# Mobile Computing:

## A Study of Internal Auditors' Awareness

2013 Research Committee

Dallas Chapter
Institute of Internal Auditors
Established 1949 | A Platinum Level Chapter

# Table of Contents

# INTRODUCTION

Business professionals around the world have been using mobile devices for everyday business activities for years. Tech savvy professionals are quick to purchase the newest mobile phones and devices the instant they are released. The use of mobile devices for business, or the concept of Mobile Computing, is not a new one in the year 2013; however, because technology and its application in business is ever-changing, the challenge for the internal audit profession has increased tenfold. The risks associated with the use of Mobile Computing to an organization continues to grow as more and more employees use mobile devices in their daily work activities. The Dallas Institute of Internal Auditors (Dallas IIA) Research Committee (Committee) wanted to research this trend to understand the awareness of Internal Audit professionals on Mobile Computing and its implications to their organizations.

The key objective of this research project is to gain an understanding of the current state of awareness of Mobile Computing and the implications of this technology to the Internal Audit profession in the Dallas and Ft. Worth areas. The Committee reviewed numerous existing studies and presentations on Mobile Computing from technology professionals in the Dallas and Ft. Worth areas, as well as other case study trends from around the country and the world. The definition and trends are outlined in this paper to help frame the level of awareness. The Committee then identified and highlighted various implications related to Mobile Computing, as it relates to the internal audit profession. In order to understand the internal audit professional awareness from a local perspective, the Committee surveyed the members of the Dallas IIA, as well as the Information Systems Audit and Control Association's North Texas

Chapter (ISACA) to gain a local perspective. The survey attempted to determine the overall awareness of Internal Auditors with respect to Mobile Computing in the respondents' respective organizations. The Committee performed various analyses on the survey results. The result and overarching themes derived from the analyses, along with future opportunities for research, are outlined in later sections of this paper.

## MOBILE COMPUTING

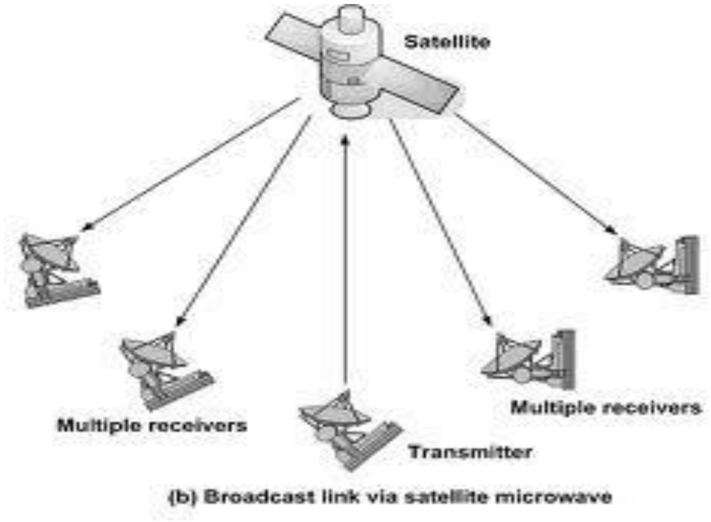
Mobile Computing has changed the way industry conducts business by offering constant connectivity, allowing users to conduct business at any place and time, and in return increasing productivity (ISACA North Texas, 2010).  According to a study conducted by Gartner (2012), mobile phones will be the most commonly used device during 2013, beating out personal computers. Within an organization, mobile devices allow employees to have access to all the necessary business resources without stepping foot in the office.

## LITERATURE REVIEW

In an effort to gain an understanding of Mobile Computing, the Committee reviewed existing studies to understand risks within internal audit. The following are definitions, articles, and studies utilized in our analysis.

### DEFINITION

Mobile Computing is defined as "an umbrella term used to describe technologies that enable people to access network services any place, anytime, and anywhere." (Kumar, 2011) Kumar also explained that Mobile Computing was originated based on the cellular concept by Don Ring of Bell Labs, USA in 1947. The cellular concept is based on a network of cells that span a large geographical area to communicate. The principle is that each mobile device uses a separate, temporary radio channel to talk to each cell site, then the cell site can communicate with many mobile devices at once while using one channel per mobile (Kumar, 2011).



(Source: Kumar, 2011)

## MOBILE DEVICE TYPES AND USES

ISACA's white paper on *Securing Mobile Device,* published in August 2010, stated that mobile devices can mean a multitude of things. They defined the following as types of mobile devices:

- Smartphones (i.e. iPhone);
- Laptops;
- Tablet Computers (i.e. iPad);
- Portable Digital Assistants (PDAs);
- USB's (Portable Universal Serial Bus Devices);
- Radio and Mobile Frequency Identification (RFID); and
- Infrared-Enabled Devices (IrDA).

Not all mobile devices are listed above, and it is important that an organization take the time to review all devices in use to determine how they want to define mobile devices. The devices listed allow for the user to communicate as well as provide information storage (ISACA, 2010). Employees are able to utilize networks, access company documents and drives, and have audio, video, and photographic capabilities. These are labeled as mobile devices because they allow the user to communicate from anywhere at any time. While mobile devices provide many benefits, they also introduce many risks.

## MOBILE COMPUTING BENEFITS, RISKS, AND STEPS TO MITIGATE

A Gartner forecast indicates during 2013, mobile phones will surpass personal computers as the most common web access device worldwide. Some benefits of Mobile Computing include:

- Increased productivity;
- Improved customer service;
- Quicker response time and problem resolution;
- Increased efficiency; and
- Work-life balance.

