The Journey to ISO 27001 Certification

Glenn Murphy, CMA, CPA, CISA, CIA, CFM, CGMA

Gideon Lenkey, CISSP

September 12, 2022

The Association of Accountants and Financial Professionals in Business

ORACLE NETSUITE

Tech-Talk Mondays Title Sponsor

www.netsuite.com

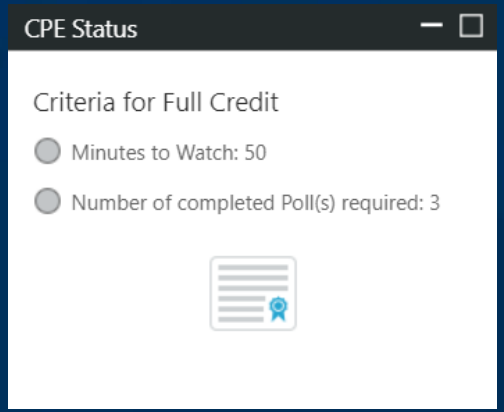
Webinar Features and CPE Credit

Q&A Asking Questions

CC Closed Captioning

? Help

CPE Credit



ima® The Association of Accountants and Financial Professionals in Business

ORACLE® NETSUITE

Moderator

Brad Hamilton, CMA, CPA

Co-Owner

Hamilton Accounting Services LLC

Member

IMA Technology Solutions & Practices Committee

ima®

The Association of Accountants and Financial Professionals in Business

ORACLE® NETSUITE

Featured Presenter

Glenn Murphy, CMA, CPA, CISA, CIA, CFM, CGMA

Principal

GRC Management Consulting, LLC

ima®

The Association of Accountants and Financial Professionals in Business

Glenn Murphy's Biography

- Glenn Murphy is the principal of GRC Management Consulting, and has over thirty years of experience in financial and operational compliance, including more than 15 years as Chief Audit Executive at four different publicly held companies. Glenn created the Sarbanes-Oxley compliance function at three of these companies and expanded these programs to encompass retail loss prevention, supply-chain social compliance, contract/royalty compliance and related activities.
- Glenn holds six financial certifications including the CMA,CISA, CIA, CFM, CGMA and CPA as well as an MBA and MS (Computer Information Systems).

Featured Presenter

Gideon Lenkey, CISSP

President and Co-Founder

RA Security Systems, Inc.

ima®

The Association of Accountants and Financial Professionals in Business

Gideon Lenkey's Biography

- Gideon Lenkey has consulted on Information Security matters since 1989. He currently specializes in cybersecurity governance and testing security controls of enterprise IT infrastructures. He also enjoys challenging investigations involving malicious hackers, corporate insiders, and extortionists.
- Gideon is the co-author of Gray Hat Hacking – The Ethical Hackers Handbook, 3rd edition. He has consulted on cybersecurity matters by both foreign and domestic government agencies and is a longtime member and frequent presenter at the FBI's NJ InfraGard. He is the past president of the NJ Chapter of the FBI's InfraGard Program and recipient of multiple FBI commendations including Outstanding Service in the Public Interest, FBI Director Robert S. Muller III, and Invaluable Assistance to FBI Newark, FBI Director Robert S. Muller III.
- Gideon is the president and co-founder of RA Security Systems, Inc., which provides security services in the areas of managed cybersecurity solutions, penetration testing, policy and procedure development, NIST CSF, 800-53 and ISO 27001 implementation, incident response, as well as law enforcement liaison and litigation support.

Learning Objectives

1. Explain the purpose of ISO 27001 certification.
2. Identify the target audience for ISO 27001 certification.
3. Recognize the need to implement an internal controls framework in preparation for ISO 27001 certification.
4. Compare ISO 27001 to other cybersecurity-related attestations (SOC2, SOC for Cyber).
5. Describe the role of your compliance programs and internal audit in the journey to ISO 27001 certification.

