified party. The indemnifying party shall not settle any Indemnity Claim without the prior written consent of the indemnified party.

**10. Approval of Deliverables.**

Client shall approve each Deliverable that conforms in all material respects to the requirements therefor set forth in the Engagement Letter. Approval of a Deliverable shall be deemed given by Client if Client has not delivered to Deloitte Consulting a notice that such Deliverable does not conform with the foregoing within fifteen days of delivery.

**11. Force Majeure.** Neither party shall be liable for any delays or nonperformance directly or indirectly resulting from circumstances or causes beyond its reasonable control, including fire, epidemic or other casualty, act of God, strike or labor dispute, war or other violence, or any law, order, or requirement of any governmental agency or authority.

**12. Survival.** All provisions that are intended by their nature to survive performance of the Services shall survive such performance, or the expiration or termination of this engagement.

**13. Interpretation.** Each of the provisions of these terms and the Engagement Letter shall apply to the fullest extent of the law, whether in contract, statute, tort (such as *negligence*) or otherwise, notwithstanding the failure of the essential purpose of any remedy. Liability limits set forth herein are intended solely to set maximum limits and are not intended as estimates of liability. Any references herein to the term "including" shall be deemed to be followed by "without limitation". The Section headings in these terms are for convenience of reference only and shall not affect the meaning or interpretation hereof. Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), the member firms of DTTL, and each of their respective affiliates (including Deloitte Consulting) and related entities, are referred to herein collectively as the "Deloitte Entities" and individually as a "Deloitte Entity." In the event of any conflict between these terms and the terms of the Engagement Letter, these terms shall control, except to the extent that the

Engagement Letter provides that specified provisions therein shall control over specified provisions of these terms.

**14. Binding Nature; Assignment and Subcontracting.** These terms and the Engagement Letter shall be binding on the parties and their respective permitted successors and assigns; provided, however, that, except as provided below, neither party may assign any of its rights or obligations (including interests or claims) relating to or in connection with this engagement, without the prior written consent of the other party. Client hereby consents to Deloitte Consulting subcontracting a portion of the Services to any Deloitte Entity and to any other third party, in each case, whether located within or outside the United States. Services performed by Deloitte Consulting's subcontractors shall be invoiced as professional fees on the same basis as Services performed by Deloitte Consulting's personnel, unless otherwise agreed. Deloitte Consulting agrees to be responsible to Client for the Services performed by its subcontractors to the same extent that Deloitte Consulting would be responsible to Client if Deloitte Consulting had performed such Services. No Deloitte Entity, other than Deloitte Consulting, and no personnel of any Deloitte Entity shall have any liability to Client relating to or in connection with this engagement, and Client will not bring any action against any such Deloitte Entity, or any personnel of any Deloitte Entity in connection with this engagement.

**15. Notices.** Any notice required under these terms or the Engagement Letter shall be (i) in writing, (ii) delivered to the representatives of the parties at the addresses set forth in the Engagement Letter, unless changed by either party by notice to the other party, and (iii) effective upon receipt.

**16. Severability.** If any of these terms or term of the Engagement Letter is unenforceable, such term shall not affect the other terms, but such unenforceable term shall be deemed modified to the extent necessary to render it enforceable, preserving to the fullest extent permitted the intent of the parties set forth in these terms or the Engagement Letter.

**17. Waivers and Amendments.** No delay or omission by a party in enforcing its rights or remedies under these terms or the Engagement Letter shall impair such right or remedy or be deemed to be a waiver thereof. No amendment or waiver of these terms or the Engagement Letter shall be valid unless in writing and signed by the parties thereto.

**18. Non-solicitation.** During the term of this engagement and for a period of one year thereafter, each of the parties agrees that its personnel (in their capacity as such) who had substantive contact with personnel of the other in the course of the performance of the Services hereunder shall not, without the other's consent, directly or indirectly solicit the services of such personnel of the other. This provision shall not restrict the right of either party to solicit generally in the media.

**19. Non-exclusivity.** Deloitte Consulting may (a) provide any services to any person or entity, and (b) develop for itself, or for others, any materials or processes, including those that may be similar to those produced as a result of the Services, provided that, Deloitte Consulting complies with its obligations of confidentiality set forth hereunder.

