

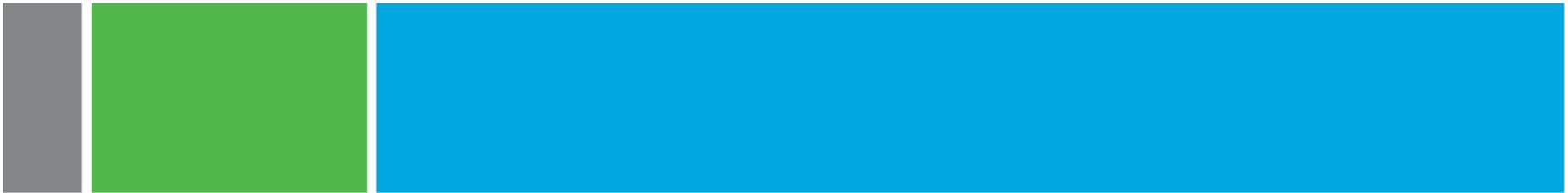
THE POWER OF BEING UNDERSTOOD

AUDIT | TAX | CONSULTING



RISK ADVISORY TRAINING

Security Trends



STATE OF MAINE

May 2016

Instructor

- Craig Finley – RSM Technology Management Consulting



Security Trends for 2013

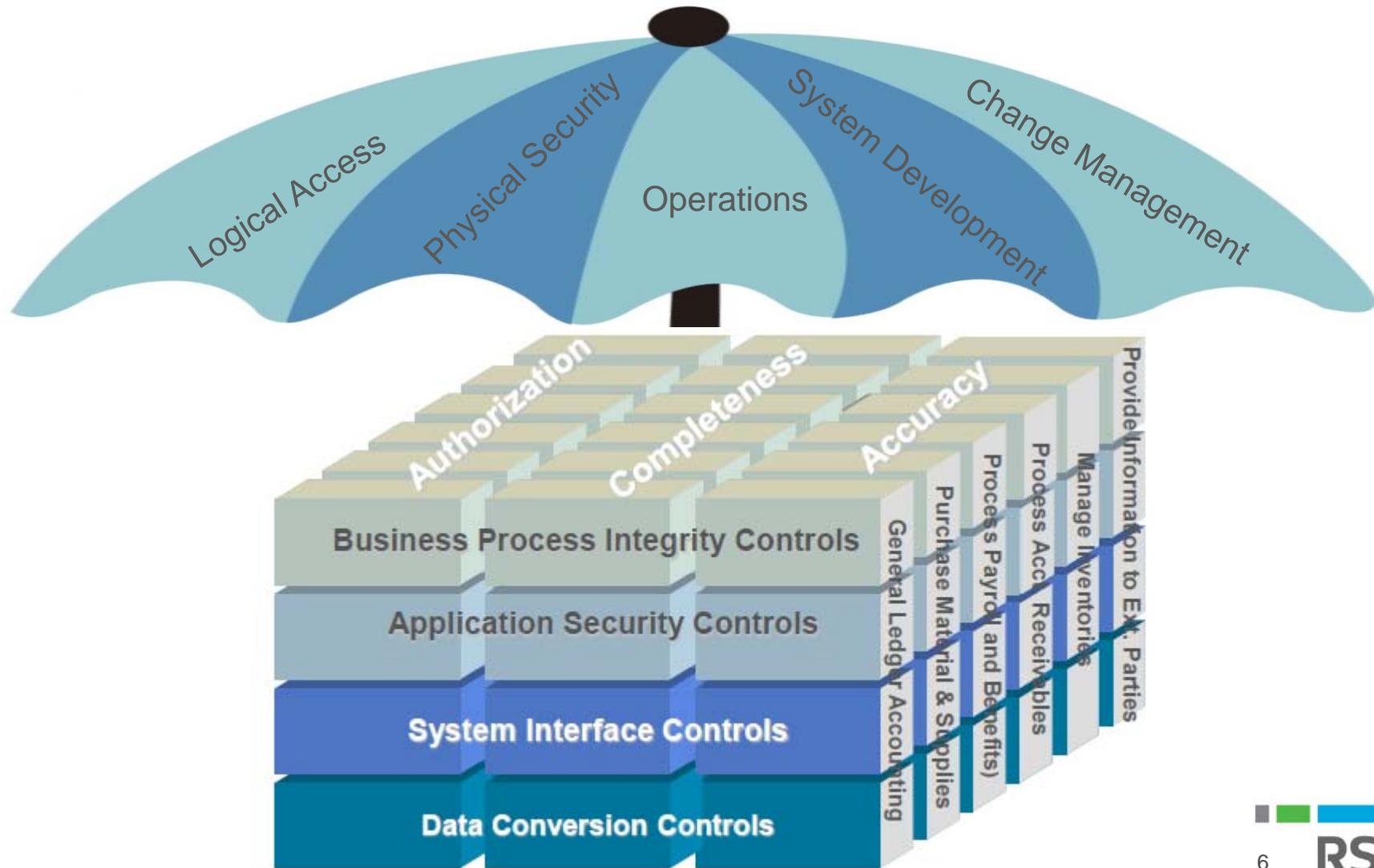
What's inside?.....

