RESOLUTION NO. 19-5B-250 AGENDA NO. 12.B.2.(1)

RESOLUTION
ROCK COUNTY BOARD OF SUPERVISORS

Finance Committee
INITIATED BY

Finance Committee
SUBMITTED BY

Diana Arneson, Asst. to IT Dir
DRAFTED BY

May 7, 2019
DATE DRAFTED

AUTHORIZING PAYMENT FOR BAKER TILLY SECURITY AUDIT

WHEREAS, the Rock County Information Technology Department recognizes that Cybersecurity is a growing priority; and,

WHEREAS, Rock County possesses substantial high-value data that needs to be protected from Cybersecurity threats; and,

WHEREAS, Public Sector organizations like Rock County must regularly assess and strengthen their cybersecurity infrastructure and processes; and,

WHEREAS, Baker Tilly has familiarity with the County's IT operations as part of the County's financial audit and the IT assessment completed in November of 2018; and,

WHEREAS, the 2019 Budget did designate funds for a security audit.

NOW, THEREFORE, BE IT RESOLVED that the Rock County Board of Supervisors duly assembled this 23rd day of May, 2019 does hereby authorize a contract with Baker Tilly, not to exceed $40,500.

19-5B-250

Respectfully submitted,

FINANCE COMMITTEE

Mary Mawhinney, Chair

Mary Beaver, Vice Chair

Brent Fox

J. Russell Podzilni

Bob Yeomans

FISCAL NOTE:

Funds were included in IT's budget for this audit.

Sherry Oja
Finance Director

LEGAL NOTE:

The County Board is authorized to take this action pursuant to secs. 59.01 and 59.51, Wis. Stats. Professional services are not subject to bidding requirements of § 59.52(29), Stats.

Richard Greenlee
Corporation Counsel

ADMINISTRATIVE NOTE:

Recommended.

Josh Smith
County Administrator

Executive Summary

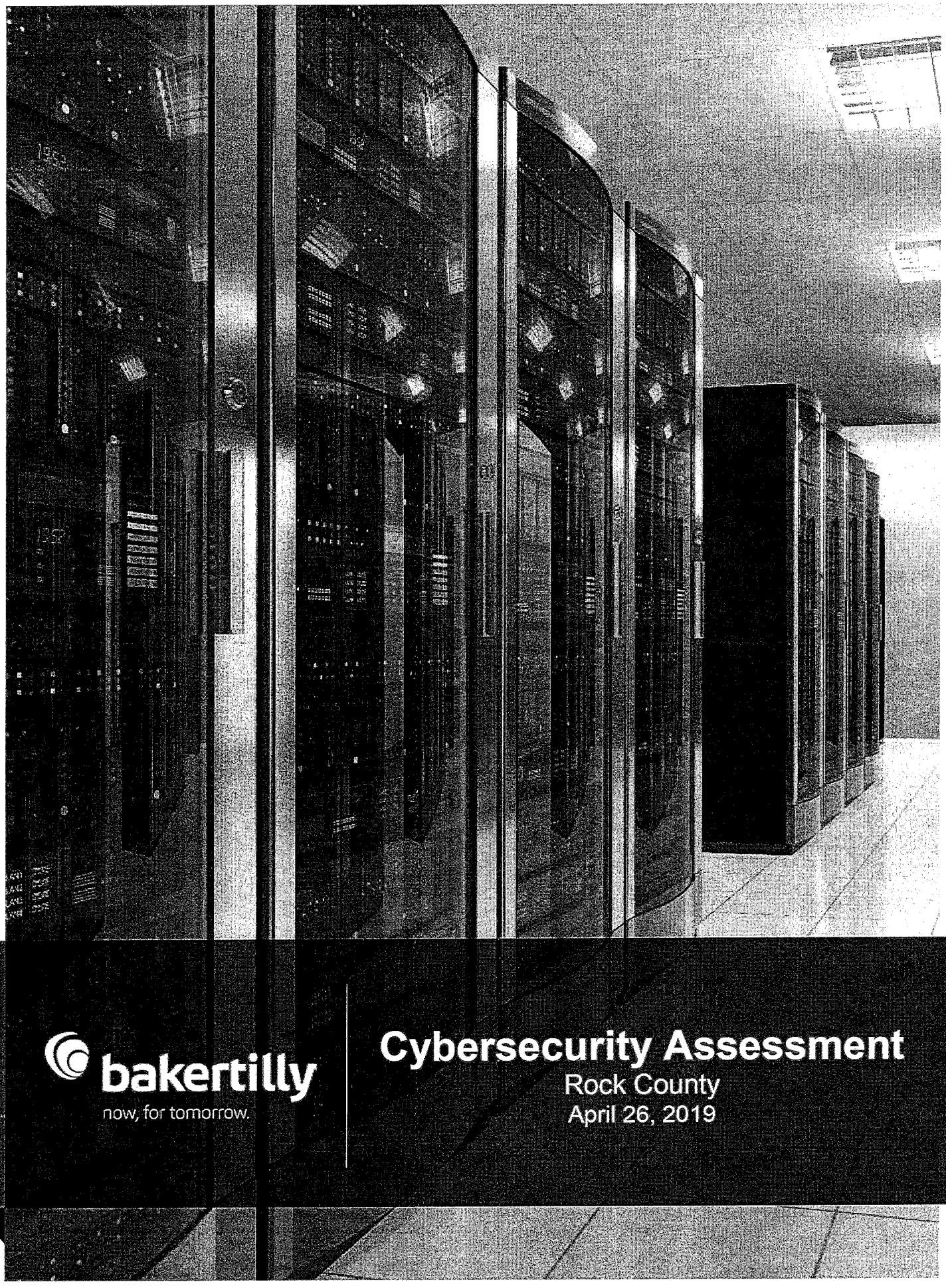
This resolution authorizes a contract with Baker Tilly to conduct an assessment of the Cybersecurity operations of Rock County's Information Technology Department.