**20. Third-Party Beneficiaries.** Any third parties referenced in any disclaimer or waiver of liability, limitation on damages or actions, or indemnity in these terms or the Engagement Letter are intended third-party

beneficiaries of such terms and may in their own right enforce such terms. Except as set forth in this Section, (a) there are no third-party beneficiaries of these terms or the Engagement Letter, and (b) no rights, benefits, or remedies of any kind or character whatsoever are conferred upon, and neither party shall owe any duty to, any person or entity other than the other party.

**21. Governing Law.** These terms, the Engagement Letter, including attachments, and all matters relating to or in connection with this engagement, shall be governed by, and construed in accordance with, the laws of the State of New York (without giving effect to the choice of law principles thereof).

**22. Disputes.**

a) Any action relating to or in connection with this engagement shall be brought and maintained exclusively in any state or federal court, in each case located in New York County, the State of New York. Each of the parties hereby expressly and irrevocably submits to the jurisdiction of such courts for the purposes of any such action and expressly and irrevocably waives, to the fullest extent permitted by law, any objection which it may have or hereafter may have to the laying of venue of any such action brought in any such court and any claim that any such action has been brought in an inconvenient forum.

b) **EACH PARTY HEREBY IRREVOCABLY WAIVES, TO THE FULLEST EXTENT PERMITTED BY LAW, ALL RIGHTS TO TRIAL BY JURY IN ANY ACTION, PROCEEDING, OR COUNTERCLAIM RELATING TO OR IN CONNECTION WITH THIS ENGAGEMENT.**

c) No action, regardless of form, relating to or in connection with this engagement, may be brought more than one year after the cause of action has accrued, except that an action for nonpayment may be brought not later than one year following the due date of the last payment owing to the entity bringing the action.

**23. Entire Agreement.** These terms and the Engagement Letter, including attachments, shall constitute the entire agreement with respect to the subject matter of this engagement and shall supersede all other oral or written representations, understandings, or agreements relating to or in connection with the subject matter hereof. In making its determination to proceed with this engagement, neither party hereto will have relied on any representations of the other party except as expressly set forth in these terms or the Engagement Letter.

# Appendix B: Workforce Analysis Form

The below reflects the workflow analysis of our Louisville, KY office from which resources will be available to support engagements with LFUCG. In addition, Deloitte plans to leverage its nationwide pool of professionals for engagements with LFUCG.

**CONFIDENTIAL – NOT FOR PUBLIC RELEASE**

**WORKFORCE ANALYSIS FORM (EEO-1 Data as of 12/31/2024)**



Name of Organization: Deloitte Consulting LLP – Louisville, KY

Categories	Total	White (Not Hispanic or Latino)		Hispanic or Latino		Black or African-American (Not Hispanic or Latino)		Native Hawaiian and Other Pacific Islander (Not Hispanic or Latino)		Asian (Not Hispanic or Latino)		American Indian or Alaskan Native (not Hispanic or Latino)		Two or more races (Not Hispanic or Latino)		Total	
		M	F	M	F	M	F	M	F	M	F	M	F	M	F	M	F
Administrators	22	7	2	0	1	0	0	0	0	10	2	0	0	0	0	17	5
Professionals	69	26	26	2	0	0	3	0	0	7	3	0	0	1	1	36	33
Superintendents																	
Supervisors																	
Foremen																	
Technicians																	
Protective Service																	
Para-Professionals																	
Office/Clerical																	
Skilled Craft																	
Service/Maintenance																	
<b>Total:</b>	91	33	28	2	1	0	3	0	0	17	5	0	0	1	1	53	38

Prepared by: Lauren Moskowitz – Programs & Compliance Manager Date: 4/16/2026

(Name and Title)

Revised 2015-Dec-15

# Appendix C: Affidavit

## AFFIDAVIT

Comes the Affiant, Mohan Kumar, and after being first duly sworn, states under penalty of perjury as follows:

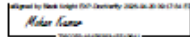
1. His/her name is Mohan Kumar and he/she is the individual submitting the proposal or is the authorized representative of Deloitte Consulting, LLP, the entity submitting the proposal (hereinafter referred to as "Proposer").
2. Proposer will pay all taxes and fees, which are owed to the Lexington-Fayette Urban County Government at the time the proposal is submitted, prior to award of the contract and will maintain a "current" status in regard to those taxes and fees during the life of the contract.
3. Proposer will obtain a Lexington-Fayette Urban County Government business license, if applicable, prior to award of the contract.
4. Proposer has authorized the Division of Procurement to verify the above-mentioned information with the Division of Revenue and to disclose to the Urban County Council that taxes and/or fees are delinquent or that a business license has not been obtained.
5. Proposer has not knowingly violated any provision of the campaign finance laws of the Commonwealth of Kentucky within the past five (5) years and the award of a contract to the Proposer will not violate any provision of the campaign finance laws of the Commonwealth.
6. Proposer has not knowingly violated any provision of Chapter 25 of the Lexington-Fayette Urban County Government Code of Ordinances, known as "Ethics Act."

