September 30, 2021

The City of Dallas 2021 Data Loss Events Analysis – Initial Report

Identifying Data Types Lost and Possible Root Causes of the 2021 Data Loss Events at The City of Dallas

ITS Risk Management, Security, and Compliance Services
THE CITY OF DALLAS

City of Dallas

Document Revision

Item	Change Description	Version	Date	Document State
1	Initial document outline	0.01	9/13/2021	DRAFT
2	DRAFT document using updated outline	0.02	9/23/2021	DRAFT
3	Revised DRAFT document with recommendations	0.03	9/29/2021	DRAFT
4	Initial report	1.00	9/30/2021	Final

Data loss Events Analysis Report Acknowledgements

The Chief Financial Officer of The City of Dallas and the Director of the Department of Information and Technology Services (ITS) acknowledge and thank the ITS Risk Management, Security, and Compliance Division and elements of other ITS divisions for their efforts in capturing, analyzing, and reporting on information and events related to The City of Dallas March 2021 data loss events. Without their assistance, expertise, and background in information and cyber security matters, the City would not have an opportunity for detailed understanding as to the causes and effects related to this event.

General Source Information Acknowledgements

The City of Dallas acknowledges and thanks the many information sources that contributed to the construction of this document. Some source information was obtained through Gartner and Forrester research services. The City acknowledges and thanks those organizations for the guidance and assistance their individual contracted services provide the City. Some source information was also gathered from the elements of the United States Government including but not limited to The National Institute of Standards and Technology (NIST), The Department of Homeland Security, The Department of

Justice, and others. The City acknowledges and thanks those organizations for the guidance and assistance their services and standards frameworks have provided the City.

Since this document is not an academic paper, detailed citations are not used. This document will generally cite the sources of information used in the construction of this report using a bracketing artifice. The artifice used is square brackets with indication of the source within the square brackets. The following is an illustration of a citation used in this document: [Source], and [Source1, Source2].

City of Dallas

Executive Summary

The purpose of this document is to identify direct, contributing, and systemic factors related to the March 2021 data loss events occurring at The City of Dallas. The report also outlines a series of recommendations that will improve the City's handling of electronic data to reduce the likelihood of such events occurring in the future.

The first event, occurring at the end of March 2021, included 22 Terabytes (TB) of data of which 14.49 TB were retrieved through assistance with Microsoft. The subsequent 7.51 TB was deleted and consider unrecoverable. This data consists of archived images, video, audio, case notes, and other items collected by the Dallas Police Department. The missing data often referred to as the "K" drive resulted in the loss of 4.1 M files.

The second incident was discovered as a result of ITS conducting a thorough audit of the 26 file servers. ITS working with the backup vendor (Commvault) has completed a technical audit against those missing files resulting in a reported loss of an additional 13.167 TB. This additional loss was associated to the Fusion servers.

Location	Volume Loss	Number of Files
K Drive	7.51 TB	4.1 million files
Fusion Server	13.167 TB	4.6 million files
CAPERS server	N/A	No data loss
City Secretary	N/A	No data loss

Subsequently, ITS has brought forensic data recovery tools, expertise, and support staff to scan and recover data from across the City of Dallas's technology infrastructure to potentially recover the deleted data, possibly stored on alternative sources. The District Attorney's office and DPD are continually providing ITS a list of priority cases to search against for the recovery effort. ITS is utilizing these specialized forensic tools and processes to recover data from alternate sources such as laptops, cameras, and other devices.

In addition, a recovery environment has been built where forensic copies of the affected systems can be restored with backups to be used in our search efforts. ITS is searching the City's entire on-premises and cloud environment including, Microsoft Office 365, email, SharePoint, and OneDrive locations for the

missing data. We understand the magnitude and seriousness of the situation and will continue to work diligently with DPD to recover as much data as possible. To date the recovery team has recovered 140,353 potential files that were deleted.

Type of Data	Beginning Balance based on Analysis	Processed To Date	Percent Completed
Est. Number of Cases	17,494	142	8.1%
DA Prioritized Cases	1,000	142	14.2%
Potential Data Files	17,291,140	140,353	8.12%
Storage Size	8.3TB		

Key factors leading to the loss of data include:

- Inadequate management controls for data management activities
- Insufficient management controls systems and oversight of staff within the ITS Infrastructure Services division
- Insufficient review and adherence to detail to enterprise change management requests related to City production environments.

There are several key takeaways from this analysis:

- Certain data is lost and is not recoverable (i.e., data is permanently lost).
- Other data was previously entered into systems supporting City processes (e.g., City prosecution of non-municipal crimes) and is still available to the City and its business partners (e.g., Dallas County District Attorney).

Corrections to be addressed:

- ITS Infrastructure Services division continues to perform changes without the proper authorization or approval causing instability to the City's production environment.
- ITS Infrastructure Services division must implement and appropriately operate adequate management controls systems including asset and inventory management systems.
- ITS must implement and appropriately operate adequate IT service management processes to remove dependencies on email and voice communications to process requests.

- ITS divisions must implement and appropriately manage Technical and Business Services catalogs that identify and define the services and activities that ITS offers to City departments and offices.
- ITS must improve it's environmental, managerial, and operational directives and documented expectations to engender quality delivery of service over current focus upon schedule dates.
- ITS must implement and operate adequate Data Governance and Data Management controls systems to enhance the use, management, and protection of City data.

Data Governance and Data Management: The Department of Information and Technology Services (ITS) and its predecessor, The Department of Communications and Information Services (CIS), has operated inadequate data governance and data management processes and procedures. The data governance and data management framework selected by ITS is effectively used by many organizations. However, prior ITS executive leadership was unwilling or unable to adequately identify and operate the processes and procedures from this framework for data management. ITS executive leadership has emphasized a need to implement and faithfully operate data governance and data management processes and procedures to mitigate the risk of future data loss events.

This report relies upon generally available information pertaining to frameworks and standards from a variety of organizations including federal government agencies, commercial research houses, and professional standards organizations. Federal agencies include but are not limited to The National Institute of Standards and Technology (NIST), The Department of Homeland Security (DHS), and The Department of Justice (DOJ). Commercial research houses include Gartner, Inc. and Forrester, Inc. Professional standards organizations include but are not limited to Axelos, Inc., purveyor of the Information Technology Infrastructure Library (ITIL) and the City adopted Version 3 of ITIL (ITILv3), and Data Management (DAMA) International, the purveyor of the Data Management Body of Knowledge (DMBOK).

This report was constructed using information made available to the authors by ITS leadership, ITS senior managers, ITS staff, Dallas Police Department staff, City Secretary's Office staff, Backup software vendor, and outside expert professionals brought into the City to assist with the data loss event. The identified conditions, causes, criterion, effects, and recommendations for each reported factor could change if additional information is provided, discovered, or disclosed.

City of Dallas

Table of Contents

Section I – Data Loss Event 1

1 Introduction 2

1.1 Archival Data State 2

1.2 Data Loss Events 2

1.3 Cost Control Efforts 3

1.4 Procedure Non-Compliance 5

1.5 Affected Systems 5

1.6 Unaffected Systems 7

1.7 Data Handling Standards and Practices 8

2 Data loss Event Timeline 10

Section II – Factors Directly Impacting Data Loss 14

3 Requirements Documentation and Risk Assessment Processes 15

4 Solution Deployment Implementation Plans Not Faithfully Executed 17

5 Access Management Controls 18

6 Vendor Engagement and Management Processes 19

Section III – Factors Contributing to Data Loss 21

7 Data Governance and Data Management 22

8 Policies, Procedures, Processes, and Standards 23

9 Inadequate IT Services Management 24

10 Enterprise change management policies, standards, and procedures 25

11 Poor staff training redundancy and review of capability 26

Section IV – Systemic Factors Surrounding Data Loss 27

12 Management Environmental Tone 28

13 Data Handling and Data Management with specific focus on the topics of Data Backup, Data Archival, and Data Migration 30

14 Inadequate Procurement Strategy 31

Section V – Remediation Efforts 32

15 Data Governance and Data Management 33

16 Procedural Changes 35

17 Data Recovery Efforts 36

Section VII – Recommendations 40

18 Recommendation 1 - Data Governance and Data Management 41

19 Recommendation 2 – Immediate Procedural Changes 42

20 Recommendation 3 – Requirements Documentation and Risk Assessment Processes 43

21 Recommendation 4 – Account and Access Management 44

22 Recommendation 5 – Vendor Engagement and Management Processes 45

23 Recommendation 6 – Innovative DPD Data Management 46

24 Recommendation 7 – Policies, Procedures, Processes, and Standards 47

25 Recommendation 8 – Inadequate IT Service Management 48

26 Recommendation 9 – Enterprise Change Management Policies, Standards, and Procedures 49

27 Recommendation 10 – Poor Staff Training, Redundancy, and Review of Capability 50

28 Recommendation 11 – Management Environmental Tone 51

29 Recommendation 12 – Data Handling and Data Management with Specific Focus on the Topic of Data Backup, Data Archival, and Data Migration 52

30 Recommendation 13 – Inadequate Procurement Strategy 53

Section VI – The City of Dallas Administrative Directives 54

31 City of Dallas Administrative Directives 55

31.1 AD 2-XX – Data Governance and Data Management (Under Development) 56

31.2 AD 2-24– Computer Security 56

31.3 AD 2-25 – Data Ownership and Classification 57
31.4 AD 2-28 – Change Management of Information Technology 59
31.5 AD 2-34 – Data Backup and Recovery Policy, Standard and Procedures 60
Section VIII – Appendices 63
32 Appendix A – Data Governance and Data Management 64
32.1 Data Management Association (DAMA) International 64
32.1.1 Introduction 64
32.1.2 Business Case: 65
32.1.3 Methodology of Development 65
32.1.4 Data Governance: 66
32.1.5 Data Modeling and Design: 67
32.1.6 Data Storage and Operations: 68
32.1.7 Data Security Management: 70
32.1.8 Reference & Master DataManagement: 71
32.1.9 Data Warehousing, Big Data & Business Intelligence Management: 72
32.1.10 Document & Content Management: 73
32.1.11 Metadata Management: 74
32.1.12 Data Quality Management: 75
32.1.13 Tactical Implementation of the Data Management and Data Governance 76
32.2 Data Management Body of Knowledge (DMBOK) Framework 76
32.2.1 Proposed Framework 76
32.2.2 Summary 78
33 Appendix B – IT Service Management 79
33.1 Services 79
33.2 Service Management 80
33.3 Functions and Processes Across the Lifecycle 81

33.3.1 Functions 81
33.3.2 Processes 81
33.4 Specialization and coordination across the lifecycle 82
33.5 A Historical Perspective of IT Service Management and the Origins of ITIL 83
33.6 ITIL Today 84
33.7 Why is ITIL so successful? 84
33.8 The ITIL Value Proposition 85
33.9 The ITIL Service Management Practices 85
33.10 Navigating the ITIL Service Management Lifecycle 86
33.11 Core Guidance Topics – Service Strategy 88
33.12 Core Guidance Topics – Service Design 89
33.13 Core Guidance Topics – Service Transition 90
33.14 Core Guidance Topics – Service Operation 90
33.15 Core Guidance Topics – Continual Service Improvement 91
34 Appendix C – National Institute of Science and Technology 92
35 Appendix D – Criminal Justice Information Systems (CJIS) 93
36 General Terms and Acronyms 95
37 IT Service Management Acronyms 96
38 Solution Acronyms 97
39 Department Codes/Acronyms 98
40 Glossary (ITILv3 Terms of Interest) 99

City of Dallas

Section I – Data Loss Event

This section provides general information pertaining to the March 2021 data loss events at The City of Dallas.

City of Dallas

1 Introduction

During late March 2021, The City of Dallas incurred a large-volume loss of archival data stored within a contracted cloud provided service. The loss of archival data occurred when the data was migrated from the cloud provided service to an on-site data archival support system maintained to sustain the long-term retention of data. The data loss impacted various operational systems of the City; predominately supporting the Dallas Police Department (DPD). Presently the City has identified an estimated loss of 7.51 TB terabytes of compressed data, with an approximated 4.1 million files, as a result of a technical audit in August 2021, a second identified incident of 13.167 TB and an additional 4.6 million files of data loss. Resulting in a total loss of 8.262 million files lost for the event.

1.1 Archival Data State

Archival Data is historical information maintained for long-term records management purposes. Backup Data, on the other hand, is a copy of current or recent operational data created to facilitate the restoration of a system's data to a current or recent state. Operational Data is data maintained within a system to enable its day-to day operation and presentation of information.

The Archival Data associated with the 2021 data loss event has been permanently removed from the City's on-site archival system and is not available for recovery within that system. The data in this incident is presumed deleted and unrecoverable. However, efforts are ongoing to recover copies or duplication of the data from other systems where available. During the course of review and processing, data is often duplicated, moved and transferred multiple times prior to residing in an archival state.

1.2 Data Loss Events

The data loss described within this report is comprised of two separately identified incidents. The first of these incidents was discovered in early April 2021 and was a result of errors made in the migration of data from a cloud provided service to an on-site data archive.

