P&N
Postlethwaite & Netterville

Risky Business: Managing Risks in the Restaurant Industry

May 24, 2017

assurance - consulting - tax - technology - **pncpa.com**

Postlethwaite & Netterville, A Professional Accounting Corporation

Agenda

12:30 pm	Human Resources – Helene Wall
1:15 pm	Internal Controls – Todd Tournillon
2:00 pm	PCI Compliance & Cybersecurity – Paul Douglas
2:45 pm	Break
3:00 pm	State & Local Tax Update – Gary Dressler
3:45 pm	Cloud Software for Restaurant Management – Karen Jones

P&N
Postlethwaite & Netterville

P&N

Postlethwaite & Netterville

Human Resources

Helene Wall, SHRM-SCP

assurance - consulting - tax - technology - **pncpa.com**

Postlethwaite & Netterville, A Professional Accounting Corporation

Agenda

1. Culture
2. Compliance
3. Structure
4. Engagement

P&N
Postlethwaite & Netterville

The Importance of Culture

P&N

Postlethwaite & Netterville

Culture and Its Importance

- The set of values, customs and beliefs of a group of people.
- Company culture is the way your employees interact with one another.
- Includes business values and vision as well as your workforce’s ability to put them into action.
- Building an intentional and strategized culture is critical to your reputation, your brand and ultimately the survival of your business.

What’s Food Got To Do With It?

“Foodways” often refer to the *Intersection of Food* in culture:

- The eating habits and culinary practices of a people, region or historical period.
- Our attitudes, practices and rituals around food are a window onto our most basic beliefs about the world and ourselves.
- Restaurants and Food Service organizations have a “leg-up” on building culture!

What's Your Culture Like?

Steps to Defining Your Culture

- Involve everyone in the organization
- Use employee surveys, focus groups, committees
- Implement customer surveys, response cards
- Evaluate internal and external responses
- Identify areas for improvement
- Implement, review, evaluate, adjust
- Be consistent and communicate frequently

Compliance

P&N

Postlethwaite & Netterville

Employment – Top 10 Federal Laws

1. Job Discrimination: Title VII of the Civil Rights Act
2. Overtime/minimum wage: Fair Labor Standards Act (FLSA)
3. Family and Medical Leave Act (FMLA)
4. Age Discrimination in Employment Act (ADEA)
5. Disability Discrimination (ADA)

Employment – Top 10 Federal Laws

6. Military Leave (USERRA)
7. Gender Pay Differences (EPA)
8. Workplace Safety (OSHA)
9. Pregnancy Discrimination Act (PDA)
10. Immigration Reform and Control Act (IRCA)

Employment – Critical Louisiana Laws

- At Will
- Minimum Wage
- Minors
- Aliens
- Drug Testing
- Medical Exams
- Smoke-Free Act
- Weapons
- Pregnancy
- Jury Duty
- Whistleblower
- Military
- Breastfeeding
- School Visitation
- Other

High Risk Activities

- Recruitment
- On-boarding
- Discipline
- Termination
- Re-hire

Recruitment

CULTURE

- Manager training?
- Candidate pool?
- Paper vs HRIS or both?
- The Interview Process
  - “Outside of the database”
  - On-line assessment – use/benefits
  - Applicant prior work history, past performance
  - Eligible for rehire status

Recruitment

CULTURE

- The Selection Process
  - Behavioral vs task-based questions
  - Working interview, *stage* and pay
  - References
- Offer of Employment
  - Exempt vs non-exempt
  - “Subject to”
  - Consistency

Onboarding

CULTURE

- New Hire
  - 1-9s, E-Verify, Visas and Enforcement
  - Other
- Orientation
  - FOH vs BOH; Kitchen vs Counter
  - Employee Handbook
  - Expectations and Performance Management
  - Job description, training, cross training

Employment Life Cycle

CULTURE

- Ongoing feedback
- 30/90 day review
- Annual review
- Wage and salary review
- Growth, development and promotion
- Ownership/career plan
- Succession plan

Uh-oh: Discipline

CULTURE

- When things aren’t working out
  - – Progressive discipline
  - – Performance improvement plans
  - – Suspension
  - – Immediate termination
- Internal investigation
- Consistency and documentation

Termination

CULTURE

- At Will
- For Cause
  - Documentation
  - Opportunity to improve
  - Consistent application of policy
- Exit Interviews and Managing Turnover
- Louisiana Separation process
- Unemployment Claims

Re-Hire

CULTURE

- Good or Bad Idea?
- How to Manage?
- How to Track?
- What to Say?

