

In this issue

- 01** 2018 cost-of-living adjustments
- 02** A 401(k) plan fix-it checklist for business owners
- 03** Addressing cyber security risks

Winter 2018

2018 cost-of-living adjustments

The IRS has released the annual cost-of-living adjustments for various retirement plan limitations, with only some of the limitations increasing for 2018. The table below compares the 2017 and 2018 numbers for many key limits.

Also, the Social Security Administration announced a \$1,200 (0.94%) increase in the Social Security taxable wage base effective January 1, 2018. This change affects retirement plans that consider Social Security in determining benefits or contributions.

	2018	2017
Defined contribution plan dollar limit on annual additions	\$55,000	\$54,000
Defined benefit plan limit on annual benefits	\$220,000	\$215,000
Maximum compensation used to determine benefits or contributions	\$275,000	\$270,000
401(k), SARSEP,* 403(b), and 457 plan deferrals	\$18,500	\$18,000
Catch-up	\$6,000	\$6,000
SIMPLE deferrals	\$12,500	\$12,500
Catch-up	\$3,000	\$3,000
Compensation defining highly compensated employee	\$120,000	\$120,000
Compensation defining key employee (officer)	\$175,000	\$175,000
SEP annual compensation triggering a contribution	\$600	\$600
IRA contribution	\$5,500	\$5,500
Catch-up	\$1,000	\$1,000
PBGC maximum guaranteed monthly benefit for a 65-year-old retiree	\$5,420.45	\$5,369.32
Social Security taxable wage base	\$128,400	\$127,200

* SEP plans established before 1997.



UBS ERISA Extra

A 401(k) plan fix-it checklist for business owners

Maintaining a retirement plan can be complicated. The following is a short checklist outlining some of the responsibilities for sponsors of 401(k) plans.¹

Is your plan document updated?

Plan sponsors must be able to demonstrate that they have a written plan in place and that they have made all required amendments within required time periods. Different sets of rules apply to amendment adoptions, depending on whether the plan is pre-approved (a prototype) or individually designed and whether amendments qualify as “interim” or “discretionary.” Contact your UBS Financial Advisor and/or tax advisor for more details.

Do plan operations conform to the plan document?

Plan operations must be consistent with the terms of the plan document. To prevent discrepancies, sponsors should conduct a regular review of the plan and its operation. Corrections must be made as soon as possible with a correction method that conforms to IRS guidelines.

If you make changes to your plan document, amend your summary plan description and inform everyone who services your plan of the changes. If you’ve made a change that is deemed material, you may also need to provide plan participants with a Summary of Material Modifications (SMM). Remember that any

changes in ownership interests and any business acquisitions may affect the non-discrimination testing for the plan.

One common plan error is improper use of the plan’s definition of “compensation” for purposes of deferrals, allocations and testing. Some plan definitions of “compensation” can be complicated—particularly if expense reimbursements, car allowances, bonuses, commissions and overtime are included—so be sure to have a qualified person perform your annual reviews.

Have matching contributions been made for all eligible employees?

Another common plan error is the failure to make matching contributions to all the appropriate employees’ accounts. Review the plan document to determine both employee eligibility requirements and the matching contribution formula and compare them to what was used.

Has your plan satisfied the Actual Deferral Percentage (ADP) and Actual Contribution Percentage (ACP) non-discrimination tests?

Plan sponsors must test traditional 401(k) plans each year to ensure that contributions made by and for non-highly compensated employees (NHCEs) are proportional to contributions made for highly compensated employees (HCEs).

An essential first step is to determine who the HCEs are. Generally, for 2018, an HCE is any employee who:

- Was a 5% owner, directly or by family attribution, at any time during the current or prior year, or

- For the prior year, was paid by the employer more than \$120,000.²

If your plan fails either the ADP or the ACP test, you must take corrective action within 2½ months after the close of the plan year or be liable for a 10% excise tax on the amount of the excess aggregate contributions.³ If corrective action is not taken within 12 months of the end of the plan year, the plan will no longer satisfy the non-discrimination requirements for qualification.⁴

Were all eligible employees identified and given the opportunity to make elective deferrals?

The plan document should contain a definition of “employee” and provide requirements for eligibility to make elective contributions.

