Duke | OFFICE *of* AUDIT, RISK & COMPLIANCE

2025

Values in Action

Respect. Excellence. Inclusion. Trust. Discovery.

ANNUAL REPORT

The Office of Audit, Risk and Compliance (OARC) advances and integrates risk awareness, internal controls and compliance requirements; collaborates on proactive and innovative improvements to business processes; and provides high quality assurance services to Duke's entities and governing boards.

Our Commitment

Our strategic objectives guide our focus on five core themes:

- **Operational excellence.** Ensure time, people and resources are efficiently deployed and effectively prepared for the work.
- **Trust and relationships.** Provide transparent, fair, unbiased and informed interactions, engagement and reporting to leadership, colleagues, clients and members of the governing boards; demonstrate genuine interest in our colleagues' goals and compassionate response to their concerns.
- **Purposeful value.** Combine an in-depth understanding of "why" with an insightful perspective on "how" to validate institutional performance; identify threats to values, compliance, controls, processes and outcomes; and recommend improvements that make Duke better prepared to achieve excellence while balancing risks and benefits.
- **Inclusion and respect.** Value, support and advocate for office and institutional culture that appreciates all perspectives, develops professional abilities, and rewards accomplishment.
- **Discovery and innovation**. Move boldly forward by embracing growth, change and improvement as opportunities for advancement and achievement; and support others in achieving excellence.

Workplace Culture in Action

Welcoming & Valued

Attract diverse talent, host events that celebrate our cultural richness, and create spaces where everyone feels respected

Recognition & Fairness

Celebrate achievements, milestones, contributions while ensuring equitable compensation and advancement opportunities

Open Communication

Encourage honest, constructive dialogue for sharing ideas, feedback, and concerns

Growth & Well-being

Provide professional development, mentorship, and access to Duke programs that support both career aspirations and personal wellness

Our Work

KEY GROUP ACCOMPLISHMENTS

Internal Audit & SPARC

- Completed campus-wide IT risk assessment and data protection projects, highlighting opportunities to strengthen institututional security posture.
- Support for DHIP integration focused on compensation workflows and accurate execution of first year incentive compensation.
- Collaborated with research operations to monitor federal government actions to evaluate the potential impact on research activities.
- Completed advisory engagements to support management response to univsersity strategic realignment and budget reductions.