Subsequently, as ITS conducted its Data Loss audit, following the Incident Response Plan, an additional data loss incident was identified. Some of the additional data loss is tied to the original incident and, some is new. This briefing is to review the additional areas of concern. The City's vendor, Commvault, and ITS continue to parse and analyze the City of Dallas environment to determine where any impacts may occur.

- On Thursday, August 26, 2021, Commvault incident ticket (210815-92) was opened.

- The ticket was an alert, to the City, for a possible data archive storage irregularity.
- ITS engaged with a response to immediately triage the alert, with the Chief Information Security Officer (CISO), ITS Infrastructure Services Assistant Director (AD), Server Support Manager, and the DPD Business Relationship Manager (BRM), to determine the severity of the new incident. the assessment, from the triage, required the engagement of Commvault support engineers.
- ITS provided the Commvault support engineers with the logs and archive policies to scan, review, and assess.
- Initial assessment results were discussed (CISO, ITS Infrastructure Services AD, Server Support Manager, and the DPD BRM, and Commvault) on Friday, August 27, 2021, and then communicated to ITS Executives.

1.3 Cost Control Efforts

In reviewing the events leading to the data loss, information available indicates the planned migration of data in late March 2021 from the cloud provided service to the on-site data archive was part of an effort to reduce the City's associated data costs.

In 2015 the City of Dallas engaged with Microsoft for Azure cloud services under Council Resolution 15-1049. The CIS department brought forth the effort to begin cloud migration process of moving digital operational loads from the City's on-premises data centers to an "in the cloud presence." The cost estimate for cloud expenditures had been recognized to be $60,000 per year to take advantage of Azure's Hybrid Storage (Storsimple). Additionally, in 2018 the City provided an additional cost expenditure for an "express route" connection to reduce network latency and rapid data services to Azure. Subsequently, these costs had not been renegotiated or presented for competitive bid to evaluate and optimize cost controlling estimations for cloud services.

In 2019, with changes to ITS management, ITS had a $908,000 expenditure associated with Azure cloud services. At that time an estimated 5% of the City's workload had been migrated to the cloud. In 2020, the workload had increased to an approximate 10%, with an increase to $1.8 million in expenses. Subsequently in 2021, the City had an approximate $122,000 monthly cost, which exceeded the cloud expenses beyond its expected $100,000 per month budget. Whereas in 2021, that workload had decreased to 7% of IT services.

Cloud migration strategies must be well-defined and properly assessed process prior to implementation. Intelligent cloud migrations efforts evaluate available options based on service and mission needs,

technical requirements, and policy. Processing and technology decisions must consider customer impact against cost and cybersecurity risk management criteria. Calculations such as server requirements, network bandwidth, and application resources all must be considered. [Gartner]

A complete architectural analysis and design must be in place prior to performing a cloud migration. Additionally, cost associated with cloud-based solutions include compute, storage, and data transfer. Consequently, those estimates must then be translated to a negotiated cost expectation with the vendor. These basic requirements and the application of cloud principles were not performed adequately, except for assumed cloud benefits. [Gartner, ITILv3]

Fiscal responsibilities and tax revenue appropriations actions place a high burden of accountability upon the City to ensure that appropriate cost estimates are developed using a realistic and accurate spend model [GAO Green Book]. It was communicated that prior to the attempted data migration and subsequent data loss, ITS performed a review of its spend patterns against the current allocated budget, showing an unsustainable spending metric. It was also communicated that as a result of the spend analysis ITS leadership's decision was to return certain workloads back to a more cost controlled on-premises storage model even though adequate risk assessments had not been performed.

In considering the need for better cost-controlled implementation, ITS leadership should have identified all potential risks. [NIST] At no point did technical and managerial resources assess cost and technical risks against best practices.

According to the National Institute of Standards and Technology (NIST), several high risks include data loss at large volumes during moves between environments and considerable process disruptions across an entire organization. To avoid detrimental organizational impacts, IT departments must consider a thorough disaster recovery plan if data goes missing. [NIST]

Based upon NIST best practices and Microsoft Azure guidelines there were inadequate backout or disaster recovery procedures for a large volume migration defined and in place to prevent this data loss. [NIST, Azure] According to Microsoft cloud usage best practice, ITS should maintain multiple methods for the prevention of data loss. Migrations of large volumes of data must be well planned and summarized. [NIST, Azure] Key technical and managerial oversight with redundancy of testing and validation for any migration is vital to any successful data transference. [NIST, Azure, Gartner] None of these measures or validations were completed or in place at the time of the March 2021 data loss events.

As best practices of cloud backup and storage is key to a well-balanced recovery effort, abandonment of the cloud effort should not be considered. However, ITS leadership must provide an appropriate cost analysis and controlled budget spending model. ITS must adhere to a best practice model by completing and reviewing strategic cost and risk analysis of that usage. These measures would have greatly reduced the risk of the "K" drive migration data loss. [Gartner, Azure]

1.4 Procedure Non-Compliance

The City of Dallas backup process has no explicit data management procedures for the archival of data. For example, data management procedures should include procedures for the migration of archival data from cloud-based solutions to on-site City archival data storage solutions. [DAMA] Vendor provided procedures when accurately followed, provide instruction to properly migrate archival data from City cloud-based storage solutions to less costly on-site archival storage solutions. These vendor-developed solution procedures, however, do not address the City's data management goals, objectives, or requirements.

The City of Dallas has determined that City personnel failed to faithfully follow the data migration procedures for archival data provided by the software vendor. [CommVault] Additionally, it has not been determined that the City personnel in question notified City management that the procedures were inaccurate, incomplete, or incorrect to permit City review and update of the archive data migration procedures.

Any software typically has a defined methodology (i.e., procedures) to using the software. These procedures, especially where data deletion can be detrimental to the City or business department use and access of data, must be well understood prior to taking actions against a production environment. In the ITS review, it was determined that either there was an obvious misunderstanding or disregard for the defined procedures on the part of the employee. Additionally, in reviewing the procedures, ITS found that the vendor's software allowed for multiple options to prevent the loss of data during a migration or move. The technician is afforded multiple warnings and multiple opportunities to cancel and review the risk associated with an action prior to completing the configuration change. In reviewing the actions of the technician, it appears that they did not heed these warnings.

1.5 Affected Systems

The ITS Data Loss Audit, following the actions required by the ITS Disaster Recovery Incident Response Plan, has identified City systems suffering impact from these data loss events. Some systems identified

were immediately known upon initial data loss. Additional systems experiencing data loss were identified after further review and investigation.

Archival and Backup Data has been permanently removed from City cloud-storage solutions and from City on-site archival data storage solutions for the following systems:

City Secretary Office:

The preliminary audit identified a 2.133 TB data loss because of the deletion of backup data to the City Secretary's server. However, after further examination, discovery of a secondary policy provided evidence the technician had duplicated the archive policy. Subsequently, as a result of further investigation through the audit with the vendor, the data was shown to be found to be intact.

- All audited data as present.

Dallas Police Department:

CAPERS – The preliminary audit identified a 244.02 GB data loss because of the deletion of backup data to the CAPERS server. However, after further examination, discovery of a secondary policy provided evidence the technician had duplicated the archive policy. Subsequently, as a result of further investigation through the audit with the vendor, the data was shown to be found to be intact.

- All audited data as present.

FUSION – Between November 20th, 2019 until August 22, 2020 434 archive jobs caused the deletion of data from the FUSION server. The backup jobs were on the "F" drive as part of the storage for server. The archive age for all volumes on the server "F" drive were set to 10 months. With the deletion occurring on March 31, 2021, any file that had not been modified prior to June 1st, 2020 was deleted.

- F drive - 13.167 TB

Archived "K" drive – The data migration from cloud storage of the archive to on-premises at the end of March 2021 by improper methodology in the migration process led to 7.51 TB of data loss. The data loss consisted of an approximate 4.1 million files from multiple divisions of the Dallas Police Department. However, the majority of the loss has seemingly affected the Family Violence Unit. This data consisted of information gathered by DPD detectives for prosecutable, adjudicated, on-going cases; or general evidence gathered.

- K drive – 7.51 TB

1.6 Unaffected Systems

After completing a thorough technical review audit on August 27th, 2021, of all archival data against the archival and backup technology, multiple systems were shown not to have suffered data volume loss or data permanently removed from City cloud-storage solutions or from City on-site archival data storage solutions for the following systems of concern:

Dallas Police Department (DPD): Records Management System (RMS). The RMS system is a primary system that is utilized by DPD for digital evidence which is then uploaded to Lumen Law Enforcement Agency Portal.

- All audited data as present.

Dallas Fire-Rescue (DFR) The DFR backup and archive systems are file shares provided to Dallas Fire Rescue for retention of files.

- All audited data as present.

Office of the City Attorney (CAO) backup and archive systems are file shares provided to City of Dallas Attorney Office for retention of files.

- All audited data as present.

City Controller's Office (CCO) backup and archive systems are file shares provided to the Controller Office for retention of files, including Advantage Financial System.

- All audited data as present.

Dallas Water Utilities (DWU) backup and archive systems are file shares provided to the Department of Water Utilities for retention of files.

- All audited data as present.

Department of Aviation (AVI) backup and archive systems are file shares provided to the Department of Aviation for retention of files.

- All audited data as present.

Department of Public Works (PBW) backup and archive systems are file shares provided to the Department of Public Works for retention of files.

- All audited data as present.

ITS e-Discovery backup and archive systems are file shares provided to the ITS eDiscovery for retention of files.

- All audited data as present.

Geographical Information Systems (GIS) backup and archive systems are file shares provided to the DBI GIS for retention of files.

- All audited data as present.

ITS Big Data Initiative backup and archive systems are file shares provided to the Big Data Information Systems for retention of files.

- All audited data as present.

1.7 Data Handling Standards and Practices

The City of Dallas has undeveloped data governance and data management policies, standards, and procedures in place. A basic Data Management Strategy document is published on the City's external website. However, the data management strategy document is out of date and has not been implemented as a formal activity and process within the City's data environment.

Data Management exists to a degree in each department based upon the individual department's needs. The current the management exists is due to municipal, County, State, or Federal regulatory requirements. Some efforts exist for Data Quality are in the use of addresses across the departments, but not in a standardized framework methodology or requirement.

The City also lacks adequate management controls systems for unstructured data. There are few controls on what data can be stored unless there are specific regulatory requirements. Backup of unstructured data occurs, but recovery testing for unstructured data is rarely performed unless there is a specific audit requirement to do so. There is rarely, if ever, an audit to ensure that all required unstructured data is backed up via approved methodologies. The management of unstructured data in a cloud environment adds difficulties requiring additional skill sets and monitoring that is usually not available or implemented.

The failure to have a complete, centralized, and enforced Data Management capability managed and enforced by a Data Governance committee is a factor in the conditions which led to an environment in

which the loss of data is possible. This failure, particularly regarding unstructured data was a significant factor, among many others that culminated in the loss and resulting inability to recover the Dallas Police Department data.

2 Data loss Event Timeline

The following timeline is related to the DPD data archive deletions.

The backup technician began the unauthorized process of "Hard Delete Client", through Commvault, beginning on March 30th and continuing until March 31, 2021.

Monday April 5, 2021 (approximately 9:00 am) – The backup technician received the first of many customers service tickets from DPD staff indicating missing or inaccessible files.

Monday April 5, 2021 (approx. 11:00 am) – The backup technician shut off all library deletions – effectively stopping the client clean-up process.

Monday April 5, 2021 (12:08 pm) – The backup technician contacted Commvault support to begin the recovery process and determine the extent of the incident.

Monday April 5, 2021 (approx. 12:30 pm) – The backup technician contacted his manager to notify of the incident. The backup technician was told to continue the recovery effort and inform the manager of the full extent.

Tuesday April 6, 2021 (7:00 am) – The backup technician's manager contacted the Infrastructure Assistant Director to inform him of the incident and the extent of the known impact.

Wednesday April 7, 2021 (3:30 pm) – The initial report indicated a total of 22 TB of storage was archived and 11 TB of files had been restored by the backup technician and the vendor by this time. Subsequent investigation through log analysis have determine the actual amounts are as follow:

- 14 TB de-duplicated data was archived in Azure storage (35 TB of "raw" file data that is not de-duplicated)
- 10.77 TB data was deleted by the events on 3/30 – 3/31
- 3.26 TB of (recovered data)
- 7.51 TB of data impacted (deleted data)

Thursday April 8, 2021 (2:00 am) – Final report from the backup technician showing the total missing archive files (approx. 11 TB initially).

NOTE: This timeline represents the actions and investigations for the missing data files from the DPD "K" drive, only. This does not include "CAPERS" or "FUSION" servers.

