White Paper

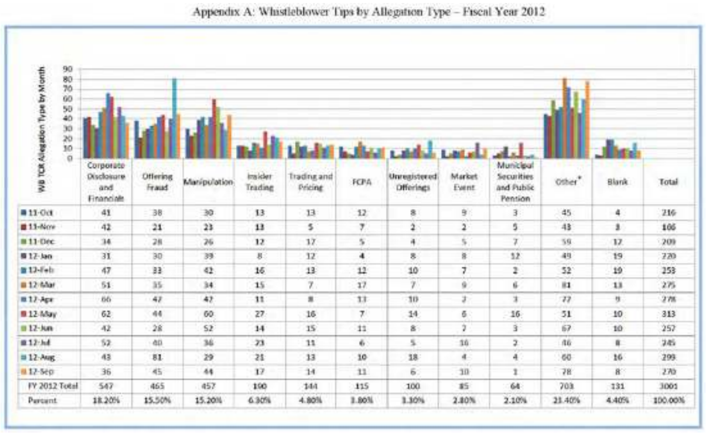
Keeping problems private to reduce risk

Encouraging internal reporting in the Dodd-Frank era

Few provisions of the Dodd-Frank Financial Regulatory Reform Act of 2010 have received as much attention—and caused as much consternation—as those authorizing monetary rewards for corporate whistleblowing. Under Dodd-Frank, company employees who go directly to the SEC with concerns about fraud or other illegal activities can receive a portion of fines, sanctions, and settlements ultimately recovered—as much as 30% of recoveries over $1 million. The first payment under this program was awarded last year on August 21, 2012 to a whistleblower who received nearly $50,000.

Ironically, the largest individual federal award in US history was paid to a whistleblower that went to prison himself for involvement in the very offense he reported. Bradley Birkenfeld, the former UBS AG (UBSN) banker who told the IRS how his former employer helped thousands of Americans evade taxes, secured a whistle-blower award of $104 million.[1]

According to the US Securities and Exchange Commission Annual Report on the Dodd-Frank Whistleblower Program, some 3,001 whistleblower reports were received in 2012.[2] Reports were submitted from all 50 states, as well as from 49 countries outside the US.


Appendix A: Whistleblower Tips by Allegation Type – Fiscal Year 2012

	Corporate Disclosure and Financials	Offering Fraud	Manipulation	Insider Trading	Trading and Pricing	FCPA	Unregistered Offerings	Market Event	Municipal Securities and Public Pension	Other*	Blank	Total
■ 11-Oct	41	38	30	13	13	12	8	9	3	45	4	216
■ 11-Nov	42	21	23	13	5	7	2	2	5	43	3	166
■ 11-Dec	34	28	26	12	17	5	4	5	7	59	12	209
■ 12-Jan	31	30	39	8	12	4	8	8	12	49	19	220
■ 12-Feb	47	33	42	16	13	12	10	7	2	52	19	253
■ 12-Mar	51	35	34	15	7	17	7	9	6	81	13	275
■ 12-Apr	66	42	42	11	8	13	10	2	3	77	9	278
■ 12-May	62	44	60	27	16	7	14	6	16	51	10	313
■ 12-Jun	42	28	52	14	15	11	8	7	3	67	10	257
■ 12-Jul	52	40	36	23	11	6	5	16	2	46	8	245
■ 12-Aug	43	81	29	21	13	10	18	4	4	60	16	299
■ 12-Sep	36	45	44	17	14	11	6	10	1	78	8	270
FY 2012 Total	547	465	457	190	144	115	100	85	64	703	131	3001
Percent	18.20%	15.50%	15.20%	6.30%	4.80%	3.80%	3.30%	2.80%	2.10%	23.40%	4.40%	100.00%

Figure-1: A chart of whistleblower tips based on SEC information illustrates the increasing rate of reports to outside authorities.