7. Proposer acknowledges that "knowingly" for purposes of this Affidavit means, with respect to conduct or to circumstances described by a statute or ordinance defining an offense, that a person is aware or should have been aware that his conduct is of that nature or that the circumstance exists.

**Continued on next page**

8. Bidder will comply with all registration requirements as a contractor where required by Section 5-85 of the Code of Ordinances of the Lexington-Fayette Urban County Government. Bidder will utilize as subcontractors on the contract only contractors who are registered as required by Section 5-85 of the Code of Ordinances. Bidder will maintain a "current" status with regard to all contractor registration requirements during the life of the contract and will ensure that all subcontractors maintain a "current" status with regard to all contractor registration requirements during the life of the contract. Bidder has authorized the Division of Procurement to verify the registration of Bidder and Bidder's subcontractors with the Division of Building Inspection.

Further, Affiant sayeth naught.

A rectangular notary seal stamp for Heather Kendrick Seward, Notary Public, State of Kentucky, with a commission expiration date of 04/20/2026.

04/20/2026

STATE OF  Kentucky

COUNTY OF  Franklin

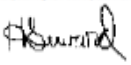
The foregoing instrument was subscribed, sworn to and acknowledged before me

04/20/2026

by  Heather Kendrick Seward  on this the \_\_\_\_\_ day

04/20/2026  
of \_\_\_\_\_, 20\_\_.

My Commission expires: \_\_\_\_\_ 8/2/2027 \_\_\_\_\_

  
\_\_\_\_\_

NOTARY PUBLIC, STATE AT LARGE

HEATHER KENDRICK SEWARD  
Notary Public  
Franklin County, Kentucky  
Commission No. KYNP76728  
My Commission Expires Aug 2, 2027

Notarial Act Performed by Audio visual communication

# Appendix D: Equal Opportunity Agreement

## EQUAL OPPORTUNITY AGREEMENT

### Standard Title VI Assurance

The Lexington Fayette-Urban County Government, (hereinafter referred to as the "Recipient") hereby agrees that as a condition to receiving any Federal financial assistance from the U.S. Department of Transportation, it will comply with Title VI of the Civil Rights Act of 1964, 78Stat.252, 42 U.S.C. 2000d-4 (hereinafter referred to as the "Act"), and all requirements imposed by or pursuant to Title 49, Code of Federal Regulations, U.S. Department of Transportation, Subtitle A, Office of the Secretary, (49 CFR, Part 21) Nondiscrimination in Federally Assisted Program of the Department of Transportation – Effectuation of Title VI of the Civil Rights Act of 1964 (hereinafter referred to as the "Regulations") and other pertinent directives, no person in the United States shall, on the grounds of race, color, national origin, sex, age (over 40), religion, sexual orientation, gender identity, veteran status, or disability be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination under any program or activity for which the Recipient receives Federal financial assistance from the U.S. Department of Transportation, including the Federal Highway Administration, and hereby gives assurance that will promptly take any necessary measures to effectuate this agreement. This assurance is required by subsection 21.7(a) (1) of the Regulations.

### The Law

- Title VII of the Civil Rights Act of 1964 (amended 1972) states that it is unlawful for an employer to discriminate in employment because of race, color, religion, sex, age (40-70 years) or national origin.
- Executive Order No. 11246 on Nondiscrimination under Federal contract prohibits employment discrimination by contractor and sub-contractor doing business with the Federal Government or recipients of Federal funds. This order was later amended by Executive Order No. 11375 to prohibit discrimination on the basis of sex.
- Section 503 of the Rehabilitation Act of 1973 states:

*The Contractor will not discriminate against any employee or applicant for employment because of physical or mental handicap.*

- Section 2012 of the Vietnam Era Veterans Readjustment Act of 1973 requires Affirmative Action on behalf of disabled veterans and veterans of the Vietnam Era by contractors having Federal contracts.
- Section 206(A) of Executive Order 12086, Consolidation of Contract Compliance Functions for Equal Employment Opportunity, states:

*The Secretary of Labor may investigate the employment practices of any Government contractor or sub-contractor to determine whether or not the contractual provisions specified in Section 202 of this order have been violated.*

\*\*\*\*\*

The Lexington-Fayette Urban County Government practices Equal Opportunity in recruiting, hiring and promoting. It is the Government's intent to affirmatively provide employment opportunities for those individuals who have previously not been allowed to enter into the mainstream of society. Because of its importance to the local Government, this policy carries the full endorsement of the Mayor, Commissioners, Directors and all supervisory personnel. In following this commitment to Equal Employment Opportunity and because the Government is the benefactor of the Federal funds, it is both against the Urban County Government policy and illegal for the Government to let contracts to companies which knowingly or unknowingly practice discrimination

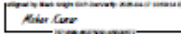
**Response to RFP 12-2026 – Information Technology Consulting and or Technical Services**

in their employment practices. Violation of the above mentioned ordinances may cause a contract to be canceled and the contractors may be declared ineligible for future consideration.

Please sign this statement in the appropriate space acknowledging that you have read and understand the provisions contained herein. Return this document as part of your application packet.

Bidders

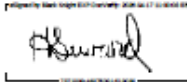
*I/We agree to comply with the Civil Rights Laws listed above that govern employment rights of minorities, women, Vietnam veterans, handicapped and aged persons.*

Original by Mark Seagraves, Notary Public, KYNP 76728  


04/17/2026

Deloitte Consulting, LLP  
Name of Business

Signature

Original by Heather Kendrick Seward, Notary Public, KYNP 76728  


4/17/2026

HEATHER KENDRICK SEWARD  
Notary Public  
Franklin County, Kentucky  
Commission No. KYNP76728  
My Commission Expires Aug 2, 2027

Notarial Act Performed by Audio visual commun

# Appendix E: LFUCG MWDBE Participation Forms



**LFUCG MWDBE PARTICIPATION FORM**  
 Bid/RFP/Quote Reference # 12-2026

The MWDBE and/or veteran subcontractors listed have agreed to participate on this Bid/RFP/Quote. If any substitution is made or the total value of the work is changed prior to or after the job is in progress, it is understood that those substitutions must be submitted to the Division of Procurement for approval immediately. Failure to submit a completed form may cause rejection of the bid.

MWBE Company, Name, Address, Phone, Email	DBE/MBE WBE/VOSB/SDVOSE	Work to be Performed	Total Dollar Value of the Work	% Value of Total Contract
1. Company: Sitek Solutions Name: Ganesh Babu Sivagurunathan Address: 1040 Monarch St, Suite 205, Lexington, KY 40513 Phone: 859 312 7415 Email: <a href="mailto:ganesh@siteksolutions.com">ganesh@siteksolutions.com</a>	MBE	TBD	TBD	TBD

The undersigned company representative submits the above list of MDWBE and veteran firms to be used in accomplishing the work contained in this Bid/RFP/Quote. Any misrepresentation may result in the termination of the contract and/or be subject to applicable Federal and State laws concerning false statements and false claims.

Deloitte Consulting  
 \_\_\_\_\_  
**Company**  
 4/17/2026  
 \_\_\_\_\_  
**Date**

  
 \_\_\_\_\_  
**Company Representative**  
 Managing Director  
 \_\_\_\_\_  
**Title**



**LEXINGTON**

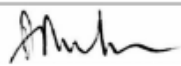
**LFUCG MWDBE SUBSTITUTION FORM**  
 Bid/RFP/Quote Reference # 12-2026

The substituted MWDBE and/or veteran subcontractors listed below have agreed to participate on this Bid/RFP/Quote. These substitutions were made prior to or after the job was in progress. These substitutions were made for reasons stated below and are now being submitted to the Division of Procurement for approval. By the authorized signature of a representative of our company, we understand that this information will be entered into our file for this project. **Note: Form required if a subcontractor is being substituted on a contract.**

SUBSTITUTED DBE/MBE/WBE/VOSB Company Name, Address, Phone, Email	DBE/MBE/WBE/VOSB/SDVOSB Formally Contracted/ Name, Address, Phone, Email	Work to Be Performed	Reason for the Substitution	Total Dollar Value of the Work	% Value of Total Contract
1.					
2.					