City of Dallas

Period 3/26-8/25/2021	Events
Tues. 03/28/2021	**CA CHG Ticket 117304 - Implement a new Azure storage library**
Weds. 03/31/2021 17:04 PM	On March 31, 2021 at 17:04, Technician deleted the Commvault storage policy Archive. The effect from this deletion was to delete all jobs associated with that storage policy. Five servers were impacted by the deletion: server. In additional the storage index was deleted. The initial investigation has centered around servers.
Tues. 04/06/2021 9:27 AM	DPD ITS BRM and the ITS Infrastructure Assistant Director notified the CIO.
Fri. 04/09/2021	CIO & CFO discussed the data loss issue
Tues. 04/13/2021 2:53 PM	CIO notified City Leadership, "Purpose of this email is to inform you of a mass data loss occurring because of an error during the performance of routine file transfers from Azure storage to the City Hall storage of the DPD file archives.", "We are setting up a meeting with DPD leadership this afternoon."
Weds. 04/14/2021	Meeting with DPD leadership and ITS DPD BRM

Period 08/26/2021	Events
Thur. 08/26/2021 18:25 PM	CISO activated the IRP for the data loss analysis
Thur. 08/26/2021 18:28 PM	Incident Manager Reached out to Assistant Director
Thur. 08/26/2021 18:30 PM	Incident Manager setup a Teams meeting
Thur. 08/26/2021 18:35 PM	P1 Ticket opened - Possible storage policy deleted from every department - March 31 2021 - Commvault notified CoD 8/26/21
Thur. 08/26/2021 18:45 PM	Triage: ITS Leadership
Thur. 08/26/2021 18:57 PM	Manager to reach out to Commvault - verifying that arch data
Thur. 08/26/2021 19:05 PM	Commvault ticket 210815-92
Thur. 08/26/2021 19:25 PM	Triage with Commvault Supt - ETA follow-up 23:30 pm Commvault follow
Thur. 08/26/2021 23:30 PM	Commvault Status Call
Fri. 08/27/2021 07:30 AM	Data Loss Analysis update
Fri. 08/27/2021 07:35 AM	Communicated status to CISO/CIO
Fri. 08/27/2021 08:05 AM	Review Assessment Matrix with AD
Fri. 08/27/2021 08:35 AM	Review Assessment Matrix with CISO
Fri. 08/27/2021 09:00 AM	Review Assessment Matrix with CIO
Fri. 08/27/2021 13:30 PM	Review Assessment Matrix with City Leadership
Fri. 08/27/2021 14:15 PM	Reached out to Infrastructure Management regarding artifacts for the City Secretary Office and RMS
Fri. 08/27/2021 15:30 PM	Meeting with the City Secretary Office
Fri. 08/27/2021 16:05 PM	Formal notice of possible data loss went to the CMO, Mayor's office, Council and the DA Office
Fri. 08/27/2021 16:25 PM	City Secretary Office noticed that they may have a separate copy of their 2019 Archive
Fri. 08/27/2021 16:30 PM	Meeting with Commvault for status on the City Secretary office and RMS

Fri. 08/27/2021 17:57 PM	Commvault updates provided to CIO
Fri. 08/27/2021 21:00 PM	Meeting with ITS Leadership
Mon. 08/30/2021 09:50 AM	Infrastructure Management - Working with Commvault to create identification tool, to identify the stubs. ETA COB 9/1
Mon. 08/30/2021 17:30 PM	Review daily activities
Wed. 09/01/2021 17:30 PM	Identification tool progress – In Progress, BRM to provide Compliance the upcoming DA cases - Completed; Wednesday kickoff Meeting with Birch Cline Consulting https://www.birchcline.com data specialist data recovery like rehydration
Thu. 09/02/2021 17:30 PM	Server Manager to confirm City Security actual data loss – possibility additional archive – CIO would like by COB; List is in process for server. Awaiting SEC communication; Commvault update meeting for 8am on 9/3
Thu. 09/02/2021 21:45 PM	(CO) change orders sent to Sr. Manager Compliance
Tue. 09/07/2021 08:30 AM	Commvault scripting: No update. ETA is 9/7 Awaiting callback from Commvault; Evidence Collection ETA is Friday 9/10; Two GTS resources started today, 9/7 – 22k email; Storage est. ETA due <5-10d>
Thu. 09/09/2021 08:30 AM	Review daily activities
Sat. 09/11/2021 11:00 AM	Technicians are on Track to meet Hitachi at City Hall @ 11am; Technician is on Standby to do the Bitcopy to the Hitachi once that is stood up later this afternoon/early evening; I will let BRM know to be prepared to let DPD know our current timeline; Technicians are standing by to do the alternative Bit Copy with the USB drives to be procured/delivered today; Either direction, we should be good to start the bit copy early this evening at the latest.
Sat. 09/11/2021 18:11 PM	We are going to span the Fusion image across two drives; technician should be starting shortly, if not already; Hitachi install is ongoing. Having a little issue getting into the brocade switches. Working that now, but system I installed, fired up and configuration is in progress
Sat. 09/11/2021 18:27 PM	Storage controller is configured as best Hitachi can do from what they knew; Hitachi created 4 Luns of 10 TB each (40 TB total) and assigned them to ports as Lun # 10 – 13; Connected cables to existing Brocade switches; We can "see" the wwns of other servers from the storage side, so connection to the Brocade is good for all 4 paths; We couldn't log into the Brocades to do the zoning however, so that is where it sits. Storage side is good now; For USB drives - technician stated the data copy process to the *.E01 image format has been started and is now running. The estimated completion time has not been returned by the tool yet, he will send out an update with that information as soon as it is available.
Sun. 09/12/2021 12:12 PM	From technician: We appear to still have approximately 52 hours left, the copy rate is slower than anticipated.; We are around 25% this morning, at the current throughput we are looking at some time Tuesday morning; I will continue to monitor and update you if anything changes.

Mon. 09/13/2021 17:30 PM	Microsoft meeting 9/10 – Process to scan, storage, rehydrating – dependency on clone completing; Commvault script 9/10 – DPD and City Secretary Office – Upgrade once clone completed – Tuesday PM 9/14; Commvault legal 9/10 – Statement – completed; Pull down Fusion Servers – In progress – ETA Tuesday PM 9/14; Hitachi walk-thru – 90% Completed 9/11; CISO – Has engaged a vendor to sift thru the data faster; CISO – Report framework kicked off for 9/30 complexation
Wed. 09/15/2021 17:30 PM	Hitachi walk-thru – Completed 9/11; Commvault script 9/10 – DPD and City Secretary Office – Upgrade once clone completed – Clone eta Tuesday PM 9/14; Technician to pick up USB by Thursday 9/16; Microsoft meeting – Process to scan, storage, rehydrating – dependency on clone completing; Commvault legal – Statement – completed 9/13; Pull down Fusion Servers – Completed 9/14; CISO – Has engaged a vendor to sift thru the data faster - Follow-up meeting for 9/16; Commvault upgrade CRB 9/16 – ETA to upgrade is 9/19; CISO– Report framework kicked off for 9/30 Report complexation - Draft ETA due 9/16;
Recovery Mode	

City of Dallas

Section II – Factors Directly Impacting Data Loss

The City of Dallas March 2021 data loss events are directly affected by the following factors present within the Department of ITS:

3 Requirements Documentation and Risk Assessment Processes

Documentation and risk assessment are critical components of best practices for change management within an Information Technology (IT) environment. They engender understanding and provide guidance to a technician of the potential and possible risks associated with a change request, as well as define the criticality of the data and activity or project. The City of Dallas Administrative Directives and standards are published to provide guidance and direction on how to complete a change. However, the criticality of changes and risk assessments must be completed and articulated to leadership and the business to fully understand the risks associated with the change.

In reviewing the planned data migration, the ITS technician involved in the data loss event insufficiently assessed and documented the potential risk of this change. This was a direct and contributing factor to the data loss. Although there was documentation, it mostly described architectural components and particular information as to where the data migration would reside. According to Information Technology Infrastructure Library (ITILv3), a best practices framework for IT service management adopted by the City's IT department in 2010, thorough documentation should include:

- Cost-benefit (Cost-effectiveness)
- Resource availability
- Identified risks
- Impact on other services and business impact
- Compliance requirements (if any)

Three ITS Infrastructure Services managers reviewed the change request leading to the March 2021 data loss events. To that end, the ITS Infrastructure Services managers either did not understand the actions to be performed, the potential risk of failure, or negligently reviewed the Change Request prior to providing authorization and approval to proceed with the Change Request.

ITS executive leadership and senior management must understand the need for necessary process documentation and comprehensive risk assessment – especially for infrequent, high-risk activities. ITILv3 provides categories and direction for documentation. ITS executive leadership and senior management must clearly set the appropriate environmental tone through documented directives and performance expectations so that all personnel understand that actions have repercussions and that appropriate risk mitigation activities must be taken to ensure desired business outcomes are achieved. Finally on this topic, ITS executive leadership and senior management must adequately perform thorough risk

assessment oversight to ensure appropriate and adequate activities are performed in a risk-reduced way.

4 Solution Deployment Implementation Plans Not Faithfully Executed

Commvault provided the City with detailed documentation for the processes and procedures necessary to effectively move data between environments (e.g., Microsoft Azure and City hosted data archival solutions). Microsoft Azure additionally provides a best practice process and procedure statements for these types of moves. The City's Administrative Directive 2-28 and ITILv3 processes and procedures relative to Change Management also require detailed implementation plans and backout plans. Development or use of poor implementation plans and procedures increase the likelihood that failures will occur during deployment.

The technician implementing the solution did not follow vendor data migration procedures or best practices identified for data handling or data migration. According to the vendor's procedural documentation the technician was non-compliant with the data migration practices detailed by Commvault and accepted by the City.

ITS leadership had insufficient oversight of the migration considering the criticality of the data. Inadequate monitoring and deviation from procedures directly contributed to the loss of City data in March 2021. Again, ITILv3 processes and procedures require appropriately detailed backout plans to ensure the integrity and operation of a production environment. The internal and external process and procedure requirements cannot be ignored without raising the risk to the City's production environment.

ITS executive leadership and senior management should take certain organizational steps to prevent future data losses of this type. Leadership must instill a sense of integrity through appropriate organizational tone. ITS executive leadership and senior management must stop deployments upon deployment script failure and begin execution of backout plans. ITS executive leadership and senior management must faithfully follow backout plans to ensure the safety of the City's production environment.

5 Access Management Controls

Identity and Access Management (IAM) is a framework of policies and technologies to ensure that the right users have appropriate access to technology resources. IAM practices help an organization identify, authenticate, and control access for individuals utilizing technology resources. Access to technology resources by individuals and/or systems is controlled through the definition and application of accounts by which access is granted. Service Accounts are accounts that are used by software (normally on a server) to carry out automated tasks such as running backups. User Accounts are used by staff in their day-to-day work to log onto a computer and perform their job duties. Administrator Accounts generally provide the highest levels of access, often allowing the user to change security settings, install, and configure software and change permissions on other user accounts. Service accounts should only provide minimized permissions necessary for the needed services of the system to prevent potential damage or data loss.

NIST special publications area define Access Management controls, systems processes, and procedures. Additionally, the City of Dallas has standards definition for different accounts, such as service, user, and administrative accounts. The practice area definition expands and discusses access management and control practices that are described in NIST 800-53 Security and Privacy Controls for Information Systems and Organizations and are the standards adopted by the City. Microsoft provides guidance to review and reduce the number of accounts in highly privileged administrative groups.

Additionally, all activities performed under an Administrator must be tracked and assigned to the administrative account. In the case of the March 2021 data loss events, system records are tied to administrative user accounts rather than to a service account “owned” by the service, constituting improper use of an Administrator Account and privileges to manage the application. In this instance, the concept of Least-Privilege Access is violated. This violation of account usage emphasizes the mismanagement of accounts by the technician and was a factor in the March 2021 data loss event. Additionally, when a technician leaves this misuse of accounts can cause disruptions to services for the backup and storage processes tied to the account. These actions created gaps in the backup process which could have caused additional damage to the backups and archives. City personnel must not use Administrator Accounts to operate services as occurred in this instance.

6 Vendor Engagement and Management Processes

The Vendor Management process ensures that vendors, the technology, and services they provide are managed to support the City's IT service goals and business expectations. Vendor management poses risk in two areas. First, according to Department of Homeland Security, vendors place additional risk on the City by allowing external access to the systems that support the Infrastructure. Additionally, the City becomes dependent on the vendor for support of the services ITS provides to the City departments. The aim of vendor management is to provide additional services where skills gaps are present and support service for resource assistance. Overdependency on vendor management of service and system are limited to the contractual obligations and are difficult to pivot to additional needs or changes within the environment.

The purpose of the Vendor Management process is to obtain value to cost from the suppliers as well as to ensure performance of the contract and agreements, while conforming to all the terms and conditions.

The main objectives of the Vendor Management process are to:

- Ensure that underpinning contracts and agreements with suppliers are aligned to business needs.
- Support and align with agreed targets in Service Level Requirements and Service Level Agreements.
- Manage relationships with suppliers.
- Manage supplier performance.
- Maintain a supplier policy and a supporting Supplier and Contract.

The ITS department is highly dependent upon vendors for the delivery of service solutions to City business systems. ITS executive and senior management must have identified scope and requirements included in the contractual negotiations prior to implementation of services. Contract management must hold vendors to measurable performance metrics. In addition, ITS personnel should have sufficient skills to address conflict issues between the vendor and the City, with a full understanding of the systems. Ultimately, ITS is accountable for systems managed by vendors and should ensure processes and procedures align with that accountability and vendor responsibility.