Table of contents

[1] http://www.bloomberg.com/news/2012-09-11/ubs-whistle-blower-birkenfeld-secures-irs-award-lawyers-say.html

[2] U.S. Securities and Exchange Commission, Annual Report on the Dodd-Frank Whistleblower Program Fiscal Year 2012; Staff of the U.S. Securities and Exchange Commission. November 2012; p 6.

Corporate compliance and risk managers have real reason for concern. After spending years building viable internal controls and reporting mechanisms in response to Sarbanes-Oxley, companies now face the possibility that their efforts could be derailed by strong financial incentives for employees to forego internal reporting mechanisms in favor of approaching authorities directly.

So what's a business to do? Some, fighting fire with fire, now offer their own generous financial rewards for internal reporting. Others prefer a more systematic approach, based on the idea that building a corporate culture of compliance has organizational benefits above and beyond regulatory concerns. Those companies focus on building robust monitoring and reporting into core business processes, actively identifying problems and addressing exceptions across all functions within the organization.

Always on risk monitoring

Continuous controls monitoring (CCM) can be instrumental in instilling a culture of compliance, by enlisting employees across functions—including finance, IT, HR, and audit—to identify, monitor, and address risks in their business. By building a strong internal system of controls, automatically monitoring those controls on a continuous basis, and providing for remediation, companies can empower their employees to address operational risks daily—and to mitigate risk before outside authorities become involved.

Automated inspection of 100% of transactions means your compliance program is always on; it's not a once-a-year retrospective. Using software to detect and surface key risk indicators on your behalf is also much more effective than the traditional needle-in-a-haystack approach to auditing.

A complete CCM solution can provide companies with a core set of unique controls that address risk and monitor for exceptions throughout the organization, which brings obvious risk-management benefits. But there are regulatory benefits as well, since a fully deployed CCM solution also demonstrates both a company's commitment to transparency and the fact that it has a well-defined internal process for addressing concerns. The latter becomes especially important if reporting becomes external and authorities seek evidence of good-faith efforts to prevent illegal activity.

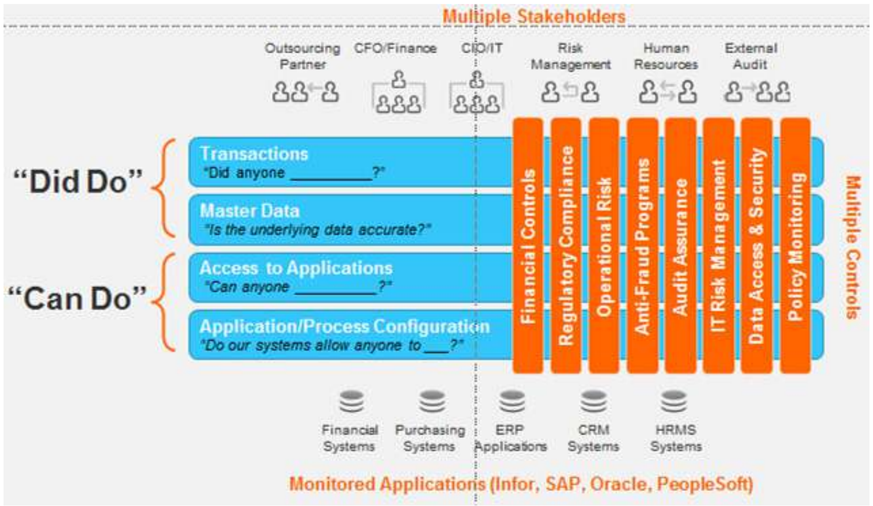


Figure-2: Organizations with "always on" risk monitoring can monitor what employees can do as well as what they did do in your business. In that way CCM systems provide continuous compliance.

Infor is in no way committing to the development or delivery of any specified enhancement, upgrade, product or functionality. See "disclaimer" paragraph contained herein.

