

WASHOE COUNTY

"Dedicated To Excellence in Public Service"

www.washoecounty.us



COMMITTEE MEMBERS

Commissioner Kitty Jung
Alt. Commissioner Jeanne Herman
Barbara Kinnison
Denise Jacobsen
Randy Brown
Matthew Buehler
Interim County Manager Dave Solaro

INTERNAL AUDITOR

Samantha Pierce

AGENDA

WASHOE COUNTY AUDIT COMMITTEE

Caucus Room

1001 E. 9th St., #A205

Wednesday, January 8, 2020

2:00 p.m.

We are pleased to make reasonable accommodations for members of the public who are disabled and wish to attend the meetings. If you should require special arrangements for an Audit Committee meeting, please call the Internal Auditor's Office at 399-8988, 24-hours prior to the meeting.

Public Comment will be available and is limited to three minutes per person and for all matters, whether listed on the agenda or not. Additionally, public comment of three minutes per person will be heard during individually numbered items on the agenda. Persons are invited to submit comments in writing on agenda items and/or attend and make comment on that item at the Audit Committee meeting. Persons may not allocate unused time to other speakers. Supporting documentation for the items on the agenda provided to Audit Committee members is available to members of the public at the County Manager's Office (1001 E. 9th Street, Bldg. A, 2nd Floor, Reno, Nevada), Samantha Pierce, Internal Auditor (775) 399-8988.

Pursuant to NRS 241.020, the Agenda for the Audit Committee has been posted at the following locations: Washoe County Administration Building (1001 E. 9th St. Bldg. A), Washoe County Courthouse—Second Judicial District Court (75 Court St.), Washoe County Central-Downtown Library (301 South Center St.), Sparks Justice Court (1675 East Prater Way), Incline Justice Court (865 Tahoe Blvd.), www.washoecounty.us/mgrsoff/internal_audit.html, and <https://notice.nv.gov>.

2:00 p.m.

1. Roll Call
2. Public Comment (comment heard under this item will be limited to three minutes per person and may pertain to matters both on and off the Audit Committee agenda)

3. Presentation of the FY19 Comprehensive Annual Financial Report (CAFR) and audit results for the year ending June 30, 2019. Representatives from Eide Bailly, LLP
4. Approval of minutes for September 5, 2019 meeting (for possible action)
5. Audit Report Update –Samantha Pierce, Internal Auditor
 - Completed:
 - Cash Control (Phase 1)
 - In Progress:
 - Cash Controls (Phase 2 & 3)
 - Human Services Agency
 - Follow-Up:
 - Three Year Review of Completed Audits
 - Other:
 - Risk Matrix & Risk Report
6. Calendaring of the fiscal year Audit Committee meetings:
 - March 11, 2020 @ 2:00 PM
 - June 4, 2020 @ 2:00 PM
7. Audit Committee Member Comments – limited to announcements or issues proposed for future agendas and/or workshops
8. Public Comment (comment heard under this item will be limited to three minutes per person and may pertain to matters both on and off the Audit Committee agenda)



November 27, 2019

To the Audit Committee
Washoe County, Nevada
Reno, Nevada

We have audited the financial statements of the governmental activities, the business-type activities, the discretely presented component unit, each major fund, and the aggregate remaining fund information of Washoe County (the County) as of and for the year ended June 30, 2019 and have issued our report thereon dated November 27, 2019. Professional standards require that we advise you of the following matters relating to our audit.

Our Responsibility in Relation to the Financial Statement Audit under Generally Accepted Auditing Standards and *Government Auditing Standards*

As communicated in our engagement letter dated March 12, 2019, our responsibility, as described by professional standards, is to form and express an opinion about whether the financial statements that have been prepared by management with your oversight are presented fairly, in all material respects, in accordance with accounting principles generally accepted in the United States of America. Our audit of the financial statements does not relieve you or management of its respective responsibilities.

Our responsibility, as prescribed by professional standards, is to plan and perform our audit to obtain reasonable, rather than absolute, assurance about whether the financial statements are free of material misstatement. An audit of financial statements includes consideration of internal control over financial reporting as a basis for designing audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control over financial reporting. Accordingly, as part of our audit, we considered the internal control of the County solely for the purpose of determining our audit procedures and not to provide any assurance concerning such internal control.

We are also responsible for communicating significant matters related to the audit that are, in our professional judgment, relevant to your responsibilities in overseeing the financial reporting process. However, we are not required to design procedures for the purpose of identifying other matters to communicate to you.

We have provided our comments regarding a material weakness during our audit in our Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards* dated November 27, 2019.

Planned Scope and Timing of the Audit

We conducted our audit consistent with the planned scope and timing we previously communicated to you.

Compliance with All Ethics Requirements Regarding Independence

The engagement team, others in our firm, as appropriate, our firm, and other firms utilized in the engagement, if applicable, have complied with all relevant ethical requirements regarding independence.

Qualitative Aspects of the Entity's Significant Accounting Practices*Significant Accounting Policies*

Management has the responsibility to select and use appropriate accounting policies. A summary of the significant accounting policies adopted by the County is included in Note 1 to the financial statements. There have been no initial selection of accounting policies and no changes in significant accounting policies or their application during 2019. No matters have come to our attention that would require us, under professional standards, to inform you about (1) the methods used to account for significant unusual transactions and (2) the effect of significant accounting policies in controversial or emerging areas for which there is a lack of authoritative guidance or consensus.

Significant Accounting Estimates

Accounting estimates are an integral part of the financial statements prepared by management and are based on management's current judgments. Those judgments are normally based on knowledge and experience about past and current events and assumptions about future events. Certain accounting estimates are particularly sensitive because of their significance to the financial statements and because of the possibility that future events affecting them may differ markedly from management's current judgments.

The most sensitive accounting estimates affecting the financial statements are:

Management's estimate of the other postemployment benefits liability is based on actuarial valuations. Actuarial valuations are based on the substantive plan and include the types of benefits in force at the valuation date and the pattern of sharing benefits between the County and the plan members. We evaluated the key factors and assumptions used to develop the postemployment benefits liability in determining that it is reasonable in relation to the financial statements taken as a whole.

Management's estimate of the pension liability is based on actuarial valuations. Actuarial valuations are based on the employee information submitted by the County to the Public Employees' Retirement System of the State of Nevada (PERS). We evaluated the key factors and assumptions used to develop the estimate of the pension liability in determining that it is reasonable in relation to the financial statements taken as a whole.

Management's estimate for pending claims – health benefits and worker's compensation is based upon third party analysis of claims trends, historical evidence, claim lag days, and current employee counts. We evaluated the key factors and assumptions used to develop the estimate of the claims IBNR in determining that it is reasonable in relation to the financial statements taken as a whole.

Financial Statement Disclosures

Certain financial statement disclosures involve significant judgment and are particularly sensitive because of their significance to financial statement users. The most sensitive disclosures affecting the County's financial statements relate to:

- Investment and investment-related activities (fair value measurement)
- Payroll other liabilities, and deferred inflows of resources (pensions and other postemployment benefits)
- Net position and fund balance (restrictions, commitments, and assignments)
- Accounting changes, correction of an error

Significant Difficulties Encountered during the Audit

We encountered no significant difficulties in dealing with management relating to the performance of the audit.

Uncorrected and Corrected Misstatements

For purposes of this communication, professional standards require us to accumulate all known and likely misstatements identified during the audit, other than those that we believe are trivial, and communicate them to the appropriate level of management. Further, professional standards require us to also communicate the effect of uncorrected misstatements related to prior periods on the relevant classes of transactions, account balances or disclosures, and the financial statements as a whole.

The following misstatements were identified as a result of our audit procedures and were brought to the attention of, and corrected by, management:

General Fund:

Due from Other Governments/ Deferred Inflow – Unavailable Grant Revenues	\$2,400,000
---	-------------

Unearned Revenue/ Fund Balance	\$3,627,832
-----------------------------------	-------------

Unearned Revenue/ Revenue	\$54,736
------------------------------	----------

Child Protective Services Fund:

Reimbursement Revenue/ Transfers In	\$6,595,229
--	-------------

Indigent Tax Levy Fund:

Transfers Out/ Payments to Others	\$6,595,229
--------------------------------------	-------------

Governmental Activities:

Due from Other Governments/ Program Revenues	\$2,400,000
---	-------------

Reimbursement Revenue/ Welfare Expenses	\$6,595,229
Unearned Revenue/ Net Position	\$3,627,832
Unearned Revenue/ Revenue	\$54,736
Agency Funds:	
Due to Others/ Financial Assurances	\$2,366,655
Equipment Services Fund:	
Capital Contributions/ Transfers In	\$50,515

The following summarizes uncorrected financial statement misstatements whose effects in the current and prior periods, as determined by management, are immaterial, both individually and in the aggregate, to the financial statements taken as a whole.

Current Year Entries:	
General Fund:	
Overstatement of estimated FEMA receivable	\$ 379,741
Other Restricted Fund:	
Overstatement of grant receivables	\$ 41,038
Governmental Activities:	
Overstatement of estimated FEMA receivable	\$ 379,741
Overstatement of grant receivables	\$ 41,038
Building and Safety Fund:	
Overstatement of OPEB Liability due to PEBP	\$ 31,334
Utility Fund:	
Overstatement of CY Revenue for PY amounts	\$ 665,391
Business-Type Activities:	
Overstatement of OPEB Liability due to PEBP	\$ 31,334
Overstatement of CY Revenue for PY amounts	\$ 665,391
Discretely Presented Component Unit (TMFPD):	
Overstatement of PERS payable	\$ 39,511
Overstatement of Due to Other Governments	\$ 8,548
Prior Year Reversing Entries:	
Utilities Fund/Business-Type Activities:	
Understatement of Accounts Payable	\$ 385,927

The effect of these uncorrected misstatements, including the effect of the reversal of prior year uncorrected misstatements, as of and for the year ended June 30, 2019 are shown below:

General Fund:

There was no effect on change in fund balance or fund balance.

Other Restricted Fund:

There was no effect on change in fund balance or fund balance.

Governmental Activities:

An overstatement of the change in net position and an overstatement in net position of \$420,779.

Building and Safety Fund:

An understatement of change in net position and an understatement of net position of \$31,334.

Utility Fund:

An overstatement of change in net position of \$279,464 and no effect on ending net position.

Business-Type Activities:

An overstatement of change in net position of \$248,130 and an understatement of net position of \$31,334.

Discretely Presented Component Unit (TMFPD):

An understatement of change in net position of \$39,511 and an understatement in net position of \$48,059.

Disagreements with Management

For purposes of this letter, professional standards define a disagreement with management as a matter, whether or not resolved to our satisfaction, concerning a financial accounting, reporting, or auditing matter, which could be significant to the County's financial statements or the auditor's report. No such disagreements arose during the course of the audit.

Representations Requested from Management

We have requested certain written representations from management that are included in the management representation letter dated November 27, 2019.

Management's Consultations with Other Accountants

In some cases, management may decide to consult with other accountants about auditing and accounting matters. Management informed us that, and to our knowledge, there were no consultations with other accountants regarding auditing and accounting matters.

Other Significant Matters, Findings, or Issues

In the normal course of our professional association with the County, we generally discuss a variety of matters, including the application of accounting principles and auditing standards, business conditions affecting the entity, and business plans and strategies that may affect the risks of material misstatement. None of the matters discussed resulted in a condition to our retention as the County's auditors.

Modifications of the Auditor's Report

We have made the following modification to our auditor's report. Emphasis of matter paragraphs were included to address a correction of errors.

Other Information in Documents Containing Audited Financial Statements

Pursuant to professional standards, our responsibility as auditors for other information in documents containing the County's audited financial statements does not extend beyond the financial information identified in the audit report, and we are not required to perform any procedures to corroborate such other information.

However, in accordance with such standards, we will review the information inputted into the data collection form and will consider whether such information, or the manner of its presentation, is materially consistent with the financial statements.

Our responsibility also includes communicating to you any information which we believe is a material misstatement of fact. Nothing came to our attention that caused us to believe that such information, or its manner of presentation, is materially inconsistent with the information, or manner of its presentation, appearing in the financial statements.

This report is intended solely for the information and use of the Board of County Commissioners, the Audit Committee, and management of Washoe County and is not intended to be and should not be used by anyone other than these specified parties.

A handwritten signature in black ink that reads "Eide Bailly LLP". The signature is written in a cursive, flowing style.

Reno, Nevada

Audit Committee Meeting
Washoe County, Nevada
Thursday, September 5, 2019 at 2:00 PM

Voting Members: Commissioner Jeanne Herman, Randy Brown, and Matthew Buehler

Non-Voting Member:

Absent: Commissioner Kitty Jung, Barbara Kinnison, Denise Jacobsen, Interim County Manager Dave Solaro

Other Attendees: Samantha Pierce (Internal Audit), Cathy Hill (Comptroller)

Agenda Item 1 - Roll Call

The meeting was called to order at 2:00 PM and Ms. Pierce performed the roll call – those listed above were present.

Agenda Item 2 - Public Comment

No public comment.

Agenda Item 3 – Update on Items Presented to the Board of County Commissioners

Both the three-year schedule and the annual report were approved by the Board on July 9, 2019.

Agenda Item 4 - Approval of minutes for June 6, 2019 meeting

Randy Brown moved to approve the minutes. Matthew Buehler seconded the motion, which carried unanimously.

Agenda Item 5 – Audit Update

Ms. Pierce updated the committee on the audits in progress which were the county-wide cash control audit and the process audit of the Human Services Agency. Ms. Pierce was hoping to have the cash control audit presented at this meeting; however, it has become much larger than originally expected and the Human Services Agency audit was started with much of the field work completed over the last month. Mr. Buehler asked if the audit had to be presented at a meeting or if it could be provided once it was completed. Ms. Pierce stated the audit must be presented at a meeting due to the open meeting law. Ms. Hill asked if there were any material items found so far and Ms. Pierce stated there was nothing material at this time to bring forward. Ms. Pierce also gave some background information that the prior audit completed in 2017 was not a county-wide audit as she had thought and that only four specific departments had been included. Ms. Pierce also updated the committee on the shadowing and interviews that had taken place for the Human Services Agency audit, as well as, the training that has been completed. Mr. Brown asked if this was the largest agency in Washoe County and Ms. Pierce stated the Sheriff's

Audit Committee Meeting
Washoe County, Nevada
Thursday, September 5, 2019 at 2:00 PM

Office was the largest with this one being one of the top three. Mr. Buehler asked if there was an opportunity for the audit committee members to shadow or attend the training and Ms. Pierce stated that all the information for this audit was confidential as it related to minors and court cases.

Ms. Pierce also talked about follow-up on the previous auditors' recommendations and the list was provided in the documents for this meeting. The list was reviewed and Ms. Pierce stated the cash control audit from 2017 would have the follow-up included in the current audit she is working and that the senior services audit would be included in the current Humans Services Agency audit as they had merged together since the prior audit was completed. The travel expense audit recommendations would have their follow-up on the audit that is scheduled as it is currently on the three-year schedule. The only audits listed that do not have something scheduled for follow-up are the grants audit, inventory audit, district attorney's office and workers compensation audit. The committee liked the list of recommendations and asked that as the follow-up occurs that the list be updated and brought back to the committee with those updates. Mr. Buehler asked if the agency has not implemented a recommendation if the committee has any recourse. Ms. Pierce stated that she was unaware of any recourse but there is an annual report that goes to the Board and that lists any recommendations that have not been implemented.

Ms. Pierce informed the committee that she is also on a sub-committee for the strategic planning goal of continuous process improvement for the County. A pilot project has been selected within the Community Services Department for the permitting process.

This was a non-action item therefore no motion was given.

Agenda Item 6 - Calendaring of meetings

The following dates were tentatively scheduled for the audit committee quarterly meetings for the rest of the fiscal year. Note on the December 5th meeting because it may be moved depending on the timing of the presentation of the Comprehensive Annual Financial Report (CAFR) to the Board of County Commissioners because then it will be presented to this committee.

This was a non-action item therefore no motion was given.

December 5, 2019 @ 2:00 PM (*)

March 5, 2020 @ 2:00 PM

June 4, 2020 @ 2:00 PM

Agenda Item 7 - Audit Committee Member Comments

Suggestion from Ms. Hill to do a presentation on the difference between elected and appointed departments.

Audit Committee Meeting
Washoe County, Nevada
Thursday, September 5, 2019 at 2:00 PM

Agenda Item 10 - Public Comment

No public comment

Adjournment

At 2:25 PM the meeting was adjourned

A dark blue vertical bar runs down the left side of the page. A blue arrow points to the right from the bar, containing the date.

12/3/2019

Cash Control Audit

Washoe County 2019

Several thin, curved, light blue lines sweep upwards from the bottom left corner of the page.

Samantha Pierce
INTERNAL AUDITOR

Executive Summary

The audit committee approved the audit over county wide cash controls at their September 6, 2018 meeting. All Agencies, Departments, Divisions and Offices were contacted in March of 2019 to provide information and documentation to the Internal Audit Division for review. The Justice Courts of Incline, Reno, Sparks and Wadsworth along with the Second Judicial Court were excluded from this audit as their cash control procedures were audited in the Minimum Accounts Standards Audit performed in fiscal year 2019. All Agencies, Departments, Divisions and Offices responded to the request for information and provided any documentation they had on their cash related transactions. Discussed in this report are brief descriptions of each Agency, Department, Division or Office, observations if site visits were performed, descriptions of procedures included in written documents and if there were recommendations from the Internal Audit Division. This comprehensive audit of all County departments was split into three phases to speed up the process of getting the information to the Board of County Commissioners and the Audit Committee. This report covers phase one.

Internal Audit Purpose

Conducting this audit reduces the risk to Washoe County by establishing that all Agencies, Departments, Offices and Divisions have the appropriate procedures in place for handling cash, checks and credit card transactions to either prevent the theft of funds received or detect that a theft has occurred and take the proper steps to investigate. Internal Audit functions as a third line of defense against risk in an organization and is uniquely positioned to provide an advisory role on the coordination of assurance, effective ways of improving existing processes and assisting management in implementing recommendations.