Employers sometimes incorrectly assume the plan doesn’t cover certain employees, such as part-time employees or those who elect not to make deferrals. Treat each employee who receives a Form W-2 as an eligible employee unless you can properly exclude that employee by the plan terms. Generally, if you did not give an eligible employee the opportunity to make elective deferrals, you will have to make a qualified nonelective contribution for the employee to compensate for the missed deferral opportunity.

Are elective deferrals within annual limits?

For 2018, plans may allow employees to defer up to \$18,500. “Catch-up” contributions of up to \$6,000 may be allowed for workers age 50 or older. Combined employer and employee contributions and any reallocated forfeitures (“annual additions”) may not exceed the lesser of



UBS ERISA Extra

100% of the participant's compensation or \$55,000 in 2018.⁵ (Catch-up contributions are not counted toward the annual additions limit.)

Have you timely deposited elective deferrals?

Generally, the employer is responsible for contributing the participants' deferrals to the plan trust as soon as the employer can, but in no event after the fifteenth business day of the following month.⁶ The U.S. Department of Labor (DOL) allows a seven-business-day safe harbor rule for plans with fewer than 100 participants.⁷

Do participant loans meet the plan document and IRS requirements?

Plan loan programs must meet a number of different requirements. ERISA requires—among other things—that a loan program be set forth in the plan and include specific information.⁸ IRS rules require an enforceable agreement and impose additional limits related to the term, amortization and loan amount.⁹

Were hardship distributions made properly?

Hardship distributions must be authorized by the plan, and distributions must be no more than necessary to meet an immediate and heavy financial need of the employee.¹⁰

In February 2017, the IRS—in a memorandum for its examiners—set forth the requirements for determining whether safe harbor hardship distributions have been adequately documented.¹¹ The memorandum prescribes the appropriate procedures for determining whether substantiation requirements for the six types of safe harbor hardship distributions have been met.

Were top-heavy minimum contributions made?

A plan is top-heavy when, as of the last day of the prior plan year, the total value of the plan accounts of key employees is more than 60% of the total value of the plan assets.¹² A “key” employee is any employee who at any time during the plan year was:

- An officer making over \$175,000 for 2018
- A 5% owner of the business
- An employee owning more than 1% of the business and making over \$150,000 for the plan year¹³

Family aggregation rules apply, so be sure to properly identify owners and their family members.

Generally, top-heavy testing is of greater concern for smaller plans or plans that have a high turnover rate. To correct the mistake, the employer must make a corrective contribution that includes lost earnings to the non-key employees. The contribution is generally 3% of compensation.

Was Form 5500 filed?

Most 401(k) plan sponsors are required to annually file Form 5500 (Annual Return/Report of Employee Benefit Plan). Generally, the due date is the last day of the seventh month after the plan year ends.¹⁴ Late-filed returns are subject to penalties from both the IRS and the DOL. The IRS penalty is \$25 per day, up to a maximum of \$15,000,¹⁵ and the DOL penalty can be up to \$1,000 per day (\$2,063 per day—after adjustment for inflation—for penalties assessed after August 1, 2016).¹⁶

Addressing cyber security risks

As news outlets continue to report on cyber security breaches at financial institutions, retailers, law firms, government agencies, Yahoo and even Equifax, the retirement plan industry is working to delineate ways to manage the unique cyber security risks presented by retirement savings plans. Earlier this year, the DOL published a helpful guide entitled “Cybersecurity Considerations for Benefit Plans” (the “Report”). This Report—written by the 2016 Advisory Council on Employee Welfare and Pension Benefit Plans—outlines existing frameworks for addressing cyber security risks and, in the Appendix, provides a concise set of essential considerations for formulating a cyber security risk management strategy.¹⁶

Potential risks

For retirement plan fiduciaries, cyber security risks can be potentially significant. At the heart of these potential risks is the unanswered question: Is personal information of participants/beneficiaries a plan asset?¹⁶ If the answer to that question is yes, then cyber security would fall within the scope of the fiduciary duty to preserve plan assets for the sole benefit of participants and beneficiaries. Further compounding the risk for plan sponsors is the fact that “[b]enefit plans often maintain and share sensitive employee data and asset information across multiple unrelated entities as a part of the benefit plan administration process.”¹⁶

Despite these risks, no comprehensive regulatory scheme is currently in place for addressing them. Instead, existing regulation comes in a patchwork



UBS ERISA Extra

of federal and state laws, regulations and other guidance. For example, the DOL explicitly imposes specific duties to protect personal information in certain circumstances,¹⁶ while other federal statutes (e.g., the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, and the Fair and Accurate Credit Transactions Act) protect private information, although not specifically in the retirement plan context. Likewise, existing protections for personally identifiable information (PII)¹⁶ and protected health information (PHI)¹⁶—set forth in HIPAA and elsewhere—generally apply to health plans rather than retirement plans.