Agenda

1. Introduction
2. Stakeholder Demands
3. ISO Certification and Alternatives
4. The Journey to ISO 27001 Certification
5. Conclusion
6. Key take aways/Q&A

Introduction

- Security Monitoring for clients identified the repeat of the same issues over time because Governance and Controls were lacking.
- Identified the NIST Cybersecurity Framework as an internationally recognized solution for clients to solve and prevent these issues.
- Experience implementing IT General Controls at companies for SOX compliance informs our view of the comprehensiveness of NIST Controls Catalog for Cyber.
- Clients' stakeholder demands led us to helping clients prepare for independent assessments.
- SF magazine articles related to this webinar topic.

“Adventure is just bad planning.”

Roald Amundsen

Stakeholder Demands

Board of Directors/Management Demands

1. Strong cybersecurity controls to mitigate cybersecurity risk to the Company and Stakeholders.
2. Do not want to take it on “faith” that actions and assurances from internal parties (CIO/CSO) comprehensively address cybersecurity risk.
3. Independent assurance compared to an objective standard.
4. Standard (minimal cost) scope of Financial/SOX audit procedures is not adequate for such assurance.

Customer Demands

1. Protection of their PII.
2. Protection of their confidential information.
3. System availability.
4. Evidence to provide to their management/insurers/customers/vendors
5. Completion of lengthy cybersecurity questionnaires and addressing concerns they may identify.

Vendor Demands

1. Protection of confidential information.
2. System availability.
3. Evidence to provide to their management/insurers/customers/vendors
4. Completion of lengthy cybersecurity questionnaires and addressing concerns they may identify.

Regulatory Demands

1. Compliance with privacy laws (including informing those whose information was compromised). Federal, state and foreign (e.g., GDPR)
2. Protection of infrastructure (utilities, ISPs, telecom, pipelines)
3. Bills to possibly prohibit payment of ransomware or at least report it (Cybersecurity Incident Notification Act, Ransom Disclosure Act, Ransomware and Financial Stability Act)
4. Bills under consideration requiring report of a cybersecurity breach (Cyber Incident Reporting Act)

Insurer Demands

1. Detailed questionnaires regarding not only what the Company is doing but also that the Company performs exercises to test their internal controls related to cybersecurity.
2. Request evidence of efforts including penetration tests, audit results, risks assessments, and monitoring of controls.
3. Some insurers insist on running the incident response with their own people.
4. Efforts ultimately determine the insurability of the Company and the rates which they pay.

Poll Question 1:

What does ISO in the context of 27001 stand for?

a. Interplanetary Standards Operation
b. International Organization for Standardization
c. Imperial Service Order
d. In Search Of

Poll Question 1 Results: (Placeholder)

ISO Certification and Alternatives

ISO 27001 Certification

- ISO/IEC 27001:2013 (ISO 27001) is the international standard that describes best practice for an ISMS (information security management system).
- Achieving accredited certification to ISO 27001 demonstrates that your company is following information security best practice.
- An independent, expert assessment of your cybersecurity practices as measured against the code of practice for information security management, ISO/IEC 27002:2013.
- The gold standard of third-party cybersecurity assurance.
- Audience is internal and external stakeholders.

SOC 1/2/3

Audience is user entities, business partners and CPAs providing services to such user entities and business partners.

- **SOC 1** - Targeted to help user entities to assess their own systems of internal controls over financial reporting (with the service organization a component). Typically, Public Companies subject to SOX. Governed by AICPA AT-C section 320
- **SOC 2** – Targeted to help user entities to assess their own systems of internal controls (with the service organization a component). Appropriate only for specified parties with sufficient knowledge and understanding of the service organization and the systems. Addresses Security, Availability, Processing Integrity, Confidentiality and/or Privacy. Governed by AICPA Trust Service Criteria.
- **SOC 3** – Interested parties of user entities. SOC 2 examination but report for general users with less detail.

