Technology disruptions are increasing the demand for cyber-related audits. More than two-thirds of participants in an FSAC webinar on cybersecurity said their internal audit function has performed cyber-related audits. Most said their functions use a combination of second line and third line of defense resources for technology/cyber testing, and outsourcing is common.

### Internal Audit Performs Cyber-related Audits

- **Yes, 65%**
- **No, 20%**
- **Uncertain, 11%**
- **Not applicable, 4%**

### Functions Relied on for Technology/Cyber Testing

- Only rely on internal audit's own activities: **21%**
- Combination of second and third line to cover cyber: **49%**
- All cyber audits performed by second line: **8%**
- Uncertain: **17%**
- Not applicable: **5%**

### Resources Used for Technology Audits

- Full-time internal technology auditors only: **25%**
- Combination of internal and external resources: **42%**
- Fully outsourced technology audit: **23%**
- Uncertain: **6%**
- Not applicable: **4%**

*Source: Polling questions from the FSAC May 2017 webinar titled Cybersecurity: How Does Internal Audit Keep Up? presented by Khalid Wasti, a partner in PwC Internal Technology Audit Solutions. Webinar attendees are members of the FSAC. Internal audit staff levels: CAE (20%), direct report CAE (8%), audit manager (20%), staff (39%), other or not applicable (13%). n = 348.*

**Visit the Center**

Find out more about the FSAC at www.theiia.org/FSAC.

Copyright 2017 by The Institute of Internal Auditors, Inc. All rights reserved. For permission to reproduce, please email fsac@theiia.org.