Structure

P&N
Postlethwaite & Netterville

HR 101 - Staffing

- 1:100 rule, subject to complexity
  - HR Director/Manager - Compliance
  - Talent Specialist
  - Compensation Specialist
  - Benefits Specialist
- Guidance and Counsel
  - Labor attorney
  - Outsourced consultant
  - Ongoing education for management and staff

HR 101 - Compliance

- Labor Posters
- Handbook and policies up-to-date
- Files, data, documentation – record retention
- Manager training: how to supervise
- Employee training: mandated and workplace policies
- Workers Compensation, Affirmative Action, Union

HR 101 - Processes

- Recruitment through Termination
- Timekeeping and Payroll
- Reimbursement
- Leave Requests
- Policy Administrative Forms
- Other

HR 101 - Technology

- HRIS and Data Security
- Excel, Accounting Software, Other
- Reporting
- Dashboards
- Social Media
- Interaction with Accounting, Payroll, Sales, Service

P&N
Postlethwaite & Netterville

HR 101 – Training & Development

- Performance Management
- Career Development
- Risk Management
  - EEOC/ADA/ADEA/Other Claims
  - Sexual Harassment, Workplace Violence, Discrimination
  - Litigation
- Branding and Reputation

Employee Engagement

P&N
Postlethwaite & Netterville

What is Engagement?

Employee engagement is the extent to which **employees** feel passionate about their jobs, are committed to the organization, and put discretionary effort into their work.

Why Does it Matter?

- Reduce Turnover
- Positively Impact Customer Satisfaction
- Expand Brand-of-Choice in Industry
- Reduce Claims and Overhead Expenses
- Increase Profit

Strategies to Increase Engagement

- Use employee surveys and act on the information
- Focus at every level: corporate / local / regional
- Provide consistent training in workforce management
- Insist on accountability by all parties
- Define goals, expectations, rewards and consequences

Action Steps

P&N
Postlethwaite & Netterville

People + Processes

- Survey your employees and managers
- Evaluate your level of compliance with employment and labor laws. Consider multi-state impact;
- Seek guidance to understand how to develop and implement improvements;
- Develop a plan that includes HR Strategy, Compliance and Communication, and
- Implement, evaluate and revise as appropriate.

Resources

Postlethwaite & Netterville

Readily Available Information

- www.shrm.org
- www.dol.gov (fact sheets)
- https://www.peoplematter.com/resources/culture-white-paper
- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2015386
- www.gallup.com

Questions?

☎ (225) 663-1237

✉ hwall@pncpa.com

www.pncpa.com

P&N

Postlethwaite & Netterville

Internal Controls

Todd Tournillon, CPA

assurance - consulting - tax - technology - pncpa.com

Postlethwaite & Netterville, A Professional Accounting Corporation

Why this topic…

- GRAND TRAVERSE COUNTY, Mi. (WPBN/WGTU)— A former manager at the Hofbrau Interlochen is facing criminal charges for allegedly stealing thousands of dollars from the restaurant. A warrant for the arrest of 39-year-old Manager was issued Tuesday morning from the Grand Traverse County Prosecutor. She's being charged with embezzlement $50,000 or more but less than $100,000, and lying to a peace officer.
- "We have a person that stole from us, was our family, loved by everybody within our company. What she did was wrong," said Hofbrau Interlochen Owner. The Owner says they put up surveillance cameras in the office/safe area of the restaurant that captured video of the Manager in October that was used as evidence by police. It shows her going into the safe and looking at a deposit before taking the money out and then leaving the room.
- "And then when she does the daily reconciliation she writes down that there's no cash in the deposit, credit cards only with question marks," he said.
- Because she was also a close family friend, he says this has brought on a mix of emotions. He says he's now the only person there who handles the money. "We're trusting and we trust people," he said. "We think people are great and they are, she just wasn't."

Why this topic…

- HOUSTON, Tx.—Several people have been charged in a sweeping credit card fraud investigation involving several Houston and Harris County restaurants. Detectives with the Harris County Sheriff's Office, US Postal Inspectors and fraud investigators with several banks worked in concert on this investigation.
- Investigators said at least 193 people had their credit cards "skimmed" and then "cloned". Investigators said "skimming" happens when someone secretly uses a portable device to record a card number, then uses the information to create a "clone" of the card.
- Investigators said the stolen card numbers were used to make fraudulent purchases totaling more than $140,000.

Why this topic…

- Seven employees of a Miami International Airport food vendor were arrested on Friday for theft and organized fraud charges connected to the business, police said.
- Company owners did video surveillance and had a cash register tied to a computer program where they were able to track the sales and compare them to the amount of money the restaurant was taking in. The computer program indicated that money being stolen. "They were putting money in their pockets."
- The Company contacted police and turned over all the computer records and video, he said.
- The police investigated and took the workers into custody.