SOC for Cyber

- General audience with a stake (management, Board of Directors, Banks) or potential stake (potential investors) in the organization. Broadly speaking, an internal audience.
- Targeted to describe and assess the cybersecurity risk management of the entity for stakeholders' benefit and action plan.
- Description, management assertion and auditor attestation related to the organization's cybersecurity risk management. **Management selects criteria** against which to evaluate controls.
- Governed by the AICPA Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls.

Poll Question 2:

Who is the intended audience for ISO 27001 certification?

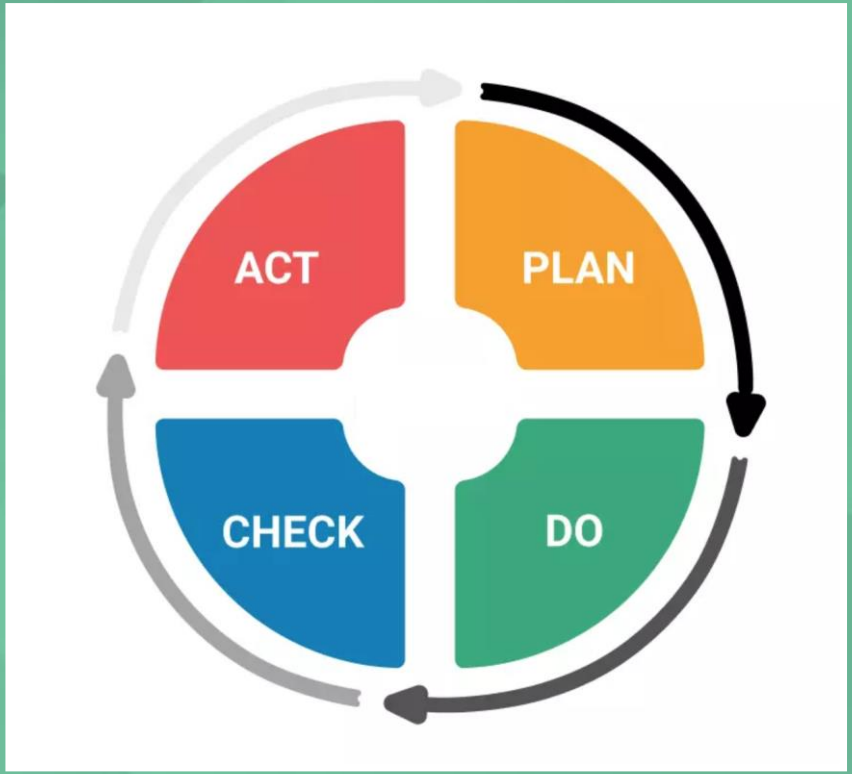
a. Board of Directors
b. Executive Management
c. IT Management
d. Customers, Vendors, and other Partners

Poll Question 2 Results: (Placeholder)

The Journey to ISO 27001 Certification

ISO Stages

1. Plan
2. Do
3. Check
4. Act



ISO Stages - Plan

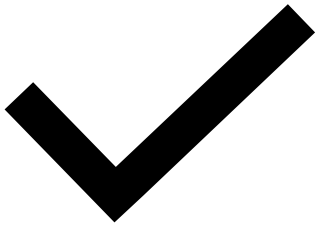
- Adopt a cybersecurity framework.
- Obtain top management commitment.
- Define a systematic approach to information security risk assessment and the risk acceptance criteria.
- Perform a risk assessment within the context of the ISMS scope.
- Identify and evaluate options for the treatment of these risks via “mapping” company controls to cybersecurity risks.
- Prepare a Statement of Applicability and a Risk Treatment Plan

ISO Stages - Do

- Finalize the Risk Treatment Plan and related documentation
- Implement the Risk Treatment Plan and planned controls
- Arrange appropriate training for affected staff and general Awareness Programs
- Manage operations and resources in line with the ISMS
- Implement procedures that enable prompt detection of, and response to, security incidents

ISO Stages - Check

Drive continuous improvement by monitoring, reviewing, testing, and auditing which can be achieved via internal audit, co-sourcing, or some combination of the two.



