Enlarged Ogdensburg City School District

Risk Assessment Update

Targeted Risk Assessment Results

2020

Executive Summary

Objectives:

- Update the District's risk assessment.
- Identify areas to perform targeted procedures based on input from management and our risk assessment.

Risk Assessment Process:

- Updated our understanding of the District and its operations.
- Interviewed various members of the Management team.
- Performed data analytics.

Targeted Area Recommendations – IT/Cyber Security:

- Policies should be updated and published on the District's website.
- Create a formal, current Acceptable Use Policy (AUP*)* and develop a system for monitoring compliance.
- Include a written declaration of duties and responsibilities in BOCES contracts.
- Ensure that all users of District data and technology equipment are subject to the District's policies.
- Develop policies for use and storage of flash drives and similar devices.
- Ensure that all users with access to District computers have training in safe computer usage. Perform periodic tests to see that users are following the training.
- Develop a password strength and protection policy.
- Consider using an electronic password program to store and safeguard passwords.
- Appoint a deputy District Treasurer to conduct online banking when the District Treasurer is not available. If that is not possible, develop and implement a strategy to limit the need for online banking when the District Treasurer is not on duty.
- Perform periodic, but at least annual reviews of the network user list and deactivate users as necessary.
- Adopt policies limiting the use of "generic" user accounts.

General Recommendations

- Review purchasing practices to ensure that POs are obtained in a timely manner for all required purchases.

Objectives

The objectives of this engagement are to complete a risk assessment for Enlarged Ogdensburg City School District for 2020. We used accounting and other data from July 1, 2018 through January 24, 2020 in the development of the risk assessment. This risk assessment will identify systems with the greatest risk to the District and make recommendations for the testing of the systems based upon a prioritized list of identified risks. It should be read with a working knowledge of the previous risk assessments.

The objective of the internal auditing program is to furnish management and the Board of Education with independent analysis, appraisals, recommendations and pertinent comments concerning the adequacy, effectiveness and efficiency of the systems of internal control, the quality of ongoing operations and internal compliance with rules and regulations.

Scope and Methodology

The main focuses of our efforts were to update our understandings from previous reports and assess the targeted area of IT/Cyber Security controls.

During our work we met with and interviewed various District personnel employed in a variety of areas including the business office, cafeteria, information technology, grants management and administration. We reviewed various documents as we considered necessary.

After analyzing the results of our work, we have prepared this report to inform the Board of Education and management of our findings and to present our prioritized list of assessed risk. Throughout the report we have made recommendations for improvements of identified weaknesses.

Audit Prioritization and Selection

The objective of the risk assessment process is to identify and prioritize areas posing the greatest risk and liability to the District. In order to obtain a priority listing, a risk approach was used to rank each of the areas.

There are at least three kinds of risk that should be considered in the risk assessment process. These risks are as follows:

Incentives or Pressures

Incentives or pressures placed on or perceived by management and/or employees often provide them with a reason to intentionally misstate financial information or misappropriate assets. In school districts, this risk may relate to excessive emphasis on meeting the budget, rumors of layoffs or the perception of being overworked and under compensated. Incentives and pressures can also arise from personal problems such as illness, debts or addictions. In our current economic environment, there is significant incentive/pressure to provide the same services using "alternate" means. In other words circumvent the budget by inappropriately coding expenditures to codes with available budget amounts, using students to raise funds for District functions or by soliciting outside donations or grants without proper Board of Education approval and oversight.

This could change significantly with the advent of the COVID 19 crisis. Future budgets may see considerably more cuts and changes. As a result of the shutdowns, IT and other controls may be subject to increased override and circumvention.

Opportunity

Circumstances existing within an entity can provide the opportunity for misstatement of financial information or misappropriation of assets. Such opportunities can arise from concentration of management in a few individuals, weak Board oversight, poor segregation of duties, or unusual or complex transactions.

Rationalization or Attitude

The attitudes, character, or ethical values of employees may allow them to rationalize misappropriations or financial statement misstatements. They may rationalize that they are paid less than others or that the District can afford it. The Board may set a tone by not implementing corrective actions to audit findings, or management may desire to artificially justify specific programs.

From our discussions with District personnel and our other work, as more fully described later in the report, we did not identify any predominant incentives or rationalizations. The budget has passed for the past several years. However, due to the recent COVID 19 crisis there is increased uncertainty related to the timing and anticipated amounts of state aid. This may affect future risk assessments. There are contracts in place for management and the unions. Employees do not seem to be overburdened with work and the pay scale is comparable to other local Districts.

The overall control environment, consisting of the integrity, ethical values and competence of the administrators and key accounting personnel appears to be strong.

District personnel were interested in the risk assessment process, and were helpful and cooperative in explaining their duties and providing requested documents. The Board and management have set an ethical tone for the District. There appears to be adequate Board oversight.

In the course of our work, it would be difficult to identify personal problems of a specific District employee, but we were not made aware of any such situation.
We deemed the following to be key systems for analysis:

- Cash Receipts/Revenues
- Cash Disbursements/Expenditures
- Internal Claims Auditor
- Payroll
- Extraclassroom
- Grants Management
- Management Override

- Financial Reporting
- Technology
- Fixed Assets
- Cafeteria
- Transportation

The following will describe the work we performed on each area, weaknesses and recommendations, and an overall conclusion as to risk.

Cash Receipts/Revenues

Key things to consider in revenue risk assessment are the over reporting of revenue and misappropriation of funds. In school districts, this is not a major issue since a majority of the revenue comes from state aid and property taxes. The revenue from state aid can be readily verified from reports obtained by the State Education Department so it is not easily misstated. Also, these funds are obtained by periodic large checks and wire transfers, so there is not a significant risk of cash being misappropriated.

School taxes are collected by the tax collector. The revenue from school taxes can be matched to the tax levy so overstatement is unlikely. Further, individual taxpayers serve as a checks and balances for misappropriation of tax collections since the City would notify taxpayers if their payments were not properly credited. We consider the risk of significant misappropriation of school tax collections to be low.

We did not notice any incentives or pressures on staff to over report revenue, nor did we notice any misguided attitudes in this area. Based on our analysis, we have assessed the risk over cash receipts/revenues to be moderate.

Controls over grant funding and cafeteria sales will be discussed and evaluated in later sections.

Cash Disbursements/Expenditures (Appendix 1 & 2)

We updated our understanding of these processes. We also used the following data analysis techniques to assist in reviewing this area:

- We reviewed the audit trail for internal control inconsistencies. None were noted.
- We reviewed the audit trail and determined that the Purchasing Agent was the only staff member approving POs in the system.
- We reviewed payment transaction data to determine whether payments were properly supported by POs.

We reviewed the results of the analysis (Appendix 1 & 2) and observed the following:

- There were 54 payments w/o POs
- In 2019 there were 16 payments dated prior to PO date
- In 2019 there were 7 Payments dated 0-5 days of PO date

- In 2019 there were 26 Payments dated 0-15 days of PO date

These results are less positive than the prior year, however considering the number of payments made do not appear to be a serious concern. However, we recommend that management and the purchasing agent review the results and determine if remedial action is necessary to prevent this from becoming an issue.

The charts in Appendix 2 show the activities for the 2019 school year. The months shown in the chart correspond to calendar months, ie 12 = December.

After considering the policies, controls and our findings, we have deemed the risk surrounding cash disbursements/expenditures to be moderate. While we did note some segregation of duties and access issues, providing opportunity, there are mitigating controls in place that would minimize the potential for misappropriation.