- IT General Controls (ITGC) Overview
- ITGC and The Business
- ITGC Areas of Focus and Testing
- IT Application Controls
- Where do ITGCs apply?

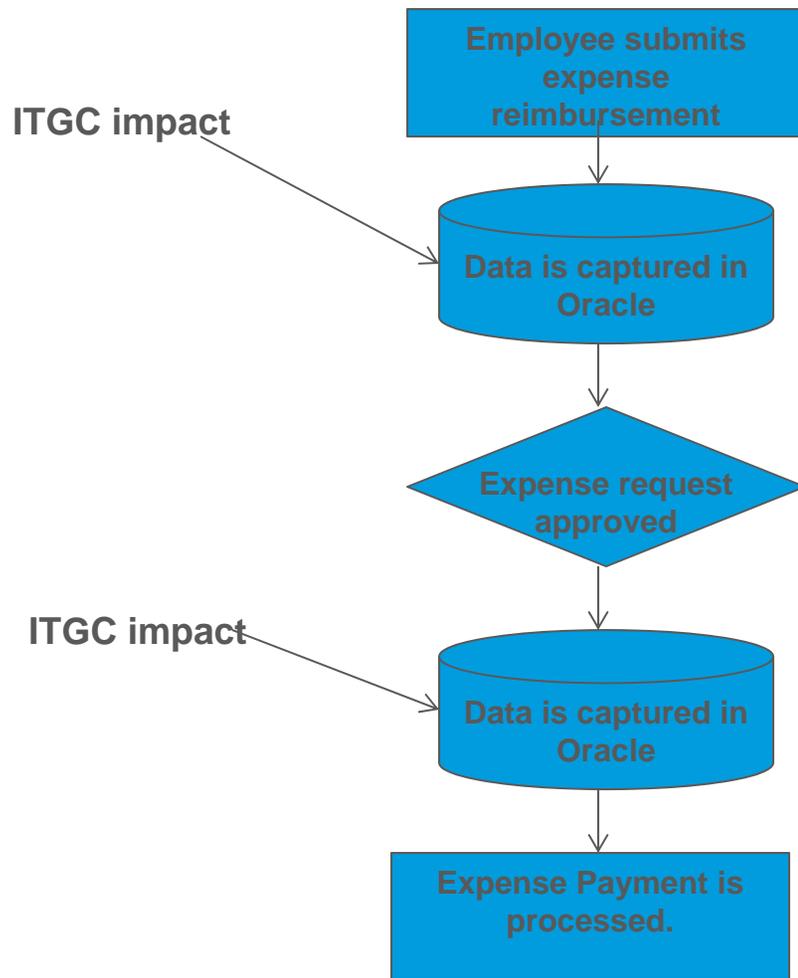
ITGC Overview

- **What are IT General Controls (ITGC)?**
 - Controls over the IT environment
 - Use frameworks to identify objectives (CoBIT)
 - Define Scope
 - What applications, on what servers, backed by what databases?
- **ITGC Defined:** Controls that apply to all systems components, processes, and data for a given organization or information technology (IT) environment. The objectives of ITGCs are to ensure the proper development and implementation of applications, as well as the integrity (completeness and accuracy) of programs, data files, and computer operations.
- **CoBIT Defined:** Information Technology (IT) governance model that helps in delivering value from IT and understanding and managing the risks associated with IT.

How do ITGC's Support the Business?