Why this topic…

- An employee of the business was arrested, but the thefts added up to so much that it was too late to save the place, the owner said. “It just slipped further and further away to the point of tens of thousands of dollars,” Pierce said of the thefts.
- Deputies arrested an employee in October. She had been with the Bistro since it opened in 2012, and was a trusted employee.
- Investigators said the employee systematically falsified customers’ orders so she could pocket their money instead of putting it all in the cash register. Investigators said she also told customers the credit card system was down, charging them cash, which she kept.
- Pierce is selling the Bistro and expects it to reopen under a new owner on Thursday.

Why this topic…

- A former part-time employee is accused of pocketing more than $112,000 while she worked as a hostess at a restaurant in a theme park.   She told investigators she started taking the money by making fraudulent cash refunds to help pay bills, according to an arrest report.
- It then became an addiction, she said. The company's financial analysts told deputies that she stole an average of $5,000 a month from the restaurant for almost two years, according to the report.
- Miller told investigators she started stealing the money in May 2013 when she was promoted to a general teller, giving her access to override and approve refunds, the report states.

Why this topic…

- The Company’s financial analysts told deputies they watched one night in March 2015, as she made numerous refunds for bills worth several hundred dollars each. She used various registers, sometimes logged in as other employees, and then would enter her personal code to approve the transactions.
- Surveillance video from that night caught her putting cash from the registers in a bag and then walking to a back office, according to the arrest affidavit. The bag was later seen empty, deputies said.
- The financial analysts questioned her that night about the odd transactions and asked if she had any of the money on her. She then pulled more than $2,700 out from under her shirt, according to the affidavit.
- Prosecutors filed charges against her a little more than two months ago and issued a warrant for her arrest. She was arrested last month in Massachusetts, records show, and brought back to Orange County on Tuesday.

Fraud and Internal Controls

- These frauds could not happen to us… they only happen at larger organizations or smaller organizations.
- We review budget to actual costs closely.
- We have a manager on –site, a purchasing director, etc.
- Our accounting person has been with us for years and has proven to be trustworthy.
- We are too small to have best practices.
- We have an experienced CEO who closely monitors operations and activities.

Control/Fraud Responsibilities

- Assess fraud risks
- Assess controls
- Have management communicate controls and changes in control when they occur
- Ask the external auditor questions during their planning and exit presentations
- Set expectations on roles (ownership vs. management)

Controls

- COSO (Appendix B) defines internal control as a process, effected by an entity’s ownership, management and other personnel. This process is designed to provide reasonable assurance regarding the achievement of objectives in effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

Control Areas to Consider

- Information systems
- Financial close/general ledger
- Financial reporting
- Paying of bills/disbursements
- Paying of employees/human resources
- Processing and recording of sales (cash and credit)
- Inventory (waste/shrinkage)
- Fixed assets/equipment
- Investments
- Cash management/debt
- Other

Controls

- Management should report/communicate controls to ownership
- Auditors can report on testing results
- Internal audit can verify on test basis
- Controls should be documented

Cost Effective Monitoring Controls

- Obtain understanding (updated at least annually) of Accounting personnel roles and responsibilities
  - Ownership/executive management should meet with Accounting team at least annually to ask about any issues/concerns and have them explain duties/roles
  - Consider having other personnel (e.g., IT, operational personnel, etc.) meet periodically to update ownership/executive management on their roles, issues, concerns and processes

Cost Effective Monitoring Controls

- If Accounting resources are limited, have ownership/executive management receive the bank statements from the bank to review prior to providing to Accounting to reconcile
  - Look for payments to cash
  - Identify unusual payments
  - Review for checks out of order
  - Review for unusual trend in deposits
  - Review for wires/ACH activity
- Review insurance coverage and who is listed/positions covered.

Cost Effective Monitoring Controls

- In the area of payroll,
  - Consider having ownership/executive management observe payroll registers/summary directly if third party service is used; a copy/summary if internally processed
  - Review W-2 for unusual amounts
  - Received quarterly list of employees and titles
  - Approve/review any non salary payments (e.g., bonus, vacation pay, etc.)
- Review activities with related parties

Cost Effective Monitoring Controls

- Obtain a computer generated list of disbursements
  - Review monthly
  - Review vendor summaries
- Require second signature on check
- Discourage use of stamped signatures
- Check signer, should not sign check without support attached/appropriately approved documentation. Consider documenting the “support” reviewed. Ask questions as appropriate.
- Assess need for use of credit cards/debit cards; if used, have management provide list of users and describe how monitored.
- Understand who can and who does post journal entries
- Key estimates
  - Have management explain methodology
  - Have management review calculations (e.g., Aging)

Cost Effective Monitoring Controls

- Have IT describe operations
  - At least annually obtain an update
  - Key procedures
  - Number of personnel/use of third parties
  - Software aging/hardware needs
- IT should develop a long-term budget regarding needs
- Security and cameras
- Inquire as to controls and oversight (e.g., who is monitoring)

