Hot Topics in Plan Audits

MORE THAN YOU EXPECT...

EVERYTHING YOU NEED

Hotter(?) Topics in Plan Audits

MORE THAN YOU EXPECT...

EVERYTHING YOU NEED

Hot-ish(?) Topics in Plan Audits

MORE THAN YOU EXPECT...

EVERYTHING YOU NEED

Proposed Audit Report

Statement on Auditing Standards

Forming an Opinion and Reporting on Financial Statements of Employee Benefit Plans Subject to ERISA

Assessing the Quality of Employee Benefit Plan Audits

U.S. Department of Labor
Employee Benefits Security Administration
Office of the Chief Accountant
May 2015

Major Deficiency Audit Rates

by Stratum

(95% Confidence Level; Statistically Significant Differences between Stratum)

Strata	Audit Reviews	Audits With Deficiencies	Standard Error	Lower Bound	Upper Bound
1-2	95	75.8%	4.4%	66.1%	83.4%
3-5	95	68.4%	4.8%	58.3%	77.0%
6-24	95	67.4%	7.7%	50.9%	80.4%
25-99	65	41.5%	9.7%	24.4%	61.0%
100-749	25	12.0%	4.9%	5.2%	25.4%
750+	25	12.0%	8.0%	3.0%	37.8%
Total Reviewed	**400**	**38.8%**	**3.5%**	**32.2%**	**45.9%**

Note: Statistics are calculated using sample weights, which account for the different amount of audits performed by each stratum. For this reason, the population average may be different from the un-weighted sample averages.

Proposed Plan Audit Report

Why do we need a new report?

- DOL study found that 39% of EBP audits had one or more major deficiencies
- In a limited scope audit, many practitioners don't think they are doing an audit because there is no opinion (it is a disclaimer)
- Plan sponsors and other users of the financials don't understand the limited scope audit

Proposed Plan Audit Report

- New report developed using input from the Department of Labor and is intended to improve the usefulness of the audit report and to improve audit quality.

- New report would be used for plan year ~~2018~~ (probably 2020) financial statements.

Proposed Plan Audit Report

- Plan sponsor take-aways
  - Limited scope audit
    - Management is responsible for determining that the institution holding the plan investments is qualified to certify the investments.
    - Management is responsible for determining that the certified information is complete and accurate.
  - No longer a disclaimer of opinion, but will include that ERISA section 103(a)(3)(c) audit was performed.

What is a Limited Scope audit?

- **Management** requests that the auditor not perform any auditing procedures with respect to investment information.

What do you need to do this?

- A qualified institution (see next slide) must certify both the completeness and accuracy of the required information.

Who is qualified?

- The DOL established requirements for qualifying institutions.

Investments held by a bank, trust company or similar institution or by an insurance carrier that is regulated, supervised, and subject to periodic examination by a state or federal agency, and related information do not have to be audited.

What isn't audited?

- The limited scope exemption only applies to the investment information (investment pricing and related investment income) certified to by the qualifying institution.