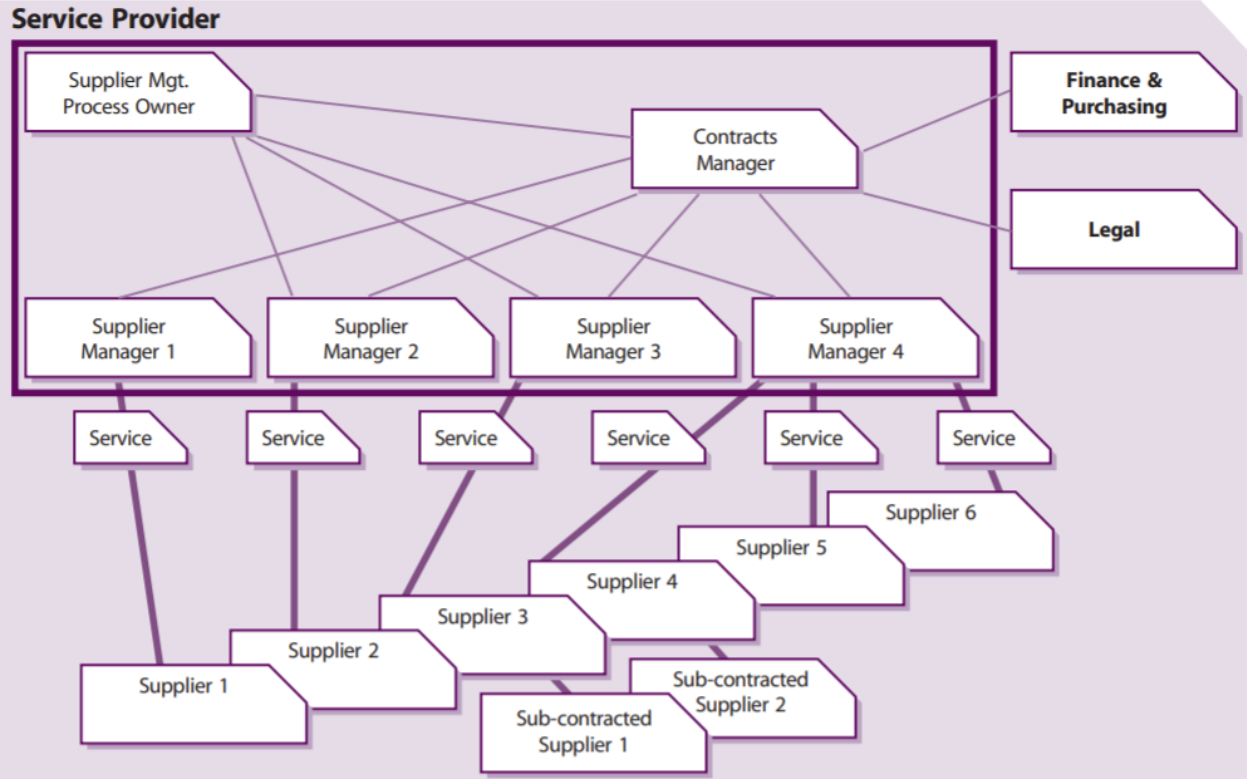


Figure 1 ITILv3 Vendor Management - Roles and Interfaces

City of Dallas

Section III – Factors Contributing to Data Loss

The following factors have been identified as contributing to the March 2021 data loss events.

7 Data Governance and Data Management

Data governance and management provides direction and guidance to the retention and handling of data. The City of Dallas has not emphasized the governance of data. Recently with the development of Data Business Intelligence and Analytics there has been a City-wide movement to protect and secure data in a better and more regulated manner. Departmental Data Stewards or similar Data Subject Matter Experts do not exist within the Departments to provide guidance and requirements for the ITS Data Custodians. This need is particularly critical when the Data Custodians are managing highly sensitive data such as evidentiary or other critical public safety data.

Due to lack of Data Governance, the requisite policies and standards are non-existent, or if in existence they are not adequate for the tasks to create the procedures to ensure well managed Data systems. The City of Dallas ITS has identified the Data Management (DAMA) International Data Management Body of Knowledge (DMBOK) as a data governance and data management standard appropriate for use. However, existing standards for the backup and then testing of recovery of data do not exist, particularly at the unstructured data level. The published AD 2-34 for backups is out of date and does not represent a modern on-premises and cloud-based infrastructure.

The City of Dallas does not have adequate data governance and data management policies and procedures to govern and appropriately manage data of all types. In addition, ITS will not be able to appropriately or adequately govern or manage data according to the requirements needed for the City of Dallas. Without proper, fully implemented Data Governance in place, the City is at risk of further loss of data, inability to recover from onsite failures causing loss of data, disaster recovery requiring recovery of data, liabilities from inappropriate exposure of data, and inability to fully realize the analytical value of the data due to a lack of quality or inability to aggregate across departments and data sets.

The City of Dallas must identify an appropriate and adequate level of Data Governance and Data Management to guide and support its operations. Creation of Administrative Directives, policies, procedures, and processes all must be developed, socialized across the City and appropriately followed to govern and provide guidance. Once identified, the City must implement, operate, and manage both data governance and data management activities.

8 Policies, Procedures, Processes, and Standards

Policies, procedures, and processes are vital components of any department to ensure the activities and services are completed in a timely manner. Subsequently, they govern the management of executives, senior managers, and employees toward not only compliance but best practices. In addition, if procedures and processes are well-defined, duplication of efforts and consistency within the processes can be matured and oftentimes automated. Previous cultures had allowed for a “jack of all trades” execution of IT Services approach. This allowed for uncontrolled access and management of systems outside the Administrative Directives and standards.

Although ITS has adopted the IT management controls based in NIST standards, there are multiple areas in which the framework has not been fully realized. There are inadequate policies, processes, and standards for staff to follow within ITS. It is evident these do not exist sufficiently within the backup and storage team or management of systems. There were little to no control artifacts for process inspection. Management controls are insufficient to provide staff guidance and direction.

Lack of knowledge regarding the creation, development, establishment, operation, and management of policies, procedures, and processes was a contributor to the data loss. However, given evidence the technician did not follow vendor technical or functional guidelines, the data loss event cannot be solely contributed to the lack of established policies, procedures, and processes. The lack of management controls systems causes organizations to perform “best effort” activities to address daily demands and activities.

All ITS divisions must establish, operate, and maintain adequate management controls systems. These should follow a best practice framework such as NIST. Management controls should be periodically reviewed and maintained for evidence of proper operations and relevancy. Additionally, these need to be available for use to the City Controller’s Office, the Chief Financial Officer, and the Office of the City Auditor. Subsequently, management controls must be mapped and documented to all daily activities for the operations of the technical systems.

9 Inadequate IT Services Management

Technology services should be guided by a standardized process. The City of Dallas adopted ITILv3 in 2010 for service delivery to the business departments. ITILv3 is an industry-wide international standard for IT service management. The service management processes identified and described in ITILv3 have enabled many IT service organizations to achieve cohesive, competent operation while reducing costs and risks to the organization. Adopted Information Technology Service Management (ITSM) practices describe industry-standard approaches to adequately identify, scope, define, design, deploy, operate, and manage IT Services to support Business Services.

Support Services should identify and define services for publication in a Technical Services Catalog. The services published within the Technical Services Catalog will allow the identification, development, and publication of appropriate Service Request types that may be automated within an IT Service Management solution for leadership monitoring and reporting.

ITS does not operate an adequate service-based model. Service is demand-driven and uneven in application to individual departments. ITS executive leadership must require oversight or change to ensure that it adequately scopes and operates IT services in support of City-desired business outcomes produced by department Business Services (e.g., Building Inspection).

Failure to identify, define, and operate effective service management processes fails to set clear expectations and may engender an inappropriate organizational “tone” which may lead to the disregard for processes and procedures. ITS Infrastructure Services does not have adequate Service Request Fulfillment processes. Failure to establish necessary service management processes and service delivery procedures were a direct contributor to the March 2021 data loss event. ITS has initiated an effort to mature its service management process based upon ITTL v3, through an implementation of an ITSM system. However, the ServiceNow system is nascent and requires time and proper process development to be effective.

ITS executive leadership and senior management must embrace both the letter and the spirit of IT service management by following the ITILv3 framework already established. ITS executive leadership must require that service management processes be followed and grant few, if any, management exceptions. Additionally, ITS senior management must periodically update service management processes and procedures to be both effective and efficient in the attainment of desired business outcomes.

10 Enterprise change management policies, standards, and procedures

As the City has chosen to adopt ITILv3 for its IT best practices services framework, adherences to those practice should be fully realized. In this instance, ITS executive leadership failed to understand the need for full compliance with the policies, processes, and procedures related to change management of enterprise information technology. Although change processes were followed by technical resources, those processes were not fully reviewed or understood to the possible effect that led to the data loss. ITILv3 change processes have certain criteria that must be met prior to approval of change to move forward.

All criteria functions could not have been properly in place. As stated, ITILv3 framework provides that all change must have a back out procedure allowing for the technical resources to reduce the risk of the change. If properly realized or reviewed the backout procedure should have provided a recoverable option for the loss of the data after the migration. The failure to understand the need for full compliance with change management policies, processes, and procedures put the City's production environment at risk leading to the data loss. Additionally, during the process validation, the data should have provided indicators to the technician and managers that there were issues that could lead to data loss.

ITS management failed to understand the risk and impact of the change. As well, additional scrutiny was not placed upon the change requestor(s) to ensure changes could not cause grave harm to the City's data or reputation. Technical changes hurried through the process with poor planning, scheduling, detail, and documentation do not identify all potential risk and are contrary to best practices or standards. Industry-accepted change management practices are identified and applied within the City's production environment. These change management practices identify specific types of change, when they are used, and the benefits to using each type of change.

ITS executive leadership must oversee and enforce necessary ITILv3 practices, as well as communicate high-risk items that may have a negative impact on the City's data environment and reputation. There must be oversight and clearly defined expectations to personnel to engender the proper operational tone as to the criticality of change management of information technology.

11 Poor staff training redundancy and review of capability

Strategic Human Capital Management practices dictate an organization routinely assess the skills needed by the organization to perform its current and future functions, assess the skills present in its current workforce and develop plans to either develop the necessary skills in its current workforce and/or supplement its workforce through recruitment or outsourcing. ITS provides training funds for its employees. The organization supports both specific and role certifications as needed to perform the job functions. Technology vendors and standards frameworks suggest the best practices for IT staff to maintain knowledge about the technologies technician's support. The vendor documentation provides detailed technical instructions on the methodology for many of the actions required. The vendor technical documentation provides caution or explicit components to instruct the technician on certain actions that could lead to a damaging problem. Instructions were either never presented, read, or reviewed by the technicians and management prior to actions leading to data deletion. ITS executive Leadership and senior management do not procure and require training on a scheduled basis to maintain the latest knowledge of those functions. Additionally, training and review by management are not completed. [NIST, ITILv3, Vendor]

The ITS storage and backup technician lacked depth, training, and expertise in best practice functional and technical procedures. Given the department's budgetary allocation for training opportunities, leadership should mandate technical training where appropriate for the job function. Additionally, this should be present as a component of the employee's performance evaluation. Follow up testing and actions would maintain staff skills and ability to properly follow best practices and technical processes. In this instance a single member from a team was able to delete and change vendor defined procedures that were out of line from best practices and the backup solution's configuration procedures. Staff lacked the expertise and knowledge creating technical mistakes and problems for the City's data management and storage.

Additionally, training and depth of job functions for various IT tasks need to be established, especially for critical areas of responsibilities. Furthermore, testing and review of those critical function areas must be completed. Trainings should be documented, tracked and required for multiple members of a team, including training offered outside of traditional environments. if the team is composed of a small number of ITS staff, other functional team members would benefit ITS and the City by allowing for a depth in knowledge for areas of critical function.

City of Dallas

Section IV – Systemic Factors Surrounding Data Loss

The following information describes systemic factors surrounding the March 2021 data loss event at The City of Dallas.

12 Management Environmental Tone

The appropriate management tone must be set through management directives and clearly documented performance expectations. Setting this tone is necessary for the organization to be successful in accomplishing its mission, which in this case is IT service delivery. Failure of ITS executive leadership and senior management to have appropriate directives and clearly documented expectations in place causes a breakdown in operational effectiveness. GAO-14-704G Standards for Internal Control in the Federal Government states in Principle 1 subcomponent 1.01 that "The oversight body and management should demonstrate a commitment to integrity and ethical values." The subcomponent requires the following leadership attributes "contribute to the design, implementation, and operating effectiveness of this principle:

- Tone at the Top.
- Standards of Conduct.
- Adherence to "Standards of Conduct".

ITS executive leadership and senior managers must employ management controls systems (e.g., policies, processes, standards, procedures, and performance expectations) but more often the practices in directing, guiding, or performing activities is by more ad-hoc methods causing confusion and low efficiency within staff and the City.