Cost Effective Monitoring Controls

- Key financial data
  - Review complete set of GAAP financial statements monthly/quarterly
  - Review budget to actual income statement comparison - By location and in total
  - Ask for a MD&A explanation to be provided
  - Inquire as to frequency of balance sheet reconciliations/understand policy
  - Obtain aging of accounts receivable (grants, pledges, other) and accounts payable
  - Review rolling 12 month cash forecasts

Cost Effective Monitoring Controls

- Sales/Revenue
  - – Controls over private event activities (signed contracts). Guarantee on number of people.
- Cashiers/Servers
  - – Reconciliations at shift close
  - – Surprise reconciliations or counts
  - – Review should be documented.

Cost Effective Monitoring Controls

- Cash Management
  - Request a rolling 12 month cash flow projection
  - Ask management to explain how investments are monitored, controlled and safeguarded as well as reliance on controls of any third parties
  - Receive periodic reports on the market value/changes in investments
  - Obtain an understanding of line of credit/debt terms and renewal
    - Collateral requirements
    - Covenant requirements
    - Debt service requirements

Cost Effective Monitoring Controls

- Other Areas
  - For inventory have management describe results of any physical counts/perpetual to physical differences. Limit physical access to certain inventory items.
  - Understand tax effect of new initiatives (consultation with external CPA if needed)
  - Require special events to be reported by those involved in process to describe gross receipts and related costs (could be part of budget process), how receipts are controlled, how costs are approved paid, etc.
  - Require periodic verification of fixed assets
  - Have executive session with external auditors
  - Require planning and exit meetings with auditors
  - Ask questions about accounting policies, adjustments, controls tested, etc.

Areas to Consider

- Having no one outside of the Accounting Department review the bank statement
- Use of credit cards/debit cards
- Profitability of programs/initiatives
- No one outside the Accounting department reviews checks/disbursements
- No one outside of payroll reviews pay/pay rate changes

Appendix

- Appendix A – What is COSO
- Appendix B – Example IT Controls

Appendix A – What is COSO

- The Committee of Sponsoring Organizations' (COSO) mission is to provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations.
- COSO was organized in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private-sector initiative that studied the causal factors that can lead to fraudulent financial reporting. It also developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.
- The National Commission was sponsored jointly by five major professional associations headquartered in the United States: the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), The Institute of Internal Auditors (IIA), and the National Association of Accountants (now the Institute of Management Accountants [IMA]). Wholly independent of each of the sponsoring organizations, the Commission included representatives from industry, public accounting, investment firms, and the New York Stock Exchange.
- The first chairman of the National Commission was James C. Treadway, Jr., Executive Vice President and General Counsel, Paine Webber Incorporated and a former Commissioner of the U.S. Securities and Exchange Commission. Hence, the popular name "Treadway Commission." Currently, the COSO Chairman is David Landsittel.

Appendix B – Example IT Controls

- All outside service providers used by the entity are evaluated to determine those who provide material financial services that may impact controls.
- All outside service providers used by the entity are evaluated to determine those who provide material financial services that may impact controls.
- A backup and data retention policy/schedule exists, specifying how often backups are to be performed, how long they are to be retained, and where the backup media is to be stored.
- Application data and file server recovery procedures are tested at least annually to ensure data integrity and recovery.
- Appropriate environmental controls (such as fire/smoke detection, temperature controls, and alternate power supply) exist to ensure the security and reliability of equipment.
- A process exists to ensure that systems incidents, problems, and errors are reported, analyzed, and resolved timely.
- An information security policy exists that defines information security objectives. This policy is supported by documents standards and procedures where necessary.
- Procedures exist and are followed to ensure timely action relating to requesting, establishing, issuing, suspending, modifying, and closing user accounts, including proper authorization.
- User access rights are removed or suspended in a timely manner when employees are terminated. Standards exist to define timeliness requirements for various situations (i.e., voluntary or involuntary termination).
- User access rights (network, application, etc.) are granted on a need-to-know, need-to-do basis that considers appropriate segregation of duties. Review of access to system occurs at least annually by key users to verify segregation of duties.
- Procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms (e.g., password length, password history, password expiration, and lockout for failed attempts).
- Access to IT facilities is secure/restricted to authorized users.
- Changes to key systems are approved and tested by users
- Adequate segregation of duties within IT exists

Questions?

Postlethwaite & Netterville

Postlethwaite & Netterville

PCI Compliance & Cybersecurity

Paul Douglas, CISA, CCSFP

assurance - consulting - tax - technology - pncpa.com

Postlethwaite & Netterville, A Professional Accounting Corporation

Agenda

- PCI DSS – What and Why?
- Challenges for Restaurants
- How to get Started?
- Self Assessment Questionnaires

What is PCI DSS?