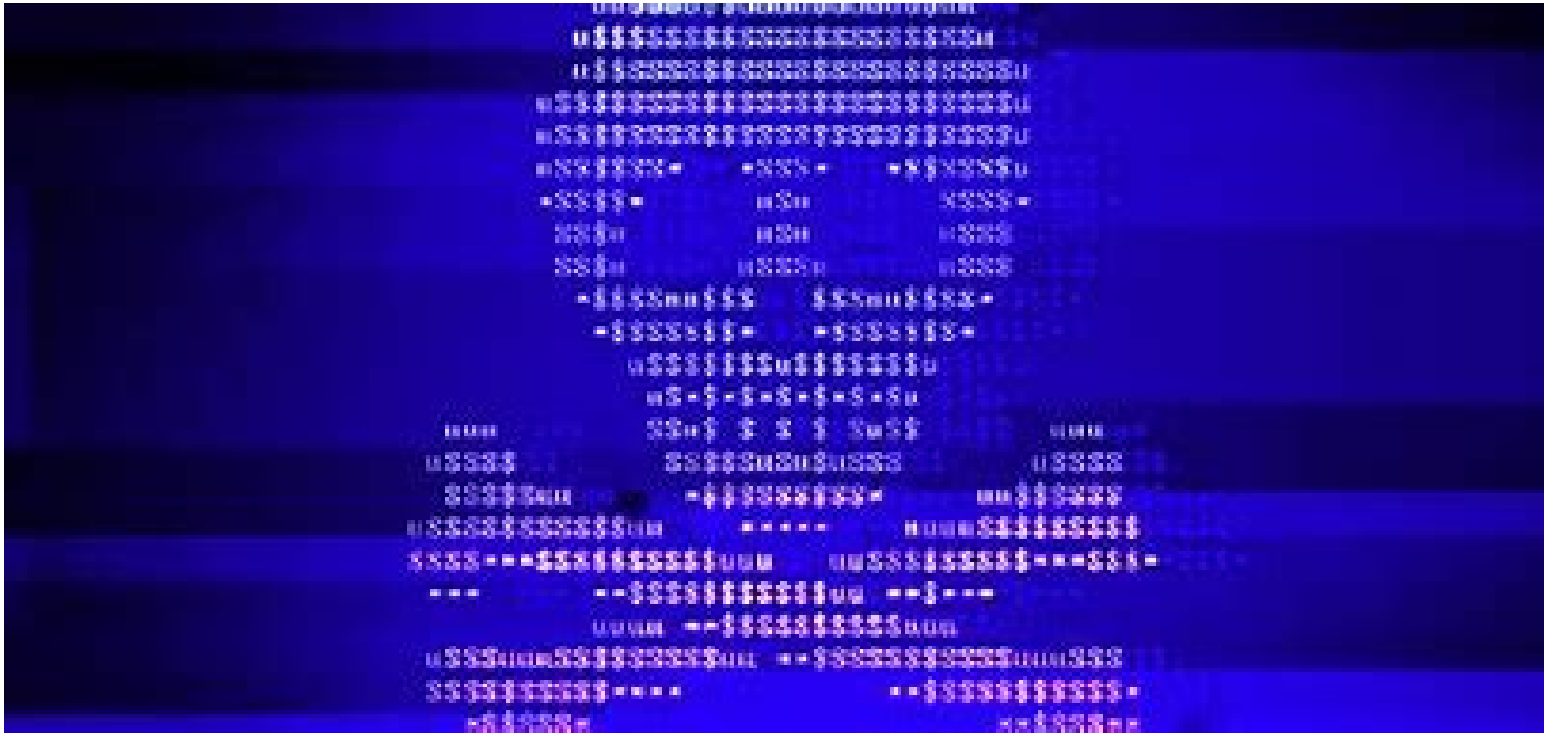
- The exemption does not apply to participant data, contributions, benefit payments, financial statement disclosures, etc.

Be ready for more questions

- When management elects to have a limited scope audit, the auditor should inquire of management about how management determined that the entity preparing and certifying the investment information is a qualified institution.

- There will also be additional representations in the representation letter.

Cybersecurity



Examples of Cyber Threats

- Ramsomware – criminals encrypt and seize a hard drive and will only release it for a high ransom
- Phishing – fraudulent emails sent with the objective of enticing the user to provide the criminal with access to a computer network
- Wire transfer email fraud – criminal pretends to be a senior executive asking employees to transfer funds
- Malware via external devices – harmful software is stored on an external drive that is inserted into and executed on a network computer

Real Life Examples

- An email, purported to be from the plan sponsor's top executive, was sent to the HR department requesting sensitive employee data. HR responded by sending the information.
- A phishing scheme was successfully carried out at a plan recordkeeper. As a result, participant accounts were breached and unauthorized distributions were made.

Real Life Examples

- A plan sponsor's internal IT department discovered malware on 50 computers. One participant account was breached and an improper distribution occurred before the malware was discovered.
- A plan sponsor had a malware infection targeting their employee health care plan. The breach exposed private health information of 1,500 people. The plan sponsor had failed to assess the risk of malware infection and adopt procedures to secure its data.

Real Life Examples

- Hackers obtained personal information of plan participants and used it to set up online profiles on the plan custodian's web platform. The hackers accessed accounts and withdrew loans from 58 accounts. The estimates of losses was $2.6 million. The plan sponsor returned the funds and provided credit monitoring to the account holders.

Real Life Examples

- A service provider received an unusual number of distribution requests for one of their plan clients. The requests were vetted through the established process and denied the requests because they were determined to be unauthorized.
- A CD-ROM and laptop that contained private data of 30,000 plan participants and beneficiaries were stolen from the vehicle of an employee of a plan sponsor. Notification, credit monitoring and insurance costs were approximately $200,000.

Real Life Examples

- A cyberattack targeting a union pension plan took control of the pension plan's computer servers and demanded a ransom in digital currency. Data at risk included employee names, birthdates, Social Security numbers and bank information. The union refused to pay and used its backup system. No evidence that the hackers accessed the data, but participants were offered 12 months of credit monitoring and identity theft services.