Bridging the Gap Between ITGC and Financial Reporting



Testing - Sample Sizes

Nature of Control	Frequency of Performance	Number Tested
Manual	Multiple Times Per Day	25
Manual	Daily	20
Manual	Weekly	5
Manual	Monthly	2
Manual	Quarterly	2
Manual	Annually	1
Programmed	Test one application for each programmed control activity	
IT General Controls	Follow the guidance above for manual and programmed aspects of IT general controls	
Non-Routine Transactions	Test 20% of the population up to a total of 25	

ITGC Areas of Focus (Logical Access)

- Logical Security
 - Access requests (New Hires, Changes, Terminations)
 - Account setup
 - Password setting
 - Monitoring access rights
- Sample Control (Terminations)
 - The IT helpdesk is notified of employee terminations by the employees manager via a helpdesk ticket. Access to systems is removed for all terminated employees within three business days (one for the Network).
- Common Issues
 - Timely removal of access

ITGC Areas of Focus (Change Management)

- Change Management / System Development
 - Description of change
 - Testing / Test environment
 - Developers
 - Approvals
- Sample Control (SDLC)
 - Software implementations, upgrades, and integrations follow a predefined Software Development Life Cycle as outlined in the SDLC SOP.
- Common Issues
 - Segregation of Duties
 - Inappropriate levels of access
 - Insufficient levels of testing

ITGC Areas of Focus (Operations)

- Computer Operations
 - Backups
 - Offsite backup storage
 - Restores
 - Issue monitoring and resolution

- Sample Control (Backup Restores/Replication)
 - In scope application and database servers are replicated offsite to a hosted data center every 15 minutes.

- Common Issues
 - Tape vs. Disk
 - Identifying a true population of backup failures.

ITGC Areas of Focus (Physical Security)

- Physical Security
 - Secure server room
 - Access rights (requests and monitoring)
- Sample Control (Data Center Access)
 - Data Center access is secured by electronic key card and restricted to authorized personnel.
- Common Issues
 - Executive Members on the access list

IT Application Controls

- Transactions or processes that are performed automatically by the application.
- Measured and tested from input to output
- Categories of Application Controls
 - Completeness checks - controls that ensure all records were processed from initiation to completion.
 - Validity checks - controls that ensure only valid data is input or processed.
 - Authentication Vs. Authorization

Where do ITGC's apply?

- IT SOX (Sarbanes Oxley)/ SOA
 - Management Testing (internal)
 - External Testing (IT SOX for public companies and Audit Reliance)
 - SSAE16 SOC1, SOC2, SOC3 (Type I and Type II)
- Internal Audit
 - HIPAA, MA Privacy
 - Implementation Reviews
 - IT Audit Readiness
- Security/Data Analysis
 - PCI/DSS compliance
 - Network Vulnerability Scanning
 - Journal Entry Testing
 - CAATS

IIA Volunteer Training – CAATS

What's inside?.....

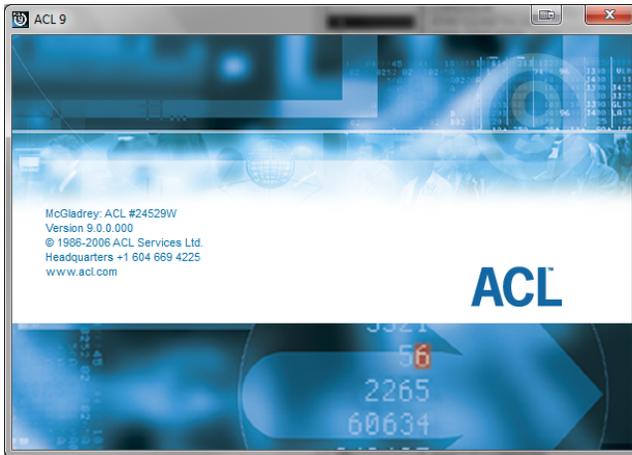
- CAATs Background
- Most Commonly Used Tools
- Importance of the DRR (Data Requirements Request)
- Benford's Law
- CAATs in Practice

CAATs Overview

- Growing field within the audit profession with a direct relationship with the growth in technology
- The practice of using computers to automate any part of the audit process
- Random Sampling vs. Sampling for Specific Risks (Ex: Insurance Claims)
- Helpful to supplement traditional audit work and/or give direction for future internal audits.
- Blackbox Vs. Whitebox Testing