The undersigned acknowledges that any misrepresentation may result in termination of the contract and/or be subject to applicable Federal and State laws concerning false statements and false claims.

Deloitte Consulting  
 Company  
4/17/2026  
 Date

  
 Company Representative  
Managing Director  
 Title

**ATTACHMENT A – SMALL AND DISADVANTAGED, MINORITY-, WOMEN-, AND VETERAN-OWNED BUSINESS OUTREACH PLAN**

Proposer Name:	<u>Deloitte Consulting</u>	Date:	<u>4/17/2026</u>
	<u>Information Technology Consulting and/or Technical Services</u>		
Project Name:	<u>Services</u>	Project Number:	<u>RFP 12-2026</u>
Contact Name:	<u>Mohan Kumar</u>	Telephone:	<u>919 264-6925</u>
Email:	<u>mkumar@deloitte.com</u>		

The mission of the Minority Business Enterprise Program is to facilitate the full participation of disadvantaged businesses, minority-, women-, veteran-, and service-disabled veteran-owned businesses in the procurement process and to promote economic inclusion as a business imperative essential to the long-term economic viability of Lexington-Fayette Urban County Government.

To that end, small and disadvantaged businesses, including minority-, woman-, veteran-, and service-disabled veteran-owned businesses, must have an equal opportunity to be utilized in the performance of contracts with public funds spent from certain discretionary agreements. By submitting its offer, Bidder/Proposer certifies that it has taken, and if there are further opportunities will take, reasonable steps to ensure that small and disadvantaged businesses, including minority-, woman-, veteran-, and service-disabled veteran-owned businesses, are provided an equal opportunity to compete for and participate in the performance of any subcontracts resulting from this procurement.

The information submitted in response to this clause will not be considered in any scored evaluation. Failure to submit this form may cause the bid or proposal to be rejected.

Is the Bidder/ Proposer a certified firm? Yes  No

If yes, indicate all certification type(s):

DBE  MBE  WBE  SBE  VOSB/SDVOSB

and supply a copy of the certificate and/or certification letter if not currently listed on the city’s Minority Business Enterprise Program’s (MBEP) certified list

**1. Include a list of firms that Bidder/ Proposer has had a contractual relationship with within the last two years that are minority-owned, woman-owned, veteran-owned or small businesses, regardless of their certification status.**

◀ Sitek Solutions ▶

**2. Does Bidder/Proposer foresee any subcontracting opportunities for this procurement?**

Yes  No

If no, please explain why in the field below. Do not complete the rest of this form and submit this first page with your bid and/or proposal.

If yes, please complete the following pages and submit all pages with your bid and/or proposal.

**Describe the steps Bidder/Proposer took to solicit small and disadvantaged businesses, including MBEs, WBEs, VOSBs, and SDVOSBs, for subcontracting opportunities for this procurement.**

**3. Check the good faith and outreach efforts the Bidder/Proposer used to encourage the participation of small and disadvantaged businesses including, MBEs, WBEs, VOSBs and SDVOSBs:**

- Bidder placed advertisements in search of prospective small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs for the solicitation.
- Bidder attended LFUCG Procurement Economic Inclusion Outreach event(s) within the past year.
- Bidder attended pre-bid and/or pre-proposal meetings for this solicitation.
- Bidder sponsored an Economic Inclusion Outreach event.
- Bidder requested a list of certified small, DBE, MBE, WBE, VOSB and/or SDVOSB subcontractors or suppliers from LFUCG.
- Bidder contacted organizations that work with small, DBE, MBE, WBE, VOSB and/or SDVOSB companies.
- Bidder sent written notices to certified small, DBE, MBE, WBE, VOSB and SDVOSB businesses.
- Bidder followed up to initial solicitations with interested small, DBE, MBE, WBE, VOSB and/or SDVOSB.
- Bidder provided small, DBE, MBE, WBE, VOSB and/or SDVOSB businesses interested in performing the solicited work with prompt access to the plans, specifications, scope of work, and requirements of the solicitation.
- Bidder made efforts to segment portions of the work to be performed by small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs, including dividing sub-bid/partnership opportunities into economically feasible units/parcels, to facilitate participation.