What am I supposed to do?

- Risk Analysis
  - Who has access to plan data?
  - What equipment may contain personal identification information?
  - Which vendors need which data?
  - What protocols are used to transfer files and data and their security?
  - Is there insurance and what does it cover?

What am I supposed to do?

- Vendor Security Questions
  - How will plan data be maintained and protected?
  - When and how will data be encrypted?
  - What liability will the vendor assume for breaches and what are their procedures in the event of a breach?
  - How and when will plan sponsors be notified if systems are breached?

What am I supposed to do?

- Vendor Security Questions
  - Do vendors provide regular reports on their security risk analysis and monitoring?
  - What level and type of insurance do they have?
  - How do security procedures apply to their subcontractors?

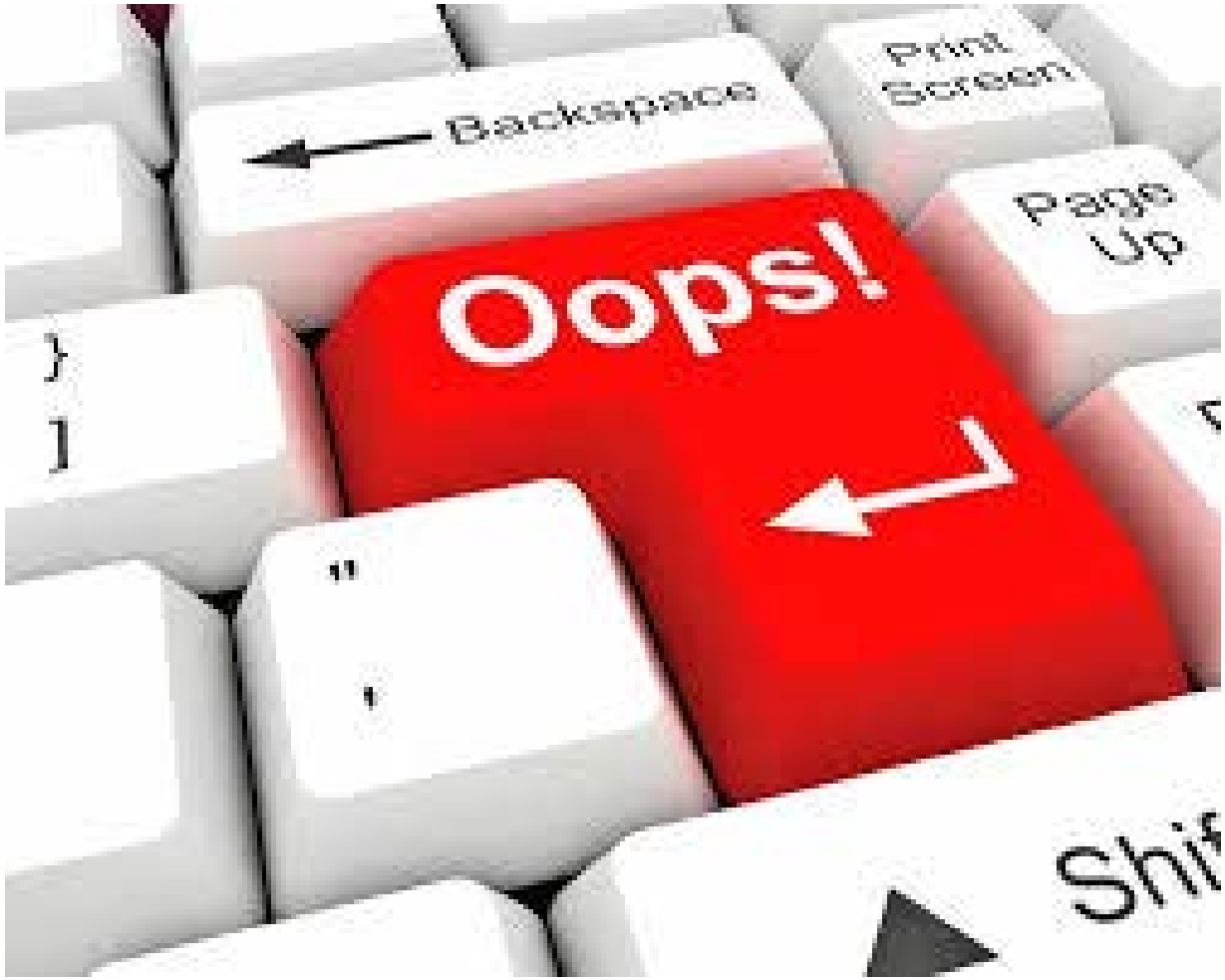
What's New?