Although mobile devices yield noticeable benefits, there are also increased risks. In order to assess risk, it is important to understand vulnerabilities which result in threats thus creating risks. Mobile devices have vulnerabilities such as data traveling over unsecure networks, mobility, loss of data, no authentication requirements, and no management of the device. In return, these vulnerabilities pose threats, such as viruses, malware, data intercept, lost or stolen device, and unsecure devices. Threats create risk. Risks of Mobile Computing could result in data interceptions, malware propagation, device corruption, exposure of confidential data, and dependence on mobile devices (ISACA, 2010).

The first step in addressing Mobile Computing risks is for an organization to develop a comprehensive policy that should apply to various mobile devices, be flexible and easy to implement, address loss and theft, include disaster response, be transparent and understandable (ISACA, 2010).

A mobile device management (MDM) policy should at least include policies to address risks such as anti-malware and firewall, application/operating system updates, application vetting, encryption, PINs, inactive-device lockout, jail break, remote wipe, and revoke access (Semer, 2013).

Due to the continuous expansion of Mobile Computing, organizations, at a minimum, should have an acceptable use document signed by all employees. This document should address the security of the devices as well as granting permission for the corporation's IT Department to inspect the device for compliance with company policy (Semer, 2013).

A white paper from 2012 entitled "Aligning internal audit" indicated that the top risk area in need of enhanced Internal Audit capability is data privacy and security (PwC, 2012). Because of the continued growth of Mobile Computing it is imperative for Internal Auditors to be aware of potential risks. Additionally, Internal Auditors should be involved in assessing and evaluating risks to ensure that Mobile Computing policies are adequate for their organizations.

# MOBILE COMPUTING TRENDS

Since both the public and private sector have experienced the convenience and benefits of Mobile Computing, it is likely that Mobile Computing will continue to expand in usage and risk. A recent study article by Gartner noted some of the emerging trends from Mobile Computing:

- 40% of the workforce will be mobile by 2016;
- 50% of non-PC devices will be purchased by employees by 2016, and by the end of the decade 50% of devices in business will have also been purchased by employees;
- 60% of industry will implement limited access network zones by 2016;
- 65% of all corporations will adopt MDM (Mobile Device Management) in the next five years to address security concerns;
- 90% of corporations will have to support at least two or more operating systems by 2017; and
- 25% of organizations will have a Chief Digital Officer by 2015.

Additionally, Gartner noted that there is an urgent need to separate personal and business operations on mobile devices. It also stated that BYOD (bring your own device) should be a top priority to address (Gartner, 2012). Semer indicated that another concern with BYOD is e-discovery. Litigation, in addition to unsecured storage of customer information, could potentially increase regulatory exposure (Semer, 2013).

Based upon our research, the Committee wanted to gauge the awareness of Internal Auditors in the Dallas and Ft. Worth areas. A survey was designed to determine awareness of Mobile Computing by assessing knowledge level and concerns of Mobile Computing, involvement in risk assessment, knowledge of company policies, ability to audit Mobile Computing policies, and training.

## RESEARCH METHOD, SURVEY DESIGN, AND DISTRIBUTION

As noted above, the Committee reviewed numerous white papers and articles around Mobile Computing. Specific data related to Internal Auditors' awareness of Mobile Computing has yet to be studied. Most of the research was sourced from information technology (IT) consultants, as well as IT auditors. With this in mind, the Committee chose to administer its own survey to gather information specific to all Internal Auditors in the Dallas and Ft. Worth area to gauge their awareness. This section discusses the survey design and administration along with the demographics of respondents and results.

The Committee started planning the study in September 2012. Initially, the Committee solicited ideas from professionals on the Committee, and then through interviews with the Committee's academic liaisons from the University of North Texas and The University of Texas at Dallas, as well as with other leaders from the Dallas IIA. The resulting list of ten potential topics was then reconciled and aligned with the IIA's stated research priorities (Institute of Internal Auditors, 2013). The final topic was selected and presented to the Dallas IIA Board Members for approval in October 2012. The team followed a project plan and timeline to meet certain milestones to complete the project.

The Committee hoped to obtain as much feedback as possible through its survey by taking advantage of the first annual Super Conference being held by the Dallas IIA on October 29, 2012. The conference planning committee agreed to distribute the survey via email to conference participants. Of the over 600 conference participants who received the email link to the survey, which consisted of mostly members of the Dallas IIA, the Committee received 158 responses.

In addition to the Super Conference, the Committee distributed the survey to the Dallas IIA members during the monthly luncheon meeting on December 6, 2012. In hopes of gathering even more data on Internal Auditors' awareness of the topic, the committee also reached out to the ISACA North Texas Chapter in December 2012.

An online survey tool was used to facilitate online data collection. The survey was held open until December 31, 2012. The Committee has learned from prior research projects that it must consider the possibility that respondents may be from professional services organizations or former Internal Auditors; therefore, the committee included instructions to respondents to use a representative client or a recent experience to answer survey questions. To encourage participation, a drawing for $25 gift cards, two at the Super Conference and two at the Dallas IIA luncheon in December, was advertised.

# SURVEY

The design of the survey was done to meet the objective of the research project, attempting to assess Internal Auditors' awareness of Mobile Computing. In order to minimize "survey fatigue", the survey was intended to take less than 10 minutes to complete. The survey consisted of 12 questions to assess awareness, and an additional four demographic questions about the respondents.

To gauge the respondents' knowledge level of the topic, the initial survey question asked their familiarity with the term "Mobile Computing." The respondents who assessed themselves as unfamiliar with Mobile Computing were asked further detailed questions to assess their overall awareness of mobile device usage.

Before the basic demographic questions were presented, the respondents were asked questions about:

- The respondents' familiarity with the term "Mobile Computing," and their awareness of the associated risks.
- The use of Mobile Computing in the individual respondent's organization, types of Mobile Computing devices used, if there is a corresponding policy related to their use, the respondent's awareness of the detailed policy around security, and any user training.