Background

Varying degrees of cash control audits have been performed by the internal audit division during 2011 and 2013, with the most current audit completed for 2017. This audit included a follow-up to the findings and recommendations of the previous audit for cash controls of 2017. The previous audit reviewed the following departments and was not completed county-wide:

- Social Services*
- Senior Services*
- Alternative Sentencing
- Health District
- Sheriff's Office
- Community Services Department**

*Prior to the merge of Social Services, Adult Services and Senior Services into the Agency of Human Services.

**Only Davis Creek Campground was included in the audit.

Washoe County Cash Operations

Within Washoe County there are twenty (20) departments who all have either a change fund or petty cash and in some instances both. There is approximately thirty thousand dollars (\$30,000) issued to these

departments for change funds and almost another thirty thousand dollars (\$30,000) issued to them in petty cash. The difference between a change fund and petty cash fund is that petty cash is used to purchase expenses for the department while the change fund is used in the collection of fines or fees due to the County when change is necessary. Both change funds and petty cash are surprised counted at least once a year by the Treasurer's Office with some assistance by the Internal Audit Division.

It is the policy of the County to require daily deposits with only a couple of exceptions. There are approximately fifty (50) deposit books issued for the departments to be able to deposit directly into the County's main bank account. While many of the departments do deposit directly to the main Washoe County bank account there are approximately thirty-five (35) other bank accounts which the departments have opened and maintain. All outside bank accounts must be reconciled monthly and a copy of that reconciliation is provided to the Treasurer's Office for review.

Tables have been included in Appendix A, detailing the change funds, petty cash and depositor information as well as bank accounts without the identifying information.

Audit Procedure

The following questions were presented to the Departments, Divisions and Offices:

- *What program/software they utilize to record payments*
- *If they maintain a bank account outside the Washoe County main account*
- *If they had change funds (cash drawers) and if so how many and the starting balance*
- *If they had a petty cash fund and how much they were authorized*
- *If the Treasurer Office had performed the annual surprise cash count*
- *The titles and names of the people who performed bank reconciliations, deposit preparation, deposit transportation, voiding payments and access to cash were asked to be provided*

The following documents were asked to be provided if available and applicable:

- *Two most recent bank reconciliations*
- *Two most recent petty cash reconciliations*
- *Treasurer's Office most recent audit*
- *Written procedures regarding the handling of cash to include*
 - *Receipting process and counterfeit process*
 - *Opening/closing process*
 - *Deposit preparation & transportation to bank*
 - *Reconciliation process*
 - *Petty cash and change fund process*
 - *Safeguarding the funds process*
 - *Insufficient funds process*
 - *Recording and voiding payments process*
 - *Credit card security process*
 - *Cash payments over 10K*

After reviewing the answers and documents provided, recommendations were sent to the departments and examples of draft a procedures, sign off sheets, balancing sheets or miscellaneous logs were provided to the departments who had recommendations related to those items, while adjustments to existing procedures were provided to departments who had procedures that needed updating.

Cash Control Audit 2019

Table of Contents

<i>Alternate Public Defender's Office</i>	<i>Included</i>	<i>Page 4</i>
<i>Alternative Sentencing</i>	<i>Included</i>	<i>Page 6</i>
<i>Animal Services</i>	<i>Included</i>	<i>Page 11</i>
<i>Assessor's Office</i>	<i>Included</i>	<i>Page 15</i>
<i>Clerk's Office</i>	<i>Included</i>	<i>Page 17</i>
<i>Juvenile Services</i>	<i>Included</i>	<i>Page 20</i>
<i>Manager's Office</i>	<i>Included</i>	<i>Page 23</i>
<i>Appendix A</i>	<i>Included</i>	<i>Page 24</i>
<i>Comptroller's Office</i>	<i>Report 2</i>	
<i>Human Resources</i>	<i>Report 2</i>	
<i>Library System</i>	<i>Report 2</i>	
<i>Medical Examiner's Office</i>	<i>Report 2</i>	
<i>Public Administrator's Office</i>	<i>Report 2</i>	
<i>Public Defender's Office</i>	<i>Report 2</i>	
<i>Public Guardian's Office</i>	<i>Report 2</i>	
<i>Recorder's Office</i>	<i>Report 2</i>	
<i>Treasurer's Office</i>	<i>Report 2</i>	
<i>Voters, Registrar of</i>	<i>Report 2</i>	
<i>Community Services Department</i>	<i>Report 3</i>	
<i>District Attorney's Office</i>	<i>Report 3</i>	
<i>District Health</i>	<i>Report 3</i>	
<i>Human Services Agency</i>	<i>Report 3</i>	
<i>Sheriff's Office</i>	<i>Report 3</i>	
<i>Technology Services</i>	<i>Report 3</i>	

Alternate Public Defender's Office (128)

Overview of Cash:

Alternate Public Defender's Office had no change funds, nor did they have any outside bank accounts as they do not accept payments from the public or other agencies. They did have a petty cash account in the amount of five hundred dollars (\$500.00) which was surprise counted on 1/25/2019 by the Washoe County Treasurer's Office and found to be out of balance by twenty cents (\$0.20) and it was recommended by the Treasurer's Office to correct the unbalance at the next replenishment request by adjusting the request by difference.

Overview of their Purpose:

The Alternate Public Defender's office was created in March of 2007. Alternate Public Defenders are licensed attorneys whose services are used when conflicts of interest arise at the Washoe County Public Defender's Office. This occurs when the Public Defender's Office has previously represented a witness, victim, or co-defendant in a new case. The office handles adult criminal cases ranging from misdemeanor domestic batteries up to and including murder cases where the prosecutor is seeking the death penalty. Any person facing criminal charges or termination of his or her parental rights and cannot afford an attorney is potentially entitled to the services of the Washoe County Alternate Public Defender's office. The attorneys in the office also handle cases involving juveniles who are involved in the juvenile justice system. All the Specialty Courts in Washoe County both at District Court and Justice Court levels are covered by Alternate Public Defender lawyers.

Observation and Procedure Review:

Reviewed the most recent replenishment request from 12/17/2018 and it was determined all necessary documents were stored in the Washoe County Account System "SAP" and all petty cash receipts were valid transactions. When the information request from the internal auditor was returned the Alternate Public Defender's Office had handwritten procedures on the form to indicate what their process was for handling their petty cash fund.

Recommendations:

The following recommendations were proposed to the Alternate Public Defender's Office and have been implemented or are in the process of implementation:

- Written confirmation of the employee reading the procedure with a sign off sheet
- Procedures for petty cash should be written and include a version number and date. The written procedures should include, at minimum, the following:
 - Procedures should reference the following:
 - County Codes 15.107 through 15.210
 - The internal control document as prepared by the Comptroller's Department
 - The accounts payable procedure manual as prepared by the Comptroller's Department
 - How the separation of duties is achieved
 - There will be no loans to staff and no cashing of personal checks
 - A limit on the dollar value of a single purchase (Ex. \$50.00)
 - Where the funds are securely stored and who has access

- How often the funds are reconciled (Ex. Quarterly)
- Who performs the reconciliation and who verifies the reconciliation
- What documentation is expected

Cash Control Audit of 2017:

The Alternate Public Defender's Office was not included in the prior cash control audit in 2017 therefore, there were no recommendations for follow-up.

Management Comment:

The written procedures were created, and the sign off sheet was implemented.

Alternative Sentencing Office (154)

Overview of Cash:

Alternative Sentencing Office utilized the case management system Scotia to record both fees charged and payments received. The office had one change fund in the amount of \$350.00 which was surprise counted by the Washoe County Treasurer's Office on 01/25/2019 and found to be in balance. The office did not have outside bank accounts nor did they have a petty cash fund.

The income received was from fees associated to the participants in the program as an alternative to jail time. The fees were as follows per NRS 211A.130: formal probation supervision fee was forty dollars (\$40.00) per month and participants who were in the specialty courts through Reno Justice Court were charged and additional ten dollars (\$10.00) per month to which some could be waived if they performed community service at the rate of ten dollars (\$10.00) per hour. Both fees could be waived for indigent participants who complete a financial application and are approved. These participants could also perform community service as a rate of ten dollars per hour (\$10.00) which would be applied toward their fees.

Part of the program was also participation in the Sober 24 program and those fees were as follows:

Sober 24 Probationers: For probationers who are subject to substance abuse testing at Sober 24, the probation fees and the CCP fees are waived and they are only required pay testing fees.

- \$25 one-time administrative assessment fee
- \$4 per drug or alcohol test administered via urine collection
- \$ 1 per alcohol test using a breathalyzer
- \$15 per substance for lab confirmation for a challenged test (If the lab confirms the test is negative, the fees paid by the participant are credited toward participant's testing fee balance and the lab fee is not charged.)
- \$5 for replacement tubes for the PBT machine

Sober 24 Courtesy Donors: Testing participants who are not on probation pay the following fees.

- \$25 one-time administrative assessment fee (except RMC and District Court)
- \$13 per urinalysis
- \$6 per breath test (except RMC and DC who are charged \$1)
- \$25 for courtesy tests done for other outside jurisdictions
- \$ 5 for replacement tubes for the PBT machine
- \$15 per substance for lab confirmation for a challenged test (negative results confirmed are not credited to the participant)

Child Protective Services (CPS) Cases: CPS cases are paid for annually by contract. Participants do not pay testing fees.

- \$5 for replacement tubes for the PBT machine
- \$15 for each substance challenged by the participant (fee is not refunded if the results are returned negative)
 - If a test is challenged by the CPS worker, there is no fee charged

Also, of importance to note, this Office had and was continuing to undergo many large changes that will affect some of the recommendation of this audit. The auditor will continue to work with the Office after

completion to ensure all changes still fit within the controls expected around cash handling. The items listed below are the changes effecting this office:

1. The office was switching from one testing software to a different testing software.
2. The office was switching from one case management software to a different case management software.
3. The office was approved three (3) new positions, Office Assistant III, during the budget process for fiscal year 2020 and will start the recruitment process July 1, 2019.
4. The office was adding participants who are at the Reno Municipal Court (approximately five hundred) on July 1, 2019.
5. The office was adding participants who are through the Second Judicial District Court (approximately seven hundred) on July 1, 2019.
6. The office also changed their testing windows to be open from 5:00 AM to 8:00 PM on weekdays with weekends and holidays having two windows from 5:00 AM to 8:00 AM and 3:00 PM to 8:00 PM. There was a total of three shifts expected with this change.

Overview of their Purpose:

The mission of the Department of Alternative Sentencing is to increase safety in the community by reducing recidivism among criminal offenders, through a rehabilitative environment that includes accountability for offenses, opportunities for gaining and applying life skills, and sanctions for regressive behaviors. Their objectives include the following: reduce the revolving door syndrome in the criminal justice system, provide guidance and structure to those who are at risk of re-arrest and incarceration, coordinate cases in a sometimes very confusing multi-jurisdictional environment, provide information, resources and education to probationers sentenced to the program in an effort to modify their behavior, strive to assist probationers in making positive changes in their lives, create a safer environment for our community and future generations, reduce the burden of public services to those who are capable of providing for themselves through guidance and structure, and provide the best service possible to the community

Observation and Procedure Review:

A review of the written procedures was completed along with a walk-through of the facility in order to better understand the mission of the office. During the facility tour it was noted the office had a front lobby where clients entered and would be assisted by one of front office staff. During the time of the walk-through and observation there were two windows during the day where clients could come in for their testing, 5:00 AM to 8:00 AM and then again from 5:00 PM to 8:00 PM, and these were worked in two shifts of office staff. The 5:00 PM to 8:00 PM window was observed by the auditor and it was noted there were two staff who checked the clients in, collected the fees, performed the breathalyzer test (PBT), input the results from the test and prepared the paperwork for the collection of the urine sample. There were two staff members, one male and one female, who performed the collection of the urine samples and submitted them to the lab for testing. Also present during the testing window was one probation officer to handle any positive testing and the arrest of client. With the use of the new software for the testing and having a better lab testing the clients were not notified of the positive results until their next screening because the lab results did not come in until the next day. The reason for the delay was due to the extensive testing for more markers, such as prescription drug use.

The building for the office was a two-story office with the second story housing the office of the Alternative Sentencing Chief, Sergeant and Administrative Secretary Supervisor as well as the secondary safe for the cash collected. The entrance door to the second floor is secured by keycard and the office where the safe is located has a keyed door that is always locked. On first story were the lobby, testing bathrooms and offices for the probation officers as well as other Washoe County employees (such as case workers with Human Services Agency). Within the area of the lobby were chairs for the clients to wait as well as the “fish-bowl” area for the staff members. Just past the chairs in the lobby was an area where classes were offered for the clients.

During the review of the detailed written procedures it was determined Alternative Sentencing had included all of the following processes and procedures and during the field visit it was determined the staff were following the procedures as written:

- Titles of staff performing responsibilities to demonstrate separation of duties
- Acceptable forms of payments listed
- Prohibition of exchanging forms of payments for cash
- Checks inspected for correct dates, not accepting post-dated checks or checks in an amount greater than the fee and are restrictively endorsed immediately
- Receipts are prepared for every transaction. The client received the original (white) copy while the yellow carbon copy was included with the deposit information and the pink carbon copy remained in the book
- Proper procedures for voiding receipts
- A section for how to handle mailed payments
- Section detailing how a refund will be handled with proper separation of duties
- Proper start of shift and end of shift procedures for counting money
- Deposit preparation procedures
- Funds are safeguarded in a safe when not in use and during the testing window when fees are received the funds are safeguarded in a drawer till which is locked
- Deposit is transported securely through the use of an armored vehicle service in conjunction with Reno Justice Court
- Change fund was surprise counted and it was balanced every night while two employees performed the count
- Electronic confirmation of the employee reading the procedure

Recommendations:

During the field visit it was determined Alternative Sentencing did not have a sign in their lobby displaying the fee schedule, however the fees were presented on their website and explained during the clients first visit. It was recommended to add a sign with the basic fee schedule and include verbiage that a receipt will be provided with every transaction and what types of payments are accepted. Also, add verbiage on the GovPay fee which is added to the amount of the fee due and is collected by the credit card processor. An example of a notice was provided to the audit contact.

The following recommendations were proposed to the Alternative Sentencing Office and have been implemented or are in the process of implementation:

- Add a version number and effective date
- Procedures should reference the following:

- County Codes 15.107 through 15.210
- The internal control document as prepared by the Comptroller's Department
- The accounts payable procedure manual as prepared by the Comptroller's Department
- Checks are inspected to verify the numerical amount matches the written amount
- Add credit card information will never be written down or stored in any manner
- Although unlikely, verbiage should be added that if a cash payment over ten thousand dollars (\$10,000.00) is received the appropriate IRS procedures will be followed
- In the section for mailed payments received and include the following:
 - Who opens the mail and who processes the payments (this should be two separate people with the first person logging the payments received without access to receipting)
 - It will be opened and processed the same business day unless due to limitations of staffing in which case the payments should be locked in the safe and processes as soon as possible, recommended within three (3) business days
- Add procedure to identify counterfeit money, examples include counterfeit pens and detection lights or machines and what bill denominations are expected to be examined, for example paper bills over \$20.00
- Add no loans to employees nor using the funds as petty cash
- Add the amount that would trigger a removal of funds from a cashiers till prior to the close of business (recommended \$1,000.00)
- Add verbiage on which position prepares the deposit.
- Change fund should be counted at the end of a shift so the new person would start with only the change fund amount. This will allow for any discrepancies to be detected during the appropriate shift.
- If more than one person will be collecting money on a shift that fund should be spilt into the different tills so that money is not comingled together and would include adding another drawer to the "fish-bowl" area
- Use of an standard balancing sheet (example provided)
- Credit cards should be swiped by the client rather than the staff member because then the card does not need to be handled by the staff member (example of machine provided)
- Payments via check were rare therefore a non-sufficient funds charge was not recommended to be added to the fee of the client, rather it was recommended that client be required to pay the fee and fees going forward using another method of payment
- Add verbiage on accounts receivable collection process and level at which testing may not occur if outstanding balance is above

Cash Control Audit of 2017:

The Alternative Sentencing Office was included in the prior cash control audit in 2017 and the recommendations as well as the status of implementation are discussed below.

1. The first recommendation was regarding the implementation of procedures to perform periodic surprise cash counts.
 - a. This had been implemented and added to their procedures under Section L. Security and Control. It was also observed during the walk-through the sheet to which the surprise count is documented.
2. The second recommendation was regarding updating the written procedures and included the following items: clarifying the process for providing receipts for payments received in the mail, adding information about credit cards being swiped by the probationer and not

department staff, proper handling of void receipts, and updating the procedures to show payments are entered directly into Scotia.

- a. This had been implemented and added to their procedures under Section F Accepting and Receipting. Receipts for mailed payments will only be provided if requested by the client. Credit cards were still swiped by the staff rather than the client and this was added to the current recommendations. Voided receipts are clearly marked as void and they are reviewed by the Administrative Secretary Supervisor. Within the written procedures the software program used was clearly defined.

Management Comment:

Worked with the internal auditor to update all procedures and develop a standardized balancing sheet. The vendor who provides the credit card machine was contacted and new equipment will be provided. Request to split the change fund was submitted and a new till drawer was ordered to accommodate the additional worker during shifts.

Animal Services (205)

Overview of Cash:

Animal Services utilized the program Chameleon to record payments. The income received was from fees associated to the licensing fees, microchipping program, redemption fees for animals, quarantine fees and animal disposal. The fee breakdown is below and was posted not only online for customers but also in the lobby area of the facility.

Licensing were annual fees and were eight dollars (\$8.00) for spayed or neutered dogs, while they were twenty dollars (\$20.00) for unaltered dogs. For senior citizens of Washoe County the fee was set at eight dollars (\$8.00). If the tag was lost and needed to be replaced the fee was five dollars (\$5.00) and late renewal penalty was ten dollars (\$10.00). The service that was offered to microchip the animals was twelve dollars (\$12.00) for implant and free to register.

When animals were impounded the fees were incrementally increased each time the animals was picked up by the office. For dogs, the first impound was thirty-four dollars (\$34.00), second was fifty dollars (\$50.00) and for the third it was one hundred dollars (\$100.00) and on top of that impound fee was a daily boarding fee of nine dollars (\$9.00). For cats, the impound fee was twenty-eight dollars (\$28.00) and there was a daily boarding fee of four dollars (\$4.00). They also offered a cat carrier for five dollars (\$5.00). Animals Services was also tasked with livestock who were held at the facility and those impound fees were forty-five dollars (\$45.00) with a daily boarding fee of eleven dollars (\$11.00). If the livestock were hauled to the facility a twenty-five dollar (\$25.00) hauling fee was charged. For small animals there was no impound fee, but the daily boarding fee was four dollars (\$4.00).