Enterprise Risk Management

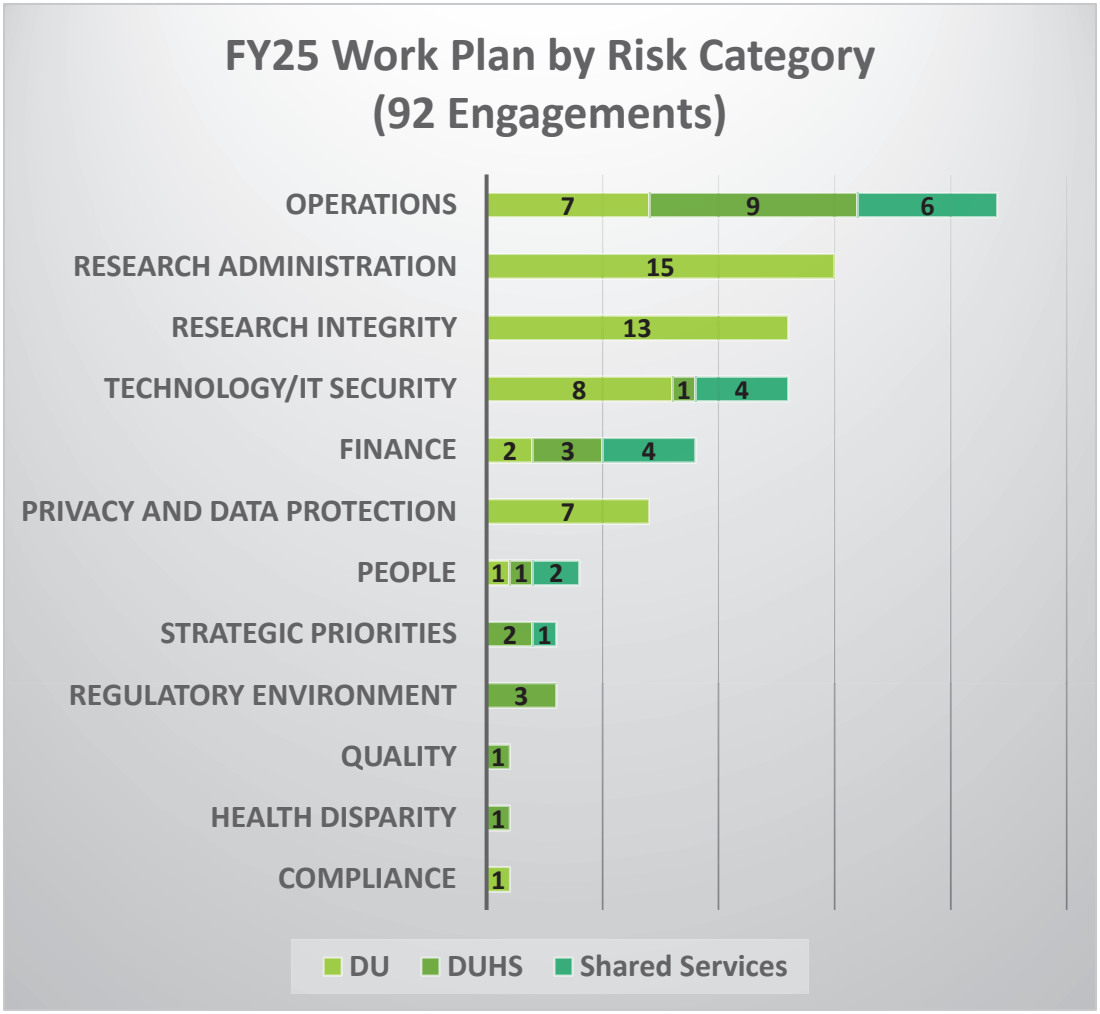
- Executive and senior leader engagement to define priorities and mitigation strategies
- Linked strategic risk priorities and governance visibility for the Board of Trustees and its committees
- Tracked emerging risk areas and incorporated into risk management concepts

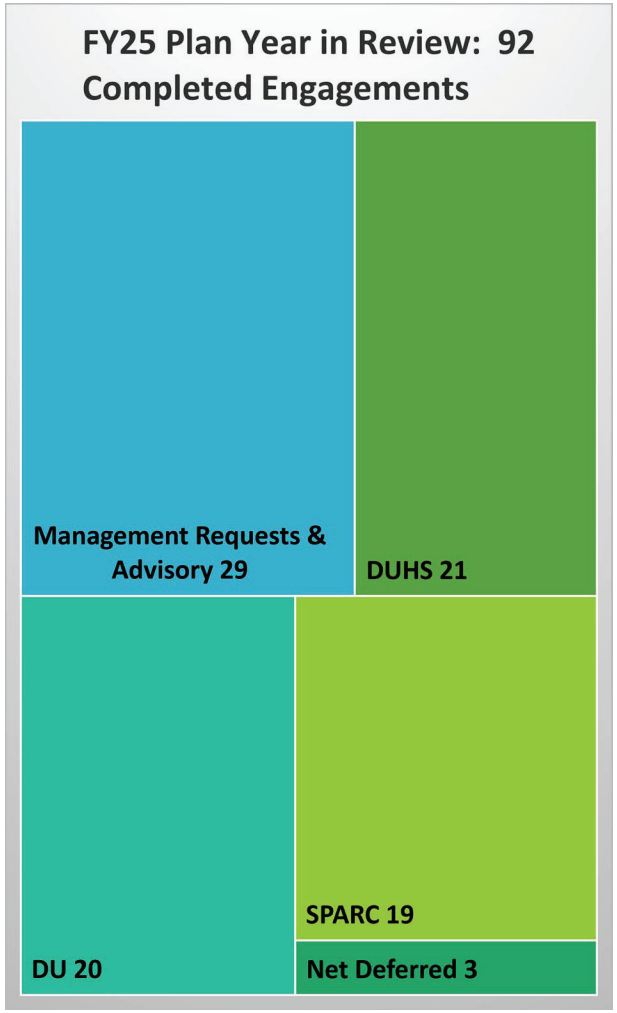
Institutional Ethics & Compliance Program

- Launched key compliance program initiatives: compliance ownership matrix, regulatory management software, and reducing training burden
- Completed 5 programmatic maturity assessments
- Developed privacy position statements to help guide local units.
- Supported privacy enablement through 288 consultations
- Administrative COI process refinement and collaboration with research partners.