- The respondents’ knowledge of Internal Audit’s involvement with Mobile Computing, via review or risk assessment, and their level of skillset related to the concept of Mobile Computing.

Participants were asked demographic questions about their primary role as an auditor (IT or Non-IT), their title or level in their organization, the size of their organization and internal audit department, and their industry affiliation.

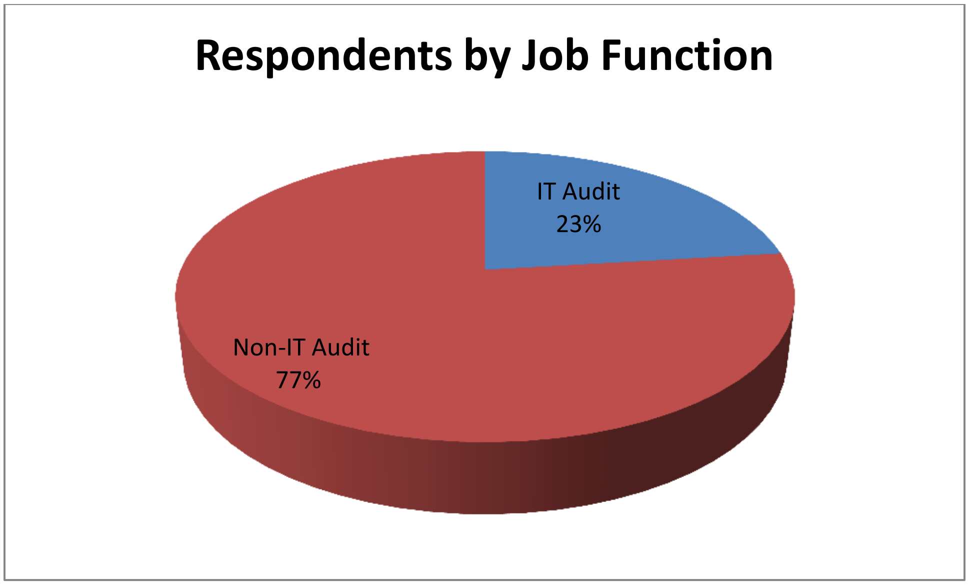
## SURVEY COMPLETION RATE AND RESULTS

The online survey was sent through email and links to approximately 600 Super Conference attendees, 2,062 Dallas IIA members, and presented to approximately 1,773 North Texas ISACA members. The initial email for the Super Conference yielded 158 completed surveys. An additional 62 surveys were completed through the online survey tool during the Dallas Chapter luncheon.  A total of 220 surveys were completed which equates to a 10% response rate of Dallas IIA members (Note: this does not include the 1,773 survey population sourced from the ISACA North Texas chapter). The relevant demographic information of the 220 respondents is noted below. Any skipped responses were excluded from our data analysis.

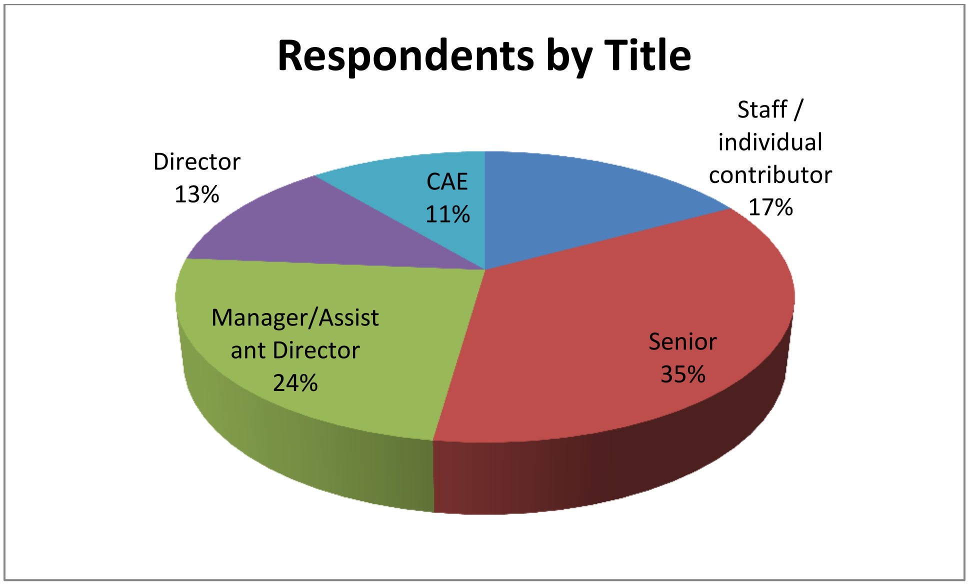
# PARTICIPANTS PROFILE

## Job Function And Levels:

Of the respondents, 23% described their job function as IT audit while 77% classified their function as Non-IT audit. This is an increase from the 8% response rate of IT auditors from last year's survey project (Dallas IIA Research Committee, 2012).