The other two services for which the office charged for was quarantines for bite animals and animal disposal. The fees for quarantined animals was ten dollars (\$10.00) daily for boarding and fifty dollars (\$50.00) for the ADL specimen fees while the disposal fee was ten dollars (\$10.00).

The office had six (6) change funds totaling seven hundred dollars (\$700.00) which was surprise counted by the Washoe County Treasurer's Office on 01/25/2019 and found to be in balance. The office did not have outside bank accounts nor did they have a petty cash fund.

Overview of their Purpose:

The mission of Animal Services is to promote responsible care of animals through education, proactive outreach and regulation making Washoe County a safe community. They focus on the public health and safety services, through sheltering, field services, and regulation enforcement and proactive programs that enhance responsible pet ownership. There is an average of 13,000 impounded animals annually either brought in by citizens or picked up by field staff. Animal Services works very diligently to reunite lost pets with their owners and for fiscal year 2018, they boast a 40% over all return to owner rate! Last year 66% of stray dogs brought into the shelter were returned home. And 7% of the cats that were brought into our shelter were returned home. This is due in part to our pro-active philosophy and our engaged community who care deeply for their pets.

Observation and Procedure Review:

A review of the written procedures was completed along with a walk-through of the facility in order to better understand the mission of the office. During the facility tour it was noted the office had a front

lobby where customers entered and would be assisted by one of front office staff. There was a hallway connecting Animals Services to the Nevada Humane Society that was used by the public and volunteers. There was a separate entrance for the public to drop off found animals and another entrance for approved people to use at night when the facility was not staffed. The “night drop” was only accessible with a code therefore it was changed regularly so-as not to get unauthorized drops at night. The facility had public areas where people could go to see if their animal was there as well as a video screen that scrolled through all animals that were being held. The restricted employee area was a u-shape and had a loading dock area where employees could park their vehicles to unload the animals in a closed and secure area. There was an area where all animals were processed to verify they did not have any injuries or sickness that could spread to the rest of the population. Along one side of the restricted area were quarantined kennels for animals that might be sick, pregnant or for any reason needed to be separated from the general area. There was also area for veterinary procedures which was utilized as a teaching area in partnership with Truckee Meadows Community College Veterinary Program. Along the other side of the restricted area was where the aggressive dogs and any dogs that were quarantined for bites were held. From this side you could also access the dispatch area as well as the administrative area, a door then led you back out to the lobby. There was also a barn area located near the loading dock where farm animals could be held, such as horses and pigs.

During the review of the detailed written procedures it was determined Animal Services had included all of the following processes and procedures and during the field visit it was determined the staff were following the procedures as written:

- Effective date of the procedure
- Titles of staff performing responsibilities to demonstrate separation of duties
- Identifying counterfeit cash
- Personal checks will not be cashed
- Checks were inspected for date to include that post-dated checks are not allowed and will not be accepted for an amount higher than the fee
- Checks were endorsed immediately
- Daily deposits were made Monday through Friday with any payments received over the weekend at clinics included in the Monday deposit
- Funds were safeguarded and locked in cash till drawers during the day for those in use while all others were locked in the safe, with all funds locked in a safe over-night
- Deposits were transported securely through the use of an armored vehicle transportation to the bank and was locked in the lobby area for pick-up
- Staff were counting their change funds to ensure accuracy prior to starting their shift and balancing their tills at the end of their shift with discrepancies investigated promptly
- The deposit was prepared by a second person and any discrepancies were again investigated promptly
- Manual receipts were stored on site
- There was a separate procedure for returned check fees charged and the procedure to add that fee to the account
- There was a separate procedure for voiding transactions

Recommendations:

During the field visit it was determined Animal Services had a sign in their lobby displaying the fee schedule as well as posting it on their website for the public. It was recommended to add verbiage to the notification that a receipt will be provided with every transaction and what types of payments are accepted. Also, add verbiage on the non-sufficient funds (NSF) fee charged of twenty-five dollars (\$25.00) for a returned check.

The following recommendations were proposed to the Animal Services Department and have been implemented or are in the process of implementation:

- Written confirmation of the employee reading the procedure
- Procedures should reference the following:
 - County Codes 15.107 through 15.210
 - The internal control document as prepared by the Comptroller's Department
 - The accounts payable procedure manual as prepared by the Comptroller's Department
 - Other internal procedures relating to cash handling (i.e. Voided Transactions and Returned Checks)
- Include a list of payments accepted (including credit cards)
- Add clarification on how to identify counterfeit money, examples include counterfeit pens and detection lights or machines and what bill denominations are expected to be examined, for example paper bills over \$20.00
- Add no loans to employees nor using the funds as petty cash
- Add credit card information will never be written down or stored in any manner
- Add check amounts will be verified that the numerical amount matches the written amount
- Although unlikely, verbiage should be added that if a cash payment over ten thousand dollars (\$10,000.00) is received the appropriate IRS procedures will be followed
- Add the amount that would trigger a removal of funds from a cashiers till prior to the close of business (recommended \$1,000.00)
- Add a section for mailed payments received and include the following:
 - Who opens the mail and who processes the payments (this should be two separate people with the first person logging the payments received without access to receipting)
 - It will be opened and processed the same business day unless due to limitations of staffing in which case the payments should be locked in the safe and processed as soon as possible, recommended within three (3) business days
- Develop a procedure for utilizing manual receipts and either reference it in the cash handling procedure or include it as a section in the cash handling procedure. When developing the procedure it should include the following:
 - Receipts are stored in a secure location with only appropriate staff having access
 - Original receipts are to be given to the customer and the carbon copy is to be kept in the receipt book
 - Unused receipts should periodically be reviewed to verify none are missing or mis-used and all used receipts should be reconciled to the Chameleon software to verify they were properly used and accounted for
 - A log should be created for documentation of this period review
- Voids or refunds should involve two staff members, preferably the staff who originally created the payment and a supervisor.

- Add a chart of what employees have access to each safe with a disclaimer that upon termination the combinations will be changed
- Add a reviewer to the deposit preparation process (i.e. after the Administrative Assistant prepares the deposit another person reviews and initials the deposit backup)
- Someone other than the person preparing the deposit should be reconciling the bank/cash desk and someone should review the reconciliation
- While the change fund was counted regularly to verify the fund was in balance it was recommended a log be developed and the change fund counted on a monthly basis by two staff members to verify the balance
- Use of a standard balancing sheet (example provided)

Cash Control Audit of 2017:

Animal Services was not included in the prior cash control audit in 2017 therefore, there were no recommendations for follow-up.

Management Comment:

Developed and implemented the recommendations into the cash handling standard operating procedure. The employees have read and acknowledged the updated cash handling. The website and fee board have both been updated as well.

Assessor's Office (102)

Overview of Cash:

The Assessor's Office had no change funds, outside bank accounts nor a petty cash account. The Assessor's Office does accept payments from customers only for a special report or a public request that was extraordinary use of personnel or technology which has not occurred since August of 2016.

Overview of their Purpose:

The Assessor's Office serves the public by providing complete, accurate and timely assessments of all property subject to taxation. The public pays their property tax through the Treasurer's office which is why the Assessor does not have need for change funds. The Assessor's Office roll includes approximately one hundred seventy nine thousand (179,000) parcels as well as thirty thousand (30,000) commercial, mobile home and aircraft accounts. The office also works with veterans, widows and other qualifying citizens to apply exemptions as applicable.

Observation and Procedure Review:

During the review of the detailed written procedures it was determined the Assessor's Office had included all the following processes and procedures:

- Proper distribution of the manual three-part receipt to include the original (white) copy to the customer, yellow copy to accompany the payment for deposit, and the pink copy to remain in the book
- Daily deposits
- Safeguard of the funds in a lockbox until deposited
- Proper void procedure to clearly write "VOID" across all three copies and to leave all three in the book
- Expectation on how to properly fill out the receipt including the date and employee completing the receipt
- Second review of the funds received and secure transportation to the Treasurer's Office for deposit
- Types of payment accepted and that if cash is used it must be exact change

Recommendations:

The following recommendations were proposed to the Assessor's Department and have been implemented or are in the process of implementation:

- Written confirmation of the employee reading the procedure
- Add a version number and effective date
- Procedures should reference the following:
 - County Codes 15.107 through 15.210
 - The internal control document as prepared by the Comptroller's Department
 - The accounts payable procedure manual as prepared by the Comptroller's Department
- Add clarification on how to identify counterfeit money, examples include counterfeit pens and detection lights or machines and what bill denominations are expected to be examined, for example paper bills over \$20.00

- Add checks will be endorsed immediately and inspected for the following:
 - Amounts will be verified that the numerical amount matches the written amount
 - The date is the current date (not post-dated)
 - Payable to is correct and the check is signed appropriately
- Add verbiage on where the manual receipts are securely stored
- Create a log that can be signed off on quarterly that unused all manual receipts are accounted for and used receipts were properly completed (example provided)

Cash Control Audit of 2017:

The Assessor's Office was not included in the prior cash control audit in 2017 therefore, there were no recommendations for follow-up.

Management Comment:

Due to the limited amount of cash received and the time/expense of implementing the recommendations this office has stopped charging the fee for reports and copies.

Clerk's Office (104)

Overview of Cash:

The Clerk's Office utilized the program Eagle Clerk to record payments. The income received was from fees associated to marriage applications and certificates as well as fictitious name filings and public records requests. The fee breakdown is below and was posted online as well as in the office for customers, the types of payment accepted and the fee for using credit cards were also posted for customers.

Fees related to marriages were license application fee of sixty dollars (\$60.00), officiant application fee of twenty five dollars (\$25.00), solemnization fee of seventy five dollars (\$75.00), affidavit for correction of marriage application of twenty five dollars (\$25.00) and affidavit of lost or destroyed marriage certificate for officiants only of fifteen dollars (\$15.00).

Fees related to the fictitious name filings were twenty dollars (\$20.00) for both the certificate as well as the termination. Bond fees for notary and rider were both twenty dollars (\$20.00), the commissioned abstractor was five dollars (\$5.00) and the replacement was six dollars (\$6.00).

There was no charge for audio tape or DVD/CD of board proceedings. Copies of items were fifty cents (\$0.50) per page. Certifications were six dollars (\$6.00) and so were certificate of search. Any other documentation required to be filed was five dollars (\$5.00). Fees were not charged or collected for the State of Nevada, Washoe County, City of Reno, City of Sparks, Washoe County School District, general improvement districts within Washoe County, or any officer of the State, Washoe County, City of Reno, City of Sparks, Washoe County School District, general improvement district, when acting in the officer's official capacity.

The office had ten (10) change funds totaling four thousand eight hundred dollars (\$4,800.00) which was surprise counted by the Washoe County Treasurer's Office on 06/18/2019 and found to be in balance. The office did not have outside bank accounts nor did they have a petty cash fund. The funds were split up as follows: six (6) cashier tills, one change fund, vault for weekend change, fund for the marriage commissioner and a quarter fund.

Outside of their normal operating duties the Clerk's Office also collects money for the Treasurer's Office (in the form of taxes), the Community Services Department (in the form of utility payments) and the Comptroller (in the form of collection money). All these payments are tracked separately and given to the appropriate department to count and include with their deposits. All must be made with exact cash, checks, money order or cashier's check.

Overview of their Purpose:

The County Clerks Office is an elected office and include a wide variety of services to the public as well as preserve and maintain many records dating back to 1861. The Marriage License Bureau serves the public by obtaining marriage licenses or researching your great grandparents' genealogy. The Business Services Division helps with fictitious names as well as notary services. The Office also is responsible for providing the most up-to-date County Code and new ordinances as well as Board of County Commissioners board records and minutes.

Observation and Procedure Review:

During the review of the detailed written procedures it was determined the Clerk's Office had included all the following processes and procedures:

- Revision date of the procedure
- Checks were inspected to verify the amount
- Waived fees were properly documented for the reason
- Voided receipts were performed by an "admin user"
- Flier to handle counterfeit money as well as fraud protection devices at each station
- Clear and proper procedures for opening and closing staff
- Proper safeguarding of the funds with locked safes and till drawers
- Separation of duties for deposit preparation and second count and verification of deposit
- Monthly reconciliation procedures
- Returned check procedures including the fees must be paid via cash, money order or cashier's check and no fee is charged; if the person does not come in to pay the fee then in the case of a notary the Secretary of State's Office is contacted to revoke the appointment as well as in the case of a fictitious name filing will be revoked
- Detailed procedures on collection of money for other departments
- In the event the computer system goes down there is a "backup backpack" securely located within the safe room which has pre-printed forms and manual receipts

Recommendations:

During the field visit it was determined the Clerk's Office had a sign at each station displaying the fee schedule as well as positing it on their website for the public. The sign also had the types of payments accepted at the service charge associated to credit card transactions.

The following recommendations were proposed to the Clerk's Office and have been implemented or are in the process of implementation:

- Written confirmation of the employee reading the procedure
- Procedures should reference the following:
 - County Codes 15.107 through 15.210
 - The internal control document as prepared by the Comptroller's Department
 - Prepare a listing of all procedures applicable to this process to identify the relationship between the documents
- Include the threshold staff should be identifying counterfeit money (example, bills over \$20.00)
- Checks should be endorsed immediately and should be inspected to verify the date is correct (i.e. not postdated)
- Add titles of positions who use each of the procedures
- Add credit card information will never be written down or stored in any manner
- Add change funds will not be used to loan money to staff, cash personal checks or used for petty cash purchases
- Although unlikely, verbiage should be added that if a cash payment over ten thousand dollars (\$10,000.00) is received the appropriate IRS procedures will be followed. The only time this might occur is if the customer is paying for property taxes so this office could refer those customers to the Treasurer's Office rather than accept the payment.

- Add the amount that would trigger a removal of funds from a cashier till prior to the close of business (recommended \$2,000.00)
- Create a written procedure for mailed payments to include:
 - Who opens the mail and who processes the payments - this should be two separate people with the first person logging the payments received without access to receipting (example provided)
 - It will be opened and processed the same business day unless due to limitations of staffing in which case the payments should be locked in the safe and processed as soon as possible, recommended within three (3) business days
- Create a log which is completed quarterly for the unused manual receipts (example provided)

Cash Control Audit of 2017:

The Clerk's Office was not included in the prior cash control audit in 2017 therefore, there were no recommendations for follow-up.

Management Comment:

All recommendations have been either added to the current procedures or a new procedure has been created and given to staff, so they are aware of the newest procedure. Logs have been created and reminders have been set to perform the tasks.

Juvenile Services (127)

Overview of Cash:

Juvenile Services utilized the program Revenue Results to record payments. The income received was from fees associated to the board and care costs, court fees, counseling or programming and restitution. The fee breakdown is below and was posted online.

Board and care costs were thirty dollars (\$30.00) a day until the initial detention hearing and if the child is ordered to be detained at the initial hearing the board and care cost is no longer assessed. If the parent or guardian refuses to pick up the child after they are approved for release the board and care cost is one hundred dollars and seventy five cents (\$100.75) per day. The courts can impose a fine and include fees for attorneys, traffic fines, court fines, assessments and restitution. If orders are given for the child to attend counseling or other programs there may be costs associated with those as well.

The office had two (2) change funds totaling four hundred dollars (\$400.00) and a petty cash account totaling three hundred dollars (\$300.00) which was surprise counted by the Washoe County Treasurer's Office on 05/16/2018 and found to be in balance. The office did not have outside bank accounts.

Overview of their Purpose:

The mission of Juvenile Services is to help create a safer community by providing a continuum of services and sanctions to at-risk youth and their families. Under the direction of the Family Division, Second Judicial District Court, Juvenile Services provides probation, case management, detention, and community services to court wards and youth ages 10 to 18 in Washoe County. Our juvenile justice approach is balanced by supporting positive youth and family development, community safety, and offender accountability.

Observation and Procedure Review:

For petty cash, reviewed the most recent replenishment request from 01/09/2019 and it was determined all necessary documents were stored in SAP and all petty cash receipts were valid transactions. During the review of the detailed written procedures it was determined Juvenile Services had included all the following processes and procedures:

- Titles of staff performing responsibilities to demonstrate separation of duties
- Identifying counterfeit cash which included the amount to be inspected, what do to with the counterfeit money, if detected, and the method of inspection
- Checks were inspected for date to include that post-dated checks were not allowed, the payable too was properly completed, the numerical amount matched the written amount and proper identification was provided
- Checks were endorsed immediately
- Include a list of payments accepted (including credit cards)
- Receipting practices were proper with a receipt generated for every transactions for the customer as well as a copy for the office
- Daily deposits were made and transported to the bank, if circumstances arose where the daily deposit was not completed the deposit was securely stored
- Funds were safeguarded and locked in cash till drawers during the day for those in use while all others were locked in the safe, with all funds locked in a safe over-night

- Staff were counting their change funds to ensure accuracy prior to starting their shift and balancing their tills at the end of their shift with discrepancies investigated promptly
- The deposit was prepared by a second person and any discrepancies were again investigated promptly
- There was a separate procedure for voiding transactions
- Although unlikely, verbiage was included that if a cash payment over ten thousand dollars (\$10,000.00) is received the appropriate IRS procedures will be followed
- Detailed procedure for payments received via the mail that included processing the payment the same day and receipt will be provided if requested section for mailed payments received and include the following:
- Voids or refunds involved two staff members, the staff who originally created the payment and a supervisor
- After preparation of the deposit a second person reviewed the deposit and initialed the paperwork
- Procedures for petty cash were written and included in the cash handling procedure and included all of the following:
 - How the separation of duties is achieved
 - Where the funds are securely stored and who has access
 - How often the funds are reconciled (Ex. Quarterly)
 - Who performs the reconciliation and who verifies the reconciliation
 - What documentation is expected

Recommendations:

The following recommendations were proposed to the Juvenile Services and have been implemented or are in the process of implementation:

- Procedures should reference the following:
 - County Codes 15.107 through 15.210
 - The internal control document as prepared by the Comptroller's Department
 - The accounts payable procedure manual as prepared by the Comptroller's Department
 - Other internal procedures relating to cash handling (i.e. Voided Transactions and Returned Checks)
- Written confirmation of the employee reading the procedure
- Effective date of the procedure
- Personal checks will not be cashed
- Add no loans to employees from the change funds
- Add not using change funds as petty cash
- Checks will not be accepted for an amount higher than the fee
- Add procedure for returned check fees charged, if applicable, and the payment must be made using a different method of payment also add to the website the fee associated with the NSF check
- Add language on mail procedure that two staff members handle the mail, the person opening it should not have access to receipting and the second person should receipt the money
- Add credit card information will never be written down or stored in any manner
- Add the amount that would trigger a removal of funds from a cashiers till prior to the close of business (recommended \$1,000.00)

- Add a section for a procedure for utilizing manual receipts. When developing the procedure it should include the following:
 - Receipts are stored in a secure location with only appropriate staff having access
 - Original receipts are to be given to the customer and the carbon copy is to be kept in the receipt book
 - Unused receipts should periodically be reviewed to verify none are missing or mis-used and all used receipts should be reconciled to the software to verify they were properly used and accounted for
 - A log should be created for documentation of this period review
- Procedures for petty cash were written and included in the cash handling procedure and should have the following added:
 - There will be no loans to staff and no cashing of personal checks
 - A limit on the dollar value of a single purchase (Ex. \$50.00)

Cash Control Audit of 2017:

Juvenile Services was not included in the prior cash control audit in 2017 therefore, there were no recommendations for follow-up.