Gaps in documented management directives and clear expectations around management control systems instantiating and commitment to the City of Dallas's core values of excellence, ethics, empathy, and equity exist. Ad-hoc project or work management techniques can lead to incidents such as the March 2021 data loss events.

ITS executive leadership and senior management may create the necessary "tone at the top" of the organization by demonstrating that effective process execution leads to quality work. Processes should not be overridden for any but the most exceptional reason.

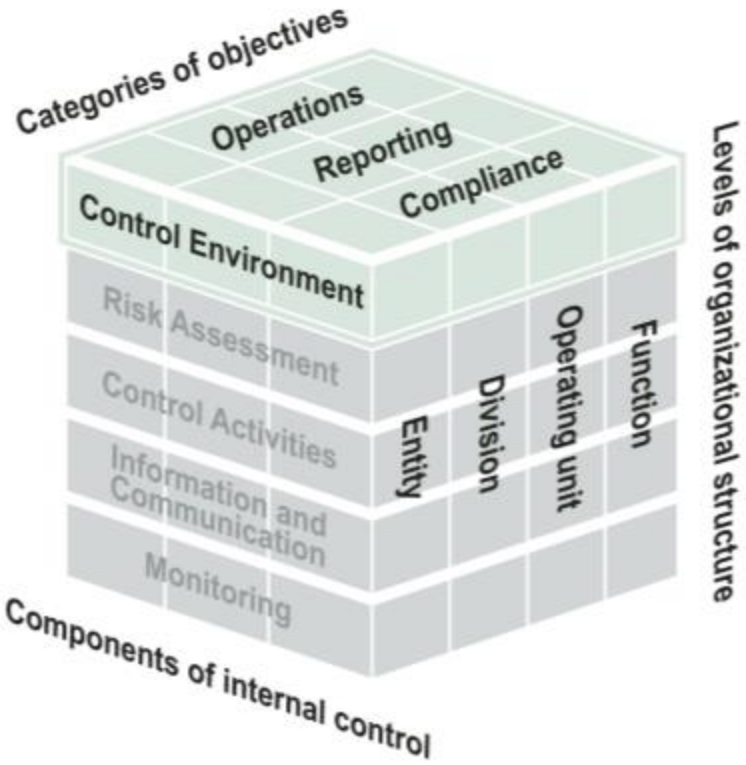


Figure 2 COSO Internal Controls Cube

13 Data Handling and Data Management with specific focus on the topics of Data Backup, Data Archival, and Data Migration

ITS Leadership must ensure that appropriate data handling policies, standards, and procedures have been implemented to ensure that areas such as data backups, data archival and data migration activities occur based upon industry standard methodologies and procedures. For example, the informal standard is that all production data should be backed up. There are no formal procedures for the backup of data and the requisite testing of recovery activities to ensure successful backup activities. There are no departmental or division auditing activities to ensure data management activities are occurring.

A lack of understanding among the ITS staff and leadership as to the importance of Data Management controls, policies, standards, and procedures and the requisite governance of these activities contributed to the March 2021 data loss event. As the City increases the amount of unstructured data it manages, it must ensure that it matures its practices around the unstructured data, such as the data files lost in this incident. That disconnect also contributed to inadequate information for data controls to manage the departmental data provided to the ITS group in the ITS group's data custodial roles. A specific issue is the lack of urgency to ensure proper backup and recovery procedures are in place and tested based on best practices and standards.

The City of Dallas should implement Industry Standard Data Management efforts with appropriate Data Governance based upon a clearly defined and approved Data Management Framework. Implementation of a data management framework can reduce the effects from the improper handling of data or the inadvertent access of data elements due to accident or malicious activity. Other possibilities of the release of regulated data could place the City under legal and/or financial liabilities.

The City must implement a Data Management System based upon an Industry standard Data Management Framework. Data Management would be overseen by a Data Governance committee having membership including Data Management Subject Management Experts, Data Analytics Subject Matter Experts, and business representatives having the knowledge of Data and Data Management, as well as the Departmental needs for proper data management activities. Backup and Recovery testing of data systems would be a critical part of the Data Management implementation. By managing data through a best practice in an industry recognized manner, the risk of data loss would be greatly reduced, posing a much-reduced risk to the City.

14 Inadequate Procurement Strategy

Not understanding the actual solution service configuration needs leads to the inaccurate provisioning of resources that can divert limited funds. Under or overprovisioning of resources also causes resource management problems. A number of resource methodologies are available to estimate the information technology resource needed to operate a solution service. As an illustration, the Microsoft Azure cloud service brand offers online resource usage estimation tools to identify the resources needed to operate a solution service. ITS does not adequately use multiple available methodologies to estimate the information technology resources needed to operate a solution service. Historically, ITS has underestimated the information technology resources required to operate a solution service.

In the case of the March 2021 data loss events, the City failed to effectively manage resources and incurred data loss as a result. ITS must require oversight or change to ensure that ITS leadership and management can inform peers and business partners of purchasing strategies. ITS leadership should increase the utilization of unbiased, qualified technical resources in guiding its consideration of long-term purchase options and strategic decisions to provide stable technology resources for future growth and current operations. Data and systems migrations are highly risky without strategic and technical planning. Additional costing needs to be assigned when procuring cloud or migration services to ensure the risk is reduced prior to a go-live state.

City of Dallas

Section V – Remediation Efforts

This section provides information pertaining to situational remediation efforts at The City of Dallas driven by the March 2021 data loss events.

15 Data Governance and Data Management

ITS has taken the following steps to review, update, and implement a Data Governance plan implementing a Data Management Strategy for the City of Dallas:

- The City has chosen to use the Data Management Association (DAMA) Framework and the DAMA Book of Knowledge version 2 (DMBOK2) as the primary guide the implementation of Data Management.
- Initial meetings and overviews have been held with the ITS executive staff with approval to move forward with the DAMA DMBOK2 Framework as the guiding methodology for the City's Data Management effort.
- The initial efforts for the Data Governance effort cover the following areas:
    - Partnering with the Data Analytics and Business Intelligence (DBI) Department to establish the Data Governance Council with appropriate members.
    - Identifying and establishing the Data Steering Committee to create the appropriate Data Management policies, standards, and where applicable the procedures to implement the requirements promulgated by the policies and standards.
    - Establish a Data Maturity Model for the City to establish a baseline of present Data Management activity levels and use as metric to evaluate improvements.
    - Establish the role of Data Stewards within the City Departments to act as liaisons between the Data Management team and the departments to ensure the data needs of the departments are being met while working within a framework of best practices for Data Management. Data Stewards should be business centric, but they will need a Subject Matter Expert level of the Departments' primary data sets, both structured and unstructured.
    - Identify the priority of Data Management Knowledge Area implementation. Initially the areas of concentration are:
        - Data Security including Privacy and Regulated Data Management.
        - Data Storage and Operations: this covers management and control of structured data, normally that data within structured database systems.
        - Document and Content Management: this covers management and control of unstructured data such as images, files stored within the City's file systems,

video, Word documents, Excel sheets, and others. As noted, an example would be the management of data related to the data loss event under review.

- Data Quality: this area is critical for Data Analytics and data's ability to provide value across the environment.
- Master Data and Metadata management: inventory and documentation of data within the City and ensuring efficient and effect use and access for all data needs.

- As needed, provide periodic updates to Executive staff on status, current progress, and periodic review of the Data Management roadmap.

16 Procedural Changes

ITS has taken the following steps to update Standard Operating Procedures and introduced a review of data governance.

- Implemented a two-person integrity control process that requires multiple employees to review and perform data migrations.
- Changed configurations in storage processes to require a minimum 14-day period before data can be permanently deleted.
- Initiated a top-to-bottom assessment of the systems and processes used in storing and archiving data for opportunities to enhance capabilities and reduce potential for data loss.
- Updated the Incident Response and Data Breach Preparedness Plan to include notification to the Mayor and City Council about any data compromises within two hours of notification of the City Executive Leadership Team.

17 Data Recovery Efforts

ITS Risk/Compliance has taken the following steps:

- Searching City systems for any remnants of the lost data.
- Started with original list provided by Server Group.
- Moved to list of parsed information.
- Initial list provided by Dallas Police Department.
- Working with current list of District Attorney's priorities.
- Searching Microsoft Office 365 environment including Email, SharePoint, and OneDrive locations.
- Writing script to search systems based on Case Number/Detective Name/search terms.
- Added outside consultant to the team to provide at is providing direction and additional resources.

Recovery Environment

A recovery environment has been built to support current and future recovery efforts. Work has begun to reconstruct the Fusion Server and data sets from BIT copy forensic images. The recovery environment allows ITS to restore data sets from historical points in time. Once data has been restored it can be validated. Once the data has been validated, searches can be performed and if the data set contains missing data, the data can be restored back to the production servers. The recovery environment will be used to test various backup and recovery procedures for any server or system in our environment that is currently being backed up by Commvault. These procedures include restoring data sets from the following backup types:

- Full backups: Back up the entire virtual machine; this is the most comprehensive backup.
- Incremental backups: Back up virtual machine data that has changed since the most recent backup.
- Synthetic Full backups: Consolidate virtual machine data from the most recent full backup with subsequent incremental backups.

Forensic Image of Fusion Server and Data

A Forensic Image was taken of the Dallas Police Department's FUSION Server and its 14.5 TB Data Drive. This BIT Copy image will preserve the Server and Data as of Saturday, September 11th. Drives have

been retrieved from DPD Datacenter and installed at City Hall where several copies are being made. One will be a Golden copy that will be preserved, an optional Cloud copy to be loaded into Azure, and a Working Copy that will be converted into an Image to be used by VMware or Azure for our "Recovery Environment" and "Data Search" project.

Content Search

Work has begun to refine our "O365 Content Search" efforts. Two shared drives were created, and access has been granted for the "Search Team." Working files, which are "Spread sheets" with missing case data have been refined and loaded on data recovery server. ITS has begun to refine the data gathering and search process to increase speed and to scale our efforts. To this point all efforts have been made by the eDiscovery team. The plan is to use contract resources to search the data for specific case criteria and to consolidate the findings into "searchable strings" that can then be easily entered 0365 Compliance Search. Currently it takes up to an hour or more to gather information and enter it into the search tool. We have also expanded our search efforts across Office 365 including Exchange Online Mailboxes, OneDrive, and SharePoint locations.

Secure Search Server

We are currently building a system that will refine and allow us to scale our Content Search efforts. In addition to the eDiscovery teams efforts, we have added additional resources including 4 technology contractors to search Exchange Online Mailboxes, OneDrive, and SharePoint when locations for missing archived and orphaned data. At this point a Dev/Test Secure Search Server has been built by our server team. This server includes SQL and a custom front end web application used to search large datafiles for several fields including but not limited to: Case Number, Case Name, Badge Number, Officer Name and file names in question. The data is then used to formulate content searches by our eDiscovery team and contractors. The data is then packaged into.pst files to be used by DPD to complete missing case data.

A production server is currently being built that will permanently host the Secure Search Application, Website and corresponding SQL Database. This server will allow imports of new data sets and give ITS, the eDiscovery team and DPD the ability to quickly search for relational data and export findings. This server is specifically designed to be used by non-technical resources to quickly perform complex SQL based data searches.

Endpoint Detection and Response (EDR)

The Content search team contractors have attended training on the EDR search tool. As part of Virus and Threat detection EDR indexes all files on all PCs and Servers. This allows us to search for specific file names across all connected endpoints in all locations. This tool is a last resort for searching all supported endpoints on the network, including both servers and user workstations. The team has console access and search permissions. When a "search" case is escalated to a point where normal content search methods are unproductive, the EDR Search will be a last resort. The tool is very specific on search criteria, so it is best used for specific files by name.

Commvault Global Search

ITS is using the Global Search Bar in the Command Center to assist with data recovery efforts. In CommCell environments where all Index Servers are either in the cloud or local, you can use the global search bar to find, add, and perform actions on entities (such as file servers, hypervisors, and users) and navigation items (such as Laptops). In searches, you can use natural language. If you have multiple service CommCell environments in a CommCell environment, global searches include all the CommCell environments.

For example, you can do the following from the global search bar: Find and delete a user, Go to a file server, Back up or restore a cloud application, Add a server, and Find files.

ITS Risk/Compliance has taken the following steps:

- Searching City systems for any remnants of the lost data started with original list provided by server group moved to list of parsed information Initial list provided by Dallas Police Department working with current list of District Attorney's priorities Searching emails.
- Writing script to search systems based on Case Number/Detective Name/search terms added outside specialist to the team that can provide additional resources and, forensic Image of Fusion Server and Data.
- A Forensic Image was taken of the Dallas Police Department's FUSION Server and its 14.5 TB Data Drive. This BIT Copy image will preserve the Server and Data as of Saturday September 11th. Drives will be retrieved from DPD Datacenter and installed at City Hall where several copies will be made. One a Golden copy that will be preserved, an optional Cloud copy to be

loaded into Azure, and a Working Copy that will be converted into an Image to be used by VMware or Azure for our “Recovery Environment” and “Data Search” project.