Internal Claims Auditor (ICA)

In prior audits we interviewed the internal claims auditor, documented our understanding of the procedures followed, reviewed some approved documents, and reviewed the Board's Policy Manual as part of our assessment of the internal claims auditor. We noted that the ICA has received formal training. She provided us with copies of her reports to the Board of Education which we reviewed.

The internal claims auditor performs one of the most crucial aspects of monitoring a school district's financial accounting system. As such, the internal claims auditor should be familiar with legal requirements associated with school district purchases (i.e. bidding rules), and Board policies. During our prior interviews with the internal claims auditor, she indicated that she reviews claims to verify conformity with Board travel policies and legal or contractual requirements, such as price quotes or bidding. In our previous audits, she said that she does not review investments made to determine if they conform to Board policy.

Based on our review of the internal claims auditor area, we have assigned a risk assessment of moderate to this area.

Payroll (Appendix 3)

We updated our understanding of these processes via electronic review, see Appendix 3.

We have deemed the risk surrounding payroll to be high. While there are the same deficiencies noted in the cash disbursement area, in the payroll area the mitigating controls are not in place. The segregation of duties issues coupled with weak monitoring, computer access, and other control issues leads to increased risk.

Extraclassroom

This area was reviewed in depth in prior reports.

We consider the extraclassroom activities to be a high risk area because it involves cash, student funds and the previously discussed conditions. As such it should be considered for a more in-depth review in the next internal audit cycle.

Grants Management

Since grant management and compliance are becoming increasingly important issues, it is vital that both coordinators and members of the business office stay up-to-date with the requirements related to the grants.

We assess the risk over grant management to be moderate. The Shared Business Manager is responsible for the financial component of grants management. Personnel appear to have a good understanding of individual grant requirements, and they are performing some monitoring procedures.

Management Override

One of the presumptions in risk assessment is the presence of management override. We considered management override to be the ability of administrators to circumvent intended policies and procedures, and also administrators' ability to circumvent laws and regulations for which there is no direct District policy or procedure.

Another example of management override is fraudulent financial reporting. This includes the intentional misstatement of information, either through the commission of acts or the omission of facts through such means as manipulation, falsification or alteration of accounting records, intentional misapplication of accounting principles, or omission of significant information.

There were no significant changes noted in this area.

We have determined that there is a high risk associated with management override. The risk is higher at the building level than for financial statement reporting. It is possible for the District budget to be circumvented by teachers and administrators by requiring student funding. It is also possible for teachers and administrators to otherwise circumvent policies and procedures. This may be at an increased risk in the COVID 19 environment. In our judgment, the effect of these overrides to the District is of high risk in relation to the other areas studied.

Financial Reporting

In general we feel that the Board of Education is being provided accurate and timely information regarding cash balances and transactions. We rate the risk assessment surrounding financial reporting to be moderate.

Information Technology and Cyber Security (Appendices 1 and 4)

Access control is an extremely important component of internal controls. Improper computer access privileges can negate effective internal controls and physical segregation of duties. Furthermore, it may make sensitive information accessible to individuals to whom it should not be available. It is important that management review all computer access privileges on a periodic basis. They should keep the employees' duties and the desired internal control structure in mind as they perform the review. They should make sure that privileges do not circumvent physical segregation of duties and that viewing privileges are granted only to employees that really need the information. The timing and frequency of these reviews should be included in written responsibilities in the BOCES contract.

The District should also consider looking into the access issues, password policies, training and other IT/Cyber Security issues that were discussed in previous risk assessments and Appendices 1 and 4.

Because of its far-reaching effect on every facet of the District's operations, we would rate the risk over technology to be high. (See Appendix 4) This area was selected for additional targeted procedures.

The charts in Appendix 1 show the WinCap user activities from 7/1/18 to 1/24/20.

Fixed Asset Inventory

We did not perform any procedures in this area.

Food Service

No significant changes were noted in this area. We have deemed the risk over the cafeteria to be moderate. The manager is knowledgeable about these regulations. The relative magnitude of any probable misappropriation in this area is low in relation to the financial statements as a whole. See Appendix 4 for discussions related to NutriKids passwords.

Transportation and Buildings & Grounds

The District outsources its transportation program. This significantly reduces the risk in this area.

Adequate systems appear to be in place and operating effectively. There is not a large inventory of parts on hand to be misappropriated for personal use. Our risk assessment for the transportation area is low.

Risk Assessment Summary

Based on the above analyses, we have ranked the systems as high risk (H), moderate risk (M) or low risk (L):

	2020
Cash Receipts/Revenues	M
Cash Disbursements/Expenditures	M
Internal Claims Auditor	M
Payroll	H
Extraclassroom	H
Grants Management	M
Management Override	H
Financial Reporting	M
Information Technology/Cyber Security	H
Fixed Assets	L
Cafeteria	L
Transportation	L

It is also important for the Board and management to keep in mind the District's strengths that help to mitigate some of the issues discussed previously. Management and members of the business office are interested and want to improve internal controls and operating systems. Building principals are involved in the budgeting and purchasing process and are starting to use WinCap to monitor their budgets and related expenditures.

The Board of Education is ultimately responsible for the safeguarding of District assets. The Board meets this responsibility by establishing a structure of internal controls designed to prevent or detect errors and irregularities. It is the Board's duty to make certain that established controls are appropriately designed and operating effectively.

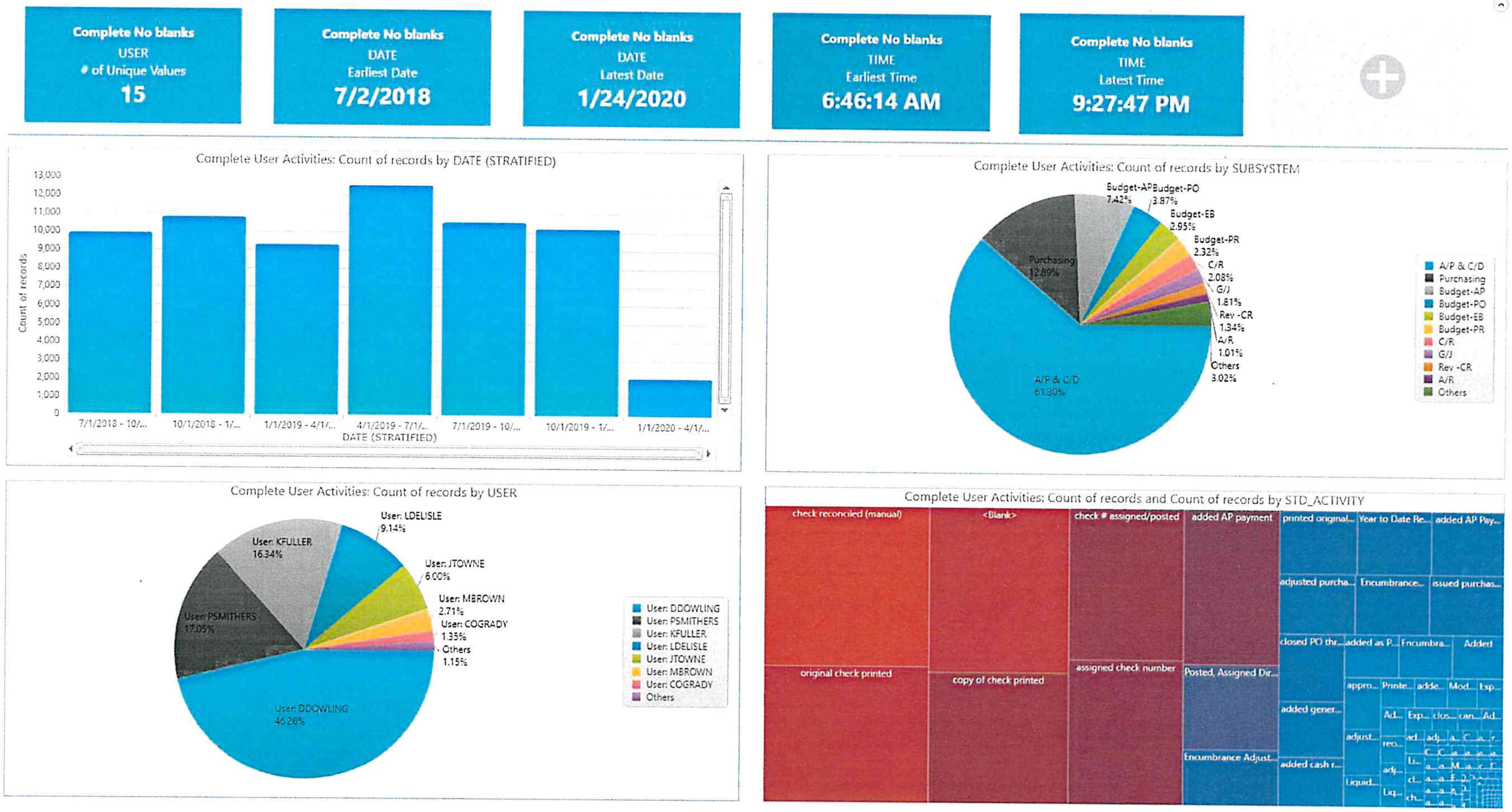
Based on our risk assessment process and discussions with Management, IT Controls was selected for a targeted review.