- **Payment Card Industry (PCI) Data Security Standard (DSS)** debuted in 2004 and is not a legal requirement.
- It is a set of industry rules created by payment card brands and is a necessity for merchants who wish to process, transmit, and store payment card data such as the card number, expiration dates, verification codes and magnetic stripe data.
- Why? To minimize payment card fraud for which the card brands are ultimately responsible.
- Merchant vulnerabilities to the payment data may appear around POS devices, computers and servers used, wireless hotspots for online purchases, in paper-based storage systems and unsecured transmission to the acquirer.
- PCI DSS and related security standards are administered by the PCI Security Standards Council, which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

Some Definitions

- ***Cardholder Data:*** The PCI Security Standards Council (SSC) defines ‘cardholder data’ as the full Primary Account Number (PAN) or the full PAN along with any of the following elements:
  - Cardholder name
  - Expiration date
  - Service code
- Sensitive Authentication Data, which must also be protected, includes full magnetic stripe data, CAV2, CVC2, CVV2, CID, PINs, PIN blocks and more.
- For the purposes of the PCI DSS, a ***merchant*** is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services.
- ***Service Provider*** is defined as a business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data.

Why be PCI DSS compliant?

- **Penalties.** The payment brands may, at their discretion fine acquiring banks $5,000 to $100,000 **per month** for non-compliance until remediation is complete which may be passed on to the merchant.

- **Loss of Payment Options.** The acquiring bank may either terminate relationship with the merchant or increase transaction fees. Details of such exposure are outlined in the merchant account agreement.

- **Cost of Recovery**. The 2016 Cost of Data Breach Study: United States by the Ponemon Institute in June 2016 reports that the average cost per lost or stolen record is $221, a 2% increase from the previous year. There was also a 7% increase in the total cost of data breach from prior year.

- **Reputational Risk to a Restaurant.** Impact to short-term and long-term sales.

Requirement Categories

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Tools for Assessing Compliance

- The PCI SSC sets the PCI security standards, but each payment card brand has its own program for compliance, validation levels and enforcement.

  More information about compliance can be found at these links:
  - American Express: www.americanexpress.com/datasecurity
  - Discover Financial Services: www.discovernetwork.com/fraudsecurity/disc.html
  - JCB International: www.jcb-global.com/english/pci/index.html
  - MasterCard Worldwide: www.mastercard.com/sdp
  - Visa Inc: www.visa.com/cisp
  - Visa Europe: www.visaeurope.com/ais

Challenges for Restaurants

P&N

Postlethwaite & Netterville

Challenges for Restaurants

The services offered and technological infrastructure within restaurants creates the following challenges to PCI DSS compliance.

- Shared access to multiple point of sale (POS) systems reduces the restaurant's ability to pinpoint the liable party. Insider threat account for about 50 percent of all security incidents (Verizon Data Breach Investigations Report).
- Public wi-fi connections in a restaurant provide additional risks, as it can present another potential avenue for hackers to gain access to POS systems.
- Restaurant POS systems are often located in areas hidden from public view, which allow a criminal to breach the POS system by installing a rogue device such as a card skimmer, without the knowledge of the merchant.
- POS Malware discreetly slips by antivirus programs and then stealthily extracts payment data, despite the presence of traditional firewalls.
- Franchises - A breached system within one franchise could impact all franchises.

Recent Breach Examples

- In February 2017, Arby’s Restaurant Group, Inc. (ARG) reported that over 350,000 credit and debit cards were compromised at multiple corporate locations due to malware in their POS systems.

- In February 2016, Wendy’s reported suspicious activity affecting some franchisee owned restaurants. Subsequently, on June 9, 2016, the Company reported that at least 1035 locations were impacted. The cause was determined to be the compromise of the service providers’ remote access credentials, resulting in malware being installed on their POS systems.

- In May 2016, Popeye's reported that 10 locations had been affected by a payment card breach due to malware on certain systems.

Cybersecurity Takeaways

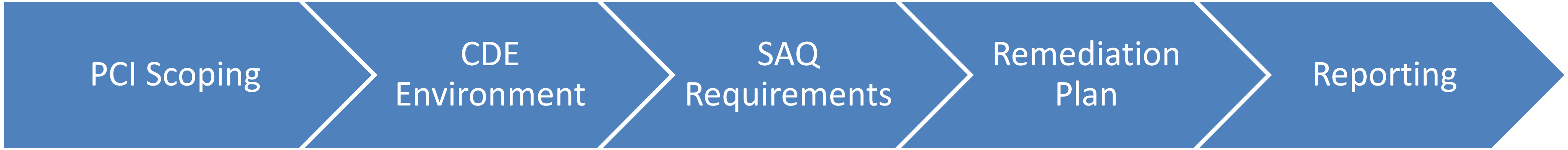
- Vulnerabilities within network infrastructure and device credentials (e.g. Wireless Router).
- Theft of user credentials and safeguarding of passwords.
- Network isolation and segmentation between locations / sensitive areas.
- Third party risk management.
- User security awareness and training (e.g. skimmer detection, phishing attacks, incident response, etc.)