- Content Search Work has begun to refine our “O365 Content Search” efforts. Two shared drives were created, and access has been granted for the “Search Team.” and working files “Spread sheets” with missing case data have been refined and loaded on data recovery server.
- We have begun to refine the data gathering and search process to increase speed and to scale our efforts. To this point all efforts have been on the eDiscovery team. The Plan is to use contract resources to search the data for specific case criteria and to consolidate the findings into “searchable strings” that can then be easily entered 0365 Compliance Search. Currently it takes up to an hour or more to gather information and enter it into the search tool. We also plan on expanding our search efforts to OneDrive and SharePoint when possible.
- EDR Contractors have been sitting in on scheduled training for the EDR search tool. This tool is a last resort for searching all supported Endpoints on the network both Servers and User workstations. The team has console access and search permissions. When a “search” case is escalated to a point where normal content search methods are unproductive, the EDR Search will be a last shot. The tool is very specific on search criteria, so it is best used for specific files by name.

Section VII – Recommendations

This section outlines general recommendations that are believed to offer potential value to data governance and data management processes, procedures, and activities at The City of Dallas. ITS offers these general recommendations because of the available self-reflection performed within the department.

18 Recommendation 1 - Data Governance and Data Management

It is recommended that ITS establish a Data Management Program for the creation and management of appropriate Data Governance for City of Dallas. Data Management can increase the visibility, reliability, scalability, integrity, and availability of data across an Enterprise. The highest priority is data availability and reliability. If data is not available, it is of no value. If data is not reliable, it is of little value. Other areas such as Data Security, Data Quality, and Metadata management, all feed off the primary availability and reliability of data.

A Data Management system properly implemented at the Enterprise level with a Governance system owned and managed in a centralized format provides for the structure and framework to implement data policies and standards across the Enterprise. The Governance team provides direction for data management to City leadership. Based upon AD 2-25, the departments should assign data stewards to understand and assist in the management of data.

The ITS Department should take the following steps:

1. Establish a Data Management group to initiate an Enterprise level Data Management Strategy implemented by a Data Governance Committee (led by DBI) and Data Steering group to oversee the process.
2. Identify business goals and objectives to ensure Data Management is in line with City departments.
3. Identify the priority areas such as lack of Data Content Management of unstructured data which was an instigating factor in the loss of data.
4. Create a roadmap with tentative timeline for the implementation of the various areas and processes of the Data Management framework.
5. Design and institute a Data Steward role within the City at the Department level. The Data Steward should be a Subject Matter Expert of the business within the department as well the data created within the department and would act as a liaison between the Data Management team and the department to ensure required policies and standards are delivered to the department, and the department institutes procedures to ensure compliance with such policies and procedures.
6. Institute analytics and metrics to measure and track maturity for data governance and management.

19 Recommendation 2 – Immediate Procedural Changes

ITS should take the following actions to update Standard Operating Procedures, and processes.

1. ITS should engage with the Vendor to review and update backup, recovery, archive, delete, etc. procedures to coincide with the vendor's optimum performance.
2. Continue searching and performing necessary technical changes to City systems for remnants of lost data.
3. Implemented a two-person integrity control process that requires multiple employees to review and perform data migrations.
4. Change configurations in storage processes to require a minimum 14-day period before data can be permanently deleted.
5. Initiate a top-to-bottom assessment of the systems and processes used in storing and archiving data for opportunities to enhance capabilities and reduce potential for data loss.
6. Update the Incident Response and Data Breach Preparedness Plan to include notification to the Mayor and City Council about any data compromises within two hours of notification of the City Executive Leadership Team.
7. Implement / validate the new BC/DR backup 3-2-2 rule:
    a. Keep 3 copies of your data.
    b. Store 2 backup copies locally but on different devices.
    c. Store 2 copies offsite (1 copy in a remote location + 1 copy to the cloud).
8. Follow Change Management procedures to ensure adequate recovery is possible.
9. Provide continuous training opportunities to improve performance.
10. ITS Risk/Compliance should perform an annual review of changes made to the policies and procedures.

20 Recommendation 3 – Requirements Documentation and Risk Assessment Processes

It is recommended that ITS leadership:

1. ITS executive leadership and senior management must understand the need for necessary process documentation and comprehensive risk assessment – especially for infrequent, high-risk activities. ITILv3 provides categories and direction for documentation.
2. ITS executive leadership and senior management must set the appropriate environmental tone that actions have repercussions and that appropriate risk mitigation activities must be taken to ensure desired business outcomes are achieved.
3. ITS executive leadership and senior management must adequately perform thorough risk assessment oversight to ensure appropriate and adequate activities are performed in a risk-reduced way.
4. ITS executive leadership must include regulatory and contractual standards compliance fulfillment before a solution may petition for a move to the City's production environment.

21 Recommendation 4 – Account and Access Management

It is recommended that ITS leadership:

1. ITS executive leadership and senior management should take certain organizational steps to prevent future data losses of this type.
2. Leadership must instill a sense of integrity through appropriate organizational tone.
3. ITS executive leadership and senior management must stop deployments upon deployment script failure and begin execution of backout plans.
4. All activities performed under an Administrator must be tracked and assigned to the administrative account.
5. City personnel must not use Administrator Accounts to operate services as occurred in this instance.

22 Recommendation 5 – Vendor Engagement and Management Processes

ITS personnel should have sufficient skills to address conflict issues between vendor and the City, with a full understanding of the systems. Ultimately, ITS is accountable for those systems managed by vendors and should ensure processes and procedures align with that accountability and vendor responsibility.

It is recommended that ITS leadership:

1. ITS executive and senior management must have identified scope and requirements included in the contractual negotiations prior to implementation of services.
2. Contract management must hold vendors to measurable performance metrics.

23 Recommendation 6 – Innovative DPD Data Management

The Dallas Police Department would benefit from the implementation of a Data Management system across the City of Dallas. The recommendation is for a centralized Data Management system with a Data Governance group designing and overseeing the implementation of Data Management. This ensures a single set of policies and standards across the City with the flexibility for each department to implement procedures based upon the department's specific needs and requirements.

Examples of specific needs within the DPD for Data Management would include:

1. The creation of one or more Data Stewards within the DPD. Each Data Steward would be an subject matter expert (SME) on data used within the DPD and the applications which use the data. The Data Steward would be responsible for liaising with the ITS Data Management team regarding the implementation of City-wide data policies and standards.
2. The DPD Data Steward(s) would be, for example, responsible for ensuring that any requirements be met based upon existing or created Administrative Directives. AD 2-25 establishes the Director of each Department as the Data Owner of that data primarily created within the department. The Data Steward will likely be the acting agent for the Data Owner in most departments. The Data Owner is responsible for the classification of the data within the department based upon the specifics within the AD. Once classified, the Data Owner/Data Steward is responsible to work with the Data Custodians (usually ITS) to ensure the data is managed based upon classification requirements.
3. Policies and Standards would exist for all areas of Data Management so each department, including the DPD would have a clear understanding and delineation of the roles of responsibilities in each area of data.
4. Periodic Auditing would be in place to ensure that data is being managed per departmental procedures. For example, if data is classified as sensitive, such as evidentiary data, the procedures should be clearly defined for the storage, backup, recovery testing, Disaster Recovery, and Change Management for the data.

24 Recommendation 7 – Policies, Procedures, Processes, and Standards

Policies, procedures, and processes are vital components of any department to ensure the activities and services are completed in a timely manner.

It is recommended that ITS leadership:

1. All ITS divisions must establish, operate, and maintain adequate management controls systems. These should follow a best practices framework such as NIST.
2. Management controls should be periodically reviewed and maintained for evidence of the proper operations and relevancy. Additionally, these need to be available for use to the City Controller's Office, the Chief Financial Officer, and the Office of the City Auditor.
3. Management controls must be mapped and documented to all daily activities for the operations of the technical systems.

25 Recommendation 8 – Inadequate IT Service Management

The service management processes identified and described in ITILv3 have enabled many IT service organizations to achieve cohesive, competent operation while reducing costs and risks to the organization.

It is recommended that ITS leadership:

1. ITS executive leadership and senior management must embrace both the letter and the spirit of IT service management by following the ITILv3 framework already established.
2. ITS executive leadership must require that service management processes be followed and grant few, if any, management exceptions.
3. ITS senior management must periodically update service management processes and procedures to be both effective and efficient in the attainment of desired business outcomes.

26 Recommendation 9 – Enterprise Change Management Policies, Standards, and Procedures

ITILv3 change processes have certain criteria that must be met prior to approval of change to move forward.

It is recommended that ITS leadership:

1. ITS executive leadership must oversee and enforce necessary ITILv3 practices, as well as communicate high-risk items that may have a negative impact on the City's data environment and reputation.
2. There must oversight and clear expectations to personnel to engender the proper operational tone as to the criticality of change management of information technology.

27 Recommendation 10 – Poor Staff Training, Redundancy, and Review of Capability

Strategic Human Capital Management practices dictate an organization routinely assess the skills needed by the organization to perform its current and future functions, assess the skills present in its current workforce and develop plans to either develop the necessary skills in its current workforce and/or supplement its workforce through recruitment or outsourcing.

It is recommended that ITS leadership:

1. Additionally, training and depth of job functions for various IT tasks need to be established, especially for critical areas of responsibilities. Furthermore, testing and review of those critical function areas must be completed.

2. Trainings should be required for multiple members of a team, including training offered outside of traditional environments. If the team is composed of a small number of ITS staff, other functional team members would benefit ITS and the City by allowing for a depth in knowledge for areas of critical function.

28 Recommendation 11 – Management Environmental Tone

The appropriate management tone must be set through management directives and clearly documented performance expectations. Setting this tone is necessary for the organization to be successful in accomplishing its mission, in this case, IT service delivery.

It is recommended that IT leadership:

1. ITS executive leadership and senior managers must appropriately and adequately employ management controls systems (e.g., policies, processes, standards, procedures, and performance expectations).

2. Remediate gaps in documented management directives and expectations around management control systems. These systems must emphasize the necessary commitment to the City of Dallas's core values of excellence, ethics, empathy, and equity exist. Ad-hoc project or work management techniques can lead to incidents such as the March 2021 data loss events and must be eliminated.

3. ITS executive leadership and senior management must create the necessary "tone at the top" of the organization by demonstrating that effective process execution leads to quality work. Processes should not be overridden for any but the most exceptional reason.

29 Recommendation 12 – Data Handling and Data Management with Specific Focus on the Topic of Data Backup, Data Archival, and Data Migration

As the City increases the amount of unstructured data is manages, it must unsure that it matures its practices around the unstructured data

It is recommended that IT leadership:

1. The City must implement a Data Management System based upon an Industry standard Data Management Framework.
2. Data Management would be overseen by a Data Governance committee having membership including Data Management Subject Management Experts, Data Analytics Subject Matter Experts, and business representatives having the knowledge of Data and Data Management, as well as the Departmental needs for proper data management activities.
3. Backup and Recovery testing of data systems would be a critical part of the Data Management implementation. By managing data through a best practice in an industry recognized manner, the risk of data loss would have been greatly reduced, posing almost zero risk to the City.

30 Recommendation 13 – Inadequate Procurement Strategy

A number of resource methodologies are available to estimate the information technology resource needed to operate a solution service.

It is recommended that IT leadership:

1. In the case of the March 2021 data loss events, the City failed to effectively manage resources and incurred data loss as a result. ITS must require oversight or change to ensure that ITS leadership and management can inform peers and business partners of purchasing strategies.

2. ITS leadership should consider longer purchase options and strategic decisions to provide stable technology resources for future growth and current operations.

3. Data and systems migrations are highly risky without strategic and technical planning. Additional costing needs to be assigned when procuring cloud or migration services to ensure the risk is reduced prior to a go-live state.

City of Dallas

Section VI – The City of Dallas Administrative Directives

The following describes what The City of Dallas Administrative Directives are and pertinent Administrative Directives for information and technology services.

31 City of Dallas Administrative Directives

An administrative directive (AD) is a document authorized and issued by the City Manager to establish operating practices and procedures for certain administrative functions and/or to supplement the broader policy direction of the town council by augmenting/clarifying ordinances and amendments to the town code or to the town's personnel policies and procedures. Administrative directives are generally focused on internal policies and practices and are designed to promote consistent business practices, improve organizational communication, reduce risk and exposure, and provide for necessary internal controls over resources and business transactions. [Marana]

Administrative directives for The City of Dallas presently may fall into one of the following categories:

- Organization
- General
- Personnel
- Finance and Purchasing
- Legal Matters
- Property

An administrative directive may be initiated and developed at the department level. Key stakeholders shall be identified by the initiating department and included in the development of the directive. It is expected that certain departments shall be identified as key stakeholders depending upon the subject matter, to include (but not limited to): [Marana]

- Employees
- Funds/monies
- Technology
- Facilities
- Records
- Communication
- Citizens/businesses/customer service
- Legislation
- Assets (e.g., equipment and vehicles)
- Emergency Planning/Operations/Management

- Law
- Safety

All draft administrative directives shall be subject to the establishment and publication process described in Administrative Directive 2-01 (AD 2-01) Administrative Directives.

All administrative directives must be approved and officially issued by the City Manager.