ISO Stages - Act

Address audit outcomes/findings as well as continually updating and improving your process with lessons learned from simulation exercises, incidents, actual threats identified and responded to, developments in information security, and other improvements.

The Journey to ISO 27001 Certification:

- Adopt a Cybersecurity Framework
- ISO Statement of Applicability
- ISO Risk Treatment Plan
- Remediate Weaknesses
- Monitor Internal Controls
- Internal Audit
- Remediate Controls Weaknesses
- ISO Certification Assessment
- Communicate ISO Certification

Adopt a Cybersecurity Framework

1. NIST Cybersecurity Framework
2. COBIT (Control Objectives for Information and Related Technology) framework created by ISACA
3. ITIL (Information Technology Infrastructure Library)

CSF Adoption – Current State

- Identify existing documented internal controls related to IT, IT Governance, and Corporate Governance.
- Identify existing undocumented IT, IT Governance, and Corporate Governance controls and document these.
- Compile lists of open IT internal control gaps identified by Internal/External audits, Penetration Tests, and other sources.
- Identify all third-parties related to IT services and obtain SOC reports for those that house and/or process Company data or provide computing services (e.g., Cloud, Payroll).

CSF Adoption – Risk Assessment

- Risk impacts the likelihood of meeting objectives and internal controls mitigate risks
- Ensure there is a strong linkage to the objectives listed in the ISO 27001 Annex A Reference Controls
- 35 objectives are listed in Annex A, and we typically identify 85 to 100 risks associated with these objectives to include in the risk assessment
- Assign risk owners
- Assign a point scale for Impact (5-1), Likelihood(1.00-0.10), and Mitigation Effectiveness (0.00-1.00)
- Impact x Likelihood = Inherent Risk
- Inherent Risk x Mitigation Effectiveness = Residual Risk

CSF Adoption – Identify Control Gaps (Risk Assess)

1. Identify high Residual Risk Scores
2. Identify additional internal controls that will further mitigate the Residual Risk
3. Prioritize the implementation of these newly identified controls
4. Implement the controls over time with monitoring activities to ensure they are effective
5. Reperform the Risk Assessment to determine the Residual Risk following implementation of additional mitigating controls and ensure the Residual Risk is at an acceptable level for the company

CSF Adoption – Map to NIST 800-53r5

1. NIST 800-53 Revision 5 “Security and Privacy Controls for Information Systems and Organizations” (Controls Catalog) (updated as of December 2020)
2. Detailed IT, Governance, Supply Chain, and Privacy controls
3. Review these controls and determine if they are applicable to the company
4. For those deemed applicable, “map” existing internal controls to these and determine if the intent of the NIST control is fully, partially, or not addressed by existing controls.

Coverage (see legend @ Mapping Legend tab	Organization Control	Control Title	Base Control	Control Identifier	Control (or Control Enhancement) Name	Control Text
			AC	AC	Access Control	
	10042	IT Policies	AC-01	AC-01	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and c. Review and update the current access control: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]
Temporary User Accounts Role-Based Access Control	10002 10070 10068 10007 10006	Network PW (AD) Requirements Privileged Access Mgt. (PAM) Priviledged User Accounts Security Provisioning System Access Policy & Config	AC-02	AC-02	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify: 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]; g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. [Assignment: organization-defined time period] when accounts are no longer required; 2. [Assignment: organization-defined time period] when users are terminated or transferred; and 3. [Assignment: organization-defined time period] when system usage or need-to-

CSF Adoption – Identify Control Gaps (Map 800-53r5)

- Identify Control Gaps for those NIST Controls not addressed or partially addressed by existing controls
- Identify and ‘map” Recommended Controls to address the Control Gaps
- Prioritize these Recommended Controls and implement them over time.

Poll Question 3:

What is the relationship of ISO 27001 certification to other IT-related compliance programs (SOX ITGCs, NIST)?

a. ISO 27001 certification is a starting point.
b. There is no relation to other IT-related compliance programs.
c. Other IT compliance programs should be mature prior to seeking ISO 27001 certification.
d. The programs are duplicative.