The intent of this Cybersecurity audit is to comprehensively examine the County's current cybersecurity activities in order to advise on how to improve processes and controls to safeguard the County's data. Page 1 of the attached proposal outlines specific areas that will be considered through an industry-standard approach. Baker Tilly will assess the current IT staff's skillsets, capabilities and capacities; existing cybersecurity processes; Rock County's IT infrastructure and physical security; as well as presently available cybersecurity tools and technical resources. These activities will yield deliverables including a risk profile and a prioritized cyber risk report which will be used to decrease the County's cybersecurity risk as well as expand available toolsets and knowledge base for use in the future.

Additionally, Baker Tilly is offering a Cybersecurity Program Design service which will identify and prioritize cyber risks as well as design governance, controls, and regulatory frameworks. The deliverables will include a 12 month roadmap for cybersecurity program enhancements to assist the County moving forward.

Baker Tilly is uniquely qualified to complete this security audit. As the County's financial auditing firm, they have familiarity with the County's organizational structure and IT controls. Additionally, Baker Tilly completed an IT assessment in November of 2018 which will serve to facilitate their research.

The resolution authorizes a contract up to $40,500 for this purpose. The 2019 budget provides funding for this expense.



bakertilly

now, for tomorrow.

Cybersecurity Assessment

Rock County

April 26, 2019

Baker Tilly Virchow Krause, LLP
8219 Leesburg Pike, Ste 800
Tysons, VA 22182
703 923 8300
703 923 8330
bakertilly.com

April 26, 2019

Mr. James Sandvig
Director, Information Technology Department
Rock County
3530 N County Rd F
PO Box 920
Janesville, WI 53547-0920

Mr. Sandvig,

Cybersecurity threats are escalating for public sector organizations. As reliance on technology and networks rises, hackers discover new opportunities to steal, corrupt and leak data, creating substantial financial, reputational and operational risks for businesses. Counties must regularly assess and enhance their cybersecurity activities to account for the always-evolving cyber risk environment.

Within this context, Rock County (the County) is extremely wise to seek a cybersecurity assessment, and Baker Tilly Virchow Krause, LLP (Baker Tilly) is pleased to submit our cybersecurity assessment tailored proposal to meet these needs. We appreciate this opportunity to expand our relationship with the County, one of our valued clients, and believe our rich experience, industry specialization and holistic approach uniquely qualify us to perform your cybersecurity assessment.

As you make your decision, remember the benefits unique to this service and our firm:

- Breadth of experience in performing cybersecurity assessments to create detailed, accurate representations of organizations' cybersecurity postures
- Ability to identify and prioritize cyber risks and control gaps using insights gained from more than 800 cybersecurity and IT engagements and our extensive industry involvement
- First-hand experience serving the County since 1993 with audit, tax and advisory services
- Considerable industry experience from serving more than 1,000 public sector clients, including hundreds of counties and municipalities
- A flexible approach that provides substantial value

We look forward to the opportunity to discuss our cybersecurity assessment with you. Please do not hesitate to call or email us as you review our proposal.

Regards,

David Ross, MBA, MEng, CIPP/E, Principal
301 792 2073 | david.ross@bakertilly.com

Barry Esch, Director, Business Development
703 923 8305 | barry.esch@bakertilly.com

Contents

bakertilly
now, for tomorrow.

1. Approach and Methodology

Benefits of our cybersecurity assessments:

Builds on industry-recognized frameworks

Reflects leading practices and lessons learned from comparable cybersecurity engagements

Blends multiple project components, giving the County comprehensive analysis

Provides increased flexibility and responsiveness

Collaborative from start to finish, ensuring your needs and priorities are addressed

Develops visibility into current security limitations and metric-driven improvement

Clarifies current-state cybersecurity

Produces actionable steps to improve security posture

Cybersecurity is a growing priority throughout the country, specifically concerning attack prevention. The County possesses substantial high-value data, which makes you a prime target for cyberattacks. Furthermore, your constituent, vendor and internal interactions, if unmediated by proper controls, can easily create vulnerabilities for bad actors to exploit in a breach.