All employees are responsible for reading, understanding and asking questions to clarify administrative directives. Failure to follow an administrative directive may be grounds for disciplinary action. [Marana]

31.1 AD 2-XX – Data Governance and Data Management (Under Development)

ITS is in the process of developing an Administrative Directive to build a stronger Data Governance and Management program.

31.2 AD 2-24– Computer Security

Administrative Directive 2-24 (AD 2-24) Computer Security provides the rules and procedures that govern the security of the City's information systems and assets. The purpose of AD 2-24 is also to protect and preserve the confidentiality, integrity, availability, accountability, and assurance of information systems and assets. AD 2-24 is broad in its scope, applying to all departments, persons, and devices that make up the City's IT systems and assets. [AD 2-24]

AD 2-24 defines different responsibilities for different parties within the organization. AD 2-24 requires that City Departments adhere to the Department of Information and Technology Services Enterprise Security Standards. [AD 2-24]

Further, City Departments are required to take reasonable measures to protect the City's IT assets, resources, and data from unauthorized access, use, disclosure, modification, and destruction in order to provide integrity, confidentiality, and availability in utilizing information resources to deliver services to the City's stakeholders. [AD 2-24]

AD 2-24 also establishes requirements for the Chief Information Officer. According to AD 2-24, the Chief Information Officer is to recommend strategic vision, policies, directions, and provide other information-technology-related advice to the City Manager. [AD 2-24]

The Chief Information Officer is also responsible for implementing effective and adequate information security policies, standards, tools, and resources to protect the City's information systems, and reduce the risks inherent in the operation of systems to store data and deliver services. [AD 2-24]

AD 2-24 also establishes requirements for City employees. City employees are required to adhere to AD 2-24, as well as other policies that govern appropriate behavior, activities, conduct, performance, and acceptable use of information systems and assets. AD 2-24 establishes the same requirements for vendors that interact with City information systems and assets. [AD 2-24]

AD 2-24 ties to other IT industry standards that deal with computer security. As such, AD 2-24 establishes the use of industry-recognized security frameworks and standards, including those from the National Institute of Science and Technology and Federal Information Publication Standards (resulting from the passage of the Federal Information Security Management Act of 2002). [AD 2-24]

Additionally, AD 2-24 makes the ITS Security division solely responsible for the planning, design, development, implementation, and governance of the security architecture that protects city networks and enables staff to leverage information resources to ensure effective service delivery. [AD 2-24]

AD 2-24 goes on to define privacy protections, general data management, and incident response management. While various topics are discussed, AD 2-24 provides high-level guidance that lays out the responsibilities and expectations of each party that deals with information resources in the course of conducting business on behalf of the City of Dallas. [AD 2-24]

31.3 AD 2-25 – Data Ownership and Classification

Administrative Directive 2-25 (AD 2-25) Data Classification and Ownership establishes classifications for data based on the confidentiality or importance of the data. [AD 2-25]

AD 2-25 applies to all data collected and maintained by the City of Dallas. This includes data residing on all City computers (microcomputers, Local Area Networks, Wide Area Networks, teleprocessing systems, operating system, mobile digital terminals, On-Line Services, Internet connections). However, the list in AD 2-25 is not intended to be exhaustive. [AD 2-25]

AD 2-25 defines different responsibilities surrounding data. AD 2-25 charges the Department of Information and Technology Services as the Physical Custodians of Data. In this role, the Department (and specifically the Security Team) is responsible for providing a list of mainframe and corporate

network data files to the departments, also known as the Data Owners, for whom the Department of Information and Technology Services is the Physical Custodian of the data. [AD 2-25]

For the Data Owners, AD 2-25 states that Data Owners are responsible for ensuring that all data collected by them or for their use is properly classified. Data Owners are also responsible for reviewing all data files on a periodic basis to ensure that each data file is properly classified and only needed users are able to access that data on City of Dallas computer systems. [AD 2-25]

AD 2-25 defines Data Classification levels as follows:

1. Confidential – either a mandatory or permissive exception to disclosure under the Texas Open Records Act. Access, at any level, must be approved by the Data Owner.
2. Production – Non-confidential data, but that data is also deemed critical because of its importance to the organization and its operation. Update access is restricted and must be approved by the Data Owner.
3. Test – Non-confidential, non-production data. Test data may be read by anyone and may be updated by the department or work group that created it (Data Owner). Update access requires the approval of the Data Owner. [AD 2-25]

AD 2-25 specifically assigns the singular role of Data Owner as the Director of the department that requested or authorized the creation of the data. However, the department Director is also able to delegate authority to approve access requests but will retain the responsibility for ensuring that the data is protected in accordance with federal, state, and local statutes. Data Owners are also required to examine all their data, based on the classifications defined in the Administrative Directive. [AD 2-25]

The Department of Information and Technology Services is also required by AD 2-25 to prepare an annual list of data files in its custody, with their classifications. Data Owners are required to review the list and accept ownership for their data files within two weeks of receiving the list. [AD 2-25]

AD 2-25 also requires all Data Owners to train their staff in the proper handling of confidential data. This training should include identification of data designated as confidential, display of confidential data in areas with public traffic, and how requests for access to confidential data, either from other City entities or the public should be handled. [AD 2-25]

AD 2-25 is under update review and will include the following:

- Additional data classification of Regulatory. This classification is used to identify data subject to specific handling procedures such as for Criminal Justice Information Systems (CJIS), and Health Insurance Portability and Accountability Act (HIPAA).
- Possible inclusion of a data classification of Evidentiary. This classification would address data such as that owned by the Dallas Police Department. This classification will require the Data Owner to provide documented methods of how such data should be handled, backed up, and retained for evidentiary purposes.
- The term Data File should be understood to include additional file types beyond flat files maintained to support previous mainframe operations.

31.4 AD 2-28 – Change Management of Information Technology

Administrative Directive 2-28 (AD 2-28) Change Management of Information Technology exists to ensure that stable information technology operating environments are maintained and that all changes to computing systems have documented guidelines, standards, and procedures to plan, coordinate, monitor and recover changes in the information technology operating environments. [AD 2-28]

According to AD 2-28, Change Management also ensures that effective, efficient changes are made by using methods and procedures that will improve the quality of the environment, which ensures changes are transparent to the customers (i.e., City Departments) by minimizing disruptions, and that an auditable record of change activity exists. [AD 2-28]

The scope of this Administrative Directive applies to all departments, all City of Dallas IT staff, and all consultants contracted by the City of Dallas who design, develop, configure, install, operate, maintain, or request changes to Information Technology. [AD 2-28]

AD 2-28 defines the scope of changes controlled by Change Management to include any modification or enhancement made to any and all IT Production environments. Examples include, but are not limited to:

- Computing equipment (e.g., desktop, laptop, server, mainframe computers);
- Mobile computing equipment (e.g., PDA, tablet devices, MDC);
- Computer applications, operating systems, and services they provide;
- Database management systems and data structure definitions;
- Distributed, web based, or cloud computing services;
- Data networking equipment and services (e.g., LAN, WAN, Wi-Fi, radio, internet);

- Telecommunications equipment and services (e.g., VoIP, IVR, 911, radio, Smartphone); and,
- Physical infrastructure supporting IT (e.g., cabling, electrical service, HVAC, access control). [AD 2-28]

AD 2-28 defines various terms and roles within the change management process. Among the most important from this directive are:

- Change Manager, which is a role identifying those resources responsible for administration of Change Management processes and activities. The Change Manager administers the overall change management process and interacts with each of the other parties involved.
- Request Initiator, who submits requests for changes, clarifies information, and performs acceptance testing.
- The Change Advisory Board is comprised of business and ITS staff. The Board reviews and approves or rejects requests for changes in alignment with technical or business strategy, cost, and risk. The Board also prioritizes the order of deployment for changes.
- The Change Tester identifies resources responsible for testing changes.
- The Release Control Board is comprised of ITS management staff and is charged with reviewing all release deployment requests for change for technical risk and readiness. The Board then approves or rejects all deployments to production.
- Finally, the change implementer reviews the support and deployment documentation, and deploys the changes to the IT environment. [AD 2-28]

31.5 AD 2-34 – Data Backup and Recovery Policy, Standard and Procedures

Administrative Directive 2-34 (AD 2-34) Data Backup and Recovery Policy, Standard and Procedures states that all Information Technology applications and systems must plan for recovery by establishing backup and retention procedures for applications and data. This document is intended as a reference for other city departments. AD 2-34 requires that all Departments within the City of Dallas are to establish minimum standards for backup and retention of their Information Technology systems and databases. [AD 2-34]

The purpose of AD-34 is to define the policy, minimum standards and procedures for backup and recovery of Information Technology hardware and software systems and data used within the City of Dallas for the Department of Information and Technology Services. Additionally, AD-34 defines

recommended minimum standards and procedures for backup and recovery for other City of Dallas departments. [AD-34]

AD 2-34 defines the roles of individual IT Managers within the Department of Information and Technology Services are responsible for:

- Incorporating backup and recovery in all hardware and software application designs according to the data owner's backup and retention requirement;
- Ensuring the backup procedures are created, complete and documented for the Data Center to follow;
- Document all backup and recovery procedures per data owner's requirements;
- Test backup systems with data owner prior to implementation into production; and
- Verify, make corrections, and turn over backup procedures and responsibilities to the Data Center. [AD 2-34]

AD 2-34 states that client departments owning the data will:

- Define all backup and retention policies and procedures prior to implementation;
- Review all backup testing results with CIS prior to implementation; and,
- Notify the Department of Information and Technology Services of any backup retention requirement changes. [AD 2-34]

In the implementation of the procedures for AD 2-34, the procedures state that data owning departments are responsible for the development of their backup and retention policies, procedures, and standards. However, AD 2-34 states that the Department of Information and Technology Services may assist the departments in the implementation of these policies, procedures, and standards. [AD 2-34]

AD 2-34 further states that all data backup and recovery procedures shall be documented by the owning department and tested by the owning department with the assistance and review by the Department of Information and Technology Services prior to implementation. [AD 2-34]

AD 2-34 defines the physical conditions (i.e., temperature, humidity) for backup storage. It also requires documentation of backup schedules and proper labeling of certain backups.

Finally, in the event a department needs restoration, the department will make a request to the Department of Information and Technology Services who will document information on the requestor of the restoration and complete the restoration. [AD 2-34]

City of Dallas

Section VIII – Appendices

The following appendices provide information and information sources that are deemed beneficial for the reader to obtain a context to IT operations provided by the City's ITS.

32 Appendix A – Data Governance and Data Management

32.1 Data Management Association (DAMA) International

Executive Summary

"Data is the oil of the 21st century". These succinct words by Peter Sondergaard, head of Gartner Research, reflects the growing importance accorded to data. Industry has come to understand that data will be the resource running the economy in years to come. [Data and information are synonymous and have been used interchangeably within this document]

The City of Dallas has been working over the last few years to use data as a valuable resource to improve the services provided and available to the citizens. Initiatives regarding Smart Cities and the Open Data Portal are just a few examples of the use of data. Following the goal to maximize the value and availability of data, the City will implement a Data Management Strategy

32.1.1 Introduction

Data management is a relatively new discipline when compared to traditional asset management disciplines such as financial management and capital management. The City should lead in this rapidly developing critical area. The City of Dallas has chosen the Data Management Association Data Management Body of Knowledge (DAMA DMBOK) framework for the management of this new asset type. The DAMA framework was chosen because it is consensus driven by the largest body of data professionals worldwide not affiliated with any specific vendor or technology. The data management terms and definitions in this document align with DAMA DMBOK. A common vocabulary in the data management domain is important for this new discipline, and DAMA, through its non-profit, consensus driven approach has created the most acceptable version of the glossary in the industry. Taking advantage of existing DAMA definitions, a glossary has not been appended to this document.

Besides establishing a common language for data management, the DAMA DMBOK provides a data management framework that is holistic and covers all sectors. Every organization is unique, and all sectors may not have equal relevance within organizations if at all. The prioritization and depth of focus on sectors is for organizations to decide.

32.1.2 Business Case:

The value proposition for data management strategies has clear benefits. Applying sound data management practices and standards leads to clear, documented, effective data, and reduces attendant liabilities with sensitive data. Better quality data results in cost savings in City government operations.

In addition to cost savings and reducing risk, data management can improve the delivery of services to Dallas citizens by:

- Ensuring the linkage of data resources to legislated mandates and City goals.
- Improving interoperability and integration of systems.
- Increasing organizational flexibility and agility to meet changing requirements.
- Identifying innovation opportunities.

Issues that occur without a centralized common Data Management strategy:

- Common issues are addressed differently, if at all.
- Lack of one common strategy results in costly reinvention of the best practices, policies, and solutions.
- Individual and unplanned approaches can lead to less desirable results.

32.1.3 Methodology of Development

The data management strategies were created based on City of Dallas Data management principals guided by City Administrative Directives and other City guidelines The strategies have been classified and enriched using the DAMA DMBOK2 framework.