ASSURANCE PROGRAM HIGHLIGHTS

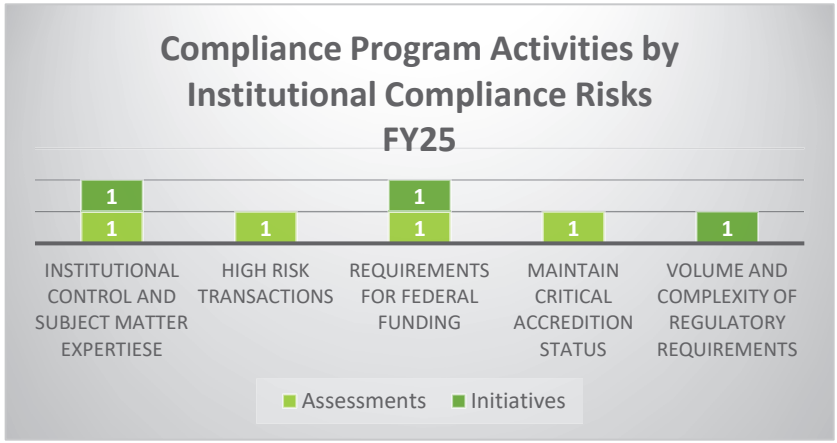
The FY25 assurance plan included 92 engagements. To accommodate 33 management requests, advisory support, and investigations, some engagements were deferred or cancelled. Ultimately, 89 assurance engagements were completed in FY25.



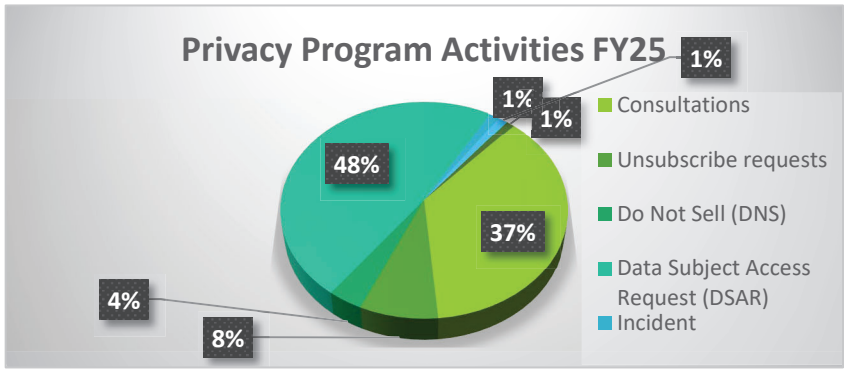


COMPLIANCE AND PRIVACY PROGRAM HIGHLIGHTS

The OARC compliance team conducted functional reviews to assess processes, resource use, and risk management, while launching new initiatives aligned with key risks.

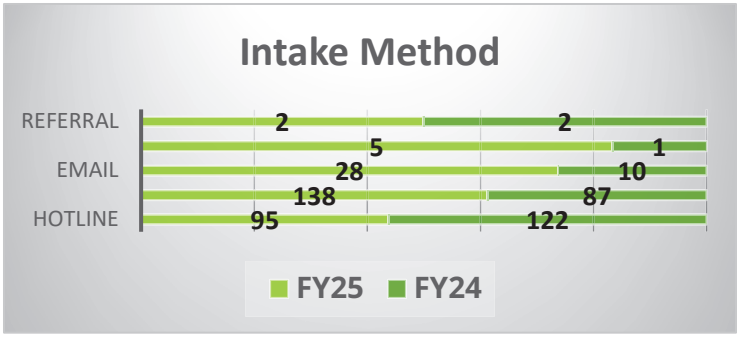


The privacy team managed risks tied to data collection, breaches, notifications, and cross-border transfers.