Poll Question 3 Results: (Placeholder)

CSF Adoption – Map to NIST CSF

- Following the Risk Assessment and the mapping to the NIST Controls Catalog, you will have a comprehensive list of Internal Controls and Recommended Controls.
- “Map” these controls to the NIST Cybersecurity Framework listing the Internal Controls first and then the Recommended Controls in orange font.

RA security systems

NIST Cybersecurity Framework - Profile
NIST Framework Version 1.1 (issued April 10, 2018) https://doi.org/10.6028/NIST.CSWP.04162018

NIST Function	NIST Category (Activity/Outcome)	NIST Subcategory (Objective)	Controls	Gap
MATURITY TOTAL				
IDENTIFY TOTAL				
IDENTIFY (ID) Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	10031 End Point Protection 10109 Information Asset Tracking & Software Update/Licensing Management	
IDENTIFY (ID)	**Asset Management (ID.AM)**	**ID.AM-2:** Software platforms and applications within the organization are inventoried	10031 End Point Protection 10109 Information Asset Tracking & Software Update/Licensing Management	
IDENTIFY (ID)	**Asset Management (ID.AM)**	**ID.AM-3:** Organizational communication and data flows are mapped	10013 System Documentation 10122 Network Architecture	
IDENTIFY (ID)	**Asset Management (ID.AM)**	**ID.AM-4:** External information systems are catalogued	10081 Third-party Risk Management Program (TPRM) 10079 SOC 1 Review 10080 SOC 2 Review	
IDENTIFY (ID)	**Asset Management (ID.AM)**	**ID.AM-5:** Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	10044 IT Organizational Structure 10048 Strategic IT Plan 10078 Enterprise Risk Management (ERM) Committee 10045 IT Risk Assessment 10105 IT Steering Committee 10106 Cyber-risk Committee 10085 Data Governance Program	
IDENTIFY (ID)	**Asset Management (ID.AM)**	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders	10024 Hiring Requirements 10044 IT Organizational Structure 10048 Strategic IT Plan 10081 Third-party Risk Management Program (TPRM) 10088 Job Descriptions 10078 Enterprise Risk Management (ERM) Committee 10045 IT Risk Assessment	

CSF Adoption – Identify Control Gaps (Map CSF)

- Determine if consideration of the Internal Controls and Recommended Control fully address the intent of the NIST Subcategory listed. If not, identify an additional Control Gap.
- Identify and ‘map” Recommended Controls to address the Control Gaps.
- Prioritize these Recommended Controls and implement them over time.

CSF Adoption – Maturity Assessment

- Assess the adequacy of the Internal Controls “mapped” to each NIST subcategory with consideration of the Gaps/Recommended Controls to address the intent of the NIST subcategory.
- Measure the maturity of the current controls to address each NIST subcategory.
- We developed a method using the Capability Maturity Model Integration (CMMI) and the NIST Implementation Tiers which assess maturity along:
  - Process Level
  - Policy Level
  - Documentation Level
  - Automation Level

CSF Adoption – Monitoring of Controls

All internal controls must be subject to a periodic performance of a Control Procedure to confirm with evidence that the internal control remains in place and operating as designed. Key aspects of this monitoring activity are:

1. Assign Control Owners
2. Set Frequency
3. Develop a step-by-step Control Procedure to assess the control
4. Require evidence of Performance
5. Ideally, use a workflow tool to assign and track the Monitoring Activity.

CSF Adoption – Remediate Control Gaps

- Prioritize Recommended Controls identified to address Control Gaps based on impact to program maturity, resource availability, and ease of implementation.
- Implement the highest priority Recommended Controls along with Monitoring Activities for these controls.
- Periodically reassess the program maturity following implementation of Recommended Controls.