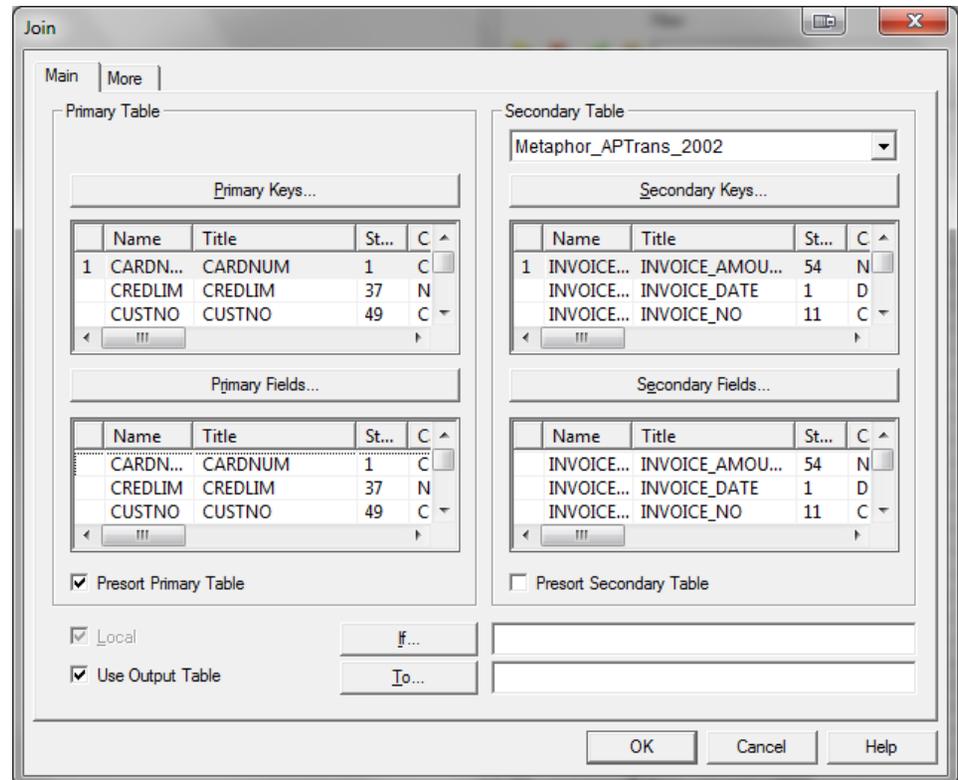


Most Commonly Used Tools



Importance of the Data Requirements Request

- What type of data do I need?
- What type of data does the client have access to?
- Does the client have the expertise to pull the data I want, in the format I need?
- Do any of the data sets in use contain sensitive information?
- Do I have the proper primary/secondary keys (fields) to join tables?



Benford's Law

- First discovered in 1881 by Simon Newcomb; Rediscovered in 1938 by Frank Benford
- “states that in lists of numbers from many (but not all) real-life sources of data, the leading digit is distributed in a specific, non-uniform way.”
- Will only work with data sets across “Multiple Orders of Magnitude”
- Data sets that prove Benford's Law exactly
 - Fibonacci Numbers
 - The Powers of 2 and almost any other number
- Benford's Law in use in auditing with CAATs

Benford's Law

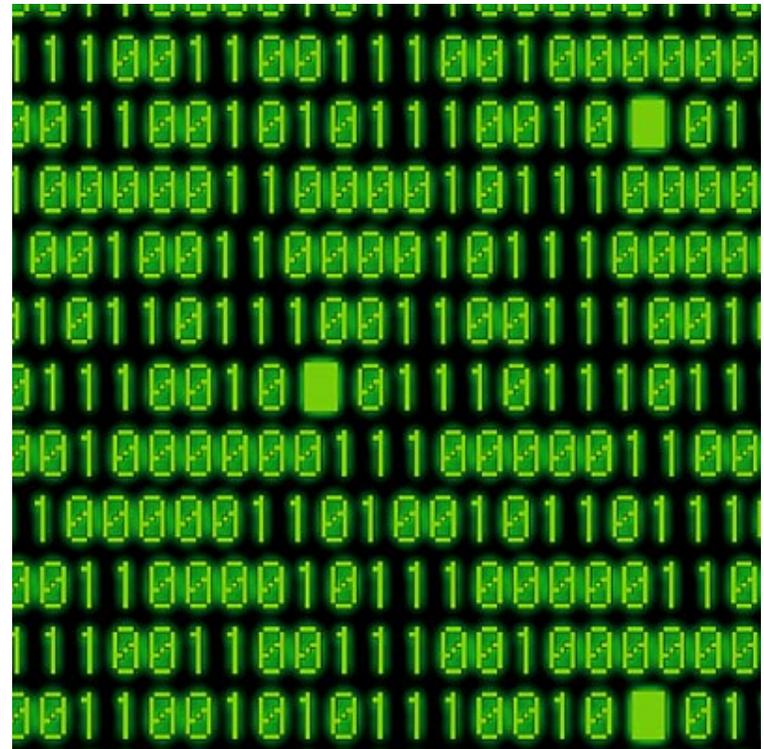
Digit	Frequency (first digit)	Frequency (second digit)
0	-	0.120
1	0.301	0.114
2	0.176	0.109
3	0.125	0.104
4	0.097	0.100
5	0.079	0.097
6	0.067	0.093
7	0.058	0.090
8	0.051	0.088
9	0.046	0.085