COMPLIANCE SERVICES HIGHLIGHTS

The following charts represent concerns that flowed through OARC Compliance Services reporting channels during FY25 and FY24 and were either triaged to other offices or handled directly by OARC.



OARC Compliance Services actively reviewed 12 concerns in FY25, performing investigations, and issuing memos for two cases. For the other ten items, the team collected additional information and then coordinated and led meetings across institutional functions to ensure appropriate handling of each concern.

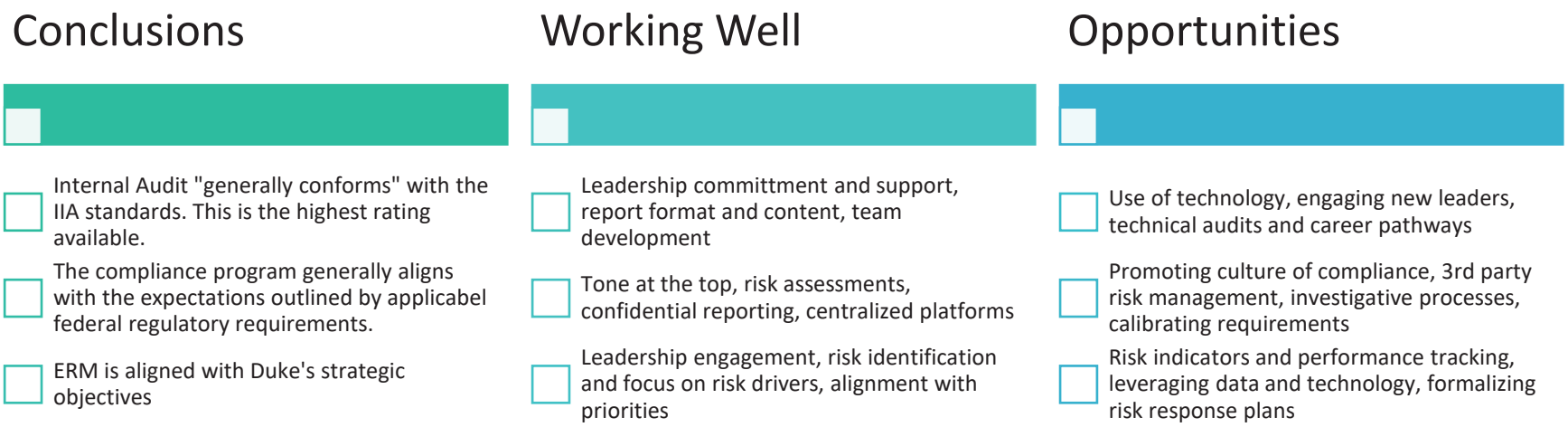
CONTINUOUS IMPROVEMENT

Under professional standards for high-performing assurance functions, an independent quality assurance review (QAR) is conducted every five years. A QAR helps to identify areas of improvement that can increase effectiveness and organizational value, identify potential blind spots that can sometimes go undetected by those closest to the work.

The independent QAR conducted in the Fall of 2024 by Deloitte assessed:

- **Internal Audit** activity for conformity with the Institute of Internal Auditor's International Standards for the Professional Practice of Internal Auditing (the Standards)
- **Institutional Compliance Program** for alignment with the U.S. Department of Justice's Elements of an Effective Compliance Program
- **Enterprise Risk Management** program for alignment with Duke objectives and leading best practices

The Deloitte team reviewed our processes and documentation, and conducted onsite interviews with OARC staff, Duke senior leaders and other key stakeholders. The QAR review identified departmental strengths and provided recommendations for continuous improvement, which were presented to the audit and compliance committees in early 2025. All management action plans will be completed during calendar 2025.