ISO Statement of Applicability

- Appendix A of ISO 27001 is a listing of Control Objectives and Controls ISO identifies as needed for appropriate cybersecurity.
- For each control, “map” the internal controls you have in place that are relevant to the ISO control.
- Determine if your current internal controls fully address the intent of the ISO control and, if not, identify a gap and a Recommended Control(s) to implement to remediate this gap.
- If any ISO controls are deemed to be not applicable to your organization, this must be fully justified and documented with appropriate reasons.
- The Statement of Applicability must be signed by a senior executive of the organization.

ISO Risk Treatment Plan

1. The Risk Assessment discussed earlier supports developing an ISO Risk Treatment Plan which enumerates the risks facing the Company and the treatments (typically internal controls) for each risk.
2. The Risk Treatment Plan should include Residual Risk measures which identify which risk are not fully mitigated.
3. The Risk Treatment Plan must be signed by a senior executive evidencing their review and acceptance of residual risks.

Monitoring of Controls

1. Refer to the section in CSF Adoption – Monitoring of Controls for activities.
2. Monitoring is essential to ensure the controls are effective for proper cybersecurity function and prior to any independent evaluation.
3. Explicit monitoring also makes independent assessment more efficient and therefore less costly.
4. Effective monitoring ensures there are “No Surprises”.

Poll Question 4:

What is required to have in place and approved by executive management and/or the Board of Directors prior to engaging a firm for certification?

a. A Statement of Applicability
b. An Internal Audit Plan
c. A Risk Treatment Plan
d. All the above

Poll Question 4 Results: (Placeholder)

Internal Audit

- Internal Audit is required as an essentially part of the “Check” activity of ISO.
- All controls should be subject to internal audit prior to consideration of ISO certification.
- Independent assessment via internal audit is an effective way to ensure that the monitoring activities of the control owners are timely and thorough.
- Management should assess the readiness of the organization for ISO certification based on the results of internal audits.

Remediate Control Issues – Internal Audit

- Issues identified during internal audits must be prioritized and addressed
  - This is an essential aspect of the “Act” stage of ISO.
- If the CSF was implemented effectively, there should be very few issues identified by internal audit.

ISO Certification Assessment

- The organization is now ready for the independent ISO 27001 assessment.
- The signed Statement of Applicability and Risk Treatment Plans must be available at the beginning of the assessment.
- There are several professional service firms that include ISO 27001 certification assessments in their service offerings.
- Given all the activities that occurred up to this point, the certification should go smoothly.

Communicating ISO Certification

- ISO 27001 Certification provides a competitive advantage in your marketplace.
- Providing evidence of ISO 27001 should eliminate or at least greatly reduce the questionnaires and discussions related to your cybersecurity preparedness from your customers and vendors.
- Your Board and Executive Management will have confidence that the organization is prepared from a cybersecurity standpoint following certification.
- ISO 27001 Certification will satisfy insurer demands and should result in competitive rates.

“

If you Fail to Plan, You are Planning to Fail

– Benjamin Franklin

Questions and Answers

Glenn Murphy, CMA, CPA, CISA, CIA, CFM, CGMA
Principal
GRC Management Consulting, LLC

Gideon Lenkey, CISSP
President and Co-Founder
RA Security Systems, Inc.

Brad Hamilton, CMA, CPA
Co-Owner
Hamilton Accounting Services LLC
Member
IMA Technology Solutions & Practices Committee

Thank You to Our Featured Presenters!

Glenn Murphy, CMA, CPA, CISA, CIA, CFM, CGMA
Principal
GRC Management Consulting, LLC

Gideon Lenkey, CISSP
President and Co-Founder
RA Security Systems, Inc.

Final Reminders

- **Complete the Evaluation poll** – 2 options
  - On your screen
  - Evaluation Survey icon at the bottom of your console
- **Access to your CPE Certificate** – 2 options
  - Click the “CPE” icon at the bottom of your console

    or
  - Click the link in your post-event e-mail
- Please print a copy of the CPE certificate for your records.
- Your CPE credit will be automatically recorded in your transcript.

Thank you!

Oracle NetSuite

www.NetSuite.com

ima®

The Association of Accountants and Financial Professionals in Business

ORACLE® NETSUITE