INTERNAL AUDIT REPORT

ICTS Prior Audit Findings

✓ A Premier Follow-Up Review

October 2014

Table of Contents

List of Figures & Tables

BACKGROUND

As part of the District's audit landscape, there are periodic types and various levels of audits carried out – triennially - by the State of Florida Auditor General's (A-G) office; and –annually – by Ernst & Young, LLP, (EY) auditing firm, respectively.

Being a state-sponsored audit operation, the A-G has been performing dedicated Information Technology (IT) audits as well as merging IT-related elements into financial and operational audits in the District and publishing the results on their official website as public records.

EY – in an external audit capacity, has been performing combined financial audits with some IT-related ERP applications component in the District. These are communicated to the School Board in management letters issued as part of the audit reports.

In addition, the Information Communications & Technology Services (ICTS) department has been engaging the services of United Data Technologies (UDT) and Illumant to perform internal penetration tests (Pen Tests) over the District's network environment. These solicited advisory services provide the District with a demonstration of vulnerabilities exposure and potential risks to information assets and the network infrastructural environment. The most recent activities were in 2010 and 2014.

Each of these audits and pen tests resulted in a number of IT-related findings and recommendations. The Internal Audit department initiated this follow-up audit of these prior findings in order to conduct an inventory and status analysis of the findings and recommendations from these audit and penetration testing activities.

OBJECTIVES, SCOPE & METHODOLOGY

OBJECTIVES

The objective of this internal follow-up activity was to evaluate the adequacy, effectiveness, and timeliness of actions taken by ICTS management on reported observations and recommendations – as submitted by the external auditors (A-G and EY) and Pen Test consultants (UDT and Illumant).

This was achieved through verification of ICTS representations by: -

- Reviewing relevant information to conclude whether ICTS management has planned, is in the process or has taken appropriate timely action to address reported audit /pen test findings and recommendations

- Evaluating related prevailing conditions (within the District's IT environment) to corroborate ICTS management's sustainment of resolved conditions through appropriate controls as reported in audit /pen test findings and recommendations.

SCOPE

To draw an accurate picture of the current conditions of previous and recent audit recommendations, we reviewed relevant documentation on certain past triennial audits carried out by the Auditor-General (A-G), annual audits carried out by Ernst & Young (EY), and penetration tests (Pen Test) - performed by UDT and ILLUMANT.

For the Internal Audit department to provide a clearer perspective on those issues that have been lingering in the ICTS domain for remediation, the following reports were reviewed: -

Released Report	Fiscal Year (FY) / Covering Period
Auditor-General (A-G)	
• Report No. 2014-147 (Mar 2014)	FY 2012-13 (Jul 2012 – Jun 2013)
• Report No. 2011-165 (Mar 2011)	FY 2009-10 (Jul 2009 – Jun 2010)
• Report No. 2008-014 (Sep 2007)	FY 2007-08 (Jul 2006 – Jun 2007)
• Report No. 2005-109 (Jan 2005)	FY 2004-05 (Jun 2004 – Sep 2004)
Ernst & Young (EY)	
• Management Letter – Dec 2011	FY 2010-11 (Jul 2010 – Jun 2011)
• **Draft** IT Management Letter – 2010	FY 2009-10 (Jul 2009 – Jun 2010)
• Management Letter – Dec 2009	FY 2008-09 (Jul 2008 – Jun 2009)
• Management Letter – Dec 2008	FY 2007-08 (Jul 2007 – Jun 2008)
• Management Letter – Nov 2007	FY 2006-07 (Jul 2006 – Jun 2007)
• Management Letter – Oct 2006	FY 2005-06 (Jul 2005 – Jun 2006)
• Management Letter – Oct 2005	FY 2004-05 (Jul 2004 – Jun 2005)
ILLUMANT	
• Data Loss Prevention Assessment	Jun 2014
• Blind Visibility and Exposure Analysis	Jul 2010
• Perimeter Security Assessment	Jul 2010
United Data Technologies (UDT)	
• Application Exploitation Assessments	Jul 2010

Table 1 - Review List of Relevant Reports

Although most of the A-G report findings were referenced up to their 2007/08-audit, the AG 2005 report was included in this review as it represented the source and onset of certain related findings.

In-Scope Exceptions

Out of the series of documentation reviewed, the following reports were excluded from this exercise: -

- EY Management Letter 2014 – descoped as final report has not yet been issued; with anticipated release date around December of 2014
- EY Management Letter 2013 (issued in Dec 2013) – had no IT related content
- EY Management Letter 2012 (issued in Dec 2012) – had no IT related content

During a reconciliation of findings and recommendations with related documentation, we noted that no management letter was issued for EY's audit activity of 2010. The only record of this activity was a draft management letter specifically representing IT observations and recommendations with related ICTS management responses.

Notwithstanding the draft version, the 2010 content was significant to this process - as this was the only document that confirmed the resolution of a 2009 finding on SAP Access. Besides, EY has been very consistent with the closure of audit recommendations by meticulously following up with resolution affirmations in their next /immediate annual audit reports. Since there was no reference to this 2009 finding in their 2011 report (despite reporting the resolution of 2007, 2006 and 2003 findings), it was appropriately considered a closed item in the 2010 period.

A follow up check on the final 2010 report with EY affirmed this oversight, and they have submitted a letter to that effect during this audit.

METHODOLOGY

This follow-up review audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing (IPPF) of the Institute of Internal Auditors and standards and guidelines of ISACA's Information Technology Assurance Framework (ITAF); including applicable contributing procedures as deemed necessary to accomplish audit objectives.

Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

We are required to note any material deficiencies in accordance with Florida Statutes, School Board Policy and sound business practices. We also offer suggestions to improve controls or operational efficiency and effectiveness.

FOLLOW-UP REVIEW

STATISTICAL OVERVIEW

As insight to the source and volume of the content examined, a total of fifteen (15) audit /penetration test reports were reviewed under the following activities (*as noted in Table 1 - Review List of Relevant Reports – page 4*): -

- IT Audits - 11 Reports (spanning 2005-2014)
- Penetration Tests - 4 Reports (spanning 2010-2014)

The content of the reviewed reports was compiled in a consolidated workbook format as an effective way to capture and present the various findings with associated recommendations, management responses and verification /reconciliation remarks.

The respective activities had the following finding /observation details - presented graphically in the form of columnar, bar and pie charts to provide an easier understanding of the prevailing conditions: –

Note: The terms "finding" and "observation" have been used interchangeably in this report, as an indication of the same event type and used to suit specific contexts, where applicable.