Baker Tilly's robust, holistic cybersecurity assessment approach will help to strengthen the County's understanding of your cybersecurity posture and risk exposure and provide viable recommendations to remediate gaps. Our goal will be to comprehensively examine your cybersecurity activities and advise the critical security control and process improvements needed to safeguard data from accidental loss, unauthorized access, use, alteration and disclosure.

To provide the maximum value and insight for the County, our proposed cybersecurity assessment methodology (detailed on the next page) covers five main categories.

- **People** – Assessment of your current staff's skills, capability and capacity with regards to cybersecurity activities.
- **Process** – Assessment of your policies, procedures and processes as it relates to cybersecurity
- **Infrastructure** – Assessment of your IT infrastructure from a cybersecurity perspective
- **Tools** – Assessment of your cybersecurity tools and technical resources
- **Physical** – A high level assessment of your physical security in protection your IT infrastructure

Optionally, we have also included three additional services that are natural extension of the assessment work.

- **Cybersecurity Program Design** (Optional)
- **Vulnerability Assessment** (Optional) – Scanning your infrastructure (internally and/or externally) for known vulnerabilities
- **Social Engineering** (Optional)

The process starts with a planning phase, where we will develop a project plan and establish expectations, and conclude with reporting, where we will share our findings and recommendation in an easy-to-understand, digestible format.

1.1 Cybersecurity Assessment Methodology

Cybersecurity Assessment

Purpose: Identify and prioritize cyber risks considering management's assessment of the context of the County's control environment, existing policies, and potential gaps in accountability, and develop actionable recommendations

Activities

- Request and review initial documentation, including policies, diagrams, and other information that will help Baker Tilly evaluate the risks within the audited areas, such as:
  - Policies, procedures and standards
  - Vendor and third-party management
  - Change management (e.g., patches, operating system and firmware upgrades, configuration changes)
  - Access management (e.g., account management, password management, elevated privileges, account access review, access monitoring)
- Work with management to understand and discuss the County's:
  - Strategic goals
  - Major initiatives and challenges
  - Recent and planned changes in processes and systems
  - Views of major risks facing the County, and how they may have evolved since the development of the current cyber risk framework
- Conduct interviews and collect data
  - Interview stakeholders regarding the risk environment, what has historically been done, past challenges, and opportunities
  - Conduct interviews and/or walkthroughs with key data and process owners
- Review existing policies, processes and practices against defined requirements
- Identify key risk areas for management focus
- Develop recommendations for risk mitigation strategies of key cyber risk areas
- Identify areas for improvement relative to IT and cybersecurity

Deliverables

- Interview meeting agendas
- Inventory of resources, projects, programs, documentation, and capabilities
- Risk profile
- Gap analysis
- Summary of draft observations
- Prioritized cyber risk listing
- One initial draft report
- One final report

1.2 Optional Additional Projects

Optional: Cybersecurity Program Design

Cybersecurity Program Design

Purpose: Identify and prioritize cyber risks considering management's assessment of the context of the County's control environment, existing policies, and potential gaps in accountability, and develop actionable recommendations

Activities

- Recommend remediation activities associated with identified gaps
- Design cybersecurity governance framework
- Design cybersecurity controls framework
- Design cybersecurity awareness/training program
- Define applicable regulatory frameworks

Deliverables

- Cybersecurity priorities
- 12-month roadmap
- Initial cybersecurity program design, including long-term cybersecurity leadership recommendations
- Final cybersecurity program design

"Having Baker Tilly come in... gave me the tools and resources I needed to be successful."

– Director of Information Technology

Optional: Vulnerability Assessment

Vulnerability Assessment

Purpose: Identify and assess the County's network-accessible vulnerabilities

Activities

- Work with the County to identify in scope hosts
- Perform vulnerability scanning procedures using our scanning appliance on identified hosts as well as perform a vulnerability check on the Wireless Guest network, using the following methods:
  - The **Credentialed Method** for internal vulnerability scanning:
    - Log into a target computer as a system administrator and issue commands to catalog the computer system's configuration, software inventory, and running services
    - Search for known vulnerabilities, including missing software maintenance and security patches as well as unsupported software and weak security settings
    - Confirm and document identified vulnerabilities
  - The **Non-Credentialed Method** for external scanning and any internal host for which login credentials are unavailable:
    - Run a network port scan to identify "live computers," their listening network service ports

Deliverables

- Written vulnerability report including:
  - Executive summary
  - Management summary
  - Assessment methodology
  - Issues and observations
  - Appendices
    - Host discovery information
    - Detailed vulnerability listing with remediation

Vulnerability Assessment

- and the associated service programs
- Discover vulnerabilities through network probing
- Search for known vulnerabilities associated with the identified network service ports and programs

"Your team was fantastic to work with again this year. I compliment the amazing team you have, and am looking forward to next year!"