Further complicating the issue is that many states have laws that provide protections for PII and PHI. However, it remains unclear to what extent these may be preempted by ERISA, as the authors of the Report recognize.¹⁶

Establishing a strategy

To help sponsors and other fiduciaries create a strategy, the Report outlines, in the Appendix, a concise summary of suggested steps for plans to take when considering a cyber security risk management strategy. These include the following:

Understand the plan's data. Ask the following questions: What data that is currently collected needs to be protected? How is the data classified? Where is the data stored? Who is accessing the data? How is data accessed? Is access properly controlled? What data is needed? What data needs to be retained? What are the threats?

Choose a framework for assessing cyber security risks. The Report references several existing cyber security frameworks that could provide the foundation for a plan's cyber security strategy.

- NIST. In 2014, the National Institute of Standards and Technology (NIST) and various private sector industry stakeholders created the Cybersecurity Framework to set voluntary standards and best practices for managing cyber security risk to critical infrastructure services that are vital to the United States. Based on the NIST framework, some components of a cyber security strategy include describing a process to identify risks, developing a program to protect data that could be at risk, stating how breaches will be detected, showing how your plan will respond and detailing how your plan will recover.
- SAFETY Act. Enforced by the Department of Homeland Security, this law provides risk management protections to firms that develop, sell or deploy anti-terrorism technologies.
- SPARK (Society of Professional Asset-Managers and Recordkeepers). This past September, SPARK announced that it had developed new "Industry Best Practices for how recordkeepers should report the cyber security capabilities to plan sponsors and plan consultants."¹⁶ According to SPARK, "These standards are not intended to provide a recommended level of cyber protection, or guarantee against a data breach or loss...[T]he intent...is to establish a base of communication between recordkeepers and the public through the use of independent third-party audits of cyber security control objectives. In this way vendors can properly

validate the robust nature of their cyber security systems and still provide assurances to clients and prospects."¹⁶

- HITRUST (Health Information Trust Alliance). HITRUST developed a Common Security Framework and Cyber Risk Management Framework to create a foundation for the HITRUST certification program for the healthcare industry.
- AICPA Initiatives and SOC Reporting. The AICPA has developed a cyber security risk management reporting framework to assist organizations in providing useful information about the effectiveness of their cyber security risk management programs. According to the AICPA, "the framework is a key component of the System and Organization Controls (SOC) for cyber security engagement, through which a CPA reports on an organization's enterprise-wide cyber security risk management program."¹⁶

Process considerations. Items to consider for the ongoing process include implementation, monitoring, testing, updating, reporting, training, hiring practices, controlling access, data retention, data destruction and third-party risk management.

Customizing a strategy. The chosen framework should be customized to fit each plan's particular needs and circumstances. Appropriate considerations include available resources, integration with the rest of the organization's administration, cost, cyber insurance, available certifications and how to keep up with new developments.



Striking the right balance. In light of their fiduciary obligations to hold plan assets for the exclusive purpose of providing benefits to participants/beneficiaries and defraying reasonable plan administration expenses, plans

“will need to determine the balance of preventive measures relative to the probability of the threat, the loss exposure, and the cost of protective action.”¹⁶

Compliance with state law. Plans will need to know the requirements of applicable state law, including proper notification and reporting of cyber breaches. Larger plans will frequently need to consider the laws of more than one state.

Additional information

Finally, the Appendix includes a list of recommended questions to be used when evaluating service providers, a section on insurance considerations, a list of common cyber security terminology and a list of useful links.

¹ IRS. “401(k) Plan Fix-It Guide.” IRS.gov. August 27, 2017. Web. Date of Access 11/1/2017. [irs.gov/retirement-plans/401k-plan-fix-it-guide](https://www.irs.gov/retirement-plans/401k-plan-fix-it-guide).