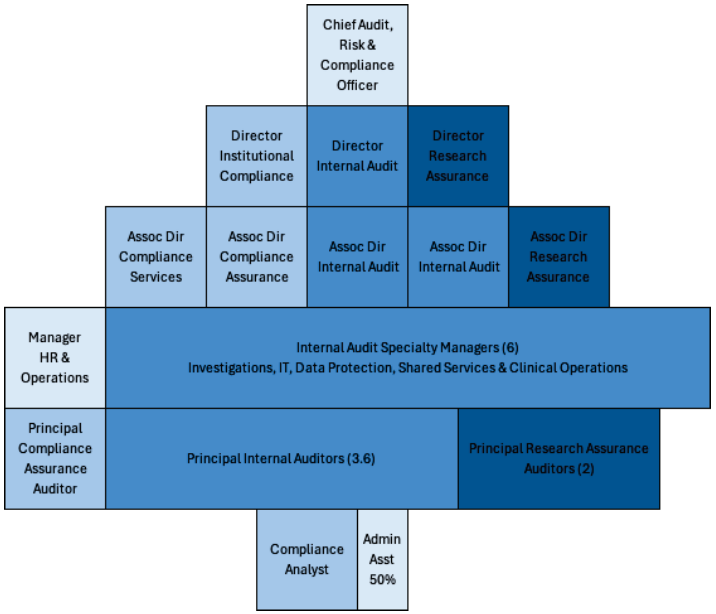
Our People

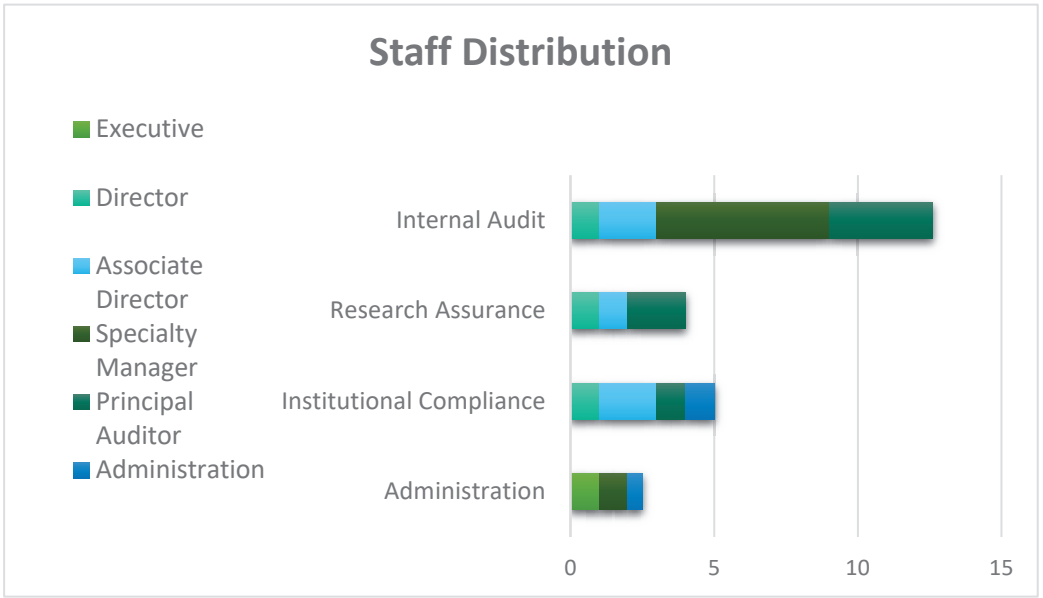
PERSONNEL AND ORGANIZATION STRUCTURE

We focus on hiring high-caliber professionals with proven experience in a combination of audit, compliance and industry settings.

We value a blend of seasoned professionals who have built knowledge and relationships specific to Duke, as well as those who are early in their careers and offer a fresh perspective. Our specialty manager and associate director roles promote continuity in areas that benefit from deeper knowledge: health system and clinical operations, IT audit, technology risk and data protection, shared services, research compliance, research program compliance, and investigations.

OARC currently has 25 positions across three teams that serve eight functional areas: university and shared services internal audit, health system internal audit, IT internal audit and data protection, sponsored programs assurance, university privacy, and institutional programs for compliance, ethics, and enterprise risk management. Please refer to Office Leadership for more information.