Management Comment:

All recommendations have been incorporated into the written procedures and distributed to the employees, so they are aware of the most current version.

Manager's Office (101)

Overview of Cash:

The Office of the County Manager had no change funds, outside bank accounts nor a petty cash account. The Manager's Office does not accept payments from customers or outside agencies nor did they have a need for petty cash.

Overview of their Purpose:

The County Manager serves as a liaison between the Board of County Commissioners, elected and appointed directors, government and community agencies, businesses, employees and county citizens.

The office is comprised of several divisions, all listed below with a brief description.

Administration facilitates presentation of issues to the Board of County Commissioners and manages administrative hearings for code violations. Budget identifies revenues from multiple sources to fund Washoe County operations, capital improvements, special programs and debt. Communications delivers information to the public and connects with them through Washoe 311, social media, website, media partners, and WCTV County news. Special Project provide leadership, strategic development, management and implementation of organization wide programs, services and initiatives on behalf of the County Manager. Emergency Management and Homeland Security maintains emergency preparedness, mitigation, response and recovery plans for Washoe County as well as manages the Regional Emergency Operations Center. Government Affairs manages issues on impact on Washoe County and promotes the County's interests at the federal, state, regional and local levels. Internal Audit conducts performance audits to assess department functions and processes to determine if they are achieving their intended purposes and doing so in an economic manner.

Observation and Procedure Review:

The written request for information was sent to each division within the Manager's Office and all respondents indicated there was no cash handling within their division. The Washoe County Account Software Program "SAP" was also utilized to verify no funds were received by the divisions.

Recommendations:

None.

Cash Control Audit of 2017:

The Office of the County Manager was not included in the prior cash control audit in 2017 therefore, there were no recommendations for follow-up.

Management Comment:

None.

Appendix A

Department	Deposit Books
Alternative Sentencing	1
Animal Services	1
Clerk's Office	1
Community Services Department *	15
Comptroller - Collections	1
Digital Communications	1
District Attorney's Office	2
District Health	1
Emergency Management	1
Human Services Agency	2
Incline Constable	1
Incline Justice Court	1
Juvenile Services	1
Library	1
Medical Examiner's Office	1
Public Administrator	1
Public Guardian	1
Recorder's Office	1
Regional Public Safety Center	1
Regional Transportation Comm	1
Reno Justice Court	1
Second Judicial District Court	1
Sheriff's Office	6
Sparks Justice Court	1
Treasurer's Office	1
Truckee Meadows Fire	1
Voter's Office	1

**Including All Parks*

Department	CHANGE FUND	PETTY CASH
Alternate Public Defender		500.00
Alternative Sentencing	350.00	
Animal Services	700.00	
Clerk's Office	4,800.00	
Comptroller's - Collections	400.00	
Community Services Department	4,080.00	50.00
Second Judicial District Court	1,750.00	
District Health	2,500.00	
Human Services Agency	500.00	1,300.00
Incline Justice Court	300.00	
Juvenile Services	400.00	300.00
Library	1,910.00	500.00
Public Administrator		2,000.00
Recorder's Office	550.00	
Reno Justice Court	3,000.00	
Sheriff's Office	1,200.00	22,100.00
Sparks Justice Court	1,100.00	
Treasurer's Office	6,000.00	
Voter's	150.00	
Wadsworth Justice Court	300.00	300.00
Total	\$ 29,990.00	\$ 27,050.00

Department	Bank
District Attorney	Well Fargo
District Attorney - Fraudulent Check Diversion Program	Nevada State Bank
District Attorney - Victim Fund	Well Fargo
District Attorney Revolving Fund	Well Fargo
District Attorney Witness Fees	Well Fargo
Human Resources - Group Health Plan	Well Fargo
Human Resources - Hometown Health	Well Fargo
Human Services Agency - HCAP	Well Fargo
Human Services Agency - NSP3	Well Fargo
Human Services Agency - Senior Services Representative Payee	Well Fargo
Incline Justice Court	Well Fargo
May Foundation Bldg Fund	Well Fargo
May Foundation Bldg Fund	Well Fargo
Parks Wilbur D May Museum Gift Shop	Well Fargo
Public Administrator	Well Fargo
Public Defender	US Bank
Public Guardian	Well Fargo
Public Guardian - Burial Collective	Well Fargo
Reno Justice Court	Well Fargo
Second Judicial District Court	Well Fargo
Second Judicial District Court Case Specific	Well Fargo
Second Judicial District Court Case Specific	Well Fargo
Second Judicial District Court Case Specific	Well Fargo
Self-Insured Risk Mgmt	Well Fargo
Sheriff Administrative Investigations	Well Fargo
Sheriff Administrative Management Account	Well Fargo
Sheriff Commissary Fund - Checking	Well Fargo
Sheriff Commissary Fund - Savings	Well Fargo
Sheriff Commissary Securities	Well Fargo
Sheriff Execution Trust Fund	Well Fargo
Sheriff Inmate Trust Fund	Well Fargo
Sparks Justice Court	Well Fargo
Treasurer - Main Account	Well Fargo
Treasurer - Payroll	Well Fargo
Treasurer - Revolving Account	Well Fargo
Wadsworth Justice Court	Washington Federal

[illegible]

[illegible]

[illegible]



Top 5 Operational Audits For a Well-Rounded Audit Plan

A successful audit team is one that not only meets its SOX requirements, but can prove itself a valuable partner to the business by identifying key areas for improving operational efficiency. For auditors, this begins with the audit plan. A well-rounded audit plan will reflect an enterprise-wide scope and coverage of risks while addressing audit projects focused on improving operational performance across the business. This brief will discuss 5 important internal audits to consider including in your audit plan.

1. CYBERSECURITY

The continued rise of cyber attacks, which occur extremely quickly and cause critical damage in little time, points to the importance of building cyber resiliency. Internal audit can help by auditing and evaluating measures that prevent an attack and also mitigate risk in the event of one.

Cyber Crime Statistics in 2019:

87%

cyber attacks
in 1 min or less

\$6T

cybercrime
damages

56%

experienced
vendor breaches

- 87% of cyber attacks occurred in minutes or less, but 68% of breaches took months or longer to discover ¹
- Cybercrime damages are predicted to exceed *\$6 trillion* by 2021
- 56% of organizations have experienced a breach caused by a vendor ²

**Educate yourself on the biggest threats to your industry - review the Verizon DBIR summary*

Recommended Audit Projects:

- **Data Encryption.** Ensure that data classification policies exist to identify and appropriately classify confidential data. Data classified as confidential or sensitive in nature should be encrypted in transit and at rest.

- **Access Management Policies and Controls.** Review access rights are granted based on properly-defined business needs and evaluate the timing of access rights termination when employees leave the organization.
- **Data Penetration Testing with Vendors.** Ensure your third-party vendors and contractors maintain and execute information security policies and controls that meet or exceed internal requirements.
- **Business Continuity Plan (BCP).** Audit the overall business continuity plan to ensure that appropriate considerations are in place for maintaining core business functions in the event of an infrastructure failure, cybersecurity incident, natural disaster, or other emergencies. Confirm if the business is performing routine BCP tabletop exercises, updating contacts and procedures on a regular basis, and distributing the BCP to all relevant parties.
- **Patch Management Policies.** Audit whether patch and vulnerability management policies are in place to ensure that patches are implemented in a timely fashion upon release and testing.
- **Employee Information Security Training.** Evaluate employee security training materials and effectiveness of training programs. Every single employee in an organization should receive and sign off on information security training materials. Training and policies should be updated on a regular basis (annually at a minimum).³

2. CULTURE AND ETHICS

Companies are facing more cultural accountability today than ever before. Unprecedented reputational risks are casting looming shadows over shareholder confidence, thanks to the rise of the #MeToo movement in response to sexual harassment in the workplace and growing public concern over consumer data privacy. Internal Audit can help mitigate future reputational risks by promoting appropriate workplace ethics and values.

Recommended Audit Projects:

- **Digital Ethics.** Evaluate how consumer information is managed and protected across the enterprise, including within departments such as marketing and sales. Identify whether ethics goals are included as a part of performance metrics and annual performance reviews.
- **Succession Planning.** Review succession planning methodology for whether the company has adequate talent retention procedures or policies. Encourage the use of cross-department trainings and hiring collaboration.
- **Gender and Racial Discrimination.** Evaluate hiring, pay, and promotion review procedures across the organization's departments. Identify potential external areas of concern,

such as employee-customer touchpoints, and evaluate employee and customer feedback. Build comparison groups from this information gathering to identify deviations in response across gender and racial demographics, highlighting potential bias.

3. DATA PRIVACY

Corporate mishandling of consumer data has become a topic of national security and poses a huge reputational risk to companies. The Facebook-Cambridge Analytica scandal and Google's \$57 million GDPR fine are two notoriously publicized examples, but organizations of all sizes and industries have experienced severe data breaches resulting in damaged public opinion of those brands.⁴ Internal audit should understand how personal information is being stored and managed and ensure there are proper security controls in place.

Recommended Audit Projects:

- **General Data Protection Regulation (GDPR) Enforcement.** If your organization serves any citizens within the European Union (EU), it is within the scope of GDPR enforcement. Perform a GDPR audit to identify all data processing objects and activities, including those stored or controlled by third party businesses or vendors. To identify whether your organization's handling of data in scope for GDPR is appropriate, consider engaging external firms or contractors who specialize in GDPR-readiness.
- **Consumer Consent.** Audit your company's compliance with consumer privacy regulations and review privacy consent policies and effectiveness across departments. Ensure that pseudonymization is in place to remove personalized identifiers.⁵

4. DATA GOVERNANCE

In contrast to consumer data, big data refers to organizational data, which is unstructured and housed in different silos. Understanding and incorporating big data into strategic business decisions poses new challenges and risks, namely data accountability and protection. Internal Audit can help ensure proper data governance controls and policies are in place.

Recommended Audit Projects:

- **Data Quality.** Areas to audit: data migration procedures, data management procedures in the event of acquisitions, data quality standards.
- **Data Analytics.** Areas to audit: policies and procedures of data analytics functions, proper storage and ownership controls around data repositories and self-service platforms, data access controls.

5. THIRD PARTY RISK

External talent, data centers, and vendors help businesses promote productivity and efficiency, but they come at the cost of incurring complex third party risks. Over two-thirds of organizations using vendors have reported fines, lost revenues, or brand damage caused by third parties. Internal audit can identify control weaknesses and recommend improvements regarding third party risk.

Recommended Audit Projects:

- **Background Checks.** One of the most basic but effective controls is ensuring third party contractors undergo and pass background checks that meet or exceed internal requirements prior to the contract start date.
- **Third Party Risk Management.** Evaluate the organization's third party risk management framework from end to end, ensuring that vendor risk is appraised across all functional areas of the business, and that risk assessments and mitigation activities are performed on a routine basis.
- **Contract Management.** Evaluate contract management processes used to track relationships with vendors. Ensure that vendor relationships are evaluated regularly and that legacy contracts include required clauses.
- **Right-to-audit Clauses.** Ensure possible rights to audit are included in all contracts and perform periodic reviews and updates
- **Monitoring and Compliance.** Assess third party compliance by developing, implementing, and performing monitoring around a compliance system that is aligned with the company's information security standards.

To learn how OpsAudit can help you manage your internal audit projects - request a product walkthrough at auditboard.com.

¹ Verizon, 2018 Data Breach Investigations Report (https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf)

² Gartner, 2019 Audit Hot Spots Report Excerpt (<https://emtemp.gcom.cloud/ngw/globalassets/en/risk-audit/documents/audit-hot-spots.pdf>)

³ Isaca, Auditing Cyber Security: Evaluating Risk and Auditing Controls (<http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/auditing-cyber-security.aspx>)

⁴ Gartner, 2019 Audit Hot Spots Report Excerpt (<https://emtemp.gcom.cloud/ngw/globalassets/en/risk-audit/documents/audit-hot-spots.pdf>)

⁵ International Association of Privacy Professionals, Top 10 Operational Impacts of the GDPR - Part 8: Pseudonymization (<https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/>)

⁶ KPMG, Top 10 Audit Concerns 2018 (<https://advisory.kpmg.us/content/dam/advisory/en/pdfs/top10auditconcerns-2018.pdf>)



ON RISK

A GUIDE TO UNDERSTANDING, ALIGNING, AND OPTIMIZING RISK

2020



TABLE OF CONTENTS

Introduction	3
Top risks for 2020 and beyond	4
Key findings	5
Methodology	6
How to use this report	7
Leveraging the methodology	8
Understanding risk	9
The stages of risk	11
Key findings explained	12
Board overconfidence	13
Views misaligned on risk maturity	14
Misalignment danger	15
Risk strategy concerns	16
Insufficient understanding of significant risks	17
Three risks to watch	18
Focus on talent	19
Conclusion	20
Cybersecurity	24
Data protection	25
Regulatory change	26
Business continuity and crisis response	28
Data and new technology	29
Third party	30
Talent management	32
Culture	33
Board information	35
Data ethics	36
Sustainability (ESG)	37
Figures	38

Dear Readers,

I have the great pleasure of introducing the inaugural edition of an exciting new report from The Institute of Internal Auditors. **OnRisk 2020: A Guide to Understanding, Aligning, and Optimizing Risk** is an innovative and insightful research report that promises to change the way organizations view and understand risk. That's a bold statement that requires some justification, so here it is.

A number of risk reports published annually provide perspectives from individual players in the risk management process. However, no single report has provided a holistic view of risk from all perspectives — until now.

OnRisk 2020 brings together the perspectives of the board, executive management, and chief audit executives (CAEs) on the risks that are top of mind for 2020 and beyond. Based on quantitative and qualitative surveys, the report lays out how each respondent group views key risks. Respondents shared their perspectives on their personal knowledge of the risks and their views of their organizations' capability to address the risks. But the most innovative and powerful benefit **OnRisk 2020** offers is a studied analysis of how those views differ and what that means to an organization's risk management.

For example, the qualitative survey found that board members are consistently more optimistic about their organizations' capability to address key risks than members of executive management are. For some risks, board member views on capability were dramatically higher than those of executive management or CAEs. Taken together, these findings raise questions about how boards build their views on capability, and how this affects decisions that drive risk strategy.

Another example relates to managing cyber risk. Addressing this ubiquitous risk remains a daunting task, and its management is a top priority. Yet because of the ever-evolving nature of cybersecurity threats, executive management, boards, and CAEs are aligned in feeling that their knowledge of cybersecurity is low.

These insights should do more than just raise awareness of the misalignments, or gaps, that may exist. Through careful analysis of the survey data as well as additional research on each risk, The IIA has identified actions each respondent group may take to improve alignment with one another and ultimately enhance the organization's ability to address the risks. This is where **OnRisk 2020** offers the most innovative and powerful benefit to organizations.

Organizations should review the analysis and recommendations related to each of the 11 key risks that follow and are encouraged to conduct a similar review of the knowledge and capability perspectives among their own organization's board, executive management, and internal audit activity.

OnRisk 2020 offers a robust look at key risks that organizations will face in the coming year, provides important benchmarking on capability to support risk and audit planning, and offers direction to help align and enhance risk management strategy and execution. I am confident you will find **OnRisk 2020** insightful, illuminating, and of immense value.

Sincerely,



Richard F. Chambers

President and CEO

The Institute of Internal Auditors



INTRODUCTION

*Risk is a **thorny** word.*

In its simplest form, it means exposure to danger, but in an organizational or business context, it takes on a much more complex definition.

For generations, investors, boards, and executive management viewed risk as something to be avoided or mitigated, but organizations that take such a defensive posture cannot thrive for long in today's dynamic marketplace driven by global competition, rapid technological change, and geopolitical uncertainty. The modern approach to risk management must view risk as opportunity, as well. This requires strategic, coordinated, and seamless collaboration among key risk management players, and success in this arena demands a clear-eyed view of each player's understanding of and ability to leverage or manage risk.

The Institute of Internal Auditors (IIA) is proud to offer *OnRisk 2020: A Guide to Understanding, Aligning, and Optimizing Risk*, a robust and comprehensive view of the top risks for the coming year based on the perspectives of key players in the risk management process — the board, which sets the risk appetite and provides strategic oversight for long-term value creation; executive management, which sets and executes risk management strategy; and the CAE, a resource for the board and management who provides assurance and insights independent from management.

In partnership with a global market research firm, The IIA has produced a unique report that captures the viewpoints from the boardroom, C-suite, and internal audit activity. It also introduces a Risk Stages Model — with stages ranging from Recognized to Maintained — that provide additional insight into developing risk management plans and strategies. In today's dynamic risk universe, risk management must effectively combine risk mitigation of potential negative outcomes with identification and prioritization of opportunities to enhance organizational value.

Through quantitative and qualitative surveys, *OnRisk 2020* not only identifies perspectives from each key player in the risk management process, it also maps how those views align. This additional insight into risk alignment provides vital data to measure how risks are understood and managed.

The mapping of how risk perspectives are aligned — or misaligned — provides deeper insight to support risk management planning in the coming year. It also sheds light into areas where misalignment can create weaknesses that can disrupt even the best risk strategies.

TOP RISKS FOR 2020 AND BEYOND

The **11 risks** below were carefully selected from a vast assortment that are likely to affect organizations in 2020 and were vetted through in-depth interviews with board members, executive management, and CAEs.

CYBERSECURITY: The growing sophistication and variety of cyberattacks continue to wreak havoc on organizations' brands and reputations, often resulting in disastrous financial impacts. This risk examines whether organizations are sufficiently prepared to manage cyber threats that could cause disruption and reputational harm.

DATA PROTECTION: Beyond regulatory compliance, data privacy concerns are growing as investors and the general public demand greater control and increased security over personal data. This risk examines how organizations protect sensitive data in their care.

REGULATORY CHANGE: A variety of regulatory issues, from tariffs to new data privacy laws, drive interest in this risk. This risk examines the challenges organizations face in a dynamic and sometimes volatile regulatory environment.

BUSINESS CONTINUITY/CRISIS RESPONSE: Organizations face significant existential challenges, from cyber breaches and natural disasters to reputational scandals and succession planning. This risk examines organizations' abilities to prepare, react, respond, and recover.

DATA AND NEW TECHNOLOGY: Organizations face significant disruption driven by the accelerating pace of technology and the growing ease of mass data collection. Consider traditional versus born-digital business models. This risk examines organizations' abilities to leverage data and new technology to thrive in the fourth industrial revolution.

THIRD PARTY: Increasing reliance on third parties for services, especially around IT, demands greater oversight and improved processes. This risk examines organizations' abilities to select and monitor third-party contracts.

TALENT MANAGEMENT: Historically low unemployment, a growing gig economy, and the continuing impact of digitalization are redefining how work gets done. This risk examines challenges organizations face in identifying, acquiring, and retaining the right talent to achieve their objectives.

CULTURE: "The way things get done around here" has been at the core of a number of corporate scandals. This risk examines whether organizations understand, monitor, and manage the tone, incentives, and actions that drive behavior.

BOARD INFORMATION: As regulators, investors, and the public demand stronger board oversight, boards place greater reliance on the information they are provided for decision-making. This risk examines whether boards are receiving complete, timely, transparent, accurate, and relevant information.

DATA ETHICS: Sophistication of the collection, analysis, and use of data is expanding exponentially, complicated by artificial intelligence. This risk examines organizational conduct and the potential associated reputational and financial damages for failure to establish proper data governance.

SUSTAINABILITY: The growth of environmental, social, and governance (ESG) awareness increasingly influences organizational decision-making. This risk examines organizations' abilities to establish strategies to address long-term sustainability issues.

KEY FINDINGS

The qualitative and quantitative interviews for *OnRisk 2020* elicited new insights about how the principal drivers of risk management interact, which risks pose the greatest challenges, and how alignment on risk management efforts impacts organizational success. Analysis of the results identified seven key findings that shed light not only into how risks are understood, but also how the ability to manage risk is perceived. In-depth examinations of these findings are found later in this report.

-
- **Boards are overconfident.** Boards consistently view the organization's capability to manage risks higher than executive management, evidence of a critical misalignment between what executive management believes and what is communicated to the board.
 - **Boards generally perceive higher levels of maturity in risk management practices.** Board members' perceptions of risk knowledge and capability place them ahead of executive management and CAEs relative to risk maturity, therefore making them more likely to believe those risks are better managed.
 - **"Acceptable misalignment"** on risk is a prevalent and dangerous mindset. A majority of respondents believe some misalignment on risk perception should be expected, with some viewing it as "healthy." While misalignment around individual knowledge of a risk may be acceptable based on varying roles, misalignment on the perception of the organization's capability to manage a risk is a serious concern.
 - **Some industries are lagging in adopting systematic approaches to risk.** Healthcare, retail/wholesale, and public/municipal industries are lagging — sometimes significantly — in developing coordinated and consistent risk management processes.
 - **Cybersecurity and Data and New Technology represent critical knowledge deficits.** Low reported knowledge and high relevance of these risks suggest risk management players should prioritize building knowledge in these two key risk areas.
 - **Data and New Technology, Data Ethics, and Sustainability risks are expected to grow in relevance.** CAEs predict brisk growth in relevance for these three key risk areas in the next five years, identifying an opportunity for organizations to take a more proactive approach.
 - **Talent Management** (and retention) are at the center of future concerns. Respondents recognize the importance of good talent and how people drive the success of a business — particularly when it comes to data and IT skills. An important shift is underway from an insufficient availability of resources to an inability to attract and retain talent with business-critical skills.
-

METHODOLOGY

The inaugural **OnRisk 2020** report is a significant step forward in collecting stakeholder perspectives on risk and risk management in support of good governance and organizational success. The combination of quantitative and qualitative research¹ provides a robust look at the top risks facing organizations in 2020 and allows for both objective data analysis and subjective insights based on responses from risk management leaders.

The **qualitative survey** is based on 90 in-depth interviews with professionals in North American boardrooms, C-suites, and internal audit functions. As part of the interviews, respondents were asked to evaluate 11 key risks on two scales: their personal awareness and knowledge of each risk and their perception of their organization's capability to address each risk. The ratings were based on a seven-point scale, with "Not at all knowledgeable" and "Extremely incapable" being the lowest ratings (1) and "Extremely knowledgeable" and "Extremely capable" being the highest ratings (7).

The combined responses for the two scales were then used to plot the position of each respondent group for each risk, where the X axis delineates perceived organizational capability, and the Y axis delineates personal knowledge of the risk (Figure 1). The values assigned for plotting purposes are derived as a percentage of respondents who scored their risk knowledge or their organization's risk capability as either 6 or 7 (top two ratings). Plotting the positions of all three respondent groups not only identifies how each group views each risk, it also graphically illustrates the degree of alignment among the groups.

The quantitative survey covers top risks as viewed by more than 600 internal audit leaders, primarily CAEs. The comprehensive survey also addressed organizational approaches to risk management, internal audit planning, resources, talent management, and internal audit's role in governance.

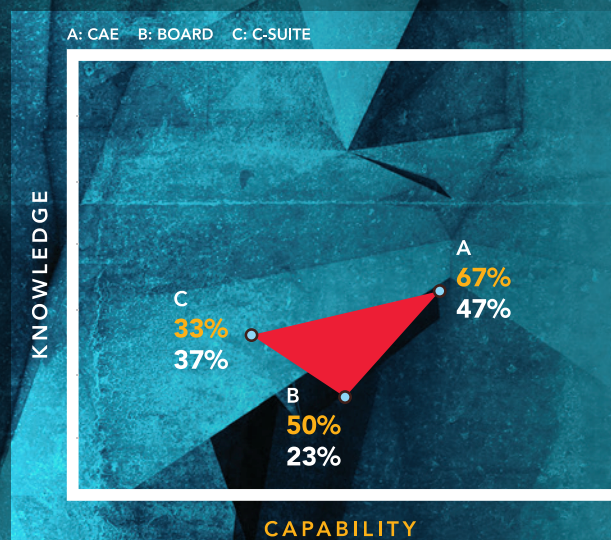


Figure 1: Personal Knowledge/Organizational Capability Graph

¹ The quantitative survey of internal audit managers and CAEs and the qualitative interviews of board members, C-suite executives, and CAEs were conducted between June 4, 2019, and June 26, 2019.

HOW TO USE THIS REPORT

Explanation of graphics

Based on in-depth interviews with 90 professionals, the personal knowledge and organizational capability of each of the three respondent groups were measured and plotted for each risk. Simple quadrant mapping (Figure 2) provides an effective and consistent tool to reflect those views.

The four quadrants of the graph correspond to the magnitude of each of the two measures. For example, responses with high ratings in knowledge and capability would be plotted in the top right quadrant. Conversely, responses with low ratings for knowledge and capability would be plotted in the lower left quadrant.



Figure 2:
Quadrant Graph

Position plotting

Positions for each of the three respondent groups are plotted on the quadrant map not only to identify the relative knowledge and capability on each risk, but also to graphically illustrate the degree of alignment among the groups that may exist. The resulting triangles — referred to simply as alignment triangles — provide a strong indicator of how well a risk is understood and managed. The size, shape, and location of each triangle also provides insights on what is driving any misalignment (see related sidebar).

Alignment Triangles: What do they mean?

The alignment triangles created by plotting each respondent group's perspectives on each risk offer insights into how the risk is currently being managed. The shape of each triangle can provide valuable information, as well.



SHORT AND NARROW

Triangles with this basic shape suggest strong alignment on what each group knows about a risk, but significant disagreement by one respondent group about the organization's capability for addressing the risk.

TALL AND NARROW

Conversely, triangles with this basic shape suggest significant range of knowledge among respondent groups, but strong alignment on their views on organizational capability.



SHORT AND BROAD

This basic shape triangle suggests disagreement by more than one respondent group, with the most significant disagreement relating to the organization's capability to address the risk.



TALL AND BROAD

This basic shape suggests misalignment by more than one respondent group, with significant disagreement on both knowledge and capability.



SMALL AND SYMMETRICAL



This shape triangle suggests strong alignment of all three respondent groups on knowledge and capability. Depending on the location of the triangle, this could reflect a risk that is well understood and managed (top right quadrant) or one that is not well understood or managed (lower left quadrant).

LEVERAGING THE METHODOLOGY

Readers of *OnRisk 2020* should review and analyze the data for each of the 11 key risks that follow and are encouraged to conduct a similar analysis of the knowledge and capability perspectives among their own organization's board, executive management, and internal audit activity.

Comments from qualitative interview participants are interspersed throughout *OnRisk 2020* to offer a glimpse into not just *what* they think of each risk, but *how* they think about them. While these comments provide some insights, it is vital for every organization to have similar discussions about how each player in the risk management process understands risk and their perspectives on the organization's capacity to manage or leverage it.

A critical step in that analysis is to undertake a clear-eyed examination of how the three risk management roles currently operate and interact and the changes that should be contemplated in those roles to enhance the risk management process. For example, one of the key findings of *OnRisk 2020* is that boards appear to be more confident in their organizations' ability to manage risk than are executive management or CAEs. It is critical to examine and understand what is behind this skewed view, and to explore the changes needed to correct it.

One reason for this misalignment may be the quality and completeness of information flowing to boards. Boards need information that is complete, accurate, and timely, and must establish proper oversight practices to ensure this.

This challenge is not unknown to boards. According to the National Association of Corporate Directors (NACD) report, *2019 Governance Outlook*, "Directors struggle to keep up with a rapidly evolving business landscape. For the second year in a row, NACD's public company governance survey found that a large majority of directors, almost 70 percent, report that their boards need to strengthen their understanding of the risks and opportunities affecting company performance."²

The cited public company governance survey also found boards are spending twice as much time reviewing information from management than from external sources, "revealing a heavy dependence on management views and analysis in fulfilling their oversight duties." What's more, more than half (53 percent) of directors indicated that the quality of information from management must improve, "suggesting the board needs better, not more, information from management."³

² National Association of Corporate Directors and Partners, *2019 Governance Outlook: Projections on Emerging Board Matters* (Arlington: NACD, 2018), 2.

³ NACD, *2018-2019 NACD Public Company Governance Survey*, (Arlington: NACD, 2018).



UNDERSTANDING RISK

Reputation and Disruption in Risk Assessments

It is important to distinguish between a risk and the potential impact stemming from risk events. Reputational damage and business disruptions are often perceived as risks when in actuality they are consequences resulting from risk events. Boards, executive management, and internal audit can devote significant time and resources responding to and managing such consequences, yet may never understand or address the underlying risk, or root cause, that resulted in the event.

Reputational damage and business disruption may result from any number of risk events. For example, a ransomware cyberattack, where hackers block access to vital information, can cripple systems until a ransom is paid. If the attack is not properly managed, the organization will likely experience reputational damage. In this case, the reputational damage results from events related to cybersecurity, business continuity, and crisis response risks.

Similar to reputational damage, business disruption may result from a number of factors. For example, the proliferation of artificial intelligence challenges traditional business models. The risk is not the disruption itself, but the organization's ability to shift away from traditional manual practices and leverage data and new technologies to remain competitive in an increasingly complex and technology-driven environment.

That being said, boards, executive management, and internal auditors should be mindful of potential impacts related to business disruption and reputational damage. These potential impacts should be embedded in analyses of risks. Particular attention should be given to how these potential impacts may vary depending upon the industry and environment in which the organization operates.

Macro Risks

Macro risks may refer to economic or financial risks, political risks, or the impact of economic or financial variables on political risk. They may have widespread and significant influence on vital areas such as supply chains, short- and long-term planning, talent management and safety, and fraud and corruption.

The intertwined nature of macro risks may make them more complex than and just as dynamic as new or unknown risks. Examples include trade and tariff policy impacts on economic performance, and climate change leading to famine or natural disasters that can trigger geopolitical instability. What's more, macro risks can affect any organization, not just those that provide products and services to international markets. Indeed, organizations whose leaders believe they are immune to macro risks could end up underestimating or developing blind spots to key risks.

While *OnRisk 2020* is not designed to address macro risks, it is important to acknowledge their role in risk management strategies.

Inherent vs. Residual

Discussions about risk management can quickly become complex when strategy, competition, costs, and other factors are considered. This layer of complexity makes an already challenging discussion that much more difficult.

One way to simplify the discussion is to understand that risk may be measured on either an inherent or residual basis.

INHERENT RISK:

A theoretical description of what could go wrong if there were no controls or other risk management techniques. Most often applied to define the potential magnitude of risks and threats.

RESIDUAL RISK:

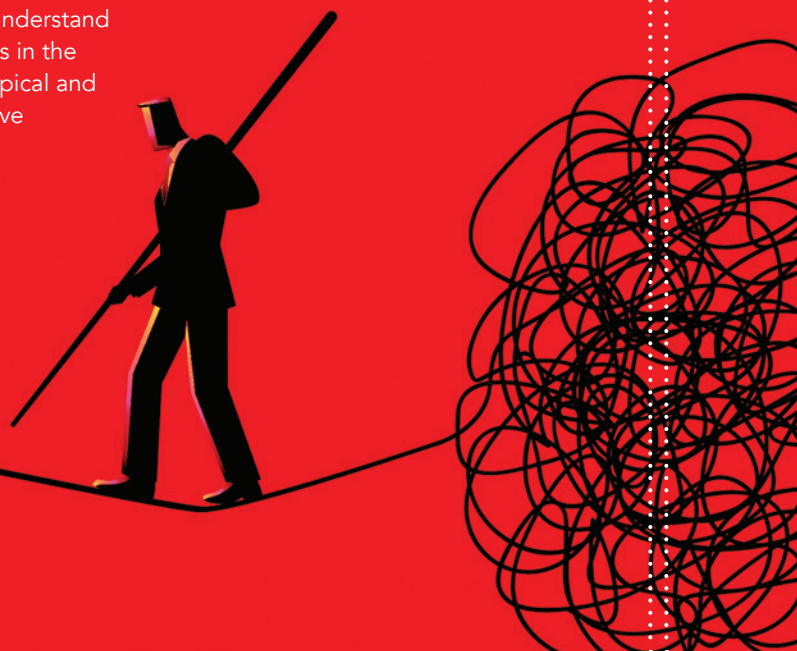
The risk remaining after management takes action to reduce the impact and likelihood of a risk event occurring, including control activities, in responding to a risk.⁴

These terms may seem like “auditor speak” to boards and executive management teams who are more likely to see risks in terms of impact and likelihood in their organization. Those viewpoints are typically associated with residual risk. In other words, boards and executive management are more likely to focus discussions on the risk that remains after risk management has reduced the impact and likelihood of a risk event occurring.

When weighing risk management resources, such as ERM and compliance programs, as well as internal audit activities, risk managers should consider the level of each risk to their organization. For example, fraud risk is well understood, and effective anti-fraud controls have been designed and tested over a long period of time. Most organizations have a strong understanding of the inherent risk fraud presents. However, the residual fraud risk depends on the controls in place in a particular organization and how effectively those controls are managed.

It is important for all players in the risk management process to understand inherent risk levels — the potential magnitude of risks and threats in the absence of risk management. This is especially applicable for atypical and emerging risks, where risk mitigation strategies are unlikely to have been developed.

⁴ Larry Sawyer et al., *Sawyer's Guide for Internal Auditors*, 6th ed. (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2012), 1: 186.



THE STAGES OF RISK

In today's dynamic, technology-driven world, risks may emerge and impact organizations, sometimes at breakneck speeds. The risks discussed in this report are grouped into one of four stages as they relate to the potential impact on organizations and the actions organizations should take to address them — Recognize, Explore, Develop, and Maintain (Figure 4).

The Risk Stages Model (Figure 3) reflects how approaches to managing specific risks evolve within the organization. The colored graphic to the right shows that risk evolution on the same scale as the risk rankings — Knowledge and Capability.

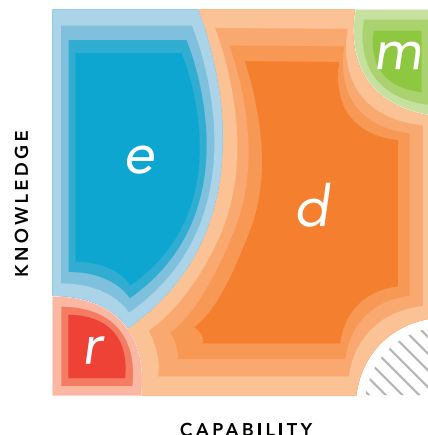


Figure 3: Risk Stages Model >
Risk stages are Recognize (r), Explore (e), Develop (d), Maintain (m).

Stages of Risk Explanation

RECOGNIZE

A risk is perceived as emerging and knowledge of the risk among stakeholders is low. Risk response strategies are not implemented or are not assumed to be effectively designed given the low understanding of the underlying risk. Monitoring processes have not been contemplated. Inherent risk levels are not well understood.

Knowledge – Low
Capability – Low

r

EXPLORE

Knowledge of the risk is growing among some but not all stakeholders. The risk may be perceived as emerging or dynamic. Risk response strategies have been contemplated, but have not been fully implemented. Monitoring processes have not been contemplated or are not implemented. Inherent risk levels are generally understood.

Knowledge – Mid to High
Capability – Low

e

DEVELOP

Risk knowledge is high, at least with management teams. Risk response strategies may be developed or in process of being implemented. Monitoring processes may be in contemplation, but are not likely to have been fully implemented. Residual risk is generally understood.

Knowledge – Low to High
Capability – Mid to High

d

MAINTAIN

Risk is well understood by all relevant stakeholders and is not perceived to be changing significantly. Risk response strategies, consistent with the perceived relevance of the risk, have been developed and implemented. Monitoring processes are utilized to ensure risk response strategies are operating effectively as designed. Residual risk levels are understood and believed to be at an acceptable level for the organization.

Knowledge – High
Capability – High

m

Figure 4: Stages of Risk Explanation

KEY FINDINGS EXPLAINED

The seven key findings introduced earlier are examined in depth in the following pages. As noted previously, the qualitative and quantitative interviews for *OnRisk 2020* were intended to elicit candid perspectives on the nature and understanding of risk management through the eyes of its three principal drivers. The analysis and examination of those views reveal important insights into interactions and alignment among respondents and informative conclusions about how those interactions and alignments impact risk management.



BOARD OVERCONFIDENCE

Boards are overconfident in their organizations' capability to address risks.

The qualitative survey responses and additional analysis uncovered a disturbing pattern. For every key risk, board members rated their organizations' capability for managing the risk higher than executive management did (Figure 5). This finding suggests boards may be failing to critically question information brought to them by executive management due to either receiving insufficient information or from limitations in their own competencies to understand and evaluate risks. The finding also suggests executive management may not be fully transparent with the board about risks and their own reservations about their organizations' ability to manage them.

Also notable is that executive management gives its highest ratings on risk management capability to Culture and Board Information, two areas often correlated with executive management performance.

The analysis explored whether boards' higher perceptions on capability were driven by low knowledge of the risks. The data did not support this hypothesis, further suggesting some level of breakdown in communication among the three parties (see Figures 7a and 7b in the section on acceptable misalignment).

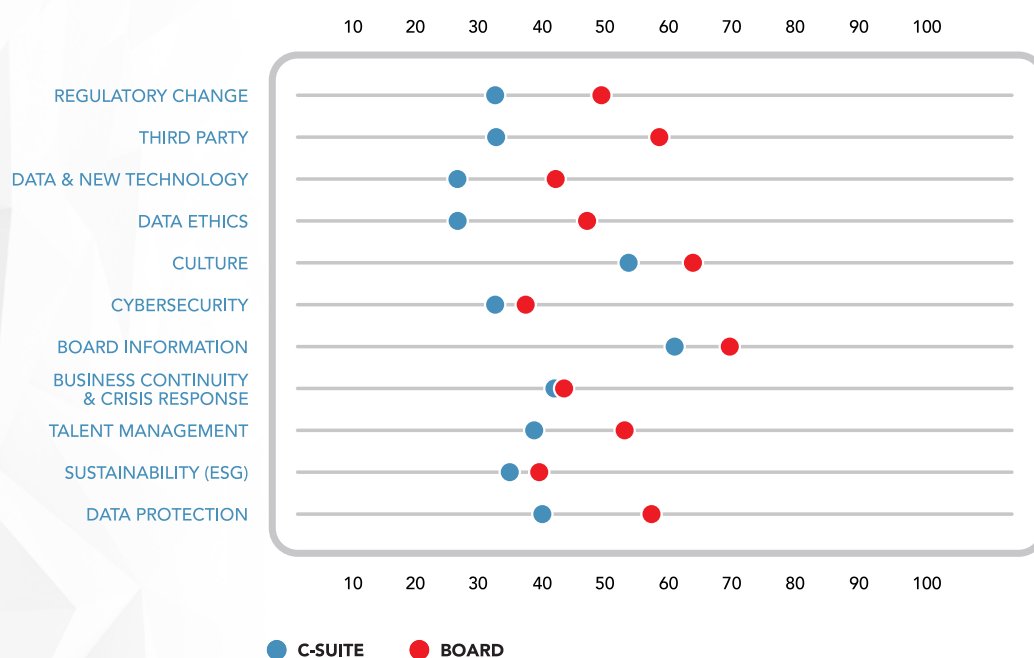


Figure 5: Organizational Risk Capability: Board and C-suite Perceptions

VIEWS MISALIGNED ON RISK MATURITY

Boards generally perceive higher levels of maturity in risk management practices.

Plotting the risk rankings on the Risk Stages Model (see section on risk stages, p. 11) confirms that boards are more optimistic in their organizations' abilities to manage risk, especially in comparison to executive management (Figure 6).

Boards consistently rate risk knowledge and capability in the range identified as *Develop*, where risk knowledge is high, risk management processes are being implemented, and residual risks are well understood.

Plotting risk rankings from executive management, meanwhile, reflects its more conservative view relative to the Risk Stages Model. Executive management ranks the majority of risks in the *Explore* stage, where knowledge of risk is growing, risks are perceived as emerging or dynamic, risk response strategies are contemplated but not fully implemented, and inherent risks level are generally understood.

CAEs' risk rankings are divided between the *Develop* and *Explore* stages, with the Data and New Technology risk rated in the *Recognize* stage, where risks are perceived as emerging, stakeholders have low knowledge of the risk, and inherent risk levels are not well understood.

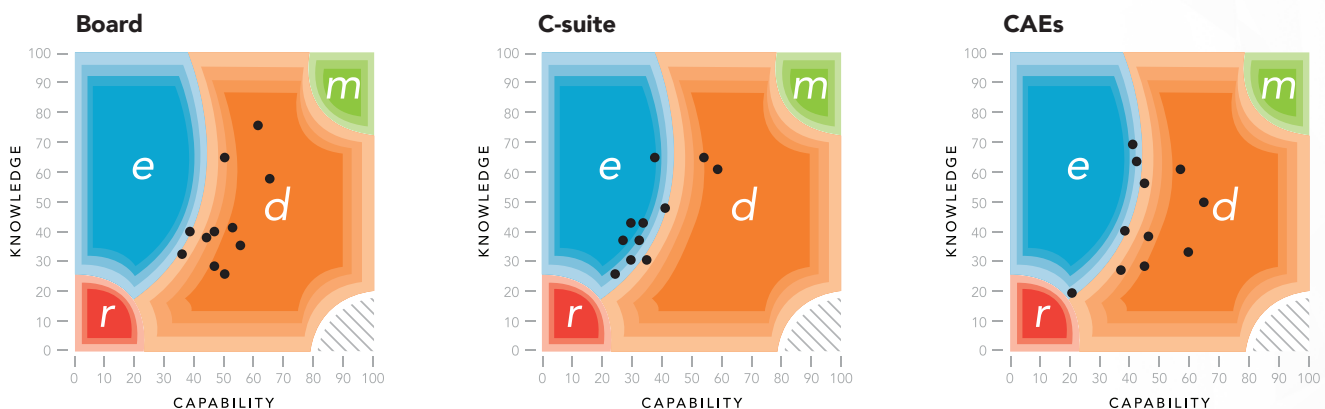
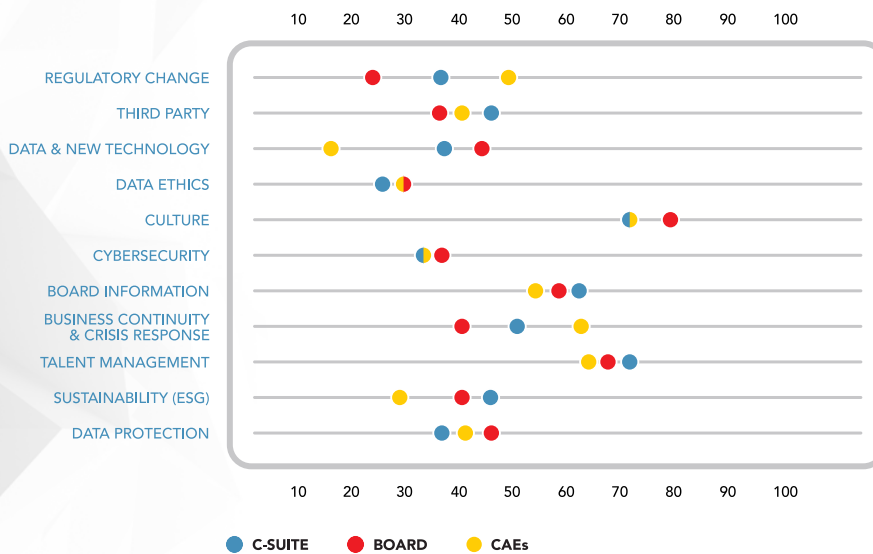


Figure 6: Organizational Capability for 11 Risks Plotted on the Risk Stages Model
Risk stages are Recognize (r), Explore (e), Develop (d), Maintain (m).

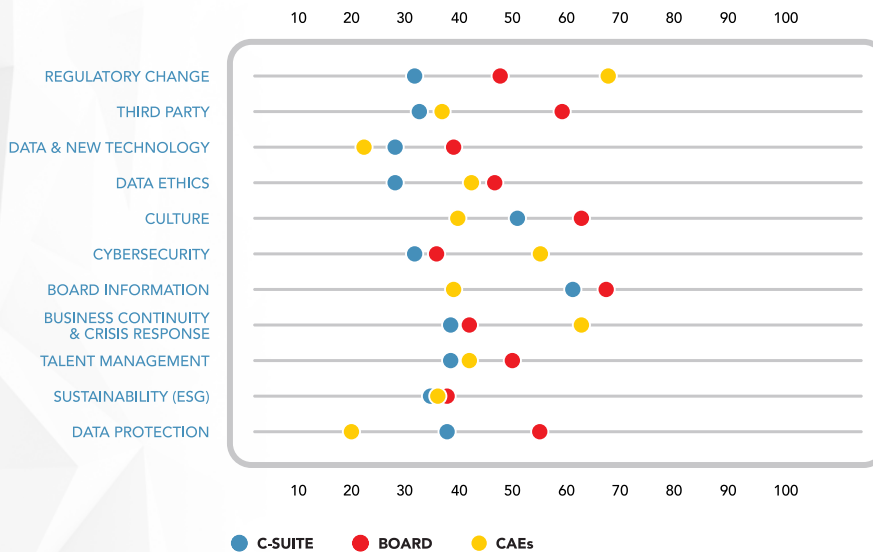
MISALIGNMENT DANGER

Acceptable misalignment is a prevalent and dangerous mindset.

Personal Knowledge



Organizational Capability



A number of respondents downplayed the danger of misalignment among the parties. Indeed, many said that there was a “healthy” level of disconnect between CAEs, board members, and executive management. But the benefits of alignment (or negatives associated with misalignment) are often viewed through a lens biased by individual knowledge rather than a broader view incorporating organizational capability. Respondents differed in perspective, with most comments from CAEs centered on day-to-day operations (tactics), while comments from board members and executive management concentrated on risk strategy. The level at which a healthy disconnection becomes an unhealthy one was not addressed, leaving a dangerously nebulous gap that, in itself, is a risk.

The figures at left reflect how the three respondent groups rated their personal knowledge of the risk and their perception of the organization’s capability to mitigate them. Note the tighter clustering for Personal Knowledge (Figure 7a) in comparison to the more widely spread ratings for Organizational Capability (Figure 7b). The disparity suggests that the comfort zone for acceptable misalignment expressed by the majority may be more benign for knowledge of the risk, where the variance is generally small, but the greater variance in perceived organizational capability logically raises a red flag.

“There is uncertainty and ambiguity in our company around risk.”

– CAE, Business Services

Figures 7a (top) and 7b (bottom): Risk Knowledge and Capability:
Alignment Among Board, C-suite, and CAEs

RISK STRATEGY CONCERNS

Some industries lag in adopting systematic approaches to risk management.

While methods vary widely, a systematic approach to identifying, managing, and monitoring risks is critical to long-term value creation. Ideally, all organizations, regardless of sector, would adopt such approaches. While the type, likelihood, and impact of risks vary across industries, a holistic approach to risk management would undoubtedly benefit every organization.

Yet only about two-thirds (67 percent) of the CAEs surveyed report that their organizations have a systematic approach to identifying, managing and monitoring risk. Perhaps surprisingly, CAEs working in the healthcare, retail/wholesale, and public/municipal sectors rated their organizations' levels of risk discipline among the lowest when compared to their peers in other industries. (Figure 8). The low percentage of systematic risk management in these industries may indicate that individual business units are operating in risk silos. That is, the organizations may excel in managing certain risks, such as patient and drug safety in healthcare or natural disaster response in the public sector; however, the organizations are unable to routinely apply what they learn across the enterprise.

Additional analysis of responses based on organizational size (by revenue) found smaller organizations are as likely to be systematic as larger ones. This finding provides evidence to dispute the theory that systematic approaches to risk management correlate with resources and justifies serious concern about the reasons for the disparity among industries.

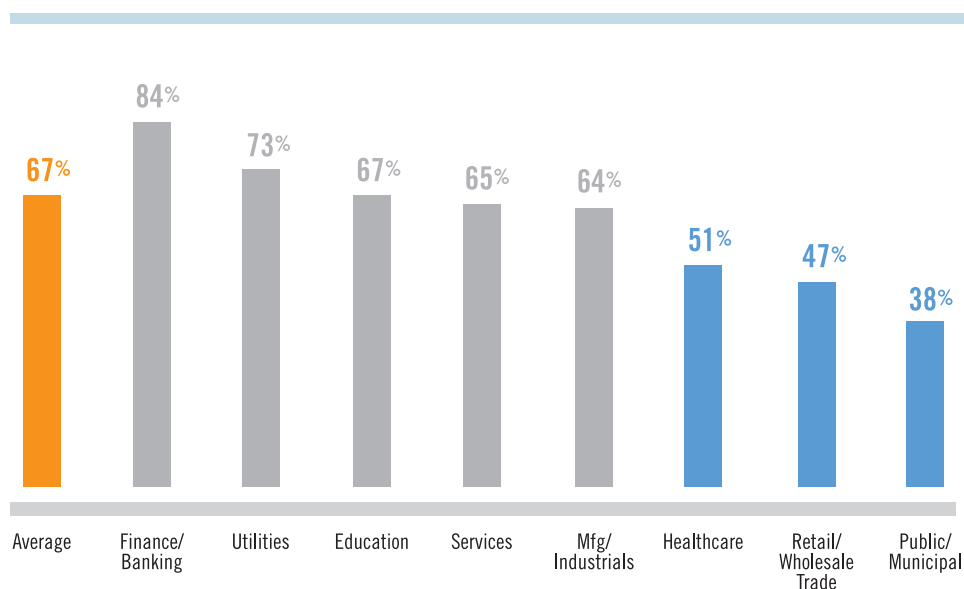


Figure 8: Systematic Approach to Risk Industry Comparison

INSUFFICIENT UNDERSTANDING OF SIGNIFICANT RISKS

Knowledge deficits in Cybersecurity, Data and New Technology can limit mitigation efforts.

Figure 9 reflects the key risks as they relate to Personal Knowledge and Organizational Relevance ratings among all respondents. This is a departure from the previous graphs of Knowledge and Capability ratings, but this comparison brings to life additional insights. The shaded area reflects those risks rated of highest relevance and lowest knowledge, thus pointing to where knowledge deficits exist. Respondents rated themselves relatively low on knowledge of Cybersecurity and Data and New Technology, yet rated the organizational relevance of those risks as high, which may make sense when the dynamic and complex nature of both risks are considered.

Data Protection and Business Continuity/Crisis Response fall just outside the shaded area, reflecting only slightly higher levels of knowledge and comparably high relevance ratings. Taken as a group, these four risks share a common element that contributes to knowledge deficits. All four involve outside entities constantly acting against the organization, whether hackers devising sinister new ways to attack or technology advancing faster than organizations can adapt and adopt.

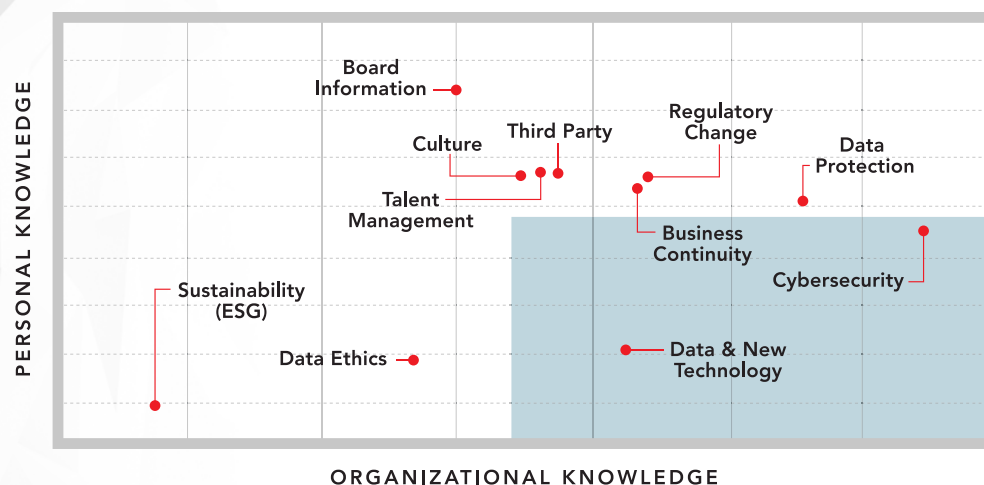


Figure 9: Personal Risk Knowledge Risk Relevance Comparison

THREE RISKS TO WATCH

Data and New Technology, Data Ethics, and ESG (Sustainability) will become more relevant risks.

The arrows in Figure 10 show predicted changes in risk relevance. Of the three risks discussed in this section, Data and New Technology was viewed as high in relevance at the time of the survey. However, as Figure 10 shows, respondents believe that the growth in the relevance of Data Ethics and Sustainability will greatly outpace the growth in relevance of the other risks over the next five years.

By beginning now to examine how they will address these risks, organizations may get ahead of the challenges associated with the risks and may discover opportunities to leverage them. For example, one of the greatest challenges in managing the risk related to Data and New Technology is assuring organizations are sufficiently flexible and prepared to adopt and adapt to technology that will support organizational growth and competitiveness. Such preparation involves building a corporate culture that is data- and cyber-savvy and readily embraces change.

In terms of Data Ethics, leaders in the boardroom and the C-suite must clearly establish organizational values, morals, and principles as guideposts to direct the collection, storage, management, and use of data while understanding the potentially significant consequences for failing to do so. Internal auditors should provide assurance that the organization is adhering to the established guideposts.

Data Ethics is closely tied to the third risk to watch, Sustainability (ESG). Organizations are under increasing pressure from activist investors, regulators, and others to show how long-term strategies reflect an understanding of resource limitations, impacts outside the organization, and overall commitment to good governance. Organizational leadership should take steps to expand its knowledge on how the organization is viewed and operates in its broader ecosystem.

RISK	CURRENT	FUTURE	CHANGE
CYBERSECURITY	86%	90%	+4 ↑
DATA PROTECTION	78%	85%	+7 ↑
REGULATORY CHANGE	66%	64%	-2 ↓
BUSINESS CONTINUITY	65%	67%	+2 ↑
DATA AND NEW TECHNOLOGY	64%	82%	+18 ↑
THIRD PARTY	60%	66%	+6 ↑
TALENT MANAGEMENT	58%	65%	+7 ↑
CULTURE	57%	58%	+1 ↑
BOARD INFORMATION	54%	51%	-3 ↓
DATA ETHICS	51%	66%	+15 ↑
SUSTAINABILITY (ESG)	30%	45%	+15 ↑

Figure 10: Risk Relevance for 11 Risks

FOCUS ON TALENT

Talent Management (and retention) are at the center of future concerns.

All three respondent groups recognize how people drive the success of the business — particularly when it comes to data and IT skills. With greater employee focus on social, political, and economic issues, and heightened competition to retain the best talent, respondents recognize company culture and employee satisfaction are increasingly important factors to success in the modern workplace. Most organizations know that filling seats with generic talent will not give them the competitive edge they need to thrive in today's rapidly changing risk landscape. Instead, organizations must find and develop individuals with the critical skills and expertise to keep up with evolving business practices and deliver innovation and growth.

Boards, executive management, and CAEs all believe their knowledge related to talent management risk is high. While the C-suite and CAE are fairly aligned in their assessments of the organizational capability to deal with such risk, board members have a slightly more optimistic perspective. This makes addressing board overconfidence that much more important.

Executive management and CAEs should collaborate to address the board's overconfidence about talent management so that all stakeholders become aligned around efforts to create formal talent management processes and diversity and inclusion initiatives to identify and attract employees with vital skills and manage the risk of losing top talent.

"Talent drives success ... data integrity and cybersecurity are mitigated based on talent, which is based on culture. This will play a key role in the future."

– Board Member, Healthcare

"Management often creates culture and values from the top down ... they know they need to take on better employees and solidify the hiring process because it's a big part of the business and will continue to be."

– CAE, Banking

CONCLUSION

The previous observations and findings were based on studied analyses of the data from the qualitative and quantitative surveys. What follows is an in-depth look at each of the key risks highlighted in the report. Carefully selected and validated by a cross-section of the three critical stakeholders, the risks covered here will impact all industries to varying degrees.

Each risk is examined based on a number of criteria, including relevance now and in the future, where the risk currently fits in the Risk Stages Model, and how the three respondent groups view the risk on the Personal Knowledge and Organizational Capability scales. These thought-provoking evaluations support the premise that alignment of the perspectives among the three respondents may significantly impact an organization's ability to manage risks and opportunities.

This section provides insightful gap analyses on risk perspectives, recommended actions for each stakeholder group aimed at improving alignment among them, and a benchmark against which to measure progress. Together, these comprise a valuable resource to which readers may refer throughout the year.

Note: The alignment triangle graphics for the following 11 risks are based on quantitative interviews of 90 combined respondents from boards, executive management, and CAEs. Each point of the triangle is labeled with a letter corresponding to each respondent group – A for CAEs, B for board members, and C for executive management. In addition, the corresponding percentage based on the top two answers for Personal Knowledge (blue) and Organizational Capability (red) are included in each label.





THE RISKS

Managing risk is the art of building value while understanding what can be gained or lost from action or inaction, the foreseen or the unforeseen, the planned or the unplanned. Those who know what they don't know can ask questions. Those who don't know what they don't know are paralyzed.



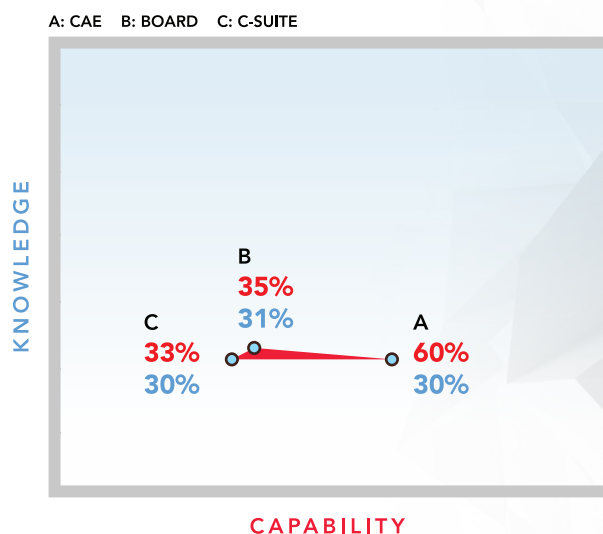
THE RISKS

CYBERSECURITY

The growing sophistication and variety of cyberattacks continue to wreak havoc on organizations' brands and reputations, often resulting in disastrous financial impacts. This risk examines whether organizations are sufficiently prepared to manage cyber threats that could cause disruption and reputational harm.

Gap Analysis:

Cybersecurity threats are a significant risk today and for the foreseeable future. The C-suite, board members, and CAEs are aligned in their perception that their knowledge of the topic is relatively low, which is likely attributable to the quick and ever-evolving nature of cyber risk. While senior leaders and board members are well aligned on their organizations' capability to address cybersecurity, CAEs appear to be overconfident. Considering their self-assessed knowledge of the topic is quite low, CAEs may be relying too readily on optimism expressed by CIOs and/or other providers of IT assurance and advice. With the C-suite's perception of capability appearing so much lower than that of the CAEs, the source of the incongruence is reason for concern.



Actions:

Board: Set expectations that management is continually providing briefings on emerging cybersecurity risks and action is being taken to address those risks. Hold management responsible and accountable for being transparent about vulnerabilities that require remediation or acceptance. Ensure that the internal audit activity is properly resourced to provide independent assurance on significant risks.

C-suite: Be transparent with the board and internal auditors about emerging cybersecurity risks and outstanding vulnerabilities. Leverage internal auditors as a resource to ensure that the controls created to mitigate or minimize cyber threats are designed and operating as intended.

CAE: Build trusting relationships with IT leadership to understand growing and emerging risks. Dedicate necessary resources to performing technical and non-technical reviews and consider hiring or co-sourcing specialty resources where necessary. Continually demonstrate professional skepticism regarding controls in place to mitigate cyber-related risks.

RISK STAGE



RISK RELEVANCE



Source: See Figure 10

THE RISKS

DATA PROTECTION

Gap Analysis:

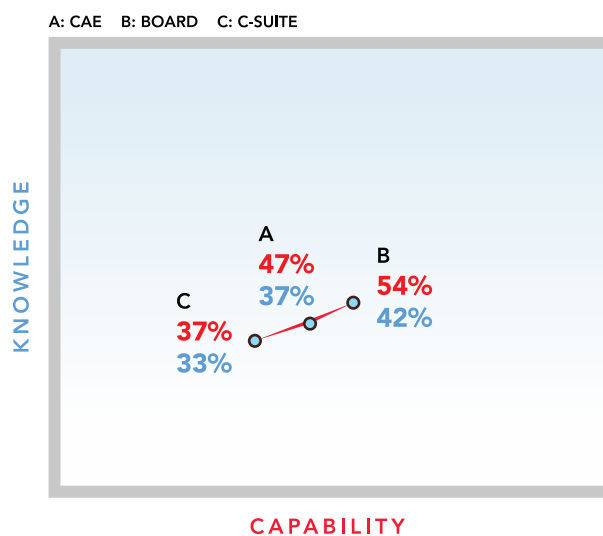
Data protection is perceived as one of the highest priority risks and is expected to become more relevant, likely in response to expected increases in regulation, financial impact, and the potential for reputational damage. While board members, executive management, and CAEs all have some knowledge related to the risk, there may be opportunity for additional learning. Boards may have an overly optimistic perspective on their organizations' capability, perhaps due to insufficient exposure to information about the risks of failure to protect sensitive data and comply with increasingly complex data protection regulations. CAEs also appear to be more optimistic about organizational capability than senior leadership, which may result from an insufficient, or delayed, internal audit focus on this emerging and growing risk.

Actions:

Board: Use knowledge of the risk to ask pointed questions to the CAE and executive management around actions being taken to identify and protect the organization's most sensitive data, as well as comply with regulations.

C-suite and CAE: Provide regular updates to the board on limitations of the organization's ability to protect data and comply with regulations as well as communicating actions being taken to address the risks and limitations. Consider the use of outside subject matter experts to consult on current status and action items.

Beyond regulatory compliance, data privacy concerns are growing as investors and the general public demand greater control and increased security over personal data. This risk examines how organizations protect sensitive data in their care.



RISK RELEVANCE



RISK STAGE



Source: See Figure 10

THE RISKS

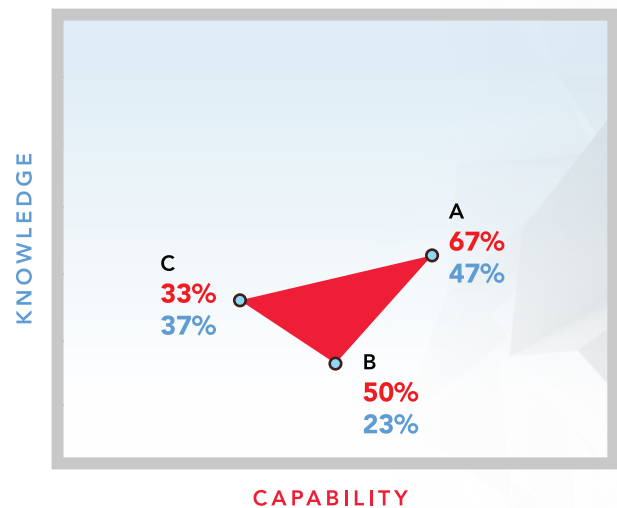
REGULATORY CHANGE

A variety of regulatory issues, from tariffs to new data privacy laws, drive interest in this risk. This risk examines the challenges organizations face in a dynamic, and sometimes volatile, regulatory environment.

Gap Analysis:

A significant misalignment exists among executive management, CAEs, and board members related to this risk. While opportunity exists to increase knowledge of regulatory change risk among all parties, this is particularly true of board members who may have a fiduciary responsibility to oversee their organizations' compliance activities. CAEs, and to a lesser extent board members, may be overly optimistic about their organizations' capabilities related to monitoring, adjusting to, and complying with regulations. This perceived capability gap should be of particular interest to those in industries, such as financial services, inherently subject to increasing and changing regulations.

A: CAE B: BOARD C: C-SUITE



Actions:

Board: Ensure adequate oversight processes have been established, particularly around mission-critical compliance issues. Set expectations that executive management regularly brief the board on new and proposed regulations relevant to the organization and that the CAE coordinates assurance coverage with providers of assurance over regulatory risks. Seek subject matter experts or other educational resources and opportunities to keep current on regulations and regulatory changes.

C-suite: Dedicate resources to continually monitor new and proposed regulatory changes. In highly regulated industries, ensure that monitoring activities are in place and properly resourced.

CAE: Dedicate audit resources to evaluating the organization's processes for monitoring and complying with regulatory change. Stay abreast of new and proposed regulatory changes, coordinate with those providing assurance over compliance risks, and be prepared to brief boards on potential impacts to operations.


RISK STAGE



RISK RELEVANCE



Source: See Figure 10



“ **The company** overall needs to see the bigger picture and keep the bigger risks in the forefront of their mind. It’s hard for departments to see beyond daily, weekly, and monthly functions. **”**

– Board Member, Tech

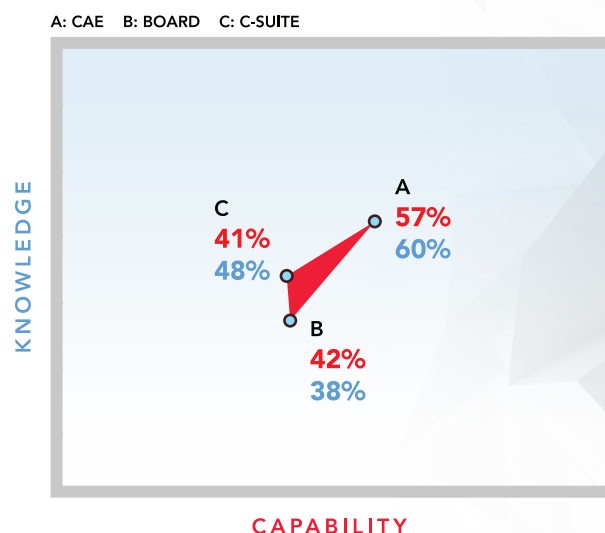
THE RISKS

BUSINESS CONTINUITY AND CRISIS RESPONSE

Organizations face significant existential challenges, from cyber breaches and natural disasters to reputational scandals and succession planning. This risk examines organizations' abilities to prepare, react, respond, and recover.

Gap Analysis:

Here, CAEs are the outlier, viewing themselves as more knowledgeable than executive management and the board and reporting a more optimistic view of organizational capability to respond to and recover from crises and maintain business continuity. The C-suite and the board are aligned in their more conservative view of their organizations' capabilities. However, board members report notably less knowledge on the topic. The incongruity between CAEs' self-assessments and those of executive management and the board begs the question of whether CAEs are unrealistically confident, or rather, have more information to share with management and the board.



Actions:

Board: Set expectations of management to provide opportunities to enhance board members' understanding of related risks and their role in the processes. Further set expectations for a periodic overview of business continuity and crisis response plans, including risk assessments of scenarios that would most likely trigger the need to use those plans.

C-suite: Continually evaluate scenarios that would require business continuity and/or crisis response plans to be used. Work with the internal auditors in a consulting capacity to brainstorm risk scenarios and improve response plans. Test and update plans periodically and communicate scenarios and plans to the board.

CAE: Review organizational business continuity and crisis response plans, as well as results of scenarios conducted by management to test readiness for more likely events. Provide consulting services to help management improve its capability. Coordinate with other providers of assurance and consulting services to provide the board with coordinated assurance at the organizational level.

RISK STAGE



RISK RELEVANCE



Source: See Figure 10

THE RISKS

DATA AND NEW TECHNOLOGY

Gap Analysis:

Although respondents ranked this risk among the top five in terms of current relevance and expect its relevance to grow more than any other on our list, CAEs rate their knowledge of the category quite low. Board members' greater perception of their organizations' capability to manage risks related to data and new technology may stem from positive information provided to them by management about the introduction of data and technology in the business without information about the underlying risks associated with those developments.

Actions:

Board: Set expectations of management that presentations demonstrating the use of data and new technology to drive the organizational strategy are balanced with information on potential negative impacts, including areas where the organization may be lagging in the use of data and new technology relative to the industry and/or competitors and the organization's ability to adapt to new technologies.

C-suite: Continue to explore new opportunities to leverage data and new technology to enhance organizational capability to meet strategic objectives. Provide balanced perspectives to the board with regards to organizational capability and challenges.

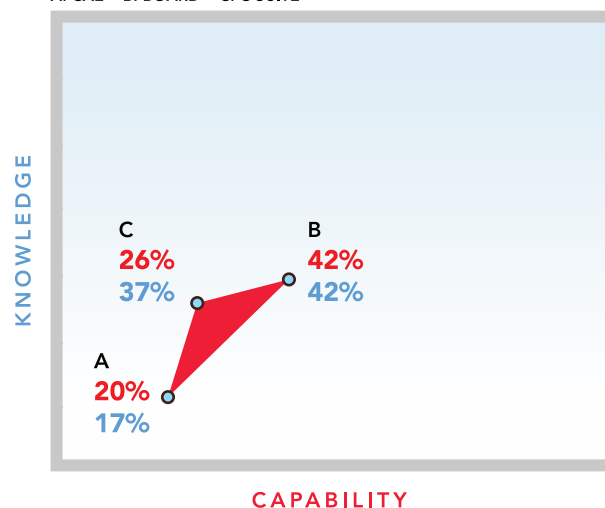
CAE: Dedicate resources to better understanding how the organization is leveraging data and technology in new ways. Ensure that risk universe and risk assessments take into account risks related to those uses of data and technology. Provide assurance on how data and new technology impact the collection, management, and protection of data.

RISK RELEVANCE



Organizations face significant disruption driven by the accelerating pace of technology and the growing ease of mass data collection. Consider traditional versus born-digital business models. This risk examines organizations' abilities to leverage data and new technology to thrive in the fourth industrial revolution.

A: CAE B: BOARD C: C-SUITE



RISK STAGE



Source: See Figure 10

THE RISKS

THIRD PARTY

Increasing reliance on third parties for services, especially around IT, demands greater oversight and improved processes. This risk examines organizations' abilities to select and monitor third-party contracts.

Gap Analysis:

As organizations continue to increase their outsourcing of business processes, risks related to third parties continue to grow. Executive management and CAEs appear to be relatively aligned regarding the capability related to the risk despite assessing their own knowledge of the category lower than their counterparts did. In contrast, board members appear much more optimistic about their organizations' abilities to engage and monitor third-party risk, despite having an admittedly lower knowledge of this risk. This misalignment may stem from boards having a limited understanding of where and how organizations depend on third parties. Further, this misalignment may be fueled by the dangerous misconception that outsourcing processes includes the transfer of risks related to those processes.

Actions:

Board: Ensure that management provides a holistic view of all significant third-party relationships, particularly those aligned with the organization's strategic objectives. Set expectations to receive briefings about any significant challenges that arise related to third-party relationships.

C-suite: Identify and prioritize all third-party relationships, giving particular attention to those that are large in value or those of any size that are key to the achievement of strategic objectives. Ensure that risks associated with each of the relationships are understood and accountability for managing the relationship has been appropriately assigned. Verify that "right-to-audit" provisions are included in all contracts.

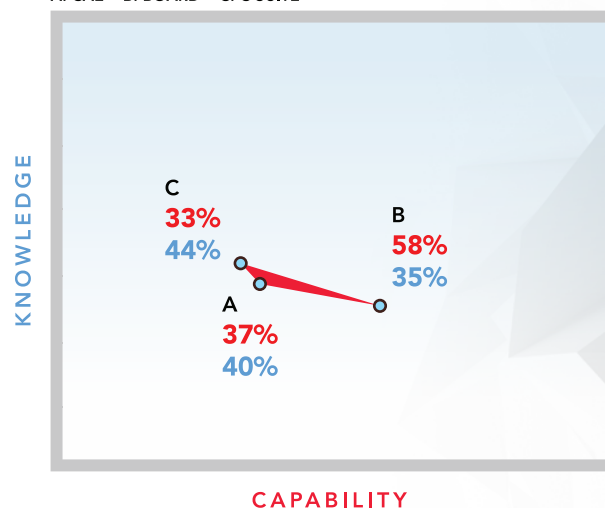
CAE: Ensure that the internal audit activity has a holistic understanding of all significant third-party relationships. Give fair consideration to how these relationships fit into the organization's ecosystem of risks. Consider dedicating audit resources to evaluating overall third-party engagement and monitoring processes as well as processes around material third-party relationships.

RISK RELEVANCE



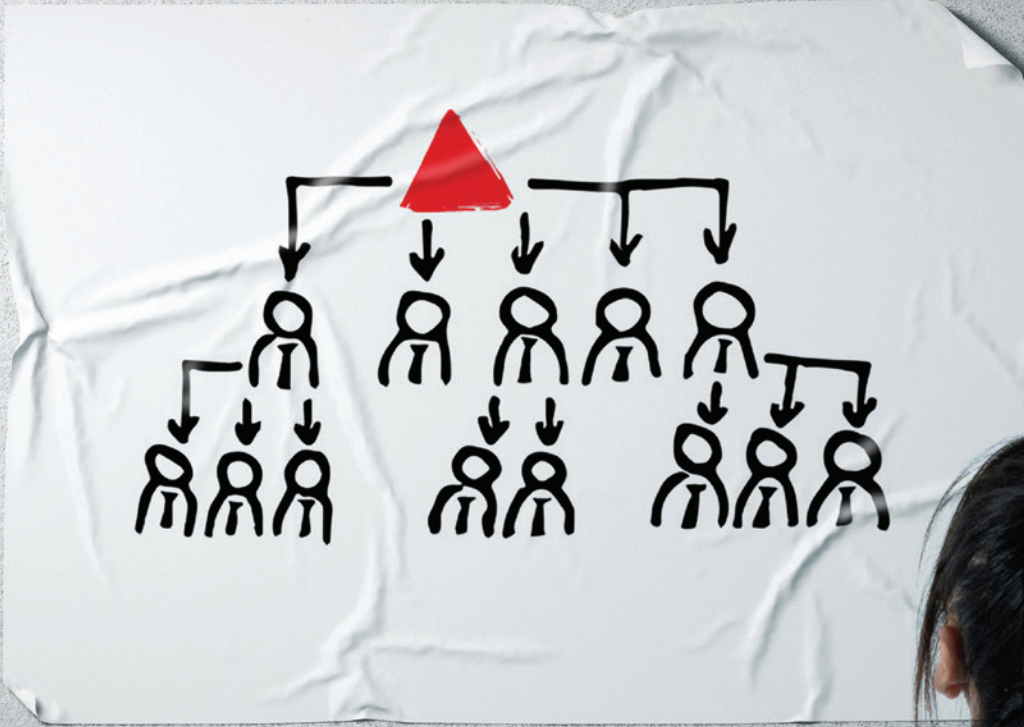
Source: See Figure 10

A: CAE B: BOARD C: C-SUITE



RISK STAGE





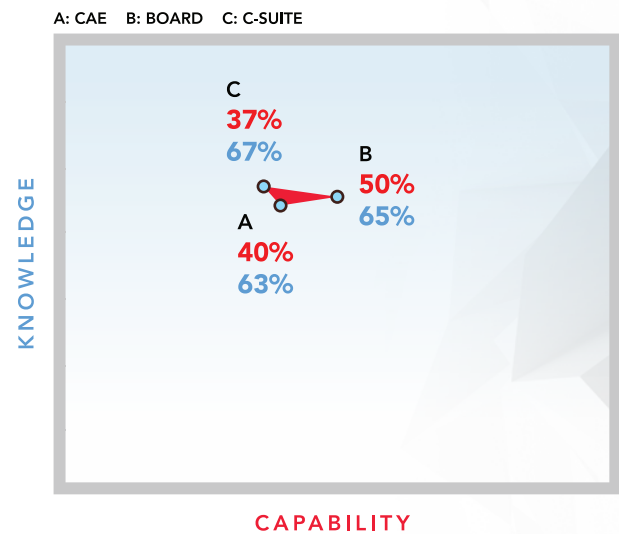
THE RISKS

TALENT MANAGEMENT

Gap Analysis:

Boards, CAEs, and members of the C-suite agree that they are relatively knowledgeable about risks related to talent management. The C-suite and CAE are fairly well aligned in their view of organizational capability to address talent management risks. Board members have a slightly more optimistic perspective, perhaps stemming from board members' primary focus on recruiting senior leadership talent. Executive management and CAEs may have a more holistic view and understand the potential talent management limitations at lower- to mid-levels, which largely remain outside the purview of the board.

Historically low unemployment, a growing gig economy, and the continuing impact of digitalization are redefining how work gets done. This risk examines challenges organizations face in identifying, acquiring, and retaining the right talent to achieve their objectives.



Actions:

Board: Make periodic inquiries of senior leaders regarding talent management processes and risks related to lower- and mid-level employees.

C-suite and CAE: Continue to monitor emerging trends and associated risks related to talent management and provide updates to the board regarding initiatives taken and risks identified.

RISK STAGE



RISK RELEVANCE



Source: See Figure 10

THE RISKS

CULTURE

Gap Analysis:

While senior leaders and CAEs are relatively confident in their knowledge around risks related to organizational culture, board members indicate they have a firm understanding of this risk, rating their knowledge of it higher than their knowledge of any other category. Board members are also more optimistic about their organizations' capability with regards to managing culture risk than are members of executive management, and CAEs are significantly less confident than either the board or the C-suite, with gaps of 25 points and 15 points, respectively.

Actions:

Board: Monitor actions taken by management to establish a positive culture within organizations, including reporting lines and safeguards, to allow for reporting of issues (whistleblowers). Seek insights from the internal audit activity for a perspective on culture independent from management.

C-suite: Set a positive tone at the top through communications and management actions. Establish management structures and reporting lines that allow for reporting of cultural issues. Recognize that incentives, both explicit and implicit, can drive unexpected and/or undesirable behaviors. Monitor and adjust accordingly.

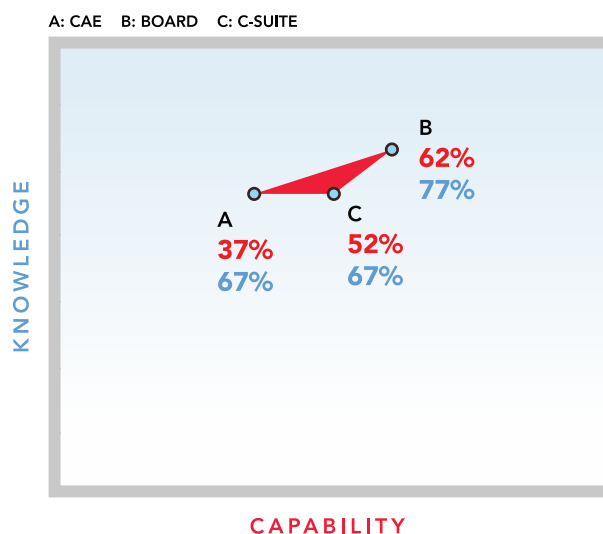
CAE: Provide feedback directly to senior leaders when culture-related issues arise. Be prepared to answer questions from board members regarding organizational culture. Provide assurance that management structures and reporting lines are conducive to the ability to report culture-related issues.

RISK RELEVANCE



Source: See Figure 10

"The way things get done around here" has been at the core of a number of corporate scandals. This risk examines whether organizations understand, monitor, and manage the tone, incentives, and actions that drive behavior.



RISK STAGE





THE RISKS

BOARD INFORMATION

Gap Analysis:

CAEs, executive management, and board members all believe they are knowledgeable about risks related to the information that goes to the board. Senior leaders and board members display confidence in the capability of organizations to provide complete, accurate, and timely information to boards to perform their duties. CAEs are less confident in the capability of the organization to provide adequate information to the board. This may be attributable to the CAE believing that executive management is less than transparent. The CAE may lack knowledge about the information being provided to the board and/or have concerns about the quality of the information the board receives. In light of the findings on board overconfidence in risk management capability, misalignment in this area may be woefully underrepresented.

Actions:

Board: Apply professional skepticism in evaluating the information received from executive management. Solicit the CAE's opinion on the quality of information being provided. Hold management accountable when information appears to be inaccurate or is not provided timely.

C-suite: Provide complete, accurate, and timely information to the board, regardless of how it may be viewed by the board. Work with the CAE to provide assurance to the board regarding the quality of information provided.

CAE: Make inquiries of board members regarding their comfort level that information they are provided is complete, accurate, and timely. With board support, consider reviewing certain board materials, such as those involving mission-critical risks, to verify and communicate whether any information is incomplete or inaccurate.

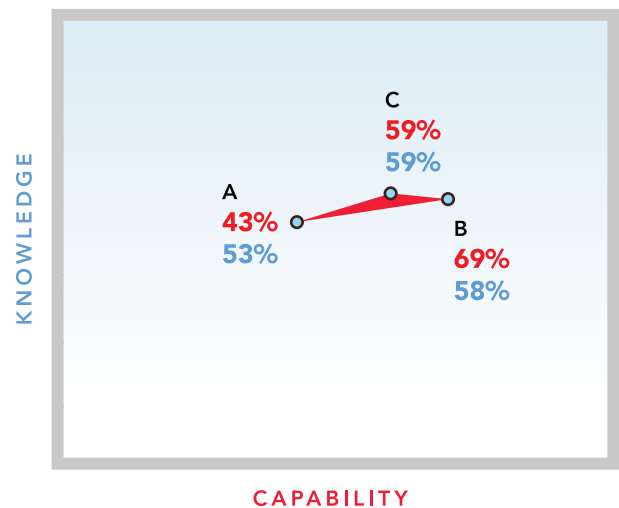
RISK RELEVANCE



Source: See Figure 10

As regulators, investors, and the public demand stronger board oversight, boards place greater reliance on the information they are provided for decision making. This risk examines whether boards are receiving complete, timely, transparent, accurate, and relevant information.

A: CAE B: BOARD C: C-SUITE



RISK STAGE



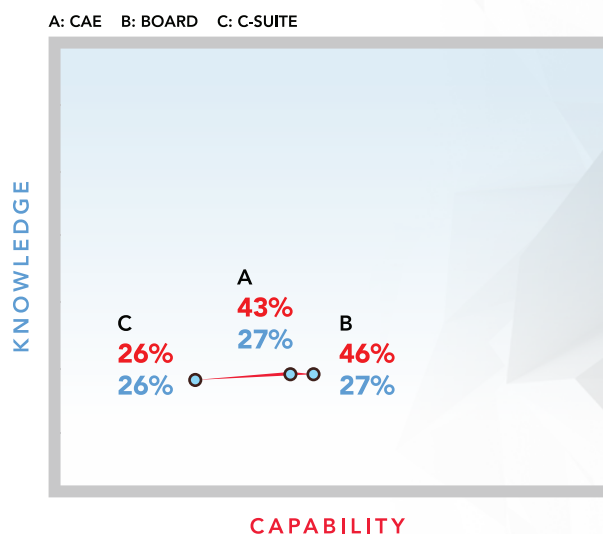
THE RISKS

DATA ETHICS

Sophistication of the collection, analysis, and use of data is expanding exponentially, complicated by artificial intelligence. This risk examines organizational conduct and the potential associated reputational and financial damages for failure to establish proper data governance.

Gap Analysis:

While the concept of risk related to data ethics is relatively new, CAEs predict that its relevance will grow rapidly over the next five years. The board and CAEs are somewhat more optimistic about their organizations' capability to manage risks related to data ethics; however, all parties are aligned in their perspective that they lack significant knowledge on the risks. As the regulatory environment around data ethics evolves, all parties certainly must expand their knowledge of this risk.



Actions:

Board: Ensure that management has established and communicated expectations around how it will ethically collect, store, and use data consistent with the values and strategies established by the board.

C-suite: Establish expectations and limitations for how data can be used by the organization to ensure that data usage is consistent with the ethical values of the organization. Consider processes to monitor that organizational use of data is consistent with communicated expectations.

CAE: Take a leadership role in educating stakeholders, including the C-suite and board, on risks related to data ethics. Encourage management to develop guideposts that are aligned with the organization's risk tolerance related to the use of data. Provide assurance around adherence to established guideposts.

RISK STAGE



RISK RELEVANCE



Source: See Figure 10

THE RISKS

SUSTAINABILITY (ESG)

Gap Analysis:

Executive management, board members, and CAEs assess their knowledge about the risks related to this relatively new and growing category as fairly limited, with senior management leading the parties in self-reported awareness and CAEs trailing 14 points behind them. The three groups are relatively aligned in their perception that their organizations' capabilities are low. This triangle depicts the organization's risk knowledge and capability moving from the *Recognize* stage into the *Explore* stage of the Risk Stages Model.

Actions:

Board: Seek additional sources of information regarding risks related to sustainability and board member responsibilities. Set expectations regarding management's responsibility to brief the board on emerging risks, organizational weaknesses, and actions being taken to remedy weaknesses.

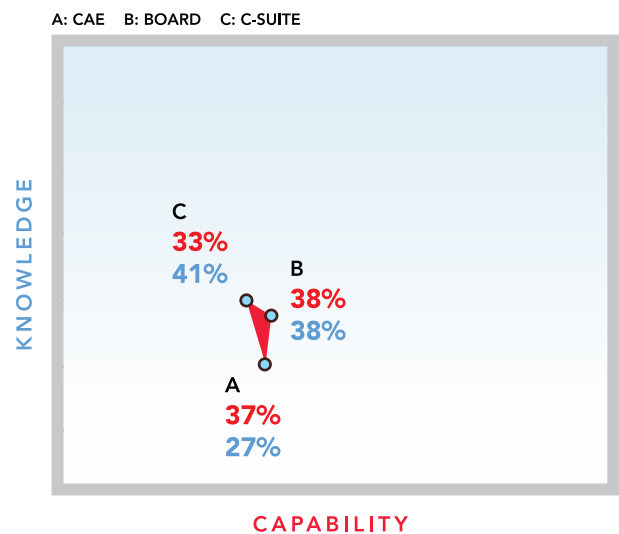
C-suite: Seek expert advice regarding actions that management can take to reduce sustainability risks and identify best practices. Set a positive tone within the organization regarding the role it takes in providing sustainable value.

CAE: Take a leadership role by becoming more educated and sharing perspectives on risks related to sustainability across the organization. Seek feedback from the C-suite and board regarding internal audit's role in evaluating and recommending best practices related to sustainability.

RISK RELEVANCE



The growth of environmental, social, and governance (ESG) awareness increasingly influences organizational decision making. This risk examines organizations' abilities to establish strategies to address long-term sustainability issues.



RISK STAGE



Source: See Figure 10

FIGURES

Figure 1 – Personal Knowledge/Organizational Capability Graph

Source: The Institute of Internal Auditors

Figure 2 – Quadrant Graph

Source: The Institute of Internal Auditors

Figure 3 – Risk Stages Model

Source: The Institute of Internal Auditors

Figure 4 – Stages of Risk Explanation

Source: The Institute of Internal Auditors

Figure 5 – Organizational Risk Capability: Board and C-suite Perceptions

Source: OnRisk 2020 qualitative interviews. Question: How capable is your company when it comes to handling each of the following risks? Combined percentage for scores of 6 or 7, with 7 being the highest level. $n = 26$ for board. $n = 27$ for executive management.

Figure 6 – Organizational Capability for 11 Risks Plotted on the Risk Stages Model

Source: OnRisk 2020 qualitative interviews. Question: How capable is your company when it comes to handling each of the following risks? Each of the plot points represents one of the 11 risks. Combined percentage for scores of 6 or 7 is reported, with 7 being the highest level. Risk stages are 1–Recognize (r), 2–Explore (e), 3–Develop (d), 4–Maintain (m). $n = 26$ for board. $n = 27$ for executive management. $n = 30$ for CAEs.

Figure 7a (top) and 7b (bottom) – Risk Knowledge and Capability: Alignment Among Board, C-suite, and CAEs

Source: OnRisk 2020 qualitative interviews. Questions: How knowledgeable are you about each of the following risks? How capable is your company when it comes to handling each of the following risks? Combined percentage for scores of 6 or 7 is reported, with 7 being the highest level. $n = 26$ for board. $n = 27$ for executive management. $n = 30$ for CAEs.

Figure 8 – Systematic Approach to Risk Industry Comparison

Source: OnRisk 2020 quantitative survey of CAEs. Question 8: Does your organization have a systematic approach to identifying and monitoring risks? The percentage of “yes” is reported. $n = 630$.

Figure 9 – Personal Risk Knowledge Risk Relevance Comparison

Source: OnRisk 2020 quantitative survey of CAEs. Question 1: How knowledgeable are you about each of the following risks? Question 2: How relevant are each of the following risks to your current organization? Combined percentage for scores of 6 or 7 is reported, with 7 being the highest level. $n = 630$.

Figure 10 – Risk Relevance for 11 Risks

Source: OnRisk 2020 quantitative survey of CAEs. Question 2: How relevant are each of the following risks to your current organization? Question 3: How relevant do you think each of the following risks will be in the next five years? Combined percentage for scores of 6 or 7 is reported, with 7 being the highest level. Those who chose not applicable/not sure for the risk rating were excluded from the calculation of the percentages. $n = 630$.



About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Disclaimer

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright

Copyright © 2019 The Institute of Internal Auditors, Inc. All rights reserved. For permission to reproduce, please contact copyright@theiia.org.

Global Headquarters

The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.globaliia.org



**The Institute of
Internal Auditors**