DOL compliance initatives

(DOL comments from a 1/26 webinar)

- Primary compliance concerns
  - Filers with first time audits
    - Records maintenance
    - Testing opening balances
  - Missing audit reports and completeness of financial information
  - Stop filers
  - Plans that incorrectly identify plan features (page 2 of Form 5500)

Common Plan Errors

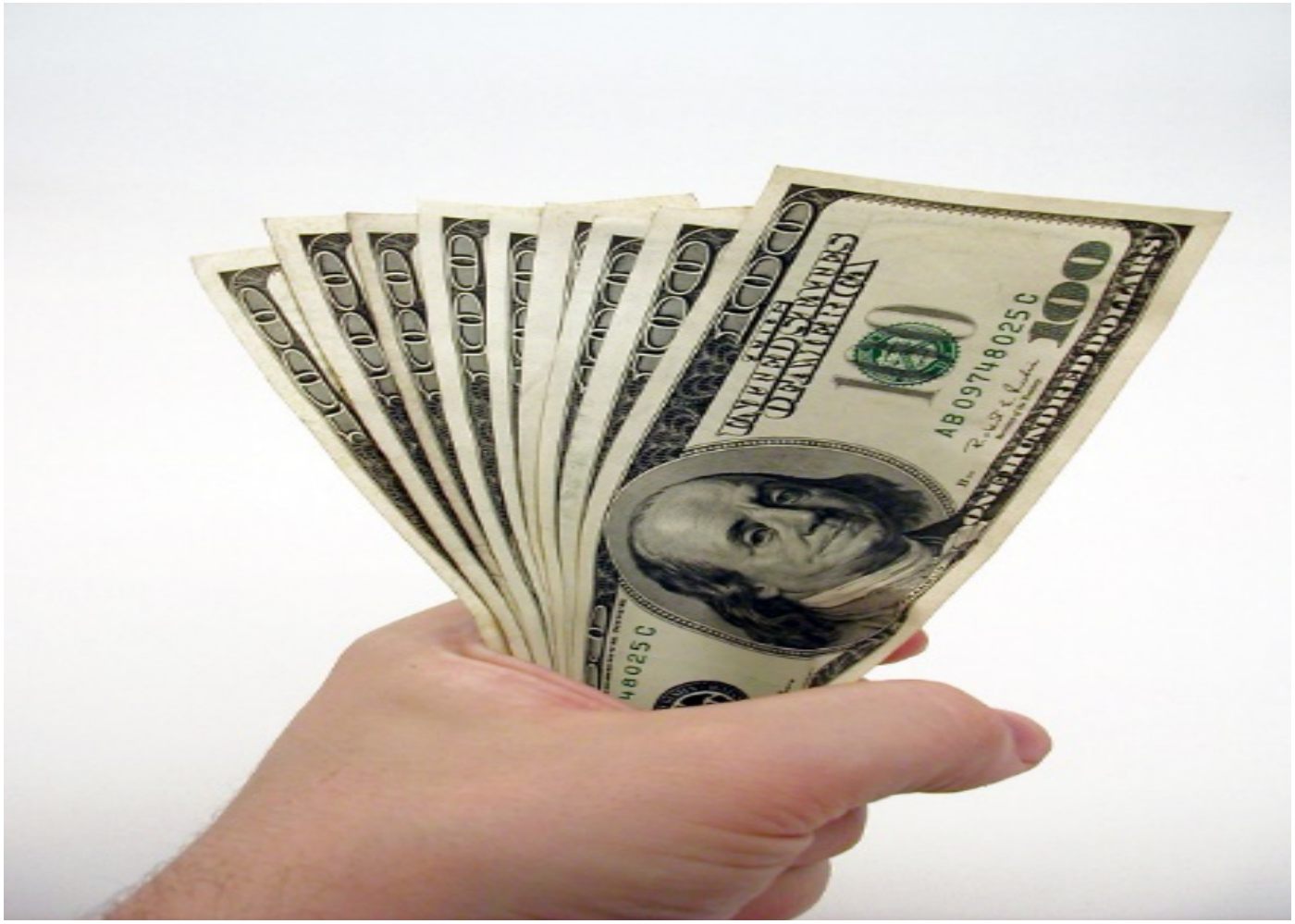


Late Remittances

Late Remittances

- Small plans – safe harbor of 7 business days
- Large plans – as soon as administratively possible ~~but no later than 15 business days~~