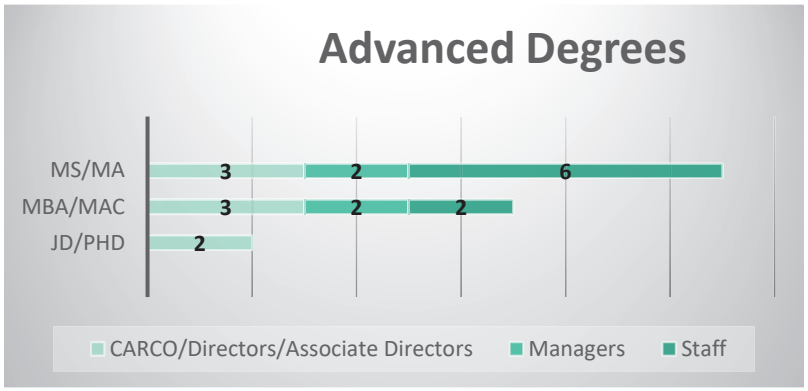
EXPERIENCE, CREDENTIALS AND PROFESSIONAL CONTRIBUTIONS

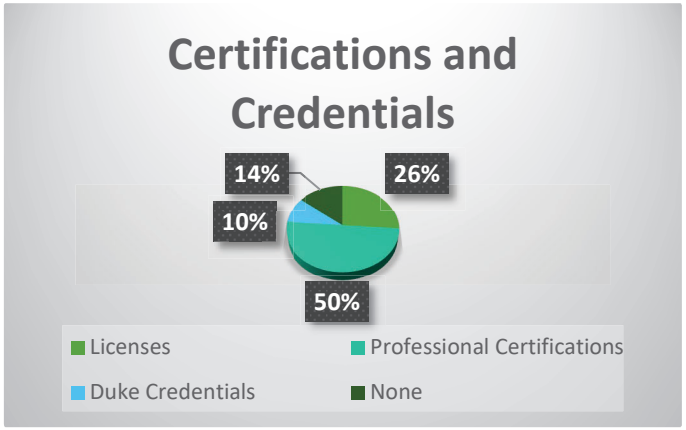
OARC hires professionals with a range of experience and expertise. We seek to recruit, retain and promote purpose-driven and highly motivated professionals who want to make meaningful contributions to health care, research and higher education.

Everyone in OARC has a personalized professional development plan that aligns with competencies at each level and with career aspirations.

Leadership positions in the office require relevant professional credentials, including advanced credentials and/or industry certifications. We encourage all team members to pursue professional credentials and certifications that support office goals, career development and specialty knowledge.

Common certifications: Certified Public Accountant (CPA), Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Healthcare Privacy Compliance Certification (CHPC), Duke's Research Costing Compliance (RCC)