City of Dallas Goals:

Dallas 365 Goals and Performance

- Economic Development
- Environment and Sustainability
- Government Performance and Financial Management
- Housing and Homeless Solutions
- Public Safety

- Quality of Life, Arts, and Culture
- Transportation and Infrastructure
- Workforce, Education and Equality

ITS Data Principles:

- Manage enterprise data as a City asset
- Enable openness and transparency
- Share data to enhance its value
- Enforce privacy and security
- Integrate common data definitions and standards
- Collaborate to eliminate duplicates
- Improve City government through data quality

32.1.4 Data Governance:

Definition: Data governance is the execution of authority and control (planning, monitoring and enforcement) over the management of data assets.

Data governance impacts all areas of data management and directly influences and prioritizes the data management strategies within this document. It is important to distinguish data governance from IT governance; it is different in that it is somewhere between business and IT governance. For instance, Health Insurance Portability and Accountability Act (HIPAA) compliance involves both business and IT participation. In organizations, data needs are framed by the business and should be audited by the business for compliance and quality while IT implements and operates the infrastructure for the data. Data governance needs to be a partnership that includes business stewards who decide on the use and control of the data and technology stewards who enable and administer the flow and storage of the data. The business stewards are trustees of the data while the technology stewards are custodians of the data. The business and technology stewards are not new jobs but a formalization of existing roles within different agencies where data governance would enable shared decision making about data assets. Data issue management, where difficult decisions need to be made, is a key activity of data governance.

Data governance often deals with data usage and its legal implications. Legal counsel is advisable within the highest data governance body to interpret laws and attempt changes, if necessary, for the greater good of the citizens of Dallas. Ensuring compliance with the laws involving data is an essential part of data governance, making auditing an essential component of the Data Governance Council.

- **Strategy:** Obtain highest possible executive level support at the City level for data
- governance.
- **Strategy:** Educate about the need for data governance.
- **Strategy:** Form working group to create the decision rights and accountability structures for a Data Governance Council.
- **Strategy:** Develop a City data governance charter based on collaboration, mutual support, and transparency.
- **Strategy:** Include representation from relevant Departments and other areas as needed
- **Strategy:** Form a data governance body to provide staff support to data governance function, facilitate meetings, prepare meeting agendas, and publish minutes.

32.1.5 Data Modeling and Design:

Definition: *Designing, implementing, and maintaining the solutions to meet the data needs of an organization.*

The practice of analyzing, designing, implementing, and maintaining data products for an organization is data development. The end data products are data models, physical data structures, and information end products such as screens and reports, all with the aim to support a range of business activities from strategy development to operations. Data development activities may include data architects, solution architects, business analysts, data analysts, software developers, database administrators, business stewards and business subject matter experts (SMEs), all working together to produce the data products. Depending upon the project and organization size, one or more of these roles may be the function of one individual. Data development touches various phases of the system development lifecycle (SDLC) where data is defined, designed, and implemented, whether in the traditional waterfall method or the shortened phases of agile methodologies.

- ***Strategy:*** *Invest in enterprise agreement on the business definitions for critical data elements in the early phases of requirements gathering, towards a business glossary.*

- ***Strategy:*** *Develop entity, attribute and table, and column naming standards and*
- *conventions.*
- ***Strategy:*** *Data should reflect actual entities and attributes of the business and not be tied to a specific application. Implement application specific requirements through data virtualization using views, stored procedures and functions.*
- ***Strategy:*** *Database processing should be pushed towards the database server by design rather than the application server.*
- ***Strategy:*** *Enforce data rules closer to the database when possible, rather than in application code.*
- ***Strategy:*** *Develop test data meeting privacy and confidentiality requirements.*
- ***Strategy:*** *Consider implementing SQL review practices between developer and DBA functions to prevent production failures, enhance performance and enhance maintainability.*
- ***Strategy:*** *Automate, to the maximum extent, the data migration from source to target platforms early in the development phases.*
- ***Strategy:*** *Have policy not to update production data directly though ad-hoc updates.*
- ***Strategy:*** *Cross train, as appropriate, DBAs in non-relational technologies such as XML, XML Schema, Namespaces and OO developers in SQL best practices using relational databases.*

32.1.6 Data Storage and Operations:

Definition: *Planning, monitoring, control, and support of structured data assets across the data assets lifecycle.*

Database operations management is among the most mature of data management areas with the best practices tested over decades and refined by large networks of professionals, primarily database administrators. Database operations management
covers two main areas a) database support and b) data technology management. Database administrators in coordination with other IT functions attempt to maximize the value of structured data assets in the organization by a) protecting and ensuring the integrity of the data, b) maximizing availability of the data and c) optimizing database performance. These goals are supported through many activities such as:

- Backup and recovery planning and management

- Database monitoring and tuning
- Ensuring appropriate versions of database technologies are being used
- Running various data operations such as loading, reorganizing databases, data statistics refresh, archival and purging
- Evaluating new data technologies appropriate to the organization

Database administration, besides being central to the database operations function, plays important roles in other data management areas such as data development and data security management.

- ***Strategy:*** *Data archival policy and standards should be developed and followed to avoid overloading of production databases leading to performance degradation over time.*
- ***Strategy:*** *The data purge policy in alignment with the City of Dallas Retention Schedule and the needs of the business should be developed and followed. This is not to be confused with the archival policy as being the same since archival and purging are two separate activities.*
- ***Strategy:*** *Organizations should verify the validity of its backups through recovery*
- *exercises at least once a year.*
- ***Strategy:*** *Production database change policy should always mandate a documented back-out plan for every change.*
- ***Strategy:*** *Have policy to always test changes in test environments with the exception of emergencies*
- ***Strategy:*** *Have policy to develop automation skills within DBA community.*
- ***Strategy:*** *Database de-normalization should be among the least preferred performance strategy within online transaction processing (OLTP) databases.*
- ***Strategy:*** *Invest in the practice of proof-of-concept activities for new andpromising technologies to build roster of suitable technologies in advance. This would help to avoid overestimation of benefits & underestimation of costs when implementation opportunities surface.*
- ***Strategy:*** *Decide and document database management software upgrade policy even if the policy is limited to reacting to vendor end-of-support ultimatums. A documented upgrade policy is in the interest of better infrastructure resource planning.*

32.1.7 Data Security Management:

Definition: Planning, development, and execution of data security policies and procedures to provide proper authentication, authorization, access and auditing of data and information.

It is not the organization size, but the business nature that dictates the effort needed for data security management. Organizations dealing with sensitive personal information would need to invest more than others for data security management. A proper balance between data access and data security should be maintained. Sweeping iron clad security policies may stifle beneficial uses of data and generate resentment within an organization. Data security, carefully managed with monitoring, auditing, and enforcement promotes trust amongst stakeholders. This trust encourages data sharing and thereby increases data value. Organizations will be reluctant to share information unless appropriate security stewardship of data can be assured. Data security should have judicious governance with stakeholders so that it is practical to be followed daily on an operational level.

Trends toward cloud computing bring special data security concerns. Organizations can move data and associated security controls, but not liability, to the cloud. Special attention should be paid to data moving to the cloud and the contractual content with the cloud vendor.

- ***Strategy:*** *Based on data security classifications, organizations need to address sensitive data exposed in test databases though data masking or de-identification.*
- ***Strategy:*** *Develop data sharing agreement templates that organizations could*
- *leverage when crafting interagency data sharing.*
- ***Strategy:*** *Organizations with sensitive data should manage, at some level, a log of*
- *access granted to roles and individuals.*
- ***Strategy:*** *Access to sensitive data should be avoided through shared accounts.*
- ***Strategy:*** *Manage access through role-based security at the group level rather than individual based accounts. Assign individuals to roles.*
- ***Strategy:*** *Grant access to sensitive data through approved and not through default opt-in.*
- ***Strategy:*** *For very sensitive information, provide for authentication and access monitoring of unusual patterns with a judicial balance of automation and human checks.*
- ***Strategy:*** *Incorporate annual auditing processes not framed with a fault-finding mindset but*

with an objective to monitor for continuous improvement.

- ***Strategy:*** *Develop a cloud-based data security strategy.*

32.1.8 Reference & Master Data Management:

Definition: Planning, implementation, and control activities to ensure consistency with a "golden version" of contextual data values.

Every business transaction record needs context. For example, when a customer places an order for a certain quantity of products, at a certain price, the customer, product, and order status are contextual data while the order quantity, discount, and price are transaction data. Organizations are facing challenges in keeping contextual data consistent across lines of businesses and systems. Contextual data maintained in silos make organization integration difficult with the inevitable inconsistencies. The root cause analysis of many data quality issues within organizations points to the need for master and reference data integration. The overall data quality in many organizations is directly correlated with the quality of the contextual data. Reference and master data management are essentially data quality programs at higher levels of the organization.

There are two kinds of contextual data, reference data and master data. In the example above, the customer and product information are master data while order status is the reference data. Reference data commonly appears as a pick list within applications. Reference data categorizes data for business purposes and, therefore, the domain values must be controlled with definitions for each value and with its relationship with other values with the domain. Master data, once defined at the entity level, does not require every element defined. The challenge with master data, however, is prevention of duplicates and the creation of a "golden" record with the merger or most accurate elements from disparate sources, and the subsequent dissemination of master data. Governance structures are essential for reference and master data management projects because data conflicts cannot always be resolved through automation and established procedures.

- ***Strategy:*** *Identify possible COIs within City government that may benefit from master data management (MDM) efforts.*
- ***Strategy:*** *Develop robust metadata, including business glossary, at the beginning of an MDM effort*

versus documentation at the end.

- ***Strategy:*** *Plan for data governance as a must - not optional, when approaching a reference or master data management project.*
- ***Strategy:*** *Invest in master and reference data management efforts as a continual program and not as a project with an end date.*
- ***Strategy:*** *Invest in master and reference data management efforts in smaller iterations to deliver and demonstrate value and continued support from stakeholders.*

32.1.9 Data Warehousing, Big Data & Business Intelligence Management:

Definition: *Data warehousing and business intelligence management (DW-BIM) covers the planning, implementation and control activities in the gathering, cleansing, integration, and presentation of data to knowledge workers for business analysis, thereby enabling informed decision making by organizations.*

Data warehousing is the activity that is concerned with the collection of data from various data sources within the organization, integrating it and storing it as a snapshot of organizational operations at different points in time. In other words, the concern is about integrated enterprise data content with a historical perspective. BIM is the complementary part of using this data content using various tools. These two activities are intertwined in that one is ineffective without quality management in the other.

The primary use of the Data Warehouse concept is being implemented in the City through the use of Big Data.

- ***Strategy:*** *Leverage and support data management component functions such as reference and master data management, data governance, data quality and metadata management.*
- ***Strategy:*** *when possible, seek and collaborate with the Big Data and Data Mining faculty and researchers of close by colleges and universities*
- ***Strategy:*** *Actively support and invest in metadata policy and processes within the organization with the business glossary process among the initial steps*
- ***Strategy:*** *Summarize and optimize last, not first. Start building with the detailed*
- *data.*

32.1.10 Document & Content Management:

Definition: Document and content management are the planning, implementation, and control activities to store, protect, and access unstructured data within electronic files and physical records that include text, graphics, images, audio and video.

This area refers to unstructured data that is not in the structured format of traditional data management systems (relational, hierarchical, object, networked, etc.). Though "store, protect and access" activities within document and content management may seem to imply an operational focus, it is very important to consider strategic aspects of data governance, architecture, security, privacy and confidentiality, metadata and classification, and data quality. Document management is more to do with storage, inventory, and control of paper or electronic documents using processes and technologies whereas content management refers to processes and technologies that are concerned with the organization, categorization and access to the content within those documents and records. Content management today is particularly important in managing content within web sites and portals. Document and content management, though distinct, are, in practice, sometimes blurred with business process and roles intertwining and vendors providing products that cover both areas. This is reflected in the Department of Information Systems' enterprise content management strategy and video strategy documents which provide further details on the strategies mentioned within this document (available from the DIS Enterprise Architecture group upon request).

- ***Strategy:*** Identify and document primary unstructured data types stored within the City
- ***Strategy:*** Document backup and recovery requirements for unstructured data
- ***Strategy:*** Based on the Requirements of AD 2-25 ensure Data Owners have properly classified Department data and provided any controls or requirements to the ITS Data Custodians
- ***Strategy:*** Validate storage requirements, storage performance metrics and other best practice activities to store and maintain the unstructured data
- ***Strategy:*** Ensure periodic audits of content data controls to ensure requisite data Policies and Standards are being followed based upon required procedures to ensure the data is stored, protected, and maintained for the City.
- ***Strategy:*** Ensure proper Security Controls are in place to ensure data privacy and access is controlled based upon any regulatory, Departmental, or other requirements based upon the

classification of the data.

32.1.11 Metadata Management:

Definition: Metadata management is the set of processes that ensure proper creation, storage, integration, and control to support the associated usage of metadata.

Lack of metadata is a nuisance for organizations large and small. The lack of meaningful and maintained metadata leads to inefficiencies such as 1) higher retraining costs with labor/vendor turnover 2) higher time-to-market for solutions and system changes 3) more time spent in research by data analysts validating or reporting data 4) incorrect business decisions based on lack of understanding of data, 5) lack of understanding between business and IT. For instance, metadata often belongs to the deferred wish-list of