Sample Tests

Area	Audit Test	Purpose of Test	Data Extracts Required	Data Extract Source
Employees	Timely association disposition	Verify ex-employees no longer on payroll	List of terminated employees: employee name ss# Address chk acct# accrued vacation vacation taken overtime billed phone #	Payroll records HR terminations
Accounts Payable	Duplicate Payments	Identify Duplicate Payments	Check# / wire # Amount Date vendor/payee # vendor invoice # amount	Check register Payment data
Sales/Accounts Receivable	Refunds	Identify high volume refund customers	Customer name refund amount date	A/R transaction data
Purchasing	Purchases under review limit	Identify purchases just under the \$ limit that requires more approval	Purchases detail	Purchases g/l

CAATs in Practice

- Payroll & Purchasing Fraud
- Regression Analysis
 - Credit Card Patterns
 - Expected Values
- Ratio Analysis
 - *The ratio of highest value to the lowest value (maximum / minimum)*
 - *The ratio of the highest value to the next highest (maximum / 2nd highest)*
 - *The ratio of the previous year to the current year*
- Time and Expense Fraud





QUESTIONS AND ANSWERS?

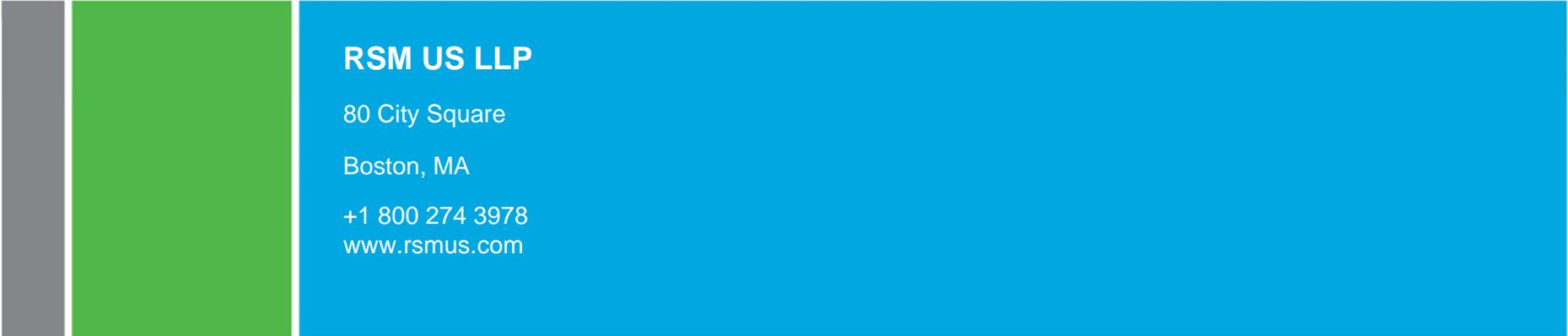
About Your instructor(s)

Craig Finley

Manager

Craig is a manager in the TMC practice and has worked for over 20 years in the public sector, specifically with local towns, cities and schools. He has spearheaded numerous projects to optimize services and reduce costs while gaining stakeholder support for change.





RSM US LLP

80 City Square

Boston, MA

+1 800 274 3978

www.rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM® and the RSM logo are registered trademarks of RSM International Association. *The power of being understood®* is a registered trademark of RSM US LLP.

© 2016 RSM US LLP. All Rights Reserved.