How to Get Started

P&N

Postlethwaite & Netterville

Getting Started



PCI Scoping

CDE Environment

SAQ Requirements

Remediation Plan

Reporting

Postlethwaite & Netterville

Getting Started

- Phase 1: PCI DSS Scoping
  - Understanding the type of business (merchant vs. service provider) and the level as established by the acquirer (based on the number of transactions or risk) to determine the approach to compliance.
  - The business type and the level does not affect the applicable PCI requirements, however the approach to compliance may vary.
  - Understanding the scope of PCI DSS specific to your restaurant group. This includes understanding how customer payments are received and processed and the different units that receive or have access to the cardholder data.
  - Identifying ways to reduce PCI DSS scope such as network segmentation, eliminating storage of the Primary Account Number (PAN), Outsourcing PCI requirements among others.

- Phase 2: Cardholder Data (CHD) Environment Overview
  - Understanding the technology environment that corresponds to the operations identified, including any technology that is outsourced to third party vendors.

Getting Started

- Phase 3: Self-Assessment Questionnaire (SAQ) or Report of Compliance
  - Identifying and completing the appropriate Self Assessment Questionnaires or Report of Compliance as determined within Phase 1.
  - An organization is either compliant or non-compliant. There is no partial compliance.
  - Compliance is validated by a signed Attestation of Compliance (AoC) submitted by an officer of the merchant or service provider.

- Phase 4: PCI DSS Compliance Plan of Action
  - Identifying a plan of action to achieve PCI DSS compliance, calculating the associated costs and the projected date of remediation.

- Phase 5: Reporting
  - Reports from the SAQs or annual attestations of compliance (AoC) are the official mechanism by which merchants and other entities verify compliance with PCI DSS to their respective acquiring financial institutions or payment card brand.

Self Assessment Questionnaires

P&N
Postlethwaite & Netterville

Self Assessment Questionnaire

- Depending on payment card brand requirements, merchants and service providers may need to submit a *Self-Assessment Questionnaire (SAQ)* for self-assessments, or a *Report on Compliance* for on-site assessments.
- There are 5 SAQ categories available to merchants and service providers in PCI-DSS v3.0, each for a specific cardholder data environment (CDE).
- Each SAQ has 2 components
  - A set of questions corresponding to the PCI Data Security Standard requirements designed for service providers and merchants. Any non-compliance may require documentation of future remediation steps and dates.
  - An Attestation of Compliance or certification that you are eligible to perform and have performed the appropriate Self-Assessment. An appropriate Attestation will be packaged with the Questionnaire that you select.

SAQ Categories

SAQ	Description
A	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.
B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dialout terminal merchants with no electronic cardholder data storage
C-VT	Merchants using only web-based virtual terminals, no electronic cardholder data storage
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage
D	All other merchants not included in descriptions for SAQ types A through C above, and all service providers defined by a payment card brand as eligible to complete an SAQ

Additional Resources

The PCI Security Standards Council (PCI SSC) website (www.pcisecuritystandards.org) contains a number of additional resources to assist organizations with their PCI DSS assessments and validations, including:

- Document Library, including:
- Frequently Asked Questions (FAQs)
- PCI training courses and informational webinars
- List of Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs)
- List of PTS approved devices and PA-DSS validated payment applications
- PCI for Small Merchants website

P&N
Postlethwaite & Netterville

References

Reference Guide (https://www.pcisecuritystandards.org/)

2016 Cost of Data Breach Study: United States (https://www.ibm.com/security/data-breach/)

The National Conference of State Legislatures (http://www.ncsl.org/)

Data Breach Examples (https://krebsonsecurity.com/)

PCI Compliance Penalties (http://www.merchantlink.com/)

Definitions (https://www.pcicomplianceguide.org)

Considerations for Restaurants (http://www.restaurant.org/)

Questions?