Forfeitures



Forfeitures

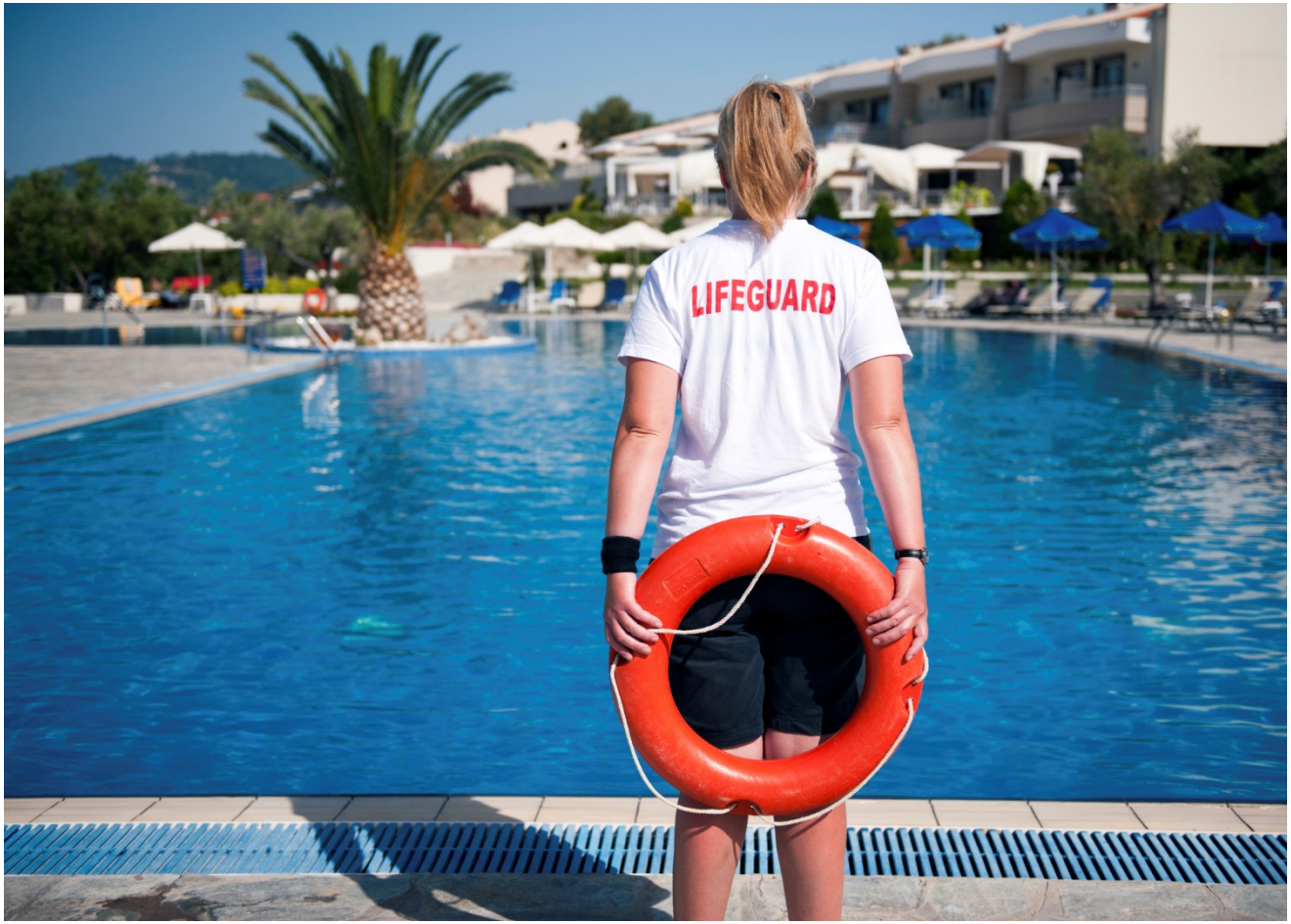
- What does plan document say?
- Match offset, pay plan expenses, allocate to participants

Definition of compensation

Definition of compensation

- Check your plan document and compare it to your payroll system
- Watch out for bonuses and commissions

Eligibility



Eligibility

- Entrance to the plan
- Participation in matching and profit-sharing contributions

Distributions

In-service distributions

- Allowed by the plan?
- Documentation required?
- Proper withholdings?

Participant loans

- Allowed by the plan document?
- Number of loans
- Repayments being made appropriately?

Hardship distributions

- Allowed by the plan document?
- Documentation of hardship and amount
- Loan already taken?

- Mark Blackburn

- (615) 309-2210
- mblackburn@lbmc.com

Questions?

www.lbmc.com