Based upon our findings and risk assessment, the Board must decide how and when to implement our recommendations, and which areas it chooses to target for further testing. We are available to help the Board establish timelines for corrective action, and to make recommendations on specific testing procedures to be performed during the next phase in the internal audit process.

Appendix 1
Information Technology Procedures

We obtained the user activity reports from July 1, 2018 to January 24, 2020. We performed the following procedures:

- We appended all of the individual activity reports into one master report.
- We reviewed the activity reports for indications of usages that are inconsistent with internal controls. No significant issues were noted.



Complete No blanks
USER
# of Unique Values
15

Complete No blanks
DATE
Earliest Date
7/2/2018

Complete No blanks
DATE
Latest Date
1/24/2020

Complete No blanks
TIME
Earliest Time
6:46:14 AM

Complete No blanks
TIME
Latest Time
9:27:47 PM

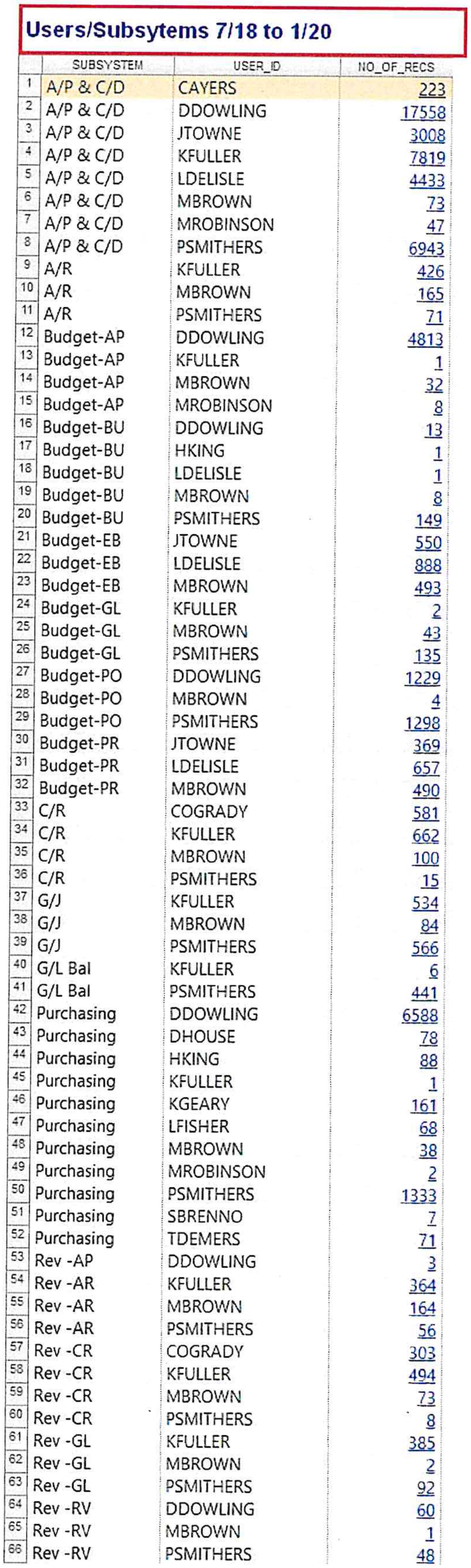
Complete User Activities: Count of records by DATE (STRATIFIED)

Complete User Activities: Count of records by SUBSYSTEM

Complete User Activities: Count of records by USER

Complete User Activities: Count of records and Count of records by STD_ACTIVITY

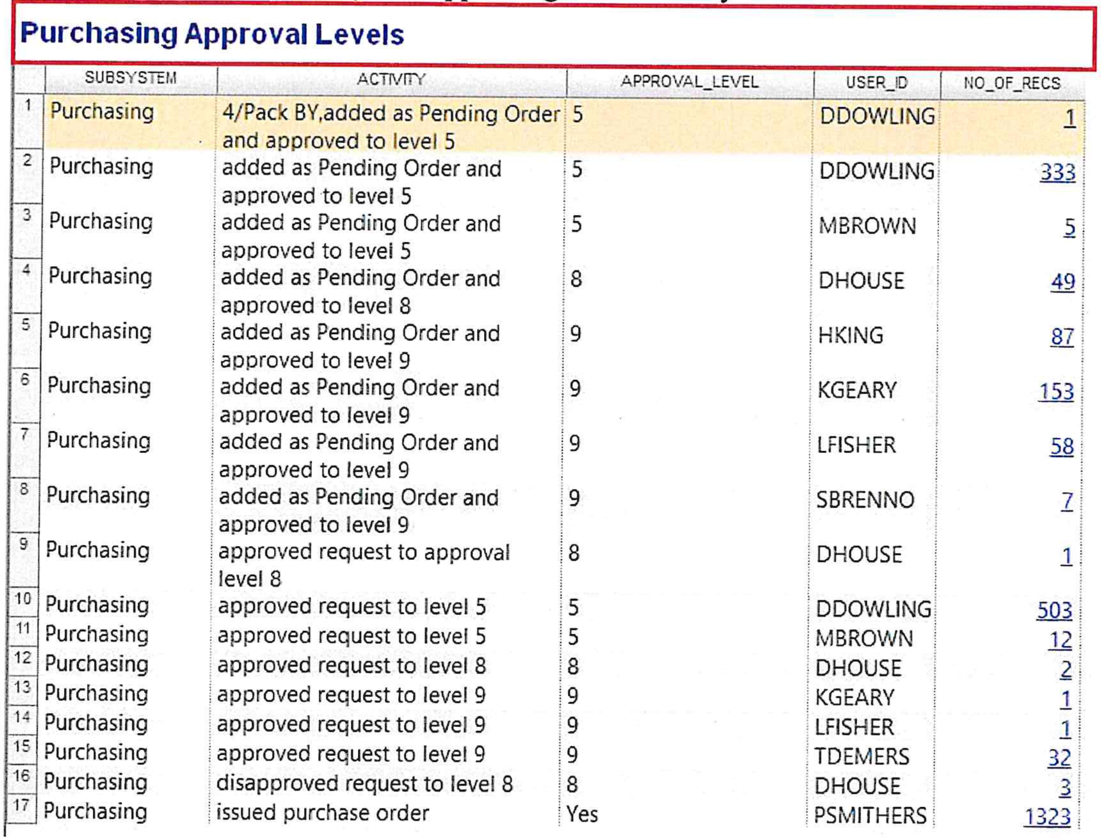
Appendix 1
Information Technology Procedures