P&N
Postlethwaite & Netterville

P&N

Postlethwaite & Netterville

State & Local Tax Update

Gary Dressler, CPA

assurance - consulting - tax - technology - **pncpa.com**

Postlethwaite & Netterville, A Professional Accounting Corporation

Agenda

1. Sales Tax and Return Preparation
2. Sales Tax Audit Issues
3. Property Taxes
4. Current Legislation

P&N
Postlethwaite & Netterville

Sales Tax and Return Preparation

- Sales Tax Issues:
  - Gratuities
  - Discounted meals for employees and others
    - Amount paid is tax base
  - Gifts cards

Sales Tax and Return Preparation

- Use Tax Issues:
  - Free meals for employees and others.
  - Appropriate use of resale certificate
    - Items utilized for take-out purchases
  - Review invoices with no sales tax and invoices from out-of-state vendors.
    - Services vs. tangible personal property
    - Software and software maintenance.
    - Furniture and equipment

Sales Tax and Return Preparation

- Miscellaneous Taxes
  - New Orleans Exhibition Hall tax
    - Limited to food and beverages.
  - New Orleans excise tax on liquor

Sales Tax and Return Preparation

- Gross sales on line 1 should be same number that flows to gross sales on P&L.
- Take deductions on appropriate lines: discounts, exemption certificates, etc.
- Use tax on line 2: totally comped meals, purchases of use items with no tax on invoice.

Sales Tax Audit Issues

- Auditors first task will be to compare line 1 from sales tax return to gross sales on income tax return.
  - – Will assess sales tax on any difference unless taxpayer can reconcile and explain.
- Will review purchases for use tax liability.
- Don’t just accept auditor findings.
  - – Invoice doesn’t always tell correct story of transaction
- Maintain appropriate records – DSR, Z-tapes, etc.

P&N
Postlethwaite & Netterville

Property Tax

- Should be rendering property to assessor. (LAT-5)
- Penalty assessments when don’t render.
- Note values on property tax bills.
- Can check rolls in July and only valid protest follows this process.
- Render by year and original cost.
- Note expensed asset transactions.
- Remove items when you no longer possess them.

Current Legislation

- HB63 – Advance sales tax
  - Limited to collection by alcohol and cigarette distributors
  - No exceptions in bill as currently written
  - State tax only – locals prohibited for collecting
- Clean Penny – Several bills to eliminate 6/30/18 sunset.

Questions?

P&N

Postlethwaite & Netterville

Cloud Software for Financial Management

Karen Jones, CAPM

assurance - consulting - tax - technology - **pncpa.com**

Postlethwaite & Netterville, A Professional Accounting Corporation

Agenda

1. Why is it hard to get good financial information
2. What to expect from a cloud-based solution
3. How to choose the right solution

P&N
Postlethwaite & Netterville

The Balancing Act

- Managing an increasing level of business complexity vs. the need for quick decision-making based in financial truth.
- Is accounting software helping you grow and compete—or holding you back?

Why is it so hard to get good financial information?

QuickBooks, Microsoft Dynamics, SAP and Oracle all pre-date the Internet.

They were never designed for today’s always-on, always-connected, always-working world. They lack the flexibility to give you the right information at the right time.

Your First Decision

- Choosing a software delivery model
- Three general options for delivery are in the market:
  - On-premises solutions
  - Hosted solutions (single tenant)
  - Cloud computing solutions (multi-tenant)

On-Premises Solutions

- Traditional model of licensing software and running it on your own servers
- May be cost-prohibitive for small companies
- Requires IT infrastructure, investment capital and expertise to support the application

Hosted Solutions (single tenant)

- Software physically resides at a remote data center
- Eliminates the responsibility of maintaining hardware infrastructure, lower up-front expense
- Costs may be associated with customizations, upgrades, integration and support

Cloud Computing Solutions (multi-tenant)

- Direct, always-on access, paid for on a per-user or per-month subscription basis
- Single set of resources, application infrastructure and database on a shared system
- No upfront fees, capital investments or long-term commitments
- Sometimes referred to as “Software as a Service” (SaaS)

Software as a Service (SaaS)

Just like Google, Amazon and online banking, cloud-based financial applications were built for the Internet age.