² Internal Revenue Code Sec. 414(q)(1); IRS Notice 2017-64.

³ Treas. Reg. Secs. 1.401(m)-2(b)(4)(i) and 1.401(k)-2(b)(5)(i).

⁴ Treas. Reg. Secs. 1.401(m)-2(b)(4)(ii) and 1.401(k)-2(b)(5)(ii).

⁵ IRS Notice 2017-64.

⁶ Labor Reg. Sec. 2510.3-102(b)(1).

⁷ Labor Reg. Sec. 2510.3-102(a)(2).

⁸ ERISA Sec. 408(b)(1); Labor Reg. Sec. 2550.408b-1(a)(1).

⁹ IRC Sec. 72(p)(2); Treas. Reg. Sec. 1.72(p)-1, Q&A 3.

¹⁰ Treas. Reg. Sec. 1.401(k)-1(d)(3)(i).

¹¹ IRS Memorandum, “Substantiation Guidelines for Safe-Harbor Hardship Distributions from Section 401(k) Plans,” February 23, 2017.

¹² IRC Sec. 416(g)(1)(A)(ii).

¹³ IRC Sec. 416(i)(1); IRS Notice 2017-64.

¹⁴ Labor Reg. Sec. 2520.104a-5(a)(2).

¹⁵ IRC Sec. 6652(e).

¹⁶ ERISA Sec. 502(c)(2); Labor Reg. Sec. 2575.2(b).

This material is provided for educational purposes and provides a general description of the rules applicable under ERISA and the Internal Revenue Code. You are encouraged to consult your legal advisors about your plan and also any potential ERISA, tax and related consequences of any investments made under such plan. This material is not, nor is it intended to constitute, legal, tax or accounting advice. Please consult with a qualified professional for legal or tax advice. UBS Financial Services Inc. will not be responsible for your reliance on these materials.

This publication is provided for informational purposes only, contains a brief summary of select topics and certain recent legislative and regulatory developments, and is not intended as a complete summary of the topics discussed or considerations necessary for making effective decisions. Please note that it is important that you evaluate this material and exercise independent judgment when making investment decisions. This information, including any description of specific investment services or products, is marketing material and is solely for the purposes of discussion and for your independent consideration. It should not be viewed as a suggestion or recommendation that you take a particular course of action or as the advice of an impartial fiduciary.

This publication is not intended as an offer, or a solicitation of an offer, to buy or sell any investment or other specific product. You should seek appropriate professional advice regarding the matters discussed in this publication in light of your specific situation. The information contained in this publication is based on information provided from third-party sources, but its accuracy cannot be guaranteed.

UBS Financial Services Inc., its affiliates and its employees are not in the business of providing tax or legal advice. Clients should seek advice based on their particular circumstances from an independent tax advisor.

Important information about advisory and brokerage services

As a firm providing wealth management services to clients, UBS is registered with the U.S. Securities and Exchange Commission (SEC) as an investment adviser and a broker-dealer, offering both investment advisory and brokerage services. Advisory services and brokerage services are separate and distinct, differ in material ways and are governed by different laws and separate contracts. It is important that you carefully read the agreements and disclosures UBS provides to you about the products or services offered. For more information, please visit our website at ubs.com/workingwithus.

UBS Institutional Consulting Services and Retirement Plan Consulting Services are investment advisory programs. Details regarding the programs, including fees, services, features and suitability, are provided in the ADV Disclosure.

The UBS Select for Corporate Plans platform includes approximately 35 third-party (non-UBS) providers, many of whom offer programs that bundle services such as investments, participant recordkeeping, trust services and plan administration. When a client chooses one of these programs, the plan's assets will not be custodied at UBS nor will UBS execute transactions for the account.

Copyright 2016 by DST. Used with permission from DST Systems Inc. and provided by UBS Financial Services Inc. for use by its Financial Advisors.

DST Systems Inc. and its employees are not affiliated with UBS Financial Services Inc. or its affiliates.

© UBS 2018. All rights reserved. The key symbol and UBS are among the registered and unregistered trademarks of UBS. UBS Financial Services Inc. is a subsidiary of UBS AG. Member FINRA/SIPC.

UBS Financial Services Inc.
ubs.com/fs
2018-31449