- Bidder negotiated in good faith with interested small, DBE, MBE, WBE, VOSB and/or SDVOSB businesses.
- Bidder provided adequate rationale for rejecting any small businesses', DBEs, MBEs, WBEs, VOSBs or SDVOSBs for lack of qualifications.
- Bidder offered assistance in obtaining bonding, insurance, financial, equipment, or other resources to small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs, in an effort to assist them in meeting project requirements.
- Bidder made efforts to expand the search for small businesses, DBEs MBEs, WBEs, VOSBs and/or SDVOSBs beyond the usual geographic boundaries.
- Bidder made other reasonable efforts to include small businesses, DBEs, MBEs, WBEs, VOSBs and/or SDVOSBs participation.

**4. Bidder/Proposer must include documentation, including the date each effort was made, the medium through which each effort was made, and the outcome of each effort with this form, regardless of the level of small, DBE, MBE, WBE, VOSB and/or SDVOSB participation. Examples of required documentation include copies of email communications, copies of newspaper advertisements, or copies of quotations received from interested small businesses, DBEs, MBEs, WBEs, VOSBs or SDVOSBs.**

4/16/26 – Telephone conversation with Sitek Solutions. Deloitte and Ganesh agreed to explore teaming in future opportunities in good faith.

4/17/26 – Email exchange between Deloitte and Sitek Solutions agreeing to exploring teaming on future LFUCG opportunities.

**For detailed information regarding outreach efforts that satisfy the MBE Program's requirements, please see "Documentation Required for Good Faith Efforts and Outreach Plans" page.**

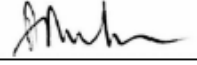
**Note: The Bidder/Proposer must be willing to report the identity of each subcontractor and the value of each subcontract to MBEP if awarded a contract from this procurement.**

**Failure to submit the documentation requested may be cause for rejection of the bid. Bidders may include any other documentation deemed relevant to this requirement, which is subject to review by the MBE Liaison. Documentation of Good Faith and Outreach Efforts must be submitted with the bid, regardless of the proposed level of SBEs, DBEs, MBEs, WBEs, VOSBs**

and/or SDVOSBs participation in the procurement. If the Good Faith and Outreach Effort Form and associated documentation is not submitted with the bid response, the bid may be rejected.

The undersigned acknowledges that all information is accurate. Any misrepresentations may result in termination of the contract and/or be subject to applicable Federal and State laws concerning false statements and claims.

Deloitte Consulting



Company

Company Representative

4/17/2026

Managing Director

Date

Title

**Response to RFP 12-2026 – Information Technology Consulting and or Technical Services**

**From:** [Ganesh Babu](#)  
**To:** [Kretsch, David](#)  
**Subject:** [EXT] RE: LFUCG Teaming in Good Faith  
**Date:** Friday, April 17, 2026 3:44:44 PM

---

Good evening David,  
Hope all is well.  
Yes glad to be part of Deloitte in LFUCG.  
As we discussed yes we are good.  
Thanks

Ganesh Babu Sivagurunathan  
1040 Monarch St, Suite 205,  
Lexington, KY 40513  
[ganesh@siteksolutions.com](mailto:ganesh@siteksolutions.com)  
Phone: 859 312 7415  
[www.siteksolutions.com](http://www.siteksolutions.com)

---

**From:** Kretsch, David <[dkretsch@deloitte.com](mailto:dkretsch@deloitte.com)>  
**Sent:** Friday, April 17, 2026 4:33 PM  
**To:** Ganesh Babu <[ganesh@siteksolutions.com](mailto:ganesh@siteksolutions.com)>  
**Subject:** LFUCG Teaming in Good Faith

Hi Ganesh,  
Thanks for the conversation on 4/16. I wanted to get on email that we agree to exploring teaming on future LFUCG opportunities. We'll have this record if needed for the future.

Have a great weekend.

Best, David

Thank you,  
David Kretsch  
Deloitte Consulting LLP  
2200 Ross Ave, Suite 1800, Dallas, TX, 75201  
Tel/Direct: +1 214 840 7855 | Fax: +1 866 397 7517 | Mobile: +1 405 708 0147  
[dkretsch@deloitte.com](mailto:dkretsch@deloitte.com) | [www.deloitte.com](http://www.deloitte.com)

Please consider the environment before printing.

This message (including any attachments) contains confidential information intended for a specific individual and purpose, and is protected by law. If you are not the intended recipient, you should delete this message and any disclosure, copying, or distribution of this message, or the taking of any action based on it, by you is strictly prohibited.