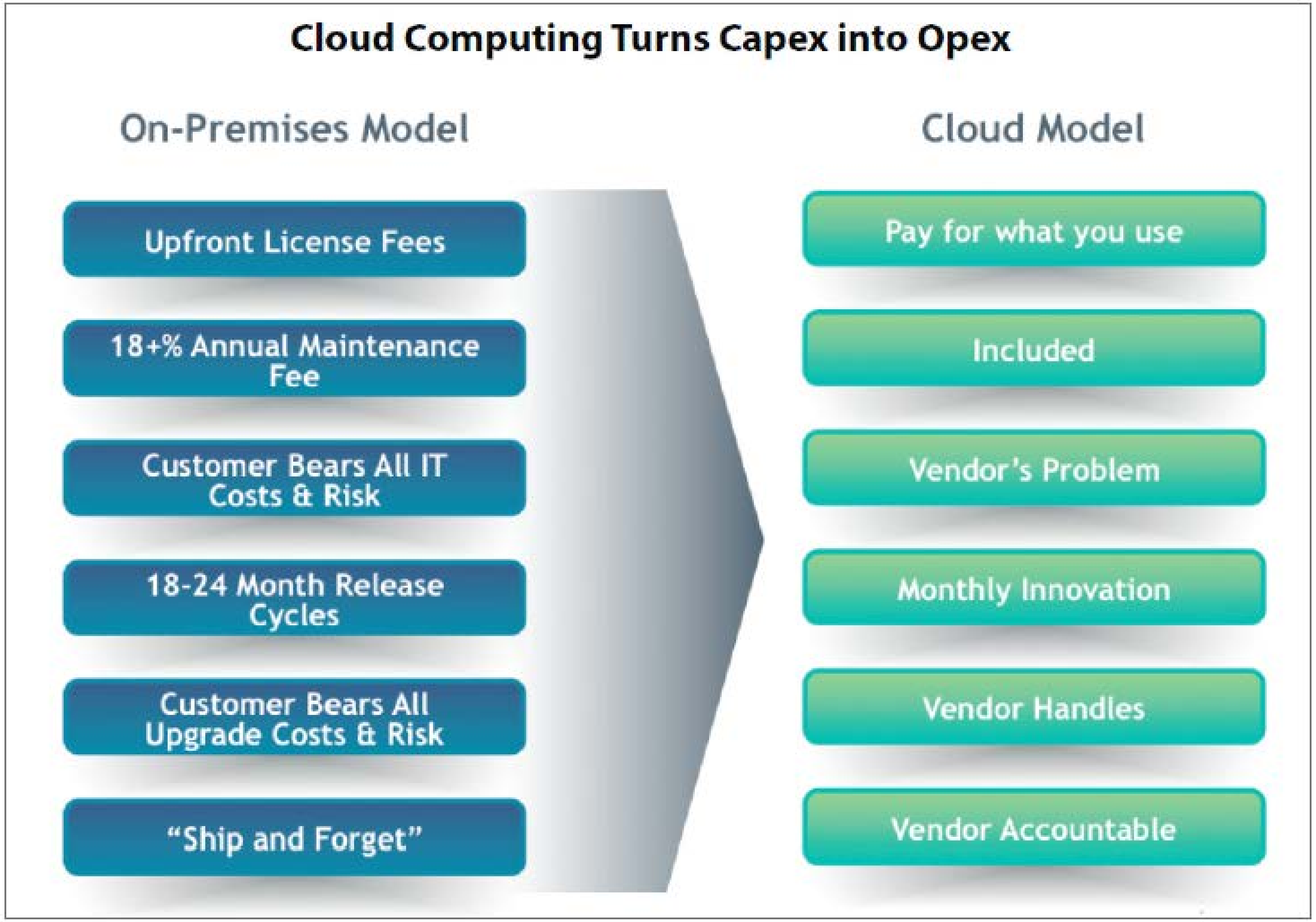
Considering Cloud

- Does my team need to work outside the office?
- Does my business need to accelerate financial processes—*without* increasing headcount or IT budget?
- Does my financial system need to integrate with other applications?

Considering Cloud

- Do my managers want or need self-service access to their relevant KPIs?
- Does my organization struggle with inefficient processes?
- Do we need to compete with bigger businesses—on a smaller budget?

Turn Capex into Opex



Cloud Computing Turns Capex into Opex

On-Premises Model	Cloud Model
Upfront License Fees	Pay for what you use
18+% Annual Maintenance Fee	Included
Customer Bears All IT Costs & Risk	Vendor's Problem
18-24 Month Release Cycles	Monthly Innovation
Customer Bears All Upgrade Costs & Risk	Vendor Handles
"Ship and Forget"	Vendor Accountable

Evaluating Solutions

- Gather requirements
- Identify top priorities and challenges
- Create a Request for Proposal (RFP)
- Research your options
- Demo or trial from short list
- Focus on product fit
- Check references, score and select

What to Look for in a Cloud Vendor

- Implementation success
- Operational track record
- Data ownership
- Infrastructure and security
- ROI/Total Cost of Ownership
- Support Agreement
- Service level agreements

SLA Must-Haves

- System availability
- Disaster recovery
- Data integrity and ownership
- Support response
- Escalation procedures
- Maintenance communications
- Product communication

How to be an Informed Buyer

- Remember that cloud vendors must earn your business every month
- Be wary of steep upfront discounts
- Factor in all the variables to avoid surprises
- Understand what you will be paying for and when

Conclusion

- Remember: You are in the power seat
  - – In today’s market, the buyers have the power
- Understand the implications of all options for financial application
- Choose the right solution for your business

P&N
Postlethwaite & Netterville

Questions?

P&N
Postlethwaite & Netterville

P&N

Postlethwaite & Netterville

A Professional Accounting Corporation