Users/Subsytems 7/18 to 1/20

	SUBSYSTEM	USER_ID	NO_OF_RECS
1	A/P & C/D	CAYERS	223
2	A/P & C/D	DDOWLING	17558
3	A/P & C/D	JTOWNE	3008
4	A/P & C/D	KFULLER	7819
5	A/P & C/D	LDELISLE	4433
6	A/P & C/D	MBROWN	73
7	A/P & C/D	MROBINSON	47
8	A/P & C/D	PSMITHERS	6943
9	A/R	KFULLER	426
10	A/R	MBROWN	165
11	A/R	PSMITHERS	71
12	Budget-AP	DDOWLING	4813
13	Budget-AP	KFULLER	1
14	Budget-AP	MBROWN	32
15	Budget-AP	MROBINSON	8
16	Budget-BU	DDOWLING	13
17	Budget-BU	HKING	1
18	Budget-BU	LDELISLE	1
19	Budget-BU	MBROWN	8
20	Budget-BU	PSMITHERS	149
21	Budget-EB	JTOWNE	550
22	Budget-EB	LDELISLE	888
23	Budget-EB	MBROWN	493
24	Budget-GL	KFULLER	2
25	Budget-GL	MBROWN	43
26	Budget-GL	PSMITHERS	135
27	Budget-PO	DDOWLING	1229
28	Budget-PO	MBROWN	4
29	Budget-PO	PSMITHERS	1298
30	Budget-PR	JTOWNE	369
31	Budget-PR	LDELISLE	657
32	Budget-PR	MBROWN	490
33	C/R	COGRADY	581
34	C/R	KFULLER	662
35	C/R	MBROWN	100
36	C/R	PSMITHERS	15
37	G/J	KFULLER	534
38	G/J	MBROWN	84
39	G/J	PSMITHERS	566
40	G/L Bal	KFULLER	6
41	G/L Bal	PSMITHERS	441
42	Purchasing	DDOWLING	6588
43	Purchasing	DHOUSE	78
44	Purchasing	HKING	88
45	Purchasing	KFULLER	1
46	Purchasing	KGEARY	161
47	Purchasing	LFISHER	68
48	Purchasing	MBROWN	38
49	Purchasing	MROBINSON	2
50	Purchasing	PSMITHERS	1333
51	Purchasing	SBRENNO	7
52	Purchasing	TDEMERS	71
53	Rev -AP	DDOWLING	3
54	Rev -AR	KFULLER	364
55	Rev -AR	MBROWN	164
56	Rev -AR	PSMITHERS	56
57	Rev -CR	COGRADY	303
58	Rev -CR	KFULLER	494
59	Rev -CR	MBROWN	73
60	Rev -CR	PSMITHERS	8
61	Rev -GL	KFULLER	385
62	Rev -GL	MBROWN	2
63	Rev -GL	PSMITHERS	92
64	Rev -RV	DDOWLING	60
65	Rev -RV	MBROWN	1
66	Rev -RV	PSMITHERS	48

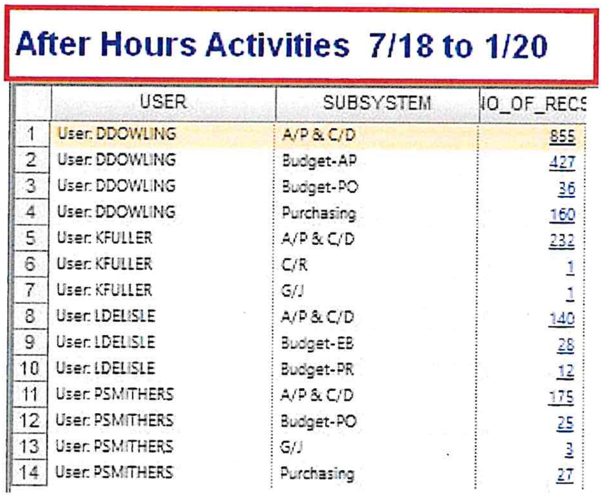
- We reviewed the activity reports for indications that purchase orders were being approved by someone other than the purchasing agent. It appears that the purchasing agent is the only one approving POs in the system.



Purchasing Approval Levels

	SUBSYSTEM	ACTIVITY	APPROVAL_LEVEL	USER_ID	NO_OF_RECS
1	Purchasing	4/Pack BY,added as Pending Order and approved to level 5	5	DDOWLING	1
2	Purchasing	added as Pending Order and approved to level 5	5	DDOWLING	333
3	Purchasing	added as Pending Order and approved to level 5	5	MBROWN	5
4	Purchasing	added as Pending Order and approved to level 8	8	DHOUSE	49
5	Purchasing	added as Pending Order and approved to level 9	9	HKING	87
6	Purchasing	added as Pending Order and approved to level 9	9	KGEARY	153
7	Purchasing	added as Pending Order and approved to level 9	9	LFISHER	58
8	Purchasing	added as Pending Order and approved to level 9	9	SBRENNO	7
9	Purchasing	approved request to approval level 8	8	DHOUSE	1
10	Purchasing	approved request to level 5	5	DDOWLING	503
11	Purchasing	approved request to level 5	5	MBROWN	12
12	Purchasing	approved request to level 8	8	DHOUSE	2
13	Purchasing	approved request to level 9	9	KGEARY	1
14	Purchasing	approved request to level 9	9	LFISHER	1
15	Purchasing	approved request to level 9	9	TDEMERS	32
16	Purchasing	disapproved request to level 8	8	DHOUSE	3
17	Purchasing	issued purchase order	Yes	PSMITHERS	1323

- We looked for activity on unusual dates or times. (Before or after hours or weekends) We reviewed the activities and did not have any significant concerns.