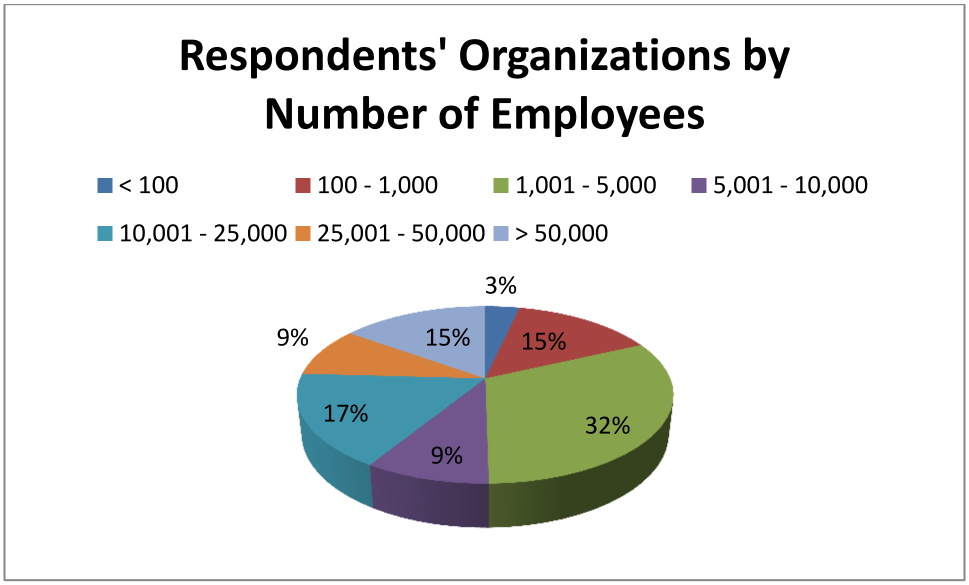


All organization levels are shown by the following distribution:

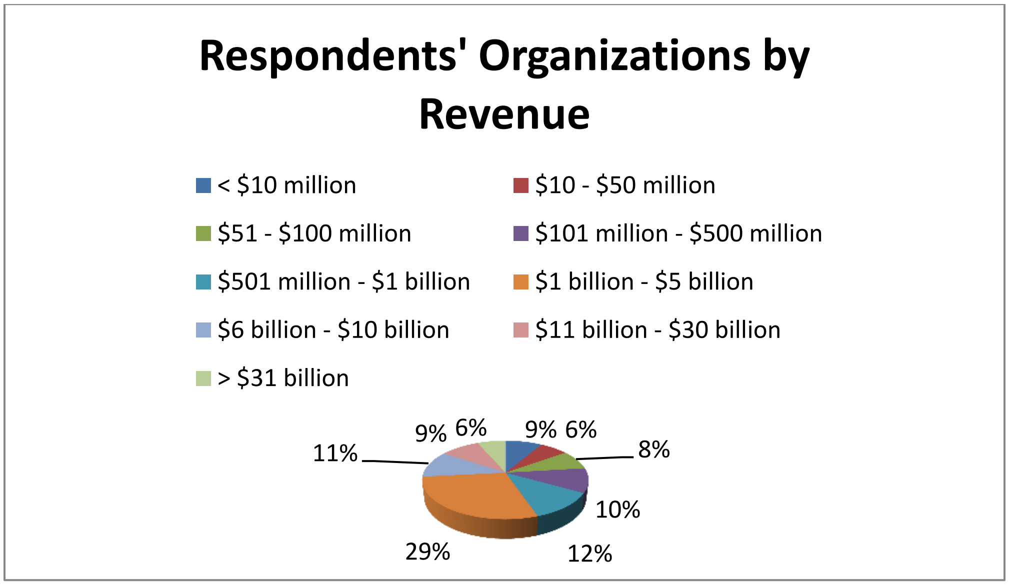


## Size Of The Respondents’ Organizations By Number Of Employees, Revenue, And Auditors:

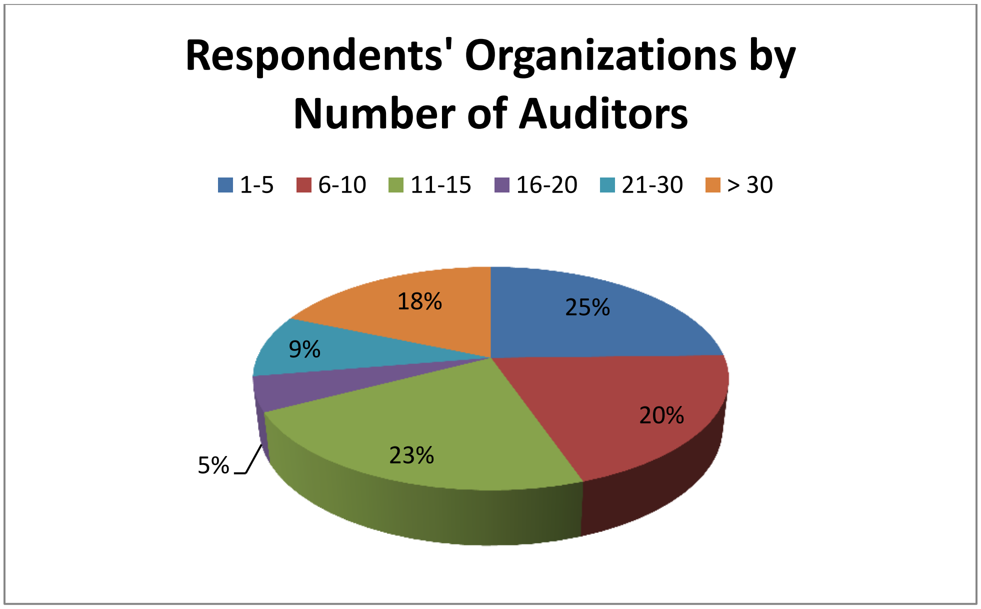
Of the respondents, 82% stated that there were over 1,000 employees in their organizations. The distribution is as follows:



The majority of the respondents were from larger firms, with 55% of the respondents reporting more than $1 billion in annual revenue. The distribution is shown below:



In addition, 55% of the respondents indicated that there were more than 10 auditors in their organizations. Below is the distribution:

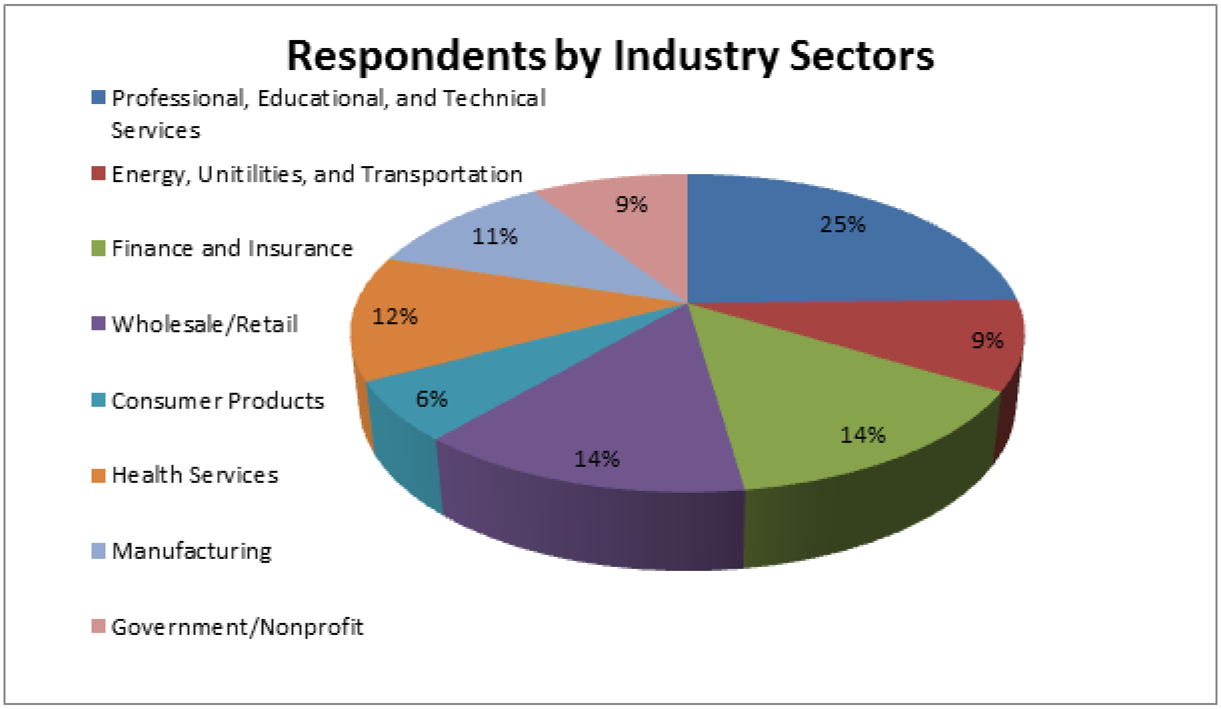


### Respondents' Industry Sectors:

A total of 22 industry sectors were represented, with the majority (76%) falling into one of the following categories:

- Professional/Educational/Technical services
- Finance and Insurance
- Wholesale/Retail
- Health Services
- Manufacturing

The distributions are as follows:

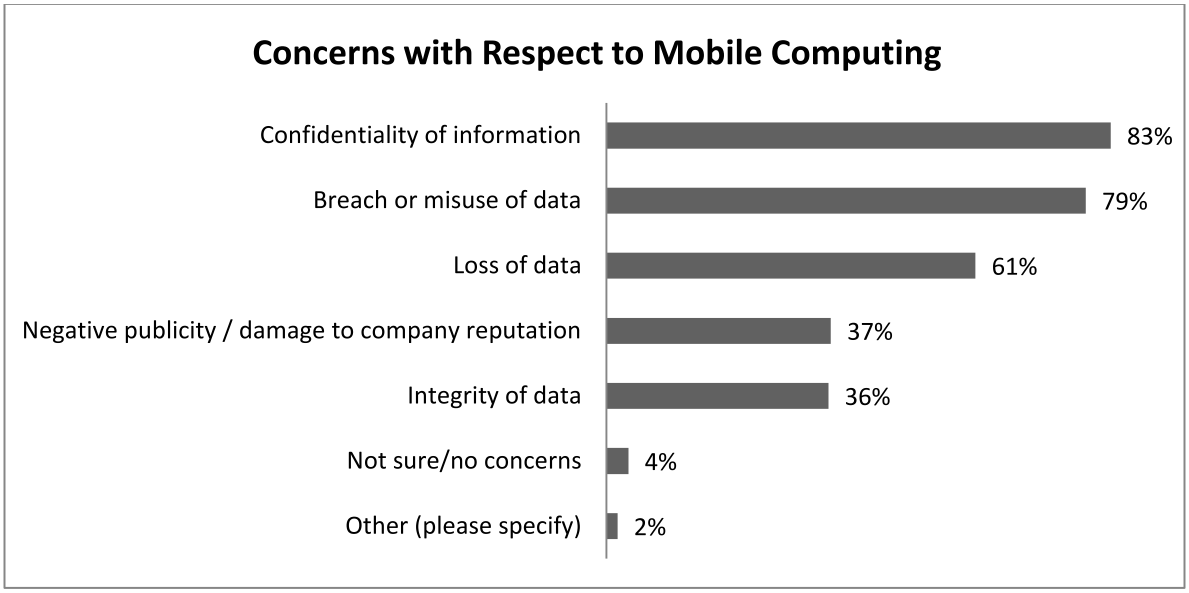


## SURVEY RESULTS

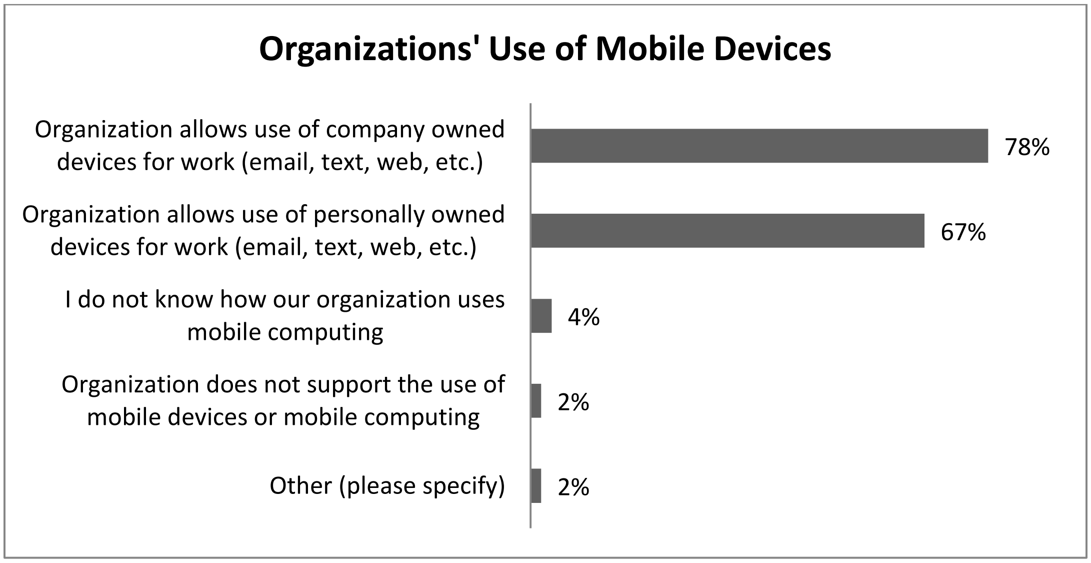
### 1. INTERNAL AUDITORS’ PERCEPTION OF MOBILE COMPUTING

The majority of respondents, or 205 (93%), indicated that they were familiar with the concept of Mobile Computing. Two respondents who said that they were unfamiliar with Mobile Computing were IT Auditors.

The respondents were asked to select all applicable concerns with respect to Mobile Computing. A summary of the responses is shown below:



When asked about their organizations' use of mobile devices, the respondents selected all applicable answers as follows:



In addition, the majority of the respondents (74%) acknowledged the existence of policies governing acceptable uses of mobile devices in their organizations.

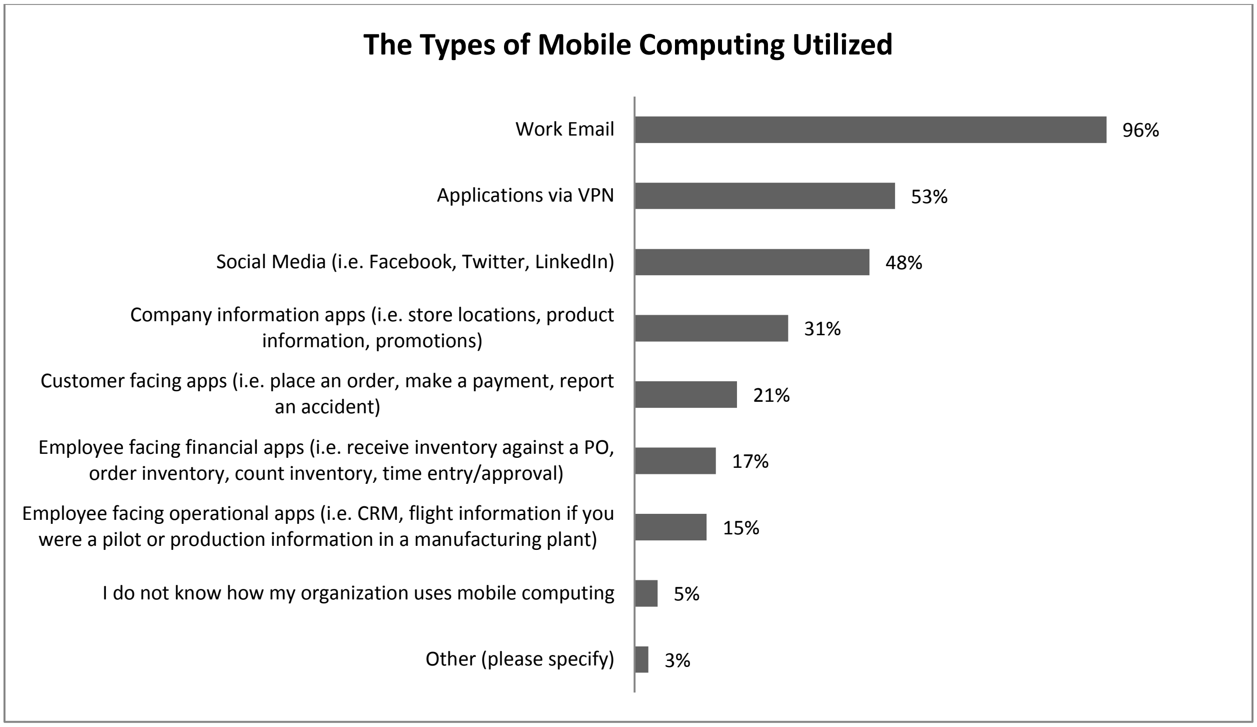
## 2. MOBILE COMPUTING POLICY COVERAGE

Over 68% of the 157 respondents (the other 63 skipped the questions) reported that the mobile policies of their organizations consisted of the following:

- Define the types of permitted mobile devices (i.e. smart phones, tablets, etc.);
- Include procedures to address lost or stolen devices; and
- Include procedures that allow data stored on lost or stolen devices to be remotely wiped.