Continuous compliance

Consider a hypothetical US-based company with domestic and overseas offices, and business dealings with foreign vendors and governments. Using CCM, the company can monitor operations across the organization—from access and configuration controls to master data and transaction controls—to identify which activities and individuals are likely to become problematic and flag them for additional attention.

With CCM, indicators of theft or fraud are immediately flagged for process owners, who can investigate rules specifically guarding against high-risk activities such as round-tripping, unauthorized shipments, inappropriate credits or discounts, and transaction splits. The company can also monitor anomalies in financial statements—so irregularities ranging from capitalization mistakes to intercompany transfers and manual postings to journals get the extra attention that they deserve. Transactions that don't check out can be remediated within the very same system.

To help ensure compliance with the Foreign Corrupt Practices Act, CCM enables monitoring of activities that tend to indicate fraud or bribery. Employees can automatically crosscheck vendor and customer master records against records of known suspicious individuals, such as those on the Specially Designated Nationals List (SDN) maintained by the US Treasury Department's Office of Foreign Assets Control (OFAC). In the same way, CCM allows employees to monitor for situations such as a sudden increase in consulting fees in a country where business is not normally conducted, or for matches of sales orders' line items to lists of sanctioned goods.

In our hypothetical company, employees can thoroughly investigate suspicious transactions as they happen, rather than months later. And they can take steps to address any issues that arise before problems snowball into the kinds of million-dollar losses that make the SEC's new provisions so potentially lucrative. Investigative tools enable employees to compile the facts relevant to a suspicious business situation, then escalate issues in accordance with a pre-determined workflow using built-in collaboration features. Dashboards and reports provide transparency and a complete audit trail of any actions taken.

Control freaks are good for business

CCM solutions help companies make good on the promise of internal reporting policies and mechanisms deemed so crucial just a few years ago. Fully deployed, a complete CCM solution provides increased visibility and control of transactions across the enterprise—along with a communications process and accountability for the inevitable exceptions and policy violations that arise.

Nothing can guarantee that employees won't be tempted by the Dodd-Frank bounties for whistleblowers, but CCM can help companies account for risk on a daily basis and foster a culture of compliance. And robust internal reporting programs that identify issues before they build to windfall-level recoveries are an important tool in keeping issues within the corporate family.

Infor is in no way committing to the development or delivery of any specified enhancement, upgrade, product or functionality. See "disclaimer" paragraph contained herein.

Traditional controls testing approach	Continuous controls monitoring (CCM) approach
Infrequent reviews: Reviews and audits of controls are conducted periodically, many controls are never tested.	Continuous and automated: Controls testing is automated and continuous.
Sample-based approach: When reviews and audits occur, they examine only a small portion of all transactions.	Examine 100% of users and transactions: CCM examines all of the relevant transactions and users for a control.
No business context: When issues or exceptions are identified additional research is required to prioritize and understand.	A 360-degree view of exceptions: Understand the risk and dollar impact of each transaction, drill around to see related information.
Ad-hoc remediation: Remediation process is ad hoc making it difficult to track status of errors, exceptions, and violations.	Closed-loop remediation: Prioritize and route exceptions to the proper business owner, automatically track status of follow-up.

Figure-3: Continuous controls monitoring (CCM) systems help organizations increase the depth, breadth, and frequency of their controls monitoring

infor™

641 Avenue of the Americas
New York, NY 10011
800-260-2640
infor.com

About Infor

Infor is the world's third-largest supplier of enterprise applications and services, helping more than 70,000 large and mid-size companies improve operations and drive growth across numerous industry sectors. To learn more about Infor, please visit www.infor.com.

Disclaimer

This document reflects the direction Infor may take with regard to the specific product(s) described in this document, all of which is subject to change by Infor in its sole discretion, with or without notice to you. This document is not a commitment to you in any way and you should not rely on this document or any of its content in making any decision. Infor is not committing to develop or deliver any specified enhancement, upgrade, product or functionality, even if such is described in this document.