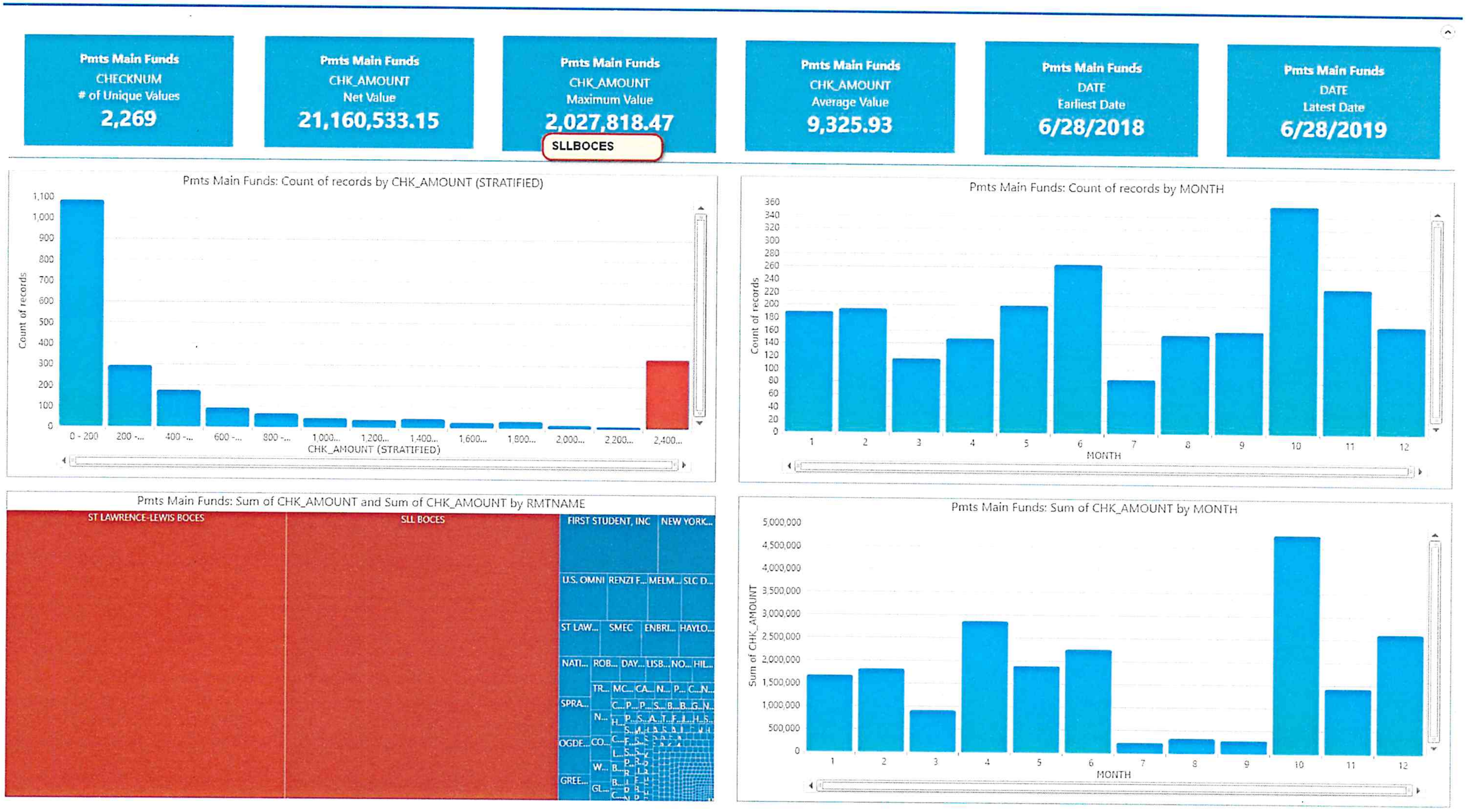


After Hours Activities 7/18 to 1/20

	USER	SUBSYSTEM	IO_OF_RECS
1	User: DDOWLING	A/P & C/D	855
2	User: DDOWLING	Budget-AP	427
3	User: DDOWLING	Budget-PO	36
4	User: DDOWLING	Purchasing	160
5	User: KFULLER	A/P & C/D	232
6	User: KFULLER	C/R	1
7	User: KFULLER	G/J	1
8	User: LDELISLE	A/P & C/D	140
9	User: LDELISLE	Budget-EB	28
10	User: LDELISLE	Budget-PR	12
11	User: PSMITHERS	A/P & C/D	175
12	User: PSMITHERS	Budget-PO	25
13	User: PSMITHERS	G/J	3
14	User: PSMITHERS	Purchasing	27

- WinCap does not provide activity reports for users' activities in the system module, so we were not able to review changes in user permissions.

Appendix 2
Payments and Purchasing Procedures



Pmts Main Funds
CHECKNUM
# of Unique Values
2,269

Pmts Main Funds
CHK_AMOUNT
Net Value
21,160,533.15

Pmts Main Funds
CHK_AMOUNT
Maximum Value
2,027,818.47
SLLBOCES

Pmts Main Funds
CHK_AMOUNT
Average Value
9,325.93

Pmts Main Funds
DATE
Earliest Date
6/28/2018

Pmts Main Funds
DATE
Latest Date
6/28/2019

Pmts Main Funds: Count of records by CHK_AMOUNT (STRATIFIED)

Pmts Main Funds: Count of records by MONTH

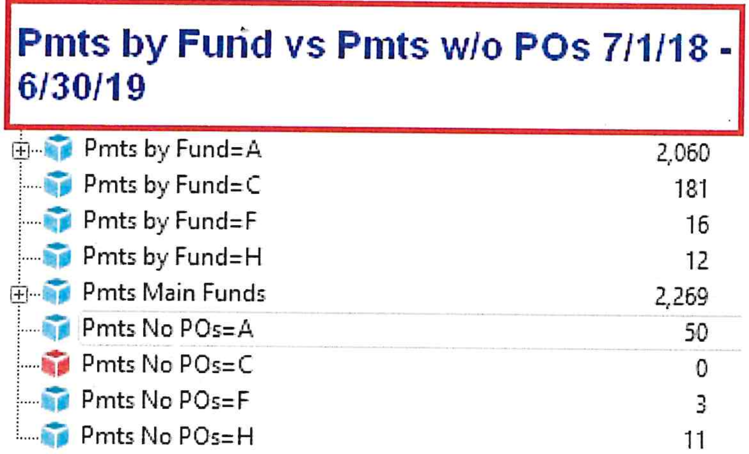
Pmts Main Funds: Sum of CHK_AMOUNT and Sum of CHK_AMOUNT by RMTNAME

Pmts Main Funds: Sum of CHK_AMOUNT by MONTH

Appendix 2
Payment and Purchasing Procedures

We performed an analysis designed to review the effectiveness of the District's use of purchase orders. The analysis indicates that the District is fairly effective in its use of purchase orders. In prior audits we had noted several types of payments where purchase orders had not been used and discussed them with the Purchasing Agent, who indicated that he would look into expanding the use of purchase orders. The number of payments without associated POs had reduced in prior years but appears to be rising. The purchasing agent should consider requiring the use of POs for all appropriate expenditures. The District should review these items and take steps to ensure that POs are obtained for all purchases as required.

The following chart shows the number of payments by fund and the number of payments by fund that were not related to a PO.



Pmts by Fund vs Pmts w/o POs 7/1/18 - 6/30/19

Pmts by Fund=A	2,060
Pmts by Fund=C	181
Pmts by Fund=F	16
Pmts by Fund=H	12
Pmts Main Funds	2,269
Pmts No POs=A	50
Pmts No POs=C	0
Pmts No POs=F	3
Pmts No POs=H	11

Examples of types of payments not associated with POs.