When asked whether their organizations allow access by devices that have been unlocked to gain full access to the operating systems using an unauthorized process known as “Jailbreaking” (iOS devices) or “Rooting” (Android devices), only 5% of the 211 respondents (the other nine skipped the question) answered “Yes,” 43% answered “No,” and 52% answered “Not sure.”

When asked to describe the types of Mobile Computing utilized in their organizations, 211 respondents (the other nine skipped the question) selected the following options:



## 3. INTERNAL AUDITORS' READINESS FOR MOBILE COMPUTING AUDIT/REVIEW

The following findings are based on 211 respondents (after excluding skipped questions).

A. Twenty-six percent indicated that their organizations had established ongoing Mobile Computing awareness training; 49% said "No," and 25% were "Not sure."

B. Fifty percent stated that their internal audit departments had the necessary skills to assess Mobile Computing; 22% said "No," and 28% were "Not sure."

   - Of the 100 respondents who said that their internal audit departments had the necessary skills to assess Mobile Computing risks and indicated their roles, 48%

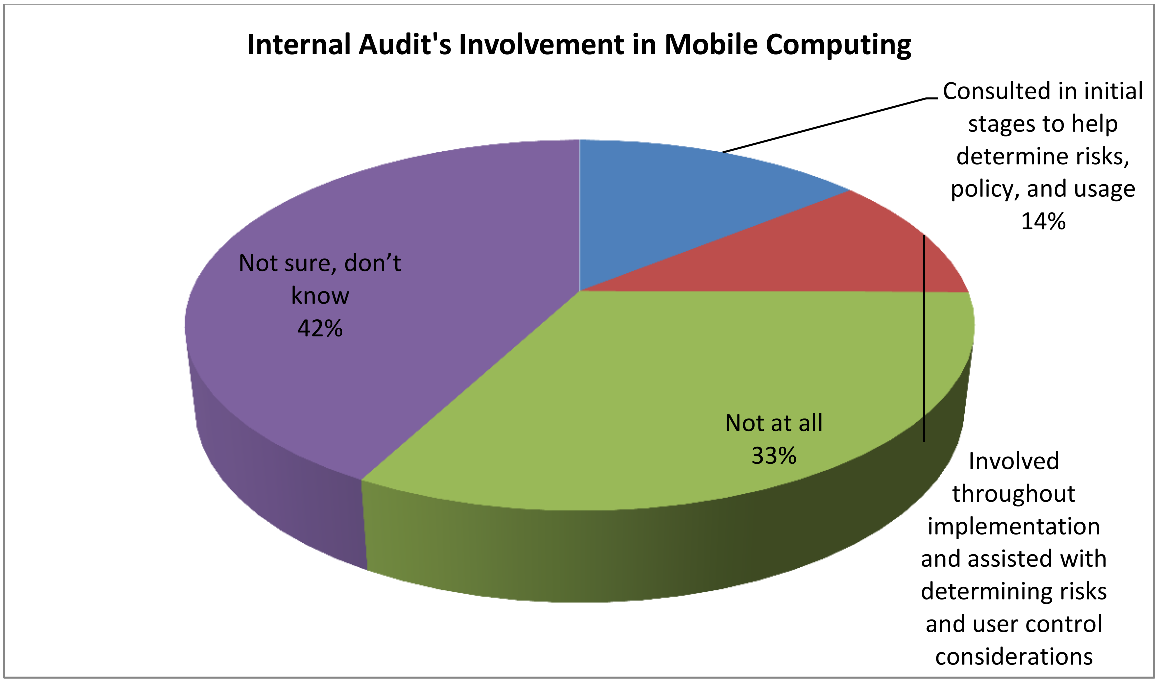
were managers and above; of the 45 respondents who said “No”, 64% were managers and above; of the 54 respondents who were “Not sure”, 33% were managers and above.

- Of the 100 respondents who said that their internal audit departments had the necessary skills to assess Mobile Computing risks and indicated their job responsibilities, 69 (69%) claimed to be Non-IT auditors and 31 (31%) claimed to be IT Auditors; of the 45 respondents who said “No”, 39 (87%) claimed to be Non-IT auditors and six (13%) claimed to be IT auditors; of the 54 respondents who said “Not sure,” 45 (83%) claimed to be Non-IT auditors and nine (17%) claimed to be IT auditors.

C. Forty-two percent said that their organizations’ risk assessment included risks associated with the utilization of mobile devices; 28% said “No,” and 30% were “Not sure.”

- Fifty-four percent of the 84 respondents, who said that their organizations’ risk assessment included risks associated with the utilization of mobile devices and indicated their roles, were managers and above; 54% of the 56 respondents who said “No” were managers and above; 34% of the 59 respondents who were “Not sure” were managers and above.

D. The following distribution indicates the internal audit departments' involvement in Mobile Computing at their organizations:



- Of the group (34 of 199 respondents or 17%) who claimed 10,001 to 25,000 employees in their organizations, 26% said that their Internal Audit departments consulted in initial stages, and 24% said their Internal Audit departments' involvement was throughout implementation and determination of risks.

- Regardless of the sizes of the rest of organizations (165 out of 199 or 83%) however, only 17% or less of respondents stated their Internal Audit departments' involvement in initial stages, and claimed their Internal Audit departments' involvement throughout implementation and determination of risks.

E. Fifteen percent said their organizations had conducted a Mobile Computing audit/review; 61% said “No,” and 24% were “Not sure.”

## CONCLUSIONS AND IMPLICATIONS

Further data analysis does not establish any strong correlations between the industry or size of the Internal Audit department and the involvement of Internal Audit in Mobile Computing.