– Chief Technology Risk Officer

Optional: Social Engineering and Phishing

Social Engineering and Phishing

Purpose: Attempt to steal user credentials or gain user system access using social engineering attacks including phishing and phone pretexting

Activities

- Collaborate with County management to scope the target employee list for social engineering emails and phone pretexting
- Conduct social engineering campaigns, which will consist of sending phishing emails and conducting phone pre-texting calls
- Collect response metrics and compile results to be presented and shared with management
- Provide a training module for identified users who do not pass the social engineering tests

Deliverables

- Phishing/phone pretexting response metrics and results

2. Pricing

"Thank you again for going beyond the call of duty and providing us with excellent value for the investment we made."

– CEO at a Client Organization

We prepared the fee in **Table 2** for the County based on the needs and objectives you have shared with us and our experience conducting similar services in the public sector industry. Our fee allows for thorough and insightful advice and services from experienced professionals without unnecessary add-ons or start-up charges. If the County commits to the **cybersecurity assessment and program design** up front, Baker Tilly will offer a $2,500 dollar discount.

Table 2: Fees

Project	Cost
Cybersecurity assessment	$30,000
Optional Cybersecurity Program Design	$10,500
Optional Vulnerability assessment	TBD
Optional Social engineering and phishing	TBD

Out-of-pocket expenses reasonably and necessarily incurred in the performance of this service will be charged in addition to the fees stated above and will be billed at the actual amounts incurred.

Our services will be performed in accordance with the Consulting Standards promulgated by the American Institute of Certified Public Accountants (AICPA). Our procedures will be performed solely to assist the organization in assessing your cybersecurity posture. Such procedures do not constitute an audit conducted in accordance with U.S. Generally Accepted Auditing Standards. Accordingly, we will not express an opinion on the results of our work.

2.1 Assumptions

We based our estimate on the assumptions detailed below. Should any of these change during the engagement, we will bring the matter to the County's attention immediately and prepare a change order detailing the new requirements and corresponding budget impact. We will not undertake additional work without the County's written approval.

Assumptions include:

- The County will provide adequate support, preparedness, and cooperation from management
- There will be no significant changes in scope
- Engagement can be serviced from the United States – should travel be necessary/desired, we will obtain the County's approval in advance and will bill the County for such travel, as incurred

- All interviews, data provided and deliverables will be in English
- The County will provide resources to assist with coordination activities such as scheduling project activities, coordination of information gathering, and securing project team space
- The County will provide timely access to needed personnel, systems and processes
- The County will provide timely feedback on prioritization of activities
- The County will provide timely feedback on deliverables

For all services listed above, project management tasks and on-going collaboration will ensure that you are informed throughout the process and there are no surprises in our final deliverables.

3. Proposed Team

Efficient project performance requires a team with experienced personnel who are knowledgeable and skilled to meet your needs from day one, as well as capable of responding to your needs promptly and efficiently. With Baker Tilly, the County will once again to have such a team.

The team consists of public sector and consulting professionals offering a depth of public sector experience, a breadth of cybersecurity skills as well as a deep understanding of public sector organizations' cybersecurity risks and threats.

The following are the key personnel on your engagement team:

- David Ross, a principal at Baker Tilly and the cybersecurity growth leader for our risk, internal audit and cybersecurity practice, who leads our VCISO efforts for clients across industries. David will serve as your engagement partner.

- Heather Acker, a partner of Baker Tilly's Madison office, who specializes in public sector clients and leads our work and manages our overall relationship with the County – as the local client partner.

- Ken Zoline a senior manager at Baker Tilly, with more than 23 years of cybersecurity and technology experience. Ken will serve as the engagement director.

- Alex Islamov, a manager with more than 12 years of leadership and management expertise focusing in the areas of IT, security, governance, risk management and IT audit programs. Alex will be your engagement manager.

Our many years of public sector experience coupled with our current consulting work allow our team to offer a unique perspective on the prominent risks and cyber threats facing public sector organizations. **Appendix I** includes detailed resumes for the proposed team members.

Presence in the State of Wisconsin

800

Qualified professionals statewide

5

Offices, including in Janesville

4. About Baker Tilly

Baker Tilly was founded in 1931 with one central objective: *use our industry specialization to help our clients improve their operations* With teams that include financial, business and industry-specific specialization, our clients work with knowledgeable professionals who understand their organizations and can create innovative solutions to help them overcome their unique challenges. Because the County will once again be working with a tailored engagement team, you can continue to expect consistent, efficient and Exceptional Client Service. **Figure 4** shows some key facts about us.

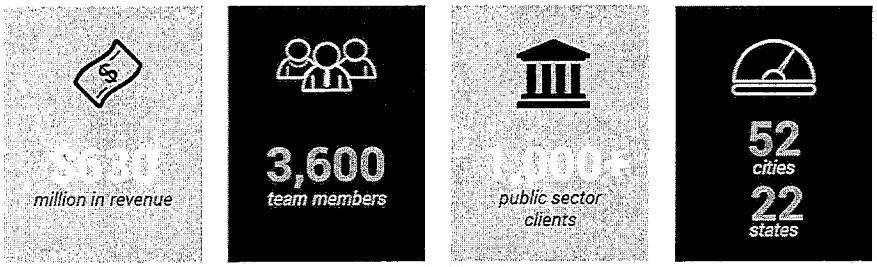
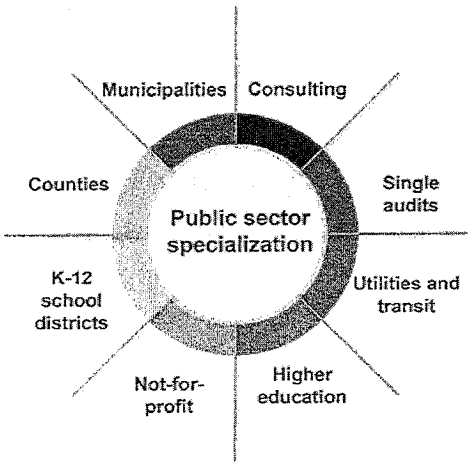


Figure 4: Key facts

Baker Tilly's more than 3,600 total staff members, including approximately 350 partners, provide a wide range of services to clients. Beyond our cyber and privacy offerings, we also provide accounting, assurance, consulting and staffing services, among others. For more than 85 years, Baker Tilly has understood that our business demands absolute integrity, a belief in the value of trusted relationships and a willingness to collaborate with every client. We will strive to continue to deepen and enhance our relationship with the County as we seek to remain your Valued Business Advisor.

4.1 Public sector Specialization

Baker Tilly is one of only a few audit firms with a dedicated public sector practice. The depth of our knowledge and experience, together with our commitment to the public sector, will translate into valuable insights into issues unique to the City. Our public sector practice group, which was formalized nearly 50 years ago, consists of a team of more than 320 professionals dedicated entirely to serve the needs of public sector clients. We recognize the complex nature of this industry and organize our partners and staff into various sub-specialty practice areas.



Nationwide, our public sector practice currently works with more than 1,000 such clients, including more than 300 municipalities, as well as state agencies, counties, public utilities, transit, school districts and many other government organizations.

We have a substantial history of public sector audit and advisory services. In addition, we offer valuable assistance in areas such as compliance audits, feasibility studies, operational reviews, consolidation and shared services consulting, information technology (IT) consulting and other advisory services.

Our approach to industry specialization ensures that the City of Minneapolis will continue to work with a team that is truly dedicated to serve governmental clients, which leads to an exceptional client service experience.

Umbaugh/Springsted Combination

You may have heard our firm recently announced some very exciting news. Springsted Inc. (Springsted) and H.J. Umbaugh and Associates, Certified Public Accountants, LLP (Umbaugh) are joining Baker Tilly in a three-way combination. **This strategic combination creates a premiere municipal advisory practice, particularly in Minnesota, and provides the City access to a range of municipal advisory specialists.**

The full combination will be effective in the first half of 2019 (Springsted has already combined with Baker Tilly). After a transition period, the combined firm will be Baker Tilly.

Of note, the County has been among our valued clients since 1993 and we are excited about the possibility to expand our relationship with you. You'll see some of the same faces who have previously served – and currently serve – you return to your cybersecurity assessment, assuring you of a team that understands your unique environment.

Benefits of our work:

1. Visibility to current security limitations and metric-driven improvement
2. Roadmap/action plan to improve security posture
3. Behavior changes to safer/sounder and measurable actions that reinforce security
4. More secure, reliable cybersecurity infrastructure and operations
5. Increased operational efficiency and effectiveness
6. Enhanced internal controls emphasizing risk detection and risk mitigation
7. Reduction of the potential for a single-point failure
8. Quicker issue resolution
9. Better strategic decision-making about cybersecurity risk mitigation

4.2 Experience in Delivering Cybersecurity Services

Decades of serving public sector organizations with risk and cybersecurity services have taught us how to manage known vulnerabilities and proactively identify new ones. Using this experience, we can provide the County with an accurate and objective view of your County to help you protect data from theft, compromise and destruction.

Baker Tilly has assisted more than 800 client organizations of all sizes with cybersecurity and IT risk-related work, who have leveraged our work to:

- Gain an enterprise perspective into the opportunities and risks associated with their cybersecurity postures
- Simulate cyber-attacks leveraging social engineering, phishing and penetration testing
- Compare their cybersecurity practices and controls against leading practices frameworks
- Better position cybersecurity initiatives, processes and systems to add value to organizations and their constituents
- Enhance governance and facilitate critical discussions about cybersecurity risk management with senior management and boards

- Gain security program leadership from senior cyber personnel
- Design impactful, strategically aligned cyber programs
- Understand root causes of control deficiencies and implications of various remediation plans, as well as develop remediation roadmaps
- Identify and prioritize the cybersecurity risks and risk management strategies relevant to their business and technical environments
- Develop security education and awareness programs
- Conduct collaborative tabletop exercises and crisis exercises to raise response capabilities and awareness
- Address existing and emerging security and privacy regulations
- Develop dashboards to measure key performance metrics and identify trends

80,000

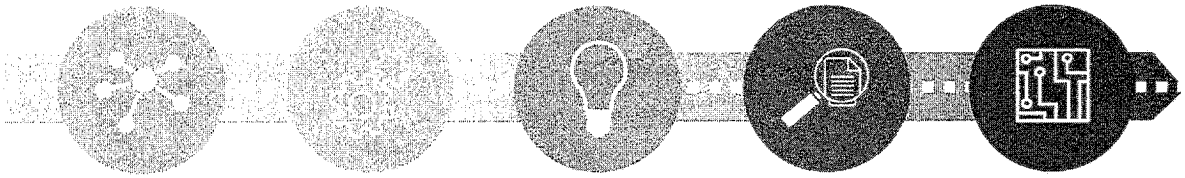
hours of cybersecurity and technology related assessments annually

When providing cybersecurity assessments for the County, you can expect us to carefully consider your culture, complexity and strategic growth goals, assuring you of cybersecurity services and strategies that reflect your unique environment and risks. Our team members perform more than 80,000 hours of cybersecurity-related assessments annually, translating into a deep understanding of IT as a business enabler. The following are two brief summaries of clients receiving cybersecurity assessment services from Baker Tilly:

- **Cybersecurity assessment:** An organization with numerous systems in multiple physical locations required an independent technical cybersecurity assessment to determine vulnerabilities in IT architecture and system configurations. Baker Tilly analyzed the IT security configurations of more than 400 systems using automated vulnerability scanning and penetration testing tools and detailed manual configuration reviews. In addition, Baker Tilly reviewed the supporting IT security processes. We identified numerous critical systems with poor security configurations and control gaps. Baker Tilly developed prioritized practical improvements for the County's security architecture, security configurations and corresponding IT processes.

- **Social engineering/phishing test:** A County sought help to assess the strength of the human element in its security. Baker Tilly performed a phishing test, creating a fictitious website masquerading as a wellness program and sending an email to targeted employees, attempting to download documents and capture their network credentials. We analyzed phishing results to identify trends, key risks and common themes and, finally, drafted a report outlining our observations as proposed mitigation strategies.

Our Cybersecurity Services



Advisory

- Strategic cyber advisory
  - Board of directors
  - C-suite
- Cyber policy & program development
- Cyber risk assessment
- Breach response preparedness planning
- Cybersecurity compliance readiness
- Pre-loss risk assessment
- Cyber risk insurance analysis
- Crisis claims consulting
- Business interruption risk advisory

Operations

- Virtual CISO/CTO
- Cybersecurity program design and implementation
- Security operations center services
- Integrated security testing services
- Penetration testing and vulnerability scanning
- Cyber hunting service
- SEIM content/ tuning service
- Incident response service

Education

- Security education and awareness programs
  - Board security education
  - Cyber hygiene
  - Social engineering
  - Phishing
  - Ransomware
- Simulation, exercises and war games
  - Board crisis exercises
  - Breach management
  - Tabletop exercises
  - Red team

Governance

- IT project risk review
- IT risk assessment
- IT effectiveness assessment
- Business continuity planning, management and testing
- Disaster recovery programs
- Supplier risk interruption (external risk)
- Compliance program assessments

Assurance

- HITRUST validation
- IT audit
  - Outsourcing
  - Co-sourcing
- IT SOX
  - Readiness
  - Testing
- SOC reporting
  - SOC for Cybersecurity
  - SOC 1 and 2
  - SOC 2 + HITRUST

Appendix I: Resumes

David Ross, MBA, MEng, CIPP/E

David is a principal and our firm's cybersecurity and privacy practice leader.

Baker Tilly Virchow Krause, LLP
Principal
8219 Leesburg Pike
Suite 800
Tysons, VA 22182
United States

T +1 (703) 923 8282
M +1 (301) 792 2073
david.ross@bakertilly.com
bakertilly.com

Education
Georgetown University – McDonough School of Business (Washington, D.C.)
Master of Business Administration

ESADE Business School (Barcelona, Spain)
Master of Business Administration

University of Maryland – A. James Clark School of Engineering (College Park, Maryland)
Master of Mechanical Engineering

Carnegie Mellon University (Pittsburgh, Pennsylvania)
Bachelor of Science, Chemistry and Industrial Management

David is a principal, leader for our privacy practice as well as cybersecurity advisory leader, who has been with Baker Tilly since 2017. David joined us in 2017 from Deloitte's cyber risk practice, where he provided strategic insight, service design, business development and engagement leadership. Previously, David was general manager of General Dynamics Commercial Cyber Services, where he was not only responsible for the design of the business, but also the launch and management of the new commercial organization. As a recognized thought leader and published author, David frequently speaks on cybersecurity strategy, innovation, business strategy, building high performing sales strategies, and critical problem solving for corporations.

Specific experience

- Serves as partner-in-charge for Virtual Chief Information Officer (VCISO) and Virtual Data Protection Officer (VDPO) engagements
- Serves as partner-in-charge on General Data Protection Regulation (GDPR) and other privacy readiness assessment services
- Provides leadership, management and strategic direction for the firm's cybersecurity practice
- Provides leadership in business development, commercialization, service design and growth strategies across RIAC practice
- Proven innovation and business transformation leader in the cybersecurity, pharmaceutical, healthcare and manufacturing sectors
- Advises clients and boards on the strategic aspects of cybersecurity
- Serial entrepreneur

Industry involvement

- National Association of Corporate Directors – Board Leadership Fellow (2016 – Present)
- American College of Corporate Directors (2016 – Present)
- Intelligence and National Security Alliance – Financial Threats Task Force (2015 – Present)
- Georgetown University McDonough School of Business – Adjunct Professor (2012 – Present)

David Ross, page 2

Industry involvement, cont.

- Latin American Board – Lecturer (2012 – 2016)
- Johns Hopkins Cary School of Business – Adjunct Professor (2012 – 2014)
- The Nantucket Project – Fellow (2012)
- Georgetown University – Entrepreneur in Residence (2011 – 2013)
- International Association of Privacy Professionals – Member (2017-present)

Community involvement

- Propagenix – Director Emeritus (2014 – Present)
- Nantucket Looms – Advisory Board Member (2012-2017)
- M3 Information – Advisory Board Member (2012 – 2013)
- Diversinet Corporation (DVNTF) – Advisory Board Member (2012)

Publications and patents

- Applying Visual Frameworks to Optimize Innovation Strategy; Global Science and Technology Forum Journal on Business Review Volume 2, No. 2 (ISSN: 2010-4804)
- The Path/Goal Problem – A Visual Framework for Visualizing Innovation; 2nd Annual International Conference of Innovation and Entrepreneurship conferences proceedings (ISSN: 2251:2039)
- Continuously Compensating Bicycle Suspension System; United States Patent 5,921,572

Thought leadership

- Contributor for Bisnow's article: Why You Should Hire a (Virtual) CISO – May 2018

Heather S. Acker, CPA

Heather Acker, Public Sector Professional Practice Leader, has been with Baker Tilly since 1997

Baker Tilly Virchow Krause, LLP
Partner
10 Terrace Ct
Madison, WI 53707
United States

T +1 (608) 240 2374 | Madison
T +1 (312 729 8188) | Chicago
heather.acker@bakertilly.com
bakertilly.com

Education
Bachelor of Business Administration in Accounting
University of Wisconsin–Madison

She is responsible for the quality oversight of the public sector assurance practice of the firm. Throughout her career, she has specialized in serving the needs of state and local government clients. Heather has experience with numerous types of financial and compliance audits including single audits. She has also helped many governments with consultation and implementation of various Governmental Accounting Standards Board (GASB) pronouncements.

Specific experience

- Leader in Baker Tilly's Professional Practice Group
- Partner of the financial audits of numerous municipalities and counties
- Partner of single audits in accordance with the Uniform Guidance
- Provides technical assistance to local governments in preparing Comprehensive Annual Financial Reports that receive the GFOA certificate for excellence
- Provides Tax Incremental Financing (TIF), Business Improvement District (BID), and Special Service Area (SSA) auditing, reporting and consulting services
- Presents audit reports to local government boards and committees
- Provides GASB strategic planning and implementation services to clients
- Provides guidance on accounting policies and procedures to improve the operation of the accounting function and strengthen internal controls
- Provides a variety of accounting and budgeting assistance to municipalities
- Oversees the Baker Tilly Public Sector Assurance Committee
- Leads the Baker Tilly Single Audit Committee
- Oversees firmwide public sector and single audit training and audit methodology updates
- Performs peer reviews
- Licensed CPA in Illinois and Wisconsin

Heather S. Acker, page 2

Industry involvement

- American Institute of Certified Public Accountants (AICPA)
- Chair of the AICPA State and Local Government Expert Panel (2016-present)
- AICPA Government Audit Quality Center (GAQC) Executive Committee (2012–2015)
- AICPA State and Local Government Expert Panel (2009–2012 and 2015-present)
- AICPA Peer Review oversight program
- GASB Tribal Government Accounting Workshop Group (TGAWG)
- Government Finance Officers Association (GFOA)
- GFOA Special Report Review Committee
- Wisconsin Institute of Certified Public Accountants (WICPA)
- Wisconsin Government Finance Officers Association (WGFOA)
- Illinois Government Finance Officers Association (IGFOA)
- Speaks at national and regional industry conferences
- Authors published articles on municipal accounting issues
- Recognized contributor to:
  - AICPA "State and Local Government Audit Guide"
  - AICPA "Government Auditing Standards and Single Audit Guide"
  - AICPA "State and Local Government Audit Risk Alert"
  - AICPA "Government Auditing Standards and Single Audit Risk Alert"
  - AICPA "State and Local Governments Illustrative Financial Statements"

Kenneth Zoline, CISSP

Ken is a senior manager with our cybersecurity and IT risk consulting practice.

Baker Tilly Virchow Krause, LLP
Senior Manager
205 North Michigan Avenue
Chicago, IL 60601
United States

T +1 (312) 729 8346
ken.zoline@bakertilly.com
bakertilly.com

Education
Master of Science in Computer Science
Illinois Institute of Technology

Bachelor of Science in Computer Science
University of Illinois–Urbana-Champaign

Ken has 23 years of advisory experience in security and networking, four years of director-level experience developing and managing an information security and risk management program for SPSS Inc. (acquired by IBM) and four years of security operations management experience working for IBM global technology services. Additionally, Ken has taught college-level cybersecurity courses.

Specific experience

- Performs cybersecurity testing: network, host and application vulnerability scanning, integrated security testing, vulnerability assessments, penetration testing, and cyber-attack simulations
- Performs control assessments (gap, maturity and compliance) for following frameworks and standards: CSC, FFIEC, ISO 27002, HIPAA Security Rule, NIST CSF, NIST SP800-53 and PCI DSS
- Performs IT and cybersecurity focused risk assessments
- Performs threat modeling and threat assessments
- Performs vulnerability management assessments
- Develops and improves clients' cybersecurity policies, standards, procedures, business processes and controls
- Develops security programs
- Provides security consultation to client executive management, committees and board of directors
- Regularly leads teams delivering a broad range of cybersecurity-related consulting services

Industry involvement

- The International Information Systems Security Certification Consortium ((ISC)²)
- Information System Security Association (ISSA)
- Infragard – Chicago
- Institute of Internal Auditors (IIA)
- Information Systems Audit and Control Association (ISACA) (presenter)
- Healthcare Financial Management Association (HFMA) (presenter)
- Cloud Security Alliance (CSA) (past contributor)

Alex Islamov, CISA, CIPT

Alex is an experienced manager within the risk, internal audit and cybersecurity practice.

Baker Tilly Virchow Krause, LLP
Experienced Manager
205 North Michigan Avenue
Chicago, IL 60601
United States

T +1 (312) 622 8315
alex.isalmov@bakertilly.com
bakertilly.com

Languages
English

Education
University of Nebraska–Lincoln
Bachelor of Business Administration (Accounting & Management Information Systems)

University of Nebraska–Lincoln
Masters of Professional Accountancy

Alex has been with the firm since 2018. He has more than 12 years of leadership and management expertise within international firm professional services and industries ranging from healthcare, telecommunications, manufacturing, oil and gas, and retail. Alex is effective at driving IT, security, governance, risk management and internal audit programs.

Specific experience

- Performs quality assurance reviews, providing advice on implementation of leading practices and assessing direct compliance with relevant regulations
- Plans, performs and executes SOC1, SOC2 and SOC2+ report projects across a wide variety of industries and frameworks (e.g., NIST, ISO 27001 and HITRUST)
- Provides assistance in identifying, documenting and testing internal control in relation to SOX compliance from both a financial and IT perspective
- Performs consulting services to plan, develop, execute and improve internal control procedures for suitability of design and operational effectiveness
- Performs organization-wide risk assessments with a focus on qualitative and quantitative evaluation of risk associated with critical application systems and infrastructure components supporting key business processes, technology and upcoming significant initiatives
- Performs information privacy and security reviews, focusing on current information privacy and security policies, procedures and practices, and the monitoring mechanisms in place to identify new information privacy and security laws and regulations

Industry involvement

- International Association of Privacy Professionals (IAPP)
- Information Systems Audit and Control Association (ISACA)
  - ISACA Vice President Tulsa Chapter 2009–2010
- Institute of Internal Auditors (IIA)