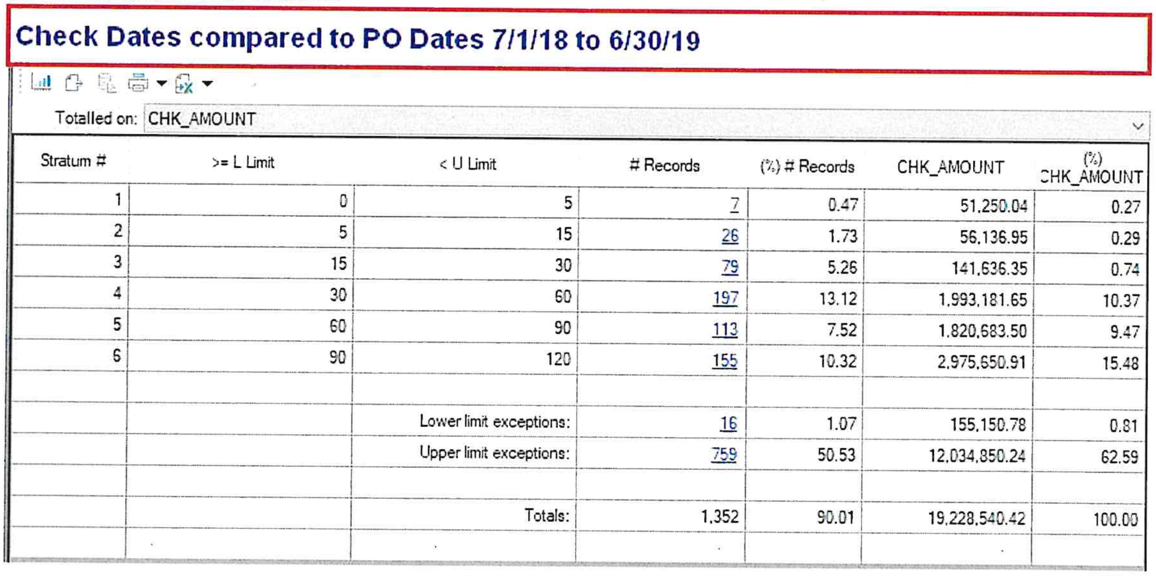
A – Legal, transfers, food service invoices

C - None

F –SLL BOCES, Teacher's Desk Consultants and PLC Associates

H - Architects, and, contractors

The following is an analysis of the time differential between when a check is written and the related PO was issued.



Check Dates compared to PO Dates 7/1/18 to 6/30/19

Totalled on: CHK_AMOUNT

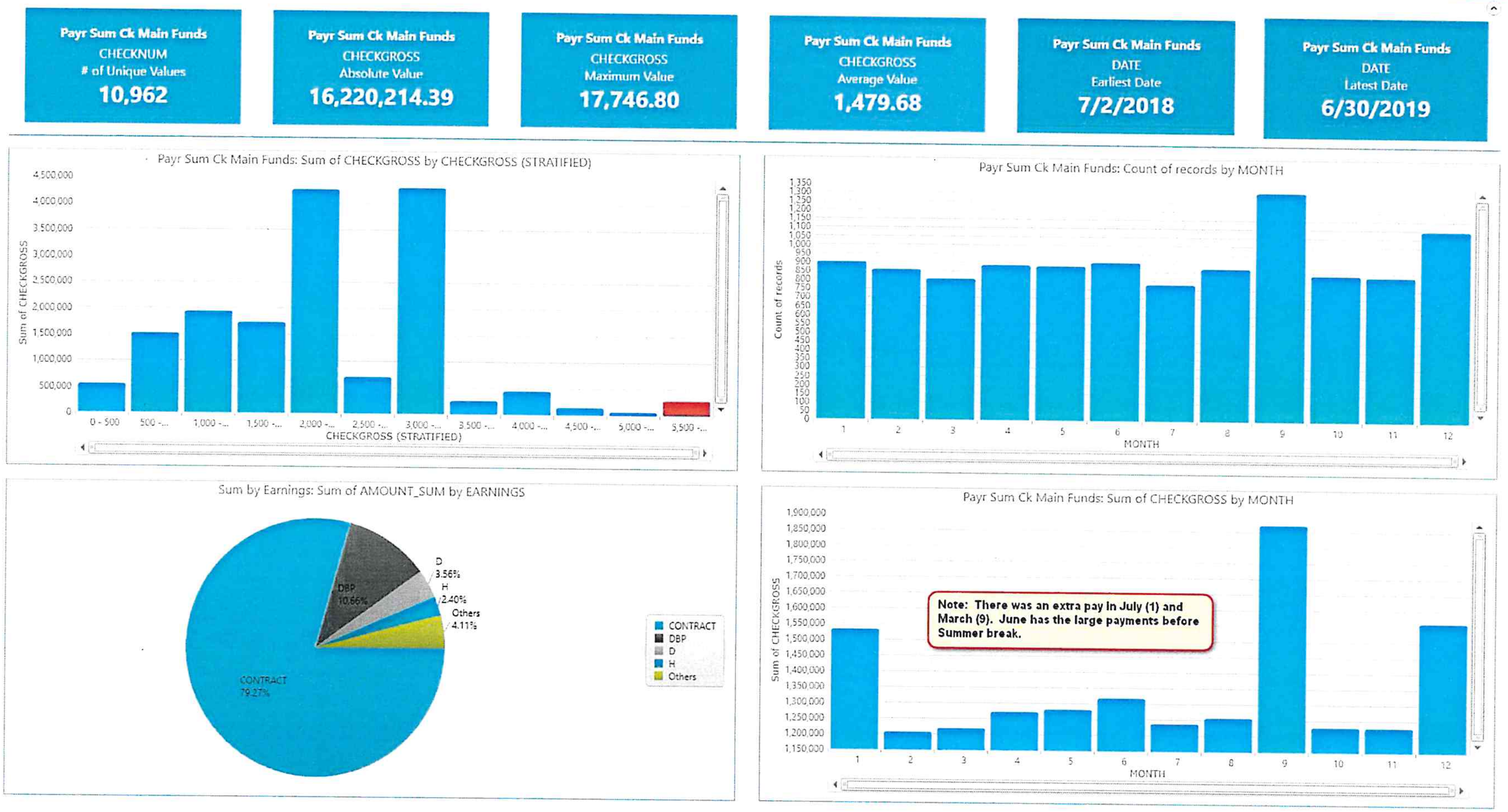
Stratum #	>= L Limit	< U Limit	# Records	(%) # Records	CHK_AMOUNT	(%) CHK_AMOUNT
1	0	5	7	0.47	51,250.04	0.27
2	5	15	26	1.73	56,136.95	0.29
3	15	30	79	5.26	141,636.35	0.74
4	30	60	197	13.12	1,993,181.65	10.37
5	60	90	113	7.52	1,820,683.50	9.47
6	90	120	155	10.32	2,975,650.91	15.48
		Lower limit exceptions:	16	1.07	155,150.78	0.81
		Upper limit exceptions:	759	50.53	12,034,850.24	62.59
		Totals:	1,352	90.01	19,228,540.42	100.00

Appendix 2
Payment and Purchasing Procedures

Generally, there should not be many payments with a very short time between the issuance of a PO and the payment. A very short interval for large numbers of transactions could be indicative of an deficient purchasing system where approvals are rushed, there is a log jam in the process or staff are not properly planning their purchases.

Appendix 3
Payroll Procedures

This chart gives an overview of the payroll data for the 2019 school year. Note that the months are calendar months and not the school's fiscal months.



Payr Sum Ck Main Funds
CHECKNUM
# of Unique Values
10,962

Payr Sum Ck Main Funds
CHECKGROSS
Absolute Value
16,220,214.39

Payr Sum Ck Main Funds
CHECKGROSS
Maximum Value
17,746.80

Payr Sum Ck Main Funds
CHECKGROSS
Average Value
1,479.68

Payr Sum Ck Main Funds
DATE
Earliest Date
7/2/2018

Payr Sum Ck Main Funds
DATE
Latest Date
6/30/2019

Payr Sum Ck Main Funds: Sum of CHECKGROSS by CHECKGROSS (STRATIFIED)

Payr Sum Ck Main Funds: Count of records by MONTH

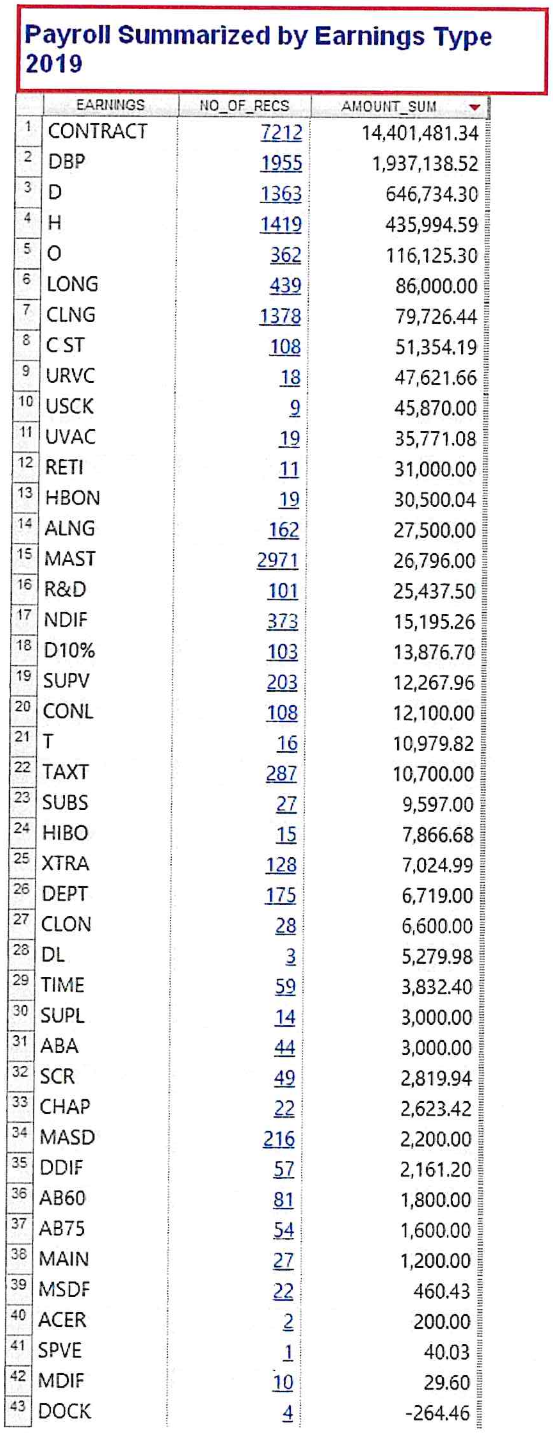
Sum by Earnings: Sum of AMOUNT_SUM by EARNINGS

Payr Sum Ck Main Funds: Sum of CHECKGROSS by MONTH

Note: There was an extra pay in July (1) and March (9). June has the large payments before Summer break.

Appendix 3
Payroll Procedures

Most schools use codes in the payroll system to identify various types of payroll payments to employees. The following table is a summary of payroll payments by code. The blank codes at the top are contractual payments. The table provides a good overview of the types of payroll payments the District is making to its employees.



Payroll Summarized by Earnings Type 2019

	EARNINGS	NO_OF_RECS	AMOUNT_SUM
1	CONTRACT	7212	14,401,481.34
2	DBP	1955	1,937,138.52
3	D	1363	646,734.30
4	H	1419	435,994.59
5	O	362	116,125.30
6	LONG	439	86,000.00
7	CLNG	1378	79,726.44
8	C ST	108	51,354.19
9	URVC	18	47,621.66
10	USCK	9	45,870.00
11	UVAC	19	35,771.08
12	RETI	11	31,000.00
13	HBON	19	30,500.04
14	ALNG	162	27,500.00
15	MAST	2971	26,796.00
16	R&D	101	25,437.50
17	NDIF	373	15,195.26
18	D10%	103	13,876.70
19	SUPV	203	12,267.96
20	CONL	108	12,100.00
21	T	16	10,979.82
22	TAXT	287	10,700.00
23	SUBS	27	9,597.00
24	HIBO	15	7,866.68
25	XTRA	128	7,024.99
26	DEPT	175	6,719.00
27	CLON	28	6,600.00
28	DL	3	5,279.98
29	TIME	59	3,832.40
30	SUPL	14	3,000.00
31	ABA	44	3,000.00
32	SCR	49	2,819.94
33	CHAP	22	2,623.42
34	MASD	216	2,200.00
35	DDIF	57	2,161.20
36	AB60	81	1,800.00
37	AB75	54	1,600.00
38	MAIN	27	1,200.00
39	MSDF	22	460.43
40	ACER	2	200.00
41	SPVE	1	40.03
42	MDIF	10	29.60
43	DOCK	4	-264.46

Appendix 4
IT Security

IT/Cyber Security controls are critical elements the District's control structure. IT impacts almost every aspect of the District's operations. A failure in IT controls/security could have a far reaching negative impact. Anything from student/staff personal private and sensitive information (PPSI) to financial reporting, banking and cash could be impacted. This is becoming increasingly important as many educational and management functions are or may be performed offsite due to the nationwide shutdown. At the time the audit was conducted the District was still in normal operations, therefore the audit did not consider the impacts of COVID 19. But it is mentioned to illustrate the importance of this area. This is also an area which has recently been the subject of NYS OSC audits. OSC considers cyber security and acceptable uses to be very important to districts. We met with appropriate District and SLLBOCES staff to develop an understanding of the IT security procedures.

General Principles On IT/Cyber Security

Authority:
There are a number of publications and guides published by the NYS Comptroller (OSC) which describe a District's responsibilities for IT/Cyber security. The OSC publications consulted in writing this report include: Cash Management Technology, Protecting Sensitive Data and Other Local Government Assets: A Non-Technical Cybersecurity Guide for Local Leaders, Information Technology Governance and Security of Personal, Private, and Sensitive Information (PPSI) in Mobile Computing Devices. We also consulted Cyber Security: Internet and Acceptable Use Policy Template from the NYS Office of Cyber Security.

Observations and Discussion

Board Policies
The Board has adopted the following policies that are related to cyber security and computer usage:

- 3000.1 Website Accessibility (2017),
- 3320 Confidentiality of Computerized Information (2003),
- 5672 Information Security Breach and Notification (2014), 5672R Information Security Breach Guidelines (2014),
- 6470 Staff Use of Computerized Information Resources (2003), 6470R Staff use of Computerized Information Resources (2009),
- 7243 Student Data Breaches (2014), 7243R Student Data Breaches: Prevention, Response and Notification (2014),
- 7314 Student Use of Computerized Information Resources (2003), 7314R Student Use of Computerized Information Resources (Acceptable Use Guidelines) (2009),
- 8270 Instructional Technology (2003),

- 8271 The Children's Internet Protection Act: Internet Content Filtering/Safety Policy (2003), 8271R Children's Internet Protection Act: Internet Content Filtering/Safety Guidelines (2009).

As shown above, many of the policies and regulations were written a number of years ago. IT and Cyber Security technology, practices and uses have changed significantly over that period of time. The Board should review these polices and update them to meet current requirements. They should consider the sources mentioned above in the authority section and consult with SLLBOCES and possibly a policy writing service.

We also noted that the District does not publish or make its policies and regulations easily available to the District's staff or general public. There are printed policy manuals, but depending on who has them, they may or may not be up to date. We suggest that the District consider publishing its policies and regulations on its website. This would simplify the process for ensuring that they are updated and that all who need them have access to them.

One of the key policies that the District should develop is a clear acceptable use policy (AUP). This policy should be published and staff should be well trained in its implementation. The policy should include the extent, if any, that personal use is allowed and the types of information that can be accessed. While we were onsite, we obtained anecdotal evidence that there is fairly widespread belief that personal use of District computers is acceptable during lunch or off duty hours. Issues related to failing to have and or failing to monitor/enforce compliance with AUP are frequent issues cited in OSC audits.

Relationship With SLLBOCES

During our audit process, we met with the SLLBOCES IT Coordinator. She described the processes and goals SLLBOCES and the District are working together to achieve. Some of these include: compliance with NYSED 2d Privacy and Security regulations, consistent policies and procedures and ensuring that the District is receiving appropriate IT services. It is important that the District and SLLBOCES work together to achieve these goals.

Contract

The District and SLLBOCES are in a contractual relationship which include but are not limited to Technology and Shared Business Office services. The District was not able to provide a document which clearly delineates the exact nature of the services being provided as well as the responsibilities that each of the parties was assuming. This is important because there could be incorrect expectations allowing issues to fall through the cracks. Some examples of deliverables that might be included in the contract include: how often hardware and software inventories should be updated and who is responsible for providing the appropriate technology for inventory maintenance (spreadsheets vs. barcode scanners and inventory software) , who is responsible for monitoring AUP compliance, IT support staffing levels (BOCES staff estimates that there are 1.7 FTEs assigned to the District), password management, etc. Similar caveats should be considered for the shared business office contract. This will protect both the District and SLLBOCES.

Since the District's management is ultimately responsible for the District's operations and internal controls, having the delineated responsibilities and a report/tracking mechanism would be useful. For example, if there is a contractual expectation that SLLBOCES will conduct an annual physical inventory of the District's IT assets, there should also be a reporting mechanism so that management can see that it was done. As of January 2020, the inventory was approximately 2 years out of date.

We also noted that there was uncertainty as to which entity's policies and procedures were applicable to BOCES employees working in the District and/or providing services using District data. These services may or may not be provided using District equipment. In some instances both District and SLLBOCES equipment may be used. The contract should specify which policies are relevant to the services and providers. The District and SLLBOCES should work together to ensure that their policies are consistent. The BOCES employees seem to believe that since they are not District employees, they are not subject to the District's policies and procedures regarding cyber security, acceptable use, etc.

Flash Drives

We noted that a BOCES employee who is critical to the operation of the Business Office frequently works from locations outside of the business office and on other computers. To facilitate this the employee backs up data and files, generally spreadsheets, to a flash drive. The drive is stored in a desk drawer. The data is then transferred to the other computers as necessary. This practice presents at least two serious issues: data security and disaster recovery. We suggest that the use of flash drives be generally discouraged and not be used for backing up District files and documents. All data should be backed up to either the District's servers or to the BOCES' servers, whichever is determined to be appropriate by both parties. This will help to ensure that the information is available to the staff member and the District and that it is properly backed up. District information stored on the SLLBOCES server should be maintained in accordance with the longer of the two entities record retention polices.

Training

We noted that the District has a program for making staff aware of Cyber Security issues, for example, how to respond to email phishing schemes. Recent OSC audits also stress the importance of not only providing training but testing to be sure that staff are following through with what they learned. We talked with several BOCES staff that provide business office and IT services to the District on District property. They were not aware of any District training regarding cyber security, acceptable use or other District policies and procedures. We suggest that these BOCES staff members be included in the District's training processes and testing processes.

Appendix 4
IT Security

Other Areas

Passwords

Proper use and protection of passwords are critical elements of a security program. The District's policies should address passwords and password management. For example: how strong a password should be, how often should changes be forced, how should they be managed and stored and who should have access to the stored passwords. Staff should receive proper training in this area and the polices should be published, monitored and enforced.

Several issues regarding passwords and their management were brought to our attention. They relate to:

- Sharing passwords. We were provided with anecdotal evidence that in some instances teaching staff provided their usernames and passwords for School Tool to substitutes to make entering attendance easier for the substitute.
- Supervisors knowing and maintaining staff passwords. The Food Service Manager knows and manages the NutriKids passwords for the cashiers. Each has their own username and password, but the manager knows them and has the ability to change them.
- Unsecure storage of passwords. In the Business Office we were shown a large notebook that contains the usernames and passwords for all key websites and programs used by the Business Office. The notebook is stored on or in a desk in the office.

It is very important that every user has their own unique username and password. This ensures that if access is designed to be restricted that only appropriate staff have access. Their use also enables the tracking of various activities. For example in WinCap all changes and transactions can be traced to the username that makes the change. If usernames are shared or common, it would be difficult to identify the changes with a particular individual. The same is true for NutriKids, where each register is assigned to an individual.

It is not enough that every user has their own unique username and password. If they are not properly secured the benefit is lost. If sensitive banking, accounting, payroll or HR usernames and passwords are compromised there could be dire consequences: unauthorized withdrawals from bank accounts, changes to payroll records or pays, unauthorized access to personal information such as social security numbers and birthdays, etc. There are several approaches that the District may wish to consider:

- Use a secure program such as KeePass to store and generate strong passwords
- Where possible use biometric authentication, such as retinal or fingerprints.
- Where appropriate use dual authentication (combination password and cell phone authentication).

Online Banking

The District has been using online banking for a number of years. There do not appear to be any formal policies and procedures regarding online banking. If there are any policies or procedures, the person doing the online banking was not aware of them.

Generally, online banking should be conducted in as secure a manner as possible. In an ideal world it would be done using a dedicated computer that is not used to access the internet for other purposes. Other uses may open vulnerabilities for viruses, hackers and other exploits. In many cases this is not practical so other security methods should be used.

The District generally uses 2 computers for its online banking, a hard-wired desktop computer which is housed in the District's network, and when the business manager is home or out of town a BOCES supplied laptop. The laptop may present the most serious security concerns. Some of these concerns include: is the laptop and its protection up to date? Are its connections to the internet secure? Has personal use put it at risk? Is the laptop adequately password protected to deny a thief access to its contents? Personal use of these computers should be strongly discouraged as it could open these computers to unnecessary vulnerabilities. The District may wish to consider appointing a deputy treasurer who can perform these functions when the business manager is not available. Appropriate internal controls should be implemented.

User Listing

We obtained an electronic copy of the District's network user listing for analysis. We reviewed the listing for generic accounts, when passwords were last changed, last login dates and matched nonstudent users to the OSC employee data file.

We noted the following:
The total list had 1,832 users: 259 domain users and 1,573 student users. There were 11 generic domain user accounts that included 6 members of the Board of Education, the remaining generic users were for substitutes, Teach, Sum, LDAP, Generic, etc. Generally, the number of generic accounts should be limited to as few as possible and only for necessary purposes. OSC audits have recently cited this as an issue.

We tried to match the nonstudent users with the OSC employee export file for 2020 to determine if there were any inactive users still listed as active on the list. There were 37 users that could not be matched indicating that they may need to be disabled. We noted nonstudent users that had not logged in to the system during the 2020 classroom school year beginning September 1, 2019. Nine of them had their last login date between 6/1/19 and 8/12/19. The farthest removed login was 9/19/18. These accounts should be investigated to see if they should be deactivated. The user list should be reviewed at least annually to disable any inactive users.

Appendix 4
IT Security