However, further analysis does reveal the following observations:

- The majority of respondents, who claimed to be unfamiliar with Mobile Computing, or who said that their internal audit departments did not have the necessary skills to assess Mobile Computing risks, were Non-IT auditors. The aforementioned response pattern indicates an opportunity for Non-IT auditors to gain more knowledge and awareness of Mobile Computing.

- The majority of the organizations that allow Mobile Computing and have relevant policies in place, but only 26% have established ongoing training and 15% have conducted a Mobile Computing audit/review (from sections 3A and 3E above.)

    - A gap exists in the support and training received by internal auditors, whose ability to effectively conduct risk assessment regarding Mobile Computing might be compromised due to lack of knowledge.

    - Internal audit departments could be constrained in their abilities to deliver the necessary assistance in Mobile Computing audit/review.

- Fifty percent of respondents either do not believe or do not know whether their internal audit departments have the necessary skills to assess Mobile Computing risks, which indicates that the capability of those organizations to react quickly and appropriately to the risk areas exposed by Mobile Computing could be limited by the lack of understanding (from section 3B above).

- Forty-two percent of organizations include the utilization of mobile devices in their risk assessment, yet only 11% of internal audit departments are involved throughout the implementation and determination of risks. This suggests there are opportunities for internal audit professionals to (from section 3C and 3D above):

Expand their involvement and consultation with operations and IT personnel in the initial stages of Mobile Computing protocols to help determine associated risks and throughout implementation with user control considerations. Expand their use of technical and other skills when it comes to assessing and mitigating risks related to Mobile Computing and therefore add value to their organizations. The results of this study show a great opportunity to close the growing knowledge gap between Mobile Computing uses, their associated risks, and Internal Auditors involvement.

# RECOMMENDATIONS AND FUTURE RESEARCH OPPORTUNITIES

The Committee notes the following recommendations and opportunities for the IIA and its professional members to pursue and gain additional insight:

- Assess training needs to enable Internal Auditors to gain a better understanding of Mobile Computing and its associated risks, at all levels of an internal audit department, including IT and Non-IT internal auditors.
- Consider the results from this study on Mobile Computing awareness as a compliment to the identified '2013 Research Project Priority Topics,' specifically 'Skills for Auditing IT" and "Using Technology to Improve Internal Audit Communications."
- Assess the legal, operational, and organizational implications and risks of Mobile Computing as it relates to HIPPA (Health Insurance Portability and Accountability Act of 1996) and FERPA (Family Educational Rights and Privacy Act of 1974.)
- Encourage internal audit professionals to communicate with IT and Operations management within their organizations to discuss the risks associated with Mobile Computing. The results of this survey should be used to communicate this need to the profession.
- Assess the need for strategic partnerships with external/other IT organizations to bring further awareness and opportunities for discussion about Mobile Computing and its risks.

- Determine the current and future extent of Mobile Computing uses for business processes for critical business functions such as ordering, processing, and approving.
- Determine the extent and use of Mobile Computing for internal communication among internal auditors. Example: TeamMate audit work papers software is creating a mobile application for internal auditors to use.
- Determine the need to create additional surveys to better understand the relationship of internal auditors' roles compared to their involvement in risk assessment, policy review, and overall risk management activities regarding Mobile Computing.
- Expand the survey and applicable research of Mobile Computing to include a wider population of Internal Auditors outside the Dallas and Ft. Worth areas, as well as to members of other organizations such as ISACA, ACFE (Association of Certified Fraud Examiners) , and ACUA (Association of College and University Auditors) to further assess awareness within a wider demographic population.

# ACKNOWLEDGEMENTS

The Committee members consisting of Joe Diaz, Debbie Mathews, Andrea Lillie, Gwen Li, and Victoria Sheehan wish to thank survey respondents who provided information necessary to perform the study. The Committee would also like to thank the board members of the Dallas IIA, our academic advisors Dr. Teresa Conover (University of North Texas) and Mark Salamasick (University of Texas at Dallas), and the UNT System Internal Audit Department, for their support and encouragement during the course of this research project.

Please contact Joe Diaz at joseph.diaz@untsystem.edu for a copy of the survey used for this study.

# BIBLIOGRAPHY

Gartner. (2012, October 30). *Gartner: How big trends in security, mobile, big data and cloud computing will change IT.* Retrieved February 6, 2013, from NetworkWorld: http://www.networkworld.com/news/2012/103012-gartner-critical-trends-263793.html?page=2

Information Systems Audit and Control Association (ISACA). (2010). *Securing Mobile Devices.* Retrieved February 3, 2013 from: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices.aspx

Institute of Internal Auditors (IIA). (2013). *Topics Awaiting Proposals for Funding and Development*. Retrieved February 15, 2013 from: https://na.theiia.org/iiarf/pages/topics-awaiting-proposals.aspx

Kumar, R.Siva (2011). *Paper Presentation on Mobile Computing.* Retrieved February 3, 2013 from: http://www.scribd.com/doc/48271633/4-mobile-computing.

PwC LLC. (2012). *Aligning internal audit*. Retrieved February 15, 2013 from: http://www.pwc.com/en_US/us/risk-assurance-services/internal-udit/publications/assets/pwc-2012-state-of-internal-audit-survey.pdf

Semer, Lance. 2013. *Auditing the BYOD Program. Ia Internal Auditor*, February, pgs. 23-27.

Ramaswamy, Ganesh. (2012). *Cloud Computing: A Study of Internal Audit's Preparedness in the Dallas Area*. Retrieved September 17, 2012 from: http://dallasiia.org/ResearchComm/11-12.pdf.