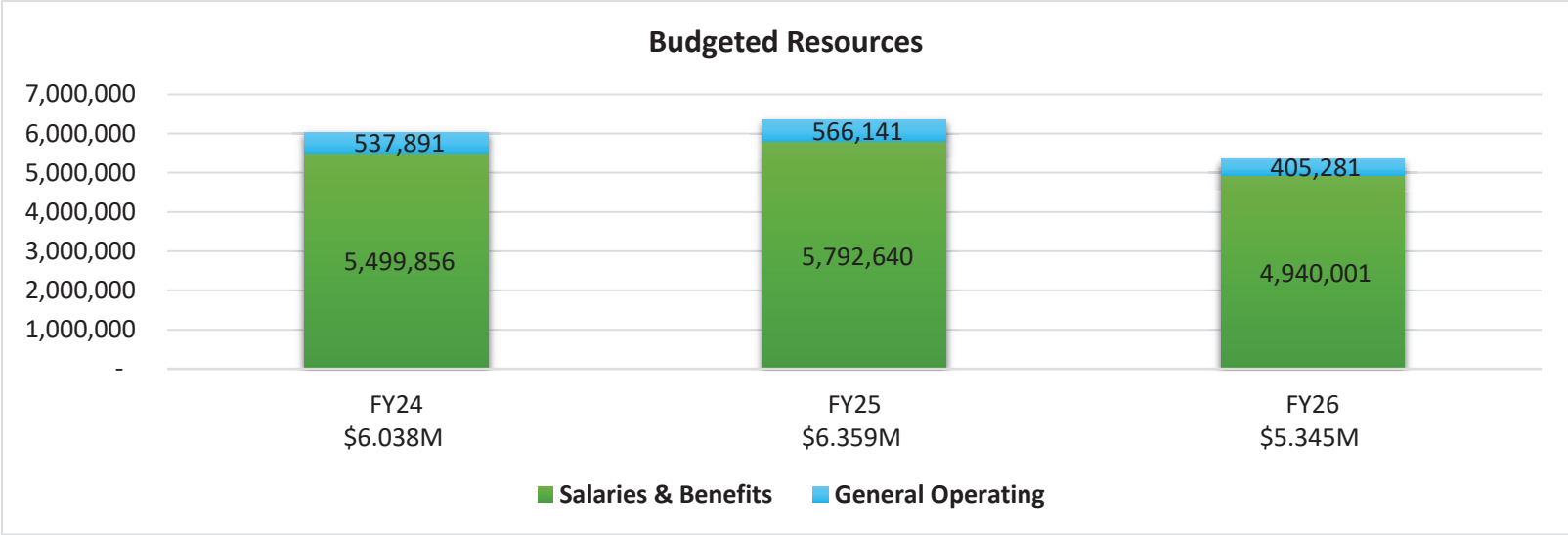


Financial Resources and Cost Realignment

Over the past 10 years, OARC has pursued continuous improvement and practiced conservative stewardship of our financial resources. Over a time that Duke's consolidated operations grew 85%, OARC's continuous improvement strategy held our departmental cost structure growth to only 22%. We accomplished this while also making technology investments that benefit all of Duke and ensuring competitive compensation to retain talent.

As part of our ongoing commitment to responsible stewardship and long-term institutional resilience, OARC has achieved the mandated 20% cost reduction target through voluntary separations (from 33 positions to 25) and non-compensation expense controls.

OARC is actively pursuing lean operating strategies and technology adoption to help us retain the breadth and depth of assurance services for all Duke entities. These realignment measures are designed to uphold our mission to provide independent oversight, promote accountability, and safeguard institutional integrity, while adapting to financial constraints and shifting priorities across Duke.



Office Leadership

Leigh Goller – Chief Audit, Risk and Compliance Officer. Leigh has institutional responsibility for directing and coordinating integrated internal audit and risk management functions, both of which have enterprise-wide scope; oversight for a federated university compliance function; and accountability to enhance the ability of these functions to advance Duke's mission. Leigh's degrees are in accounting (UNC Charlotte) and liberal studies (Duke), and she is a CPA.

Kelley Hikade – Director of Institutional Compliance Programs. Kelley oversees the university's privacy program, compliance services (including dual interests management, sanction monitoring, and case coordination), and a federated compliance structure. She holds a BBA in International Business, an MBA in Marketing from the University of Memphis, and a Pharmaceutical & Medical Device Compliance and Law Certification from Seton Hall University School of Law.

Vanessa Peoples – Director of Sponsored Programs Assurance and Research Compliance (SPARC). Vanessa's team conducts assurance reviews to assess risk and evaluate the effectiveness of programs supporting sponsored programs administration and clinical research across Duke's research enterprise. She holds a B.S. in Finance from the University of Delaware, an M.B.A. from North Carolina Central University, and is a Certified Internal Auditor.

Joanna Rojas – Director of Internal Audit. Joanna leads the internal audit team, providing independent insight on governance, risk management, and internal controls for Duke University, the health system, DUMAC, Inc., and related entities. Her team conducts risk-based audits across financial, operational, compliance, and IT processes. She holds a B.S. from Florida State University, an M.B.A. from Florida Gulf Coast University, and is a Certified Information Systems Auditor.

Associate Directors for Internal Audit, Compliance Services and Privacy. These positions are held by **Ken Stern** (internal audit), **Summer Webbink** (compliance services), **Krista Kenney** (research assurance) and **Alexandra Marban** (compliance and privacy). Ken, Summer, Krista, and Alexandra have a combination of experience in corporate finance, public accounting, law, internal audit, research operations, and privacy program.