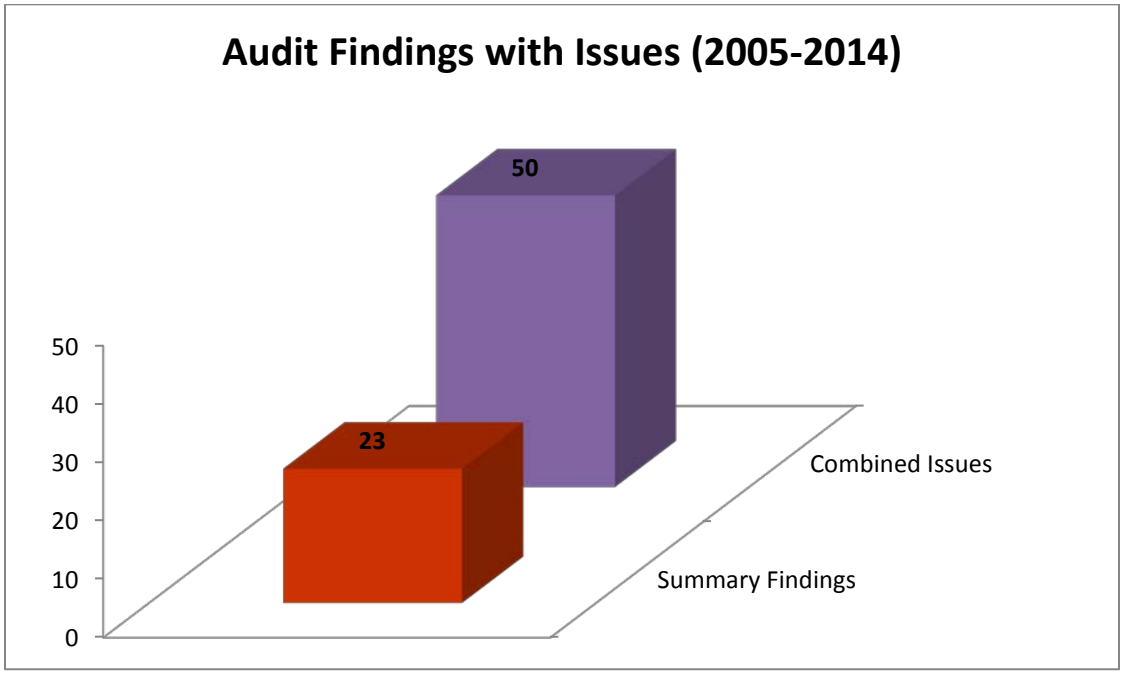

Figure 1 - Audit Findings with associated Issues

The A-G and EY findings were presented in their reports in summary findings. As these reported findings contained series of related issues, we broke those issues out as subsets of their respective findings and treated them as a separate group. This made it easier to address each issue for our audit and will make it easier for ICTS follow-up since each of those listed issues had to be addressed as individual items by ICTS.

Similarly, the UDT and ILLUMANT penetration test observations were also consolidated into separate blocks of summary observations alongside their combined issues: -

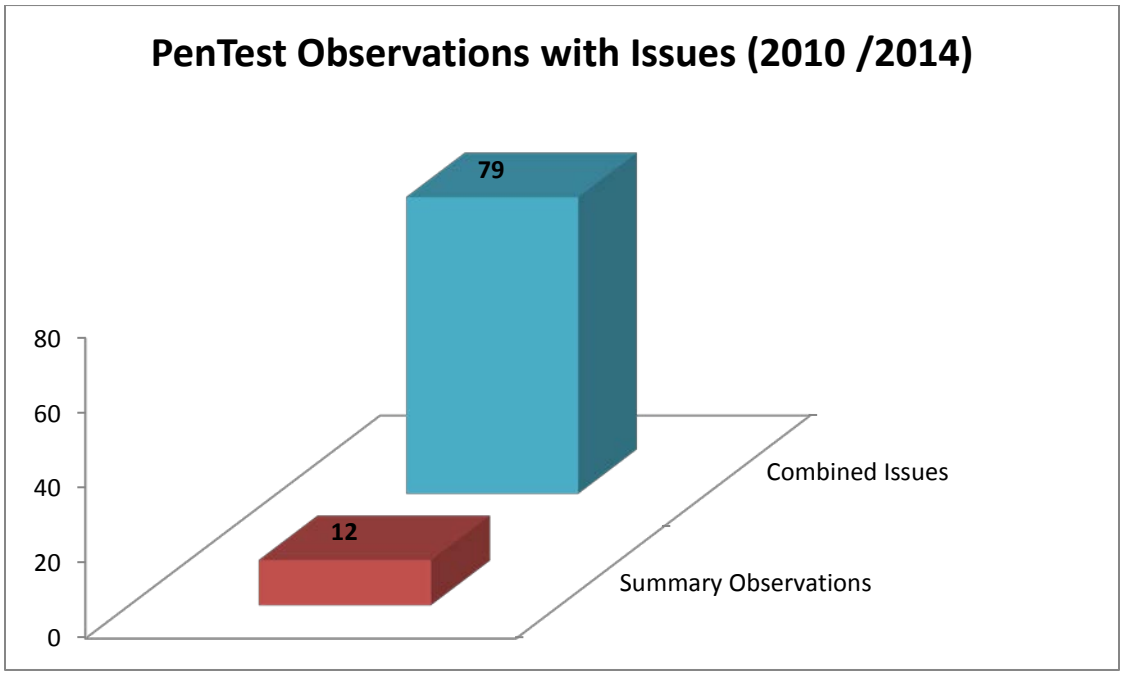

Figure 2 – Pen Test Observations with associated Issues

The following sections of this report present our findings as a result of reviewing the reports indicated in '*Table 1*', and verifying management representations of actions taken to address the findings in them.

AUDITS

Our initial approach was to break down the indicated summary findings into types – based on frequency of finding occurrences (in findings reported just once or repeatedly) and severity of combined issues (either sensitive or routine). The frequency and severity counts are represented below: -

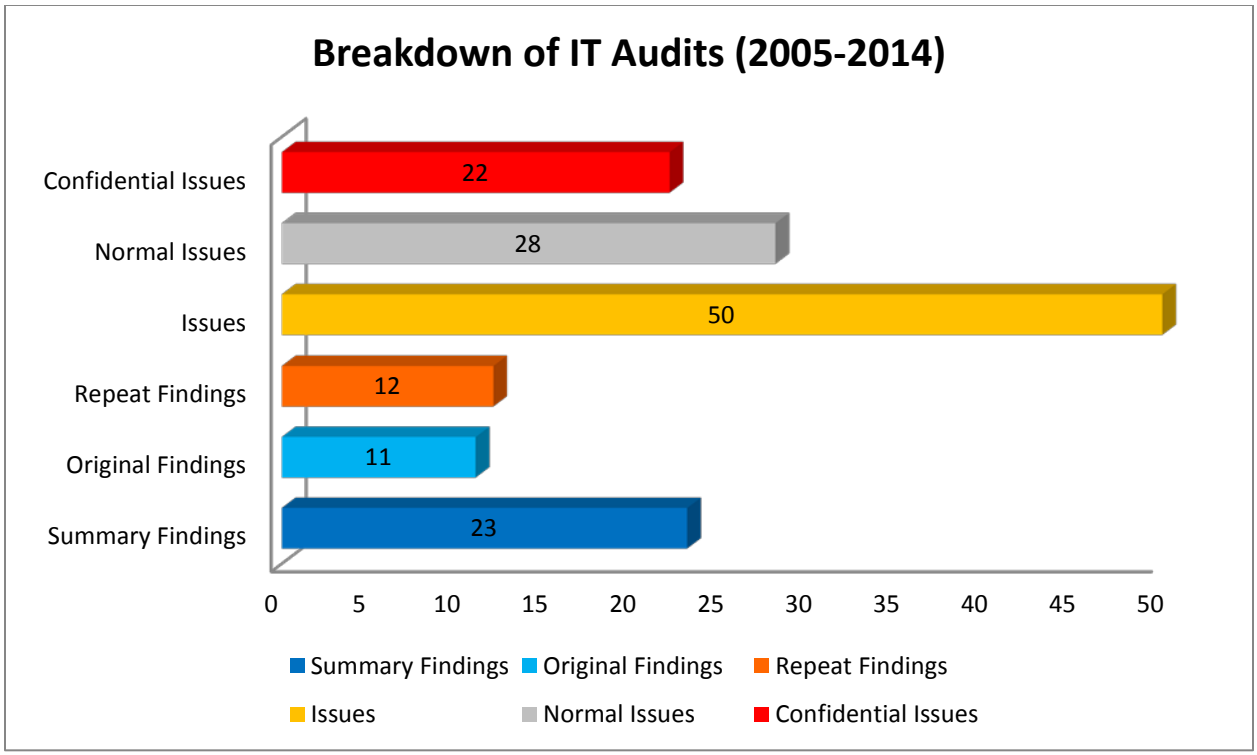

Figure 3 - Breakdown of Prior IT Audits

Highlight Notes: -

- 44% of the finding issues were "confidential" items (term coined by the A-G) - and purposefully excluded from particular A-G final reports to avoid compromising the District's IT systems.

- 52% of the summary finding were repeated items - and were particularly A-G reported findings. There was an average of 3 to 5 repetitive issue findings in every A-G audit activity; which was consistent with the series of report remarks.

A frequency /severity pie chart is provided below depicting their associated percentiles across summary findings and combined issues: -

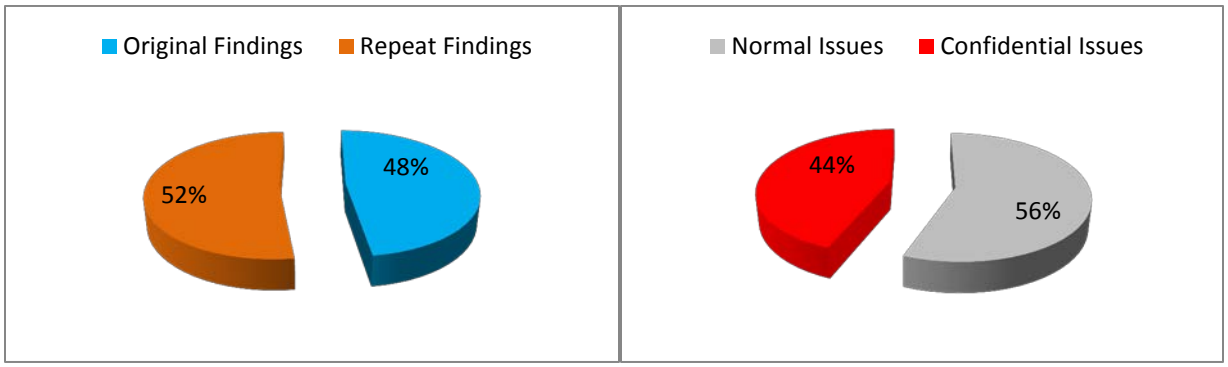

Figure 4 - Breakdown of Prior IT Audits (Frequency /Severity Pie)

Due to the magnitude of audit materials and in order to present a consolidated viewpoint, the A-G | EY issues were combined (i.e. ERP_SAP/Oracle|Windows-based platform services), and grouped under related content - culminating into the following six (6) categories of technology disciplines: -

- **Access Management (A M)**: -
  - User Access Rights Review policies & procedures
  - Excessive SAP System Access Privileges
  - No policies & procedures for Access & Revocation
  - SAP Access Authorization Requests

- **Continuity & Disaster Preparedness (C & DP)**: -
  - Business Continuity /DRP deficiencies
  - Ineffective Off-site Backup Procedures

- **Data Loss Prevention (DLP)**: -
  - No established DLP program
  - Handling of Classified /Sensitive Data/Digital Privacy
  - Ineffective Hardware sanitization procedures

- **General Controls (GC)**: -
  - Security Control deficiencies in User Authentication
  - Unutilized software security features and lack of ERP-based security controls
  - Unutilized software security features and lack of Windows-based security controls
  - Security Control deficiencies in Logging and Monitoring
  - Ineffective Monitoring of System Security Events
  - Ineffective Physical Security Controls

- **Information Security Management (ISM)**: -
  - No dedicated Security Program
  - Chief Information Security Office(r)
  - Ineffective IT Risk Management Process

- **Systems Development & Maintenance (SD & M)**: -
  - No ISDM
  - No Software Acquisition Policies
  - No Patch Management Policies & Procedures
  - Change & Release Management - User Acceptance Testing Procedures

The charts in Figures 5 and 6 – provide a graphical representation of the number and percentage of audit issues (out of the 50 combined issues) as per the above-listed categories:

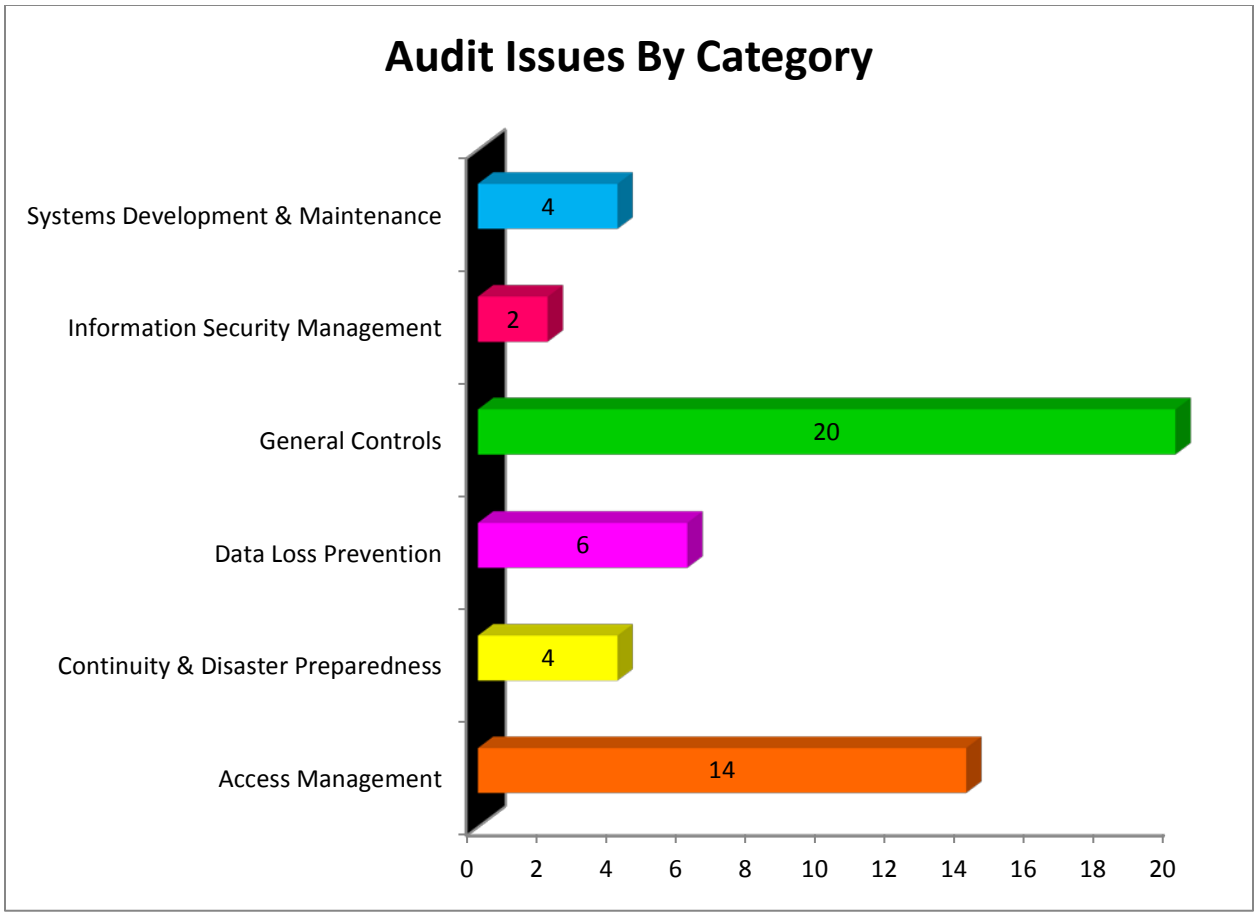

Figure 5 - Audit Issues by Category

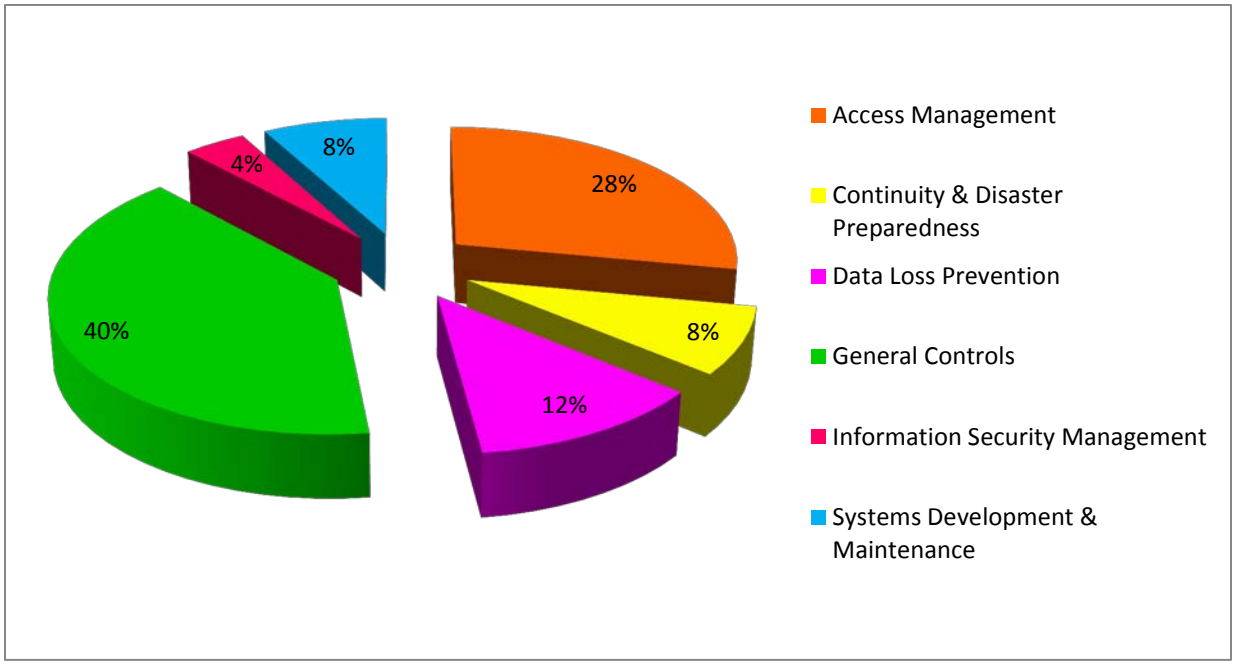

Figure 6 – Percentage of Audit Issues by Category

PENETRATION TESTS

Since these activities were carried out under unique unrelated assessments, we followed a different approach in the breakdown of indicated summary observations into types – by basing them only on the severity of combined issues (ranging from critical to low risks).

The severity counts are represented in below charts (*figures 7 and 8*): -

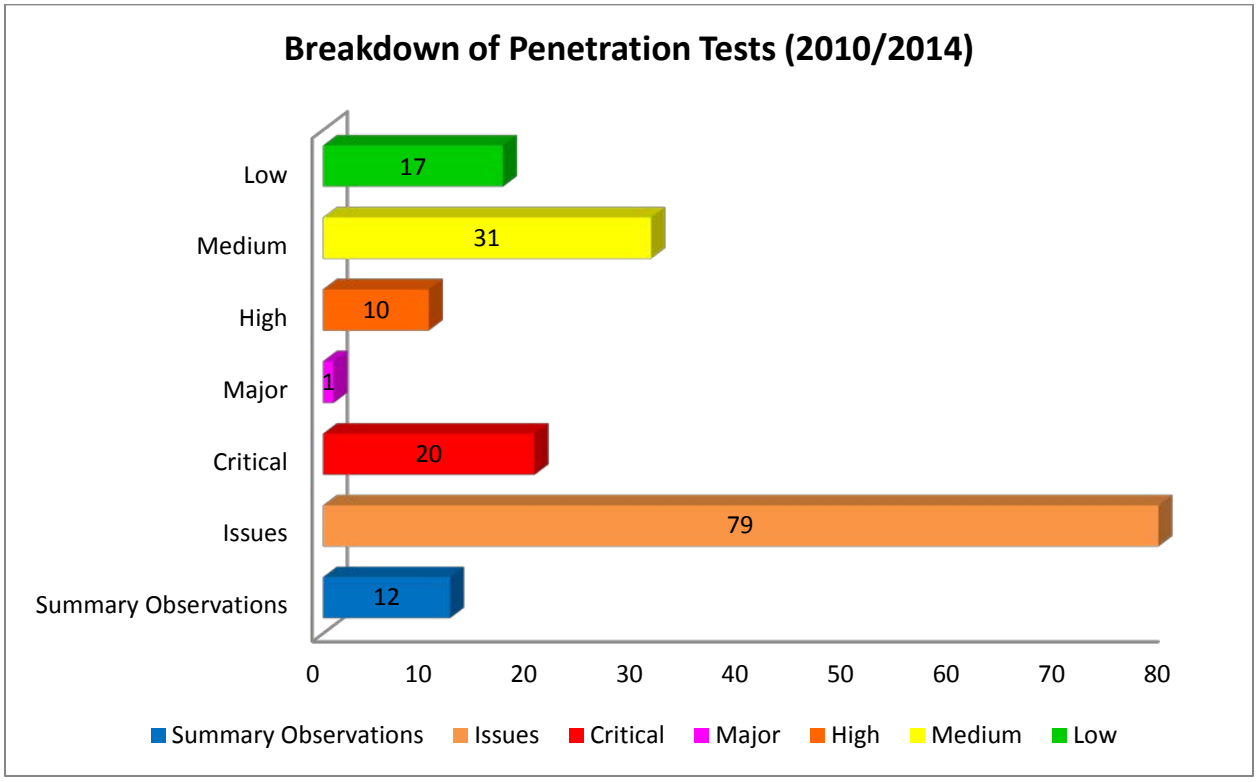

Figure 7 - Breakdown of Prior Penetration Tests by Severity

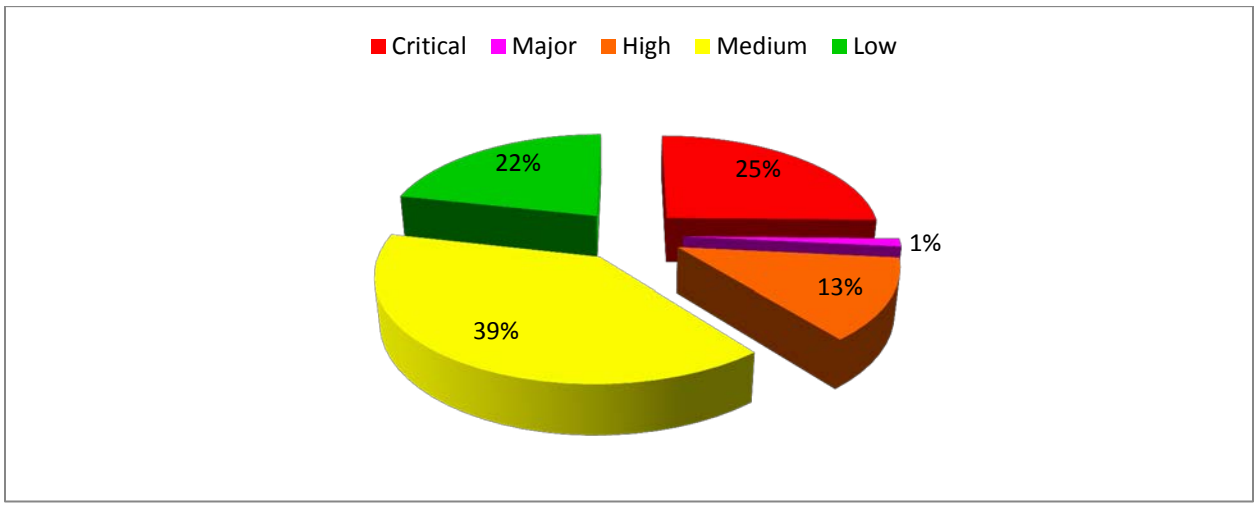

Figure 8 - Breakdown of Prior Penetration Tests (Severity Pie)

Similar to the audit process, and for a consolidated presentation, the UDT | ILLUMANT observation issues were grouped by uniquely-related content - culminating into the following three (3) categories of technology disciplines: -

- **Data Loss Prevention (DLP)**: -
  - Data-in-Motion
  - Data-at-Rest

- **Network Security Controls (NSC)**: -
  - VoIP
  - WLAN
  - Blind Visibility and Exposure Analysis (BVEA)
  - Perimeter Security Assessment (PSA)

- **Web-Application Security Controls (WASC)**: -
  - Outlook Web Access
  - Progress Book
  - SAP Portal

The chart in *Figure 9* – provides a graphical representation of the number of penetration test observations (out of the 79 combined issues) in the categories listed above:

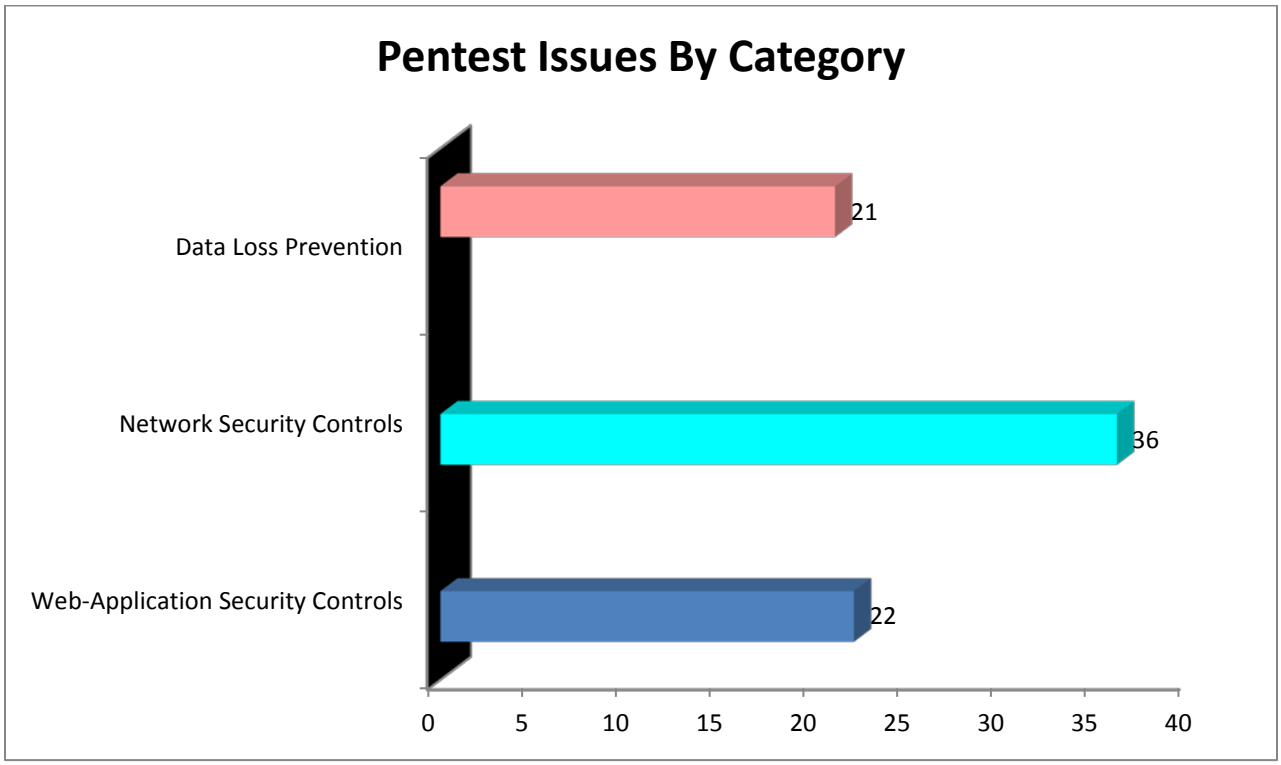

Figure 9 – Pen Test Issues by Category

CONCLUSIONS & NEXT STEPS

With regard to the first objective of this audit (repeated below) we offer the following analysis.

- **Reviewing relevant information to conclude whether ICTS management has <u>planned, is in the process or has taken appropriate timely action</u> to address reported audit /pentest findings and recommendations**: -

<u>STATE OF AUDIT RESOLUTIONS</u>

The A-G and EY issued complementary reference statements in corresponding reports and management letters. In a similar fashion, we compiled and determined the completion status of the summary findings with the associated issues in the following analysis.

With this approach, we derived the resolution statuses by their respective finding categories and severity - as displayed below (*figures 10-12*): -

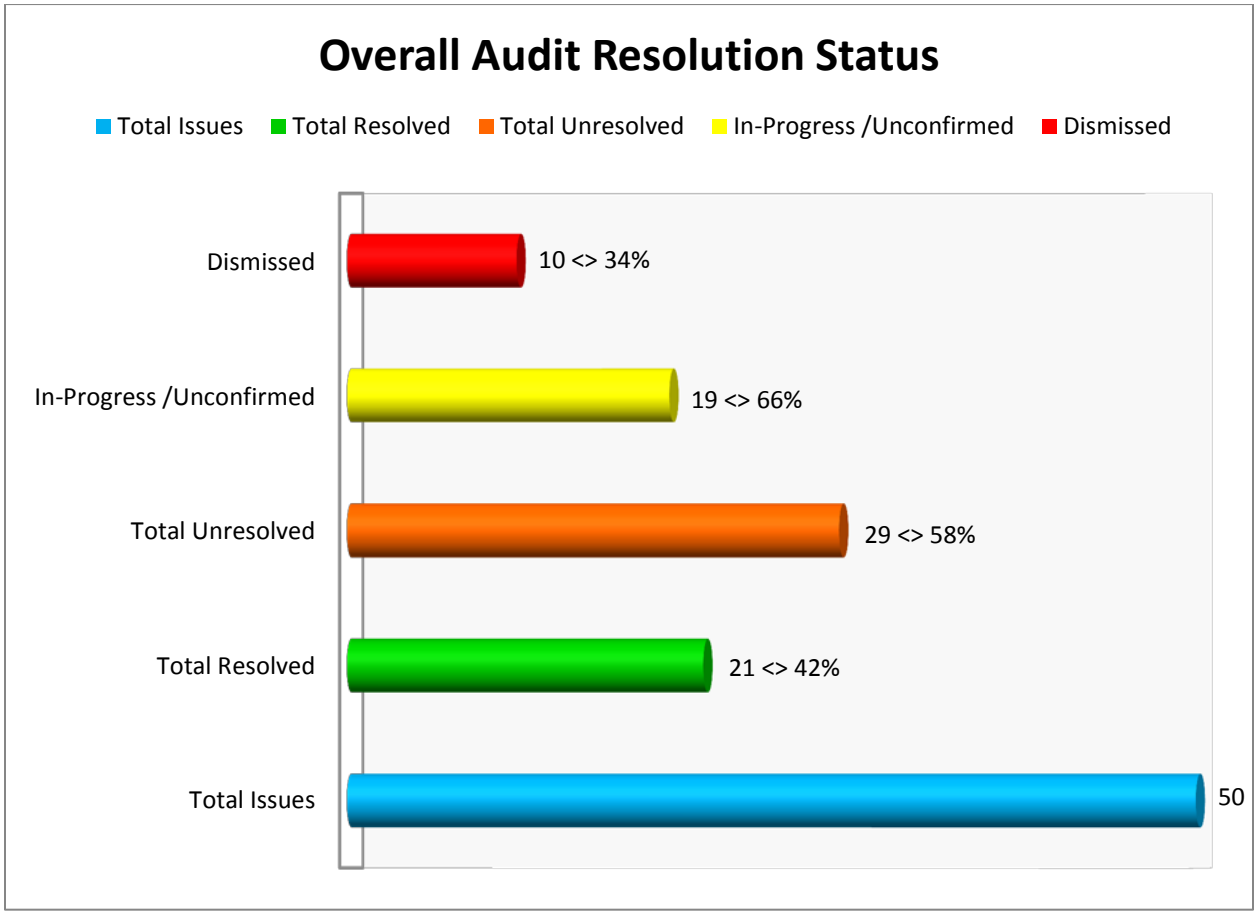

Figure 10 - Overall Audit Resolution Status with Percentiles

- The percentages of dismissed and in-progress (unconfirmed/inconclusive) results are in relation to the total unresolved issues.

The general overview is broken down into the various categories as below: -

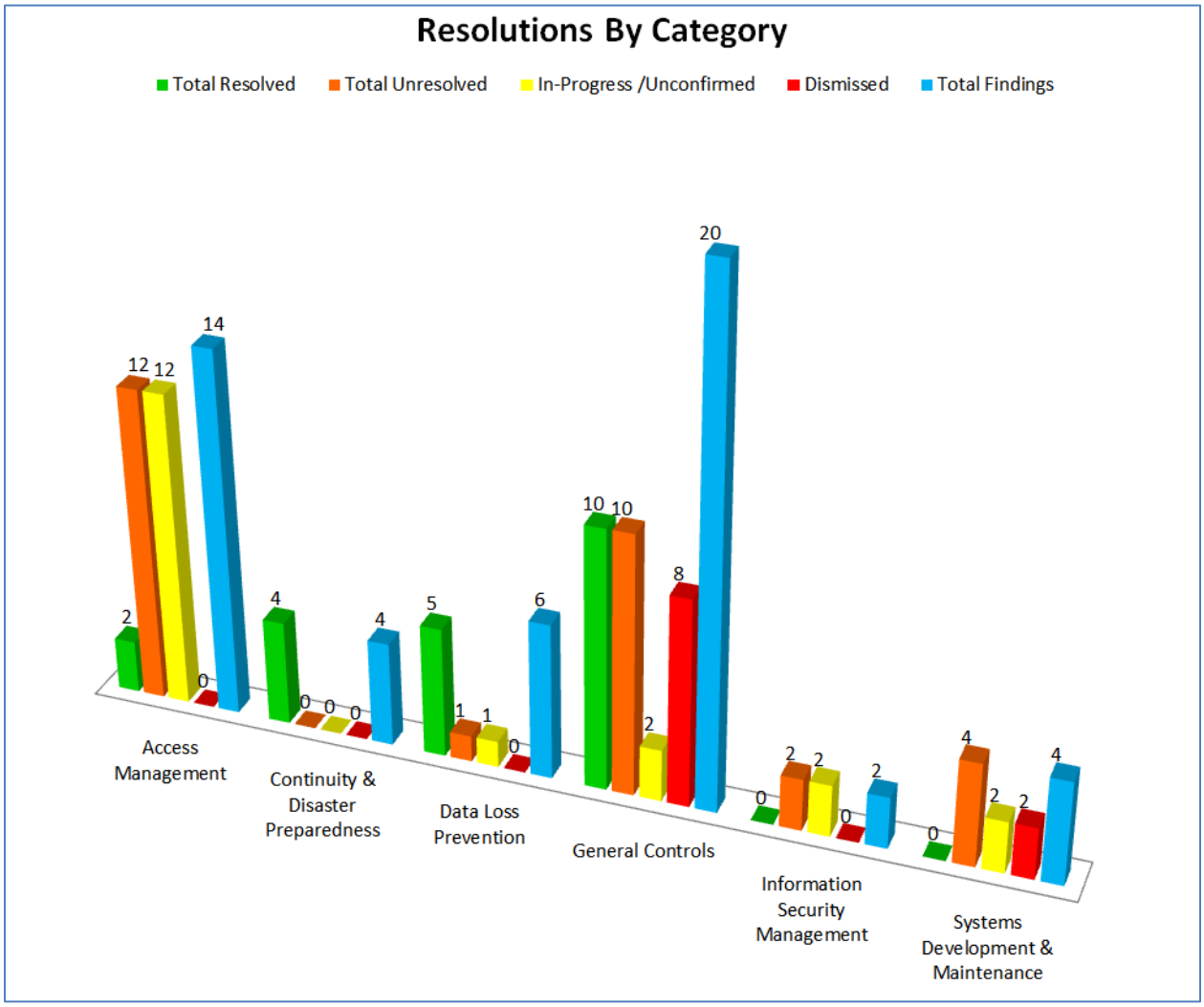

Figure 11 – Audit Resolutions by Category

In summary, most of the audit finding issues were related to IT General Controls (40%) and Identity/Access Management (28%) – and had been reported within dated ranges of 2005---2013

Taken Appropriate Timely Action > **Resolved**

- 42% of issues have been resolved (21 out of 50)
- 4 out of the indicated 6 categories had resolved items
- All issues related to IT Continuity & Disaster Preparedness have been resolved (this was the only finding category with a 100% resolution status)
- 48% of resolved issues (10 out of 21) was related to General Controls; followed by - 24% on Data Loss Prevention; 19% on IT Continuity & Disaster Preparedness; and - 9% on Access Management
- Out of the 22 confidential issues –27% have been resolved (figures 3 and 12)
- Out of the 28 normal issues – 54% have been resolved (figures 3 and 12)

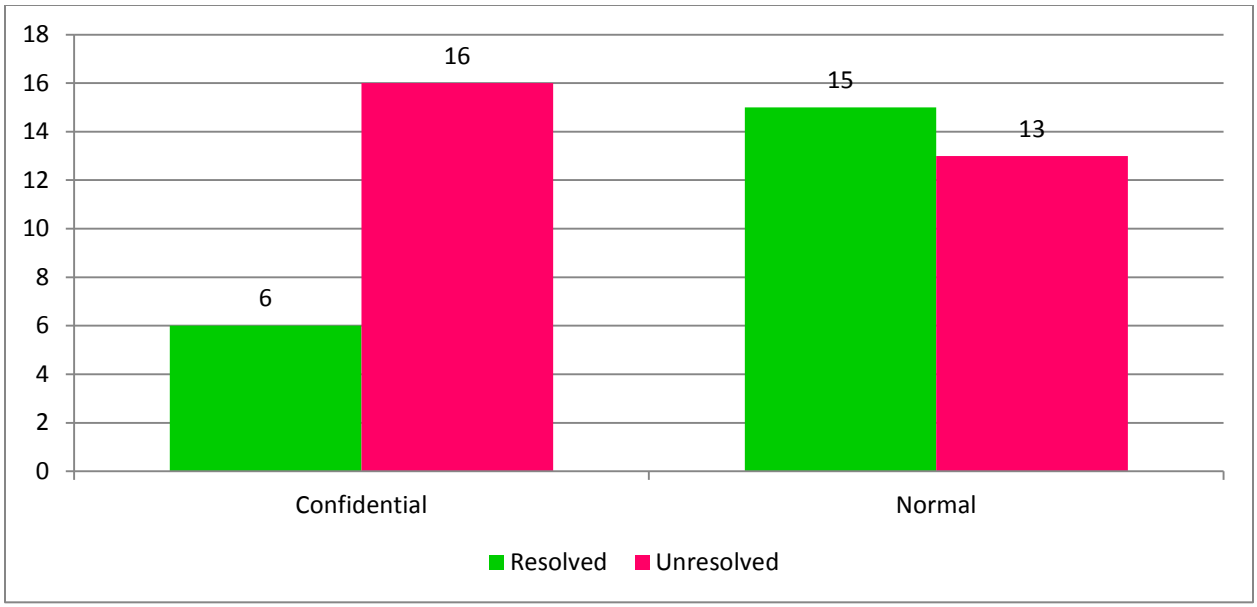

Figure 12 - Audit Resolution Status (by Severity)

Planned /In-Progress > **Unresolved**

- 58% of issues remain unresolved (29 out of 50)
- 2 out of the indicated 6 categories had none of their related issues resolved (i.e. all issues related to Information Security Management and Systems Development & Maintenance remain unresolved (with the earliest reported finding issue since 2005)
- The unresolved issues date as far back as 2005 (e.g. no established formal procedure documentation on Systems Development Life Cycle (SDLC)) and as recent as 2013 (e.g. no established Data Loss Prevention (DLP) program)
- 41% of unresolved issues (12 out of 29) was related to Access Management; followed by - 35% on General Controls; 14% on Systems Development & Maintenance; 7% on Information Security Management; and - 3% on Data Loss Prevention
- Out of the 22 confidential issues – 73% are unresolved (figures 3 and 12)
- Out of the 28 normal issues – 46% are unresolved (figures 3 and 12)

Detailed reports of all findings and statuses of this audit have been compiled and shared with ICTS management for use in addressing these matters subsequent to this report.

STATE OF PENETRATION TEST RESOLUTIONS

As with the audit findings, we sorted the pen test completion statuses by respective observation categories and severity with overview - as noted below (*figures 13-15*): -

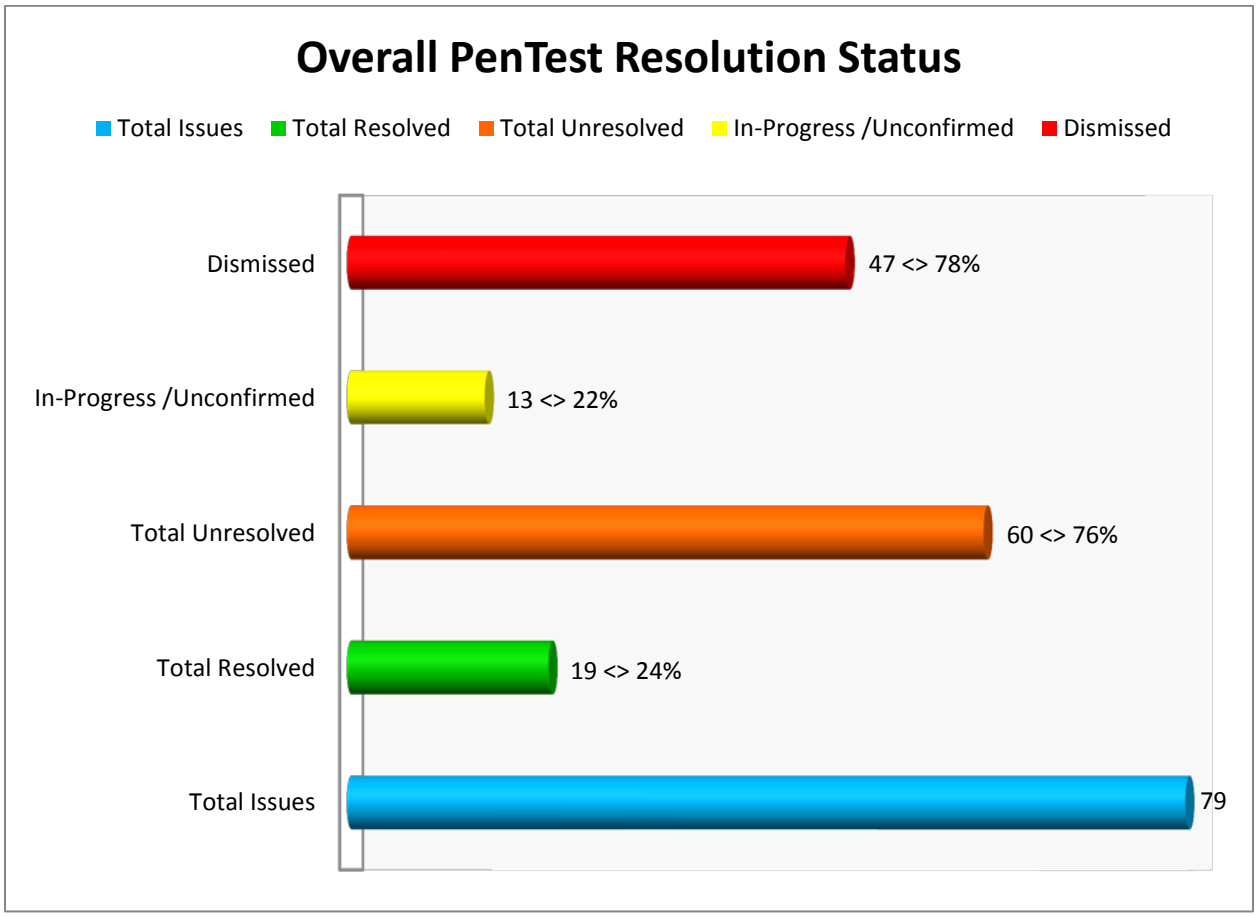

Figure 13 - Overall Pen Test Resolution Status

- The percentages of dismissed and in-progress are in relation to the total unresolved issues.

The general overview is broken down into the various categories as below: -

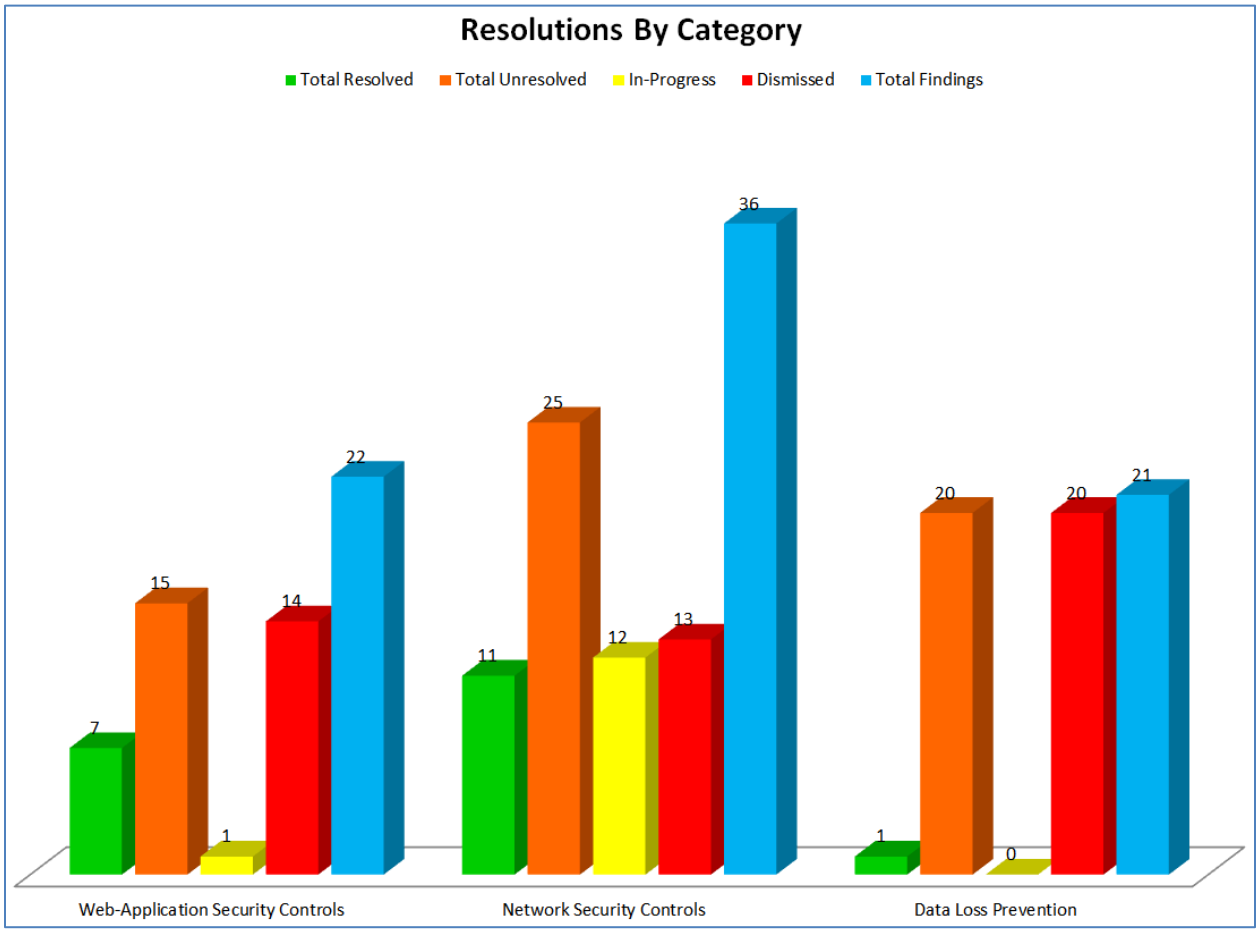

Figure 14 – Pen Test Resolutions by Category

In summary, the majority of the pen test issues were related to Network Security Controls (46%); and co-incidentally in close numerical alignment with the related audit category (i.e. IT General Controls (@ 40% of audit finding issues)) – which had all been reported in 2010

Taken Appropriate Timely Action > **Resolved**

- 24% of issues have been resolved (19 out of 79)
- All 3 categories had resolved items (ranging from a high 11 to a low 1)
- The largest percentage of resolved issues - 58% (11 out of 19) were related to Network Security Controls; followed by - 37% on Web-Applications Security Controls; and least - 5% on Data Loss Prevention
- The only major severity issue has been resolved (related to storage of sensitive information)
- Out of the 10 high risk issues – 40% have been resolved (figures 7, 8 and 15)
- Out of the 31 medium risk issues – 29% have been resolved (figures 7, 8 and 15)
- Out of the 17 low risk issues – 29% have been resolved (figures 7, 8 and 15)

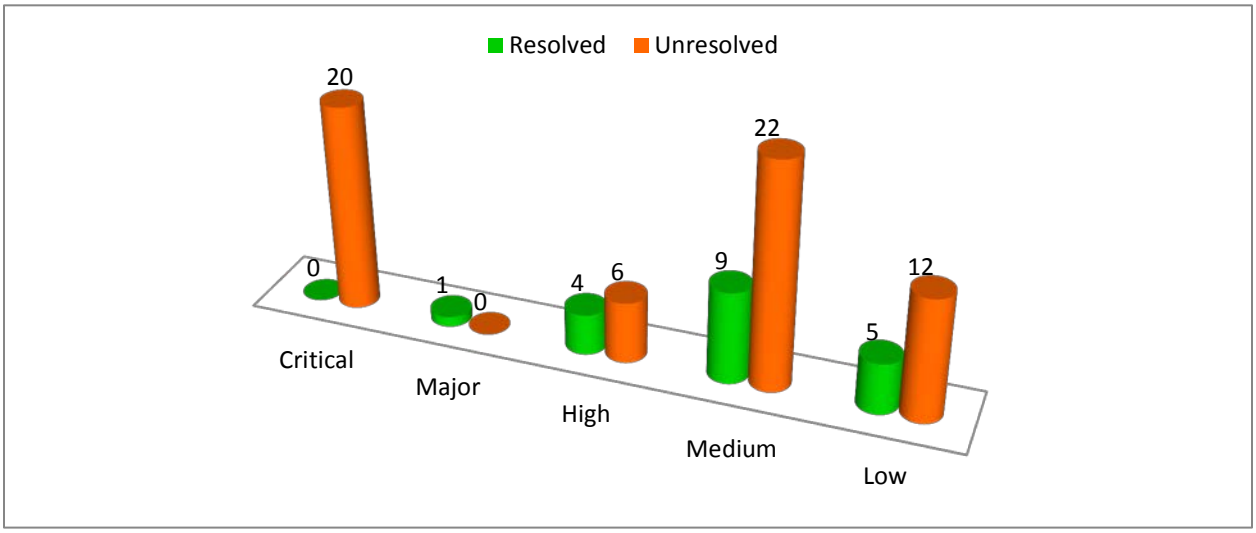

Figure 15 – Pen Test Resolutions by Severity

Planned /In-Progress > **Unresolved**

- 76% of issues remain unresolved (60 out of 79)
- Most of the unresolved issues are dated from 2010 (under Network & Web-Applications Security Controls)
- The largest percentage of unresolved pentest issues – 42% (25 out of 60) were related to Network Security Controls; followed by - 33% on Data Loss Prevention; and least - 25% on Web-Application Security Controls
- None of the 20 critical issues (related to data-in-motion) have been resolved – 100% unresolved (figures 7, 8 and 15)
- Out of the 10 high risk issues – 60% are unresolved (figures 7, 8 and 15)
- Out of the 31 medium risk issues – 71% are unresolved (figures 7, 8 and 15)
- Out of the 17 low risk issues – 71% are unresolved (figures 7, 8 and 15)

As in the case of the audit findings, details of the pen test issues have been shared with ICTS management.

APPRAISAL OF CONTROLS ENVIRONMENT

For the purpose of establishing whether the right levels of controls are in place – as a pre-condition for maintaining a mitigated risk environment – we recognized the following in accordance with the second stated objective of this audit (repeated below): -

- **Evaluating related prevailing conditions (within the District's IT environment) to corroborate ICTS management's sustainment of resolved conditions through appropriate controls as reported in audit /pen test findings and recommendations.**

To obtain reasonable assurance on the completeness and sustainability of remedial actions, our background evaluation of the existing IT environment resulted in the following findings: -

- ICTS does not maintain a formalized risk register that could aid the determination of inherent and residual risks with the infusion of corresponding controls.

- In light of this underlying factor - we are unable (at this stage) to test the effectiveness and independently affirm the adequacy of the current IT controls capability or to reliably assess the resilience of the ICTS general controls environment - whether the right conditions have been set to prevent the relapse or reoccurrence of such reported findings;

- Internal Audit will address this situation in an upcoming audit on IT general internal controls and with an anticipated revamp of the ICTS risk assessment process as part of the district's annual entity-wide risk assessment.

NEXT STEPS…

We encourage the ICTS management to consider the recommendations below in an effort to handle the remaining issues as highlighted in this report: -

- As noted previously, Internal Audit has submitted detailed records of the findings and statuses. Of particular note is the summary of unresolved findings which will need to be considered as (currently) unmitigated in the risk assessment process.

  Acceptance of these findings will signify three important positions: -
  - The closure of this extensive follow-up activity with no intention to re-open this case process – serves as a baseline for subsequent audit /pen test exercises to be conducted by either Internal Audit or external parties;
  - Provides ICTS with a self-paced remedial tasks workbook to address the specified in-progress /inconclusive finding issues. This would also be an opportunity for ICTS to establish and apply compensating controls, where applicable;
  - Provides ICTS with an opportunity to make informed risk decisions on those audit findings /pen test observations and recommendations which have not been addressed. We strongly recommend ICTS management's commitment in focusing on those unresolved issues because not addressing them - even the low risk items - might lead to escalated complicated issues in a matter of time.

- ICTS should prepare their staff in building awareness ahead of the anticipated enhancement of the risk assessment process; the Internal Audit department will be a supporting partner to aid this intended implementation;
- A formalized risk register should be developed to serve as a listing of inherent and residual risks along with corresponding controls. As stated, this will provide the risk versus controls record for ease of subsequent evaluations and revisions of IT controls and instill a level of resilience to the general controls environment. This should reduce weak control instances and forestall the probable reoccurrence of such reported findings and resultant time-consuming follow-up reviews;

In closing, we wish to thank the ICTS management and particularly the Audit Focal Point (Ms. Cirene Powell), for their cooperation and assistance during this follow-up review; as well as the respective technical teams for their efforts in providing feedback during the evidence gathering process of this exercise.

Francis Amanquah, CISA, IT Auditor

MEMORANDUM

Information Communications & Technology Services

Date: January 15, 2015

To: Linda Lindsey
Senior Director, Internal Audit

From: Frankie Elmore
Chief Information Officer, ICTS

Subject: ICTS Prior Audit Findings Report Formal Response

In response to the ICTS Prior Audit Findings Report produced by your office, I have received and reviewed the findings and I am in agreement with the identified technology security risks remaining to be resolved as the result of past external audits and penetration tests. The fulfillment of the objectives has provided ICTS with the basis from which a risk registry will be developed. The risk registry will provide ICTS with a centralized location from which security audit related tasks will be managed.

A corrective action plan (CAP) has been developed to address findings identified in the ICTS Prior Audit Findings Report. In the CAP, ICTS has addressed corrections planned, who will implement the corrections, and the implementation dates.

I want to extend my appreciation for performing the audit review, as it has assisted in compiling and organizing unresolved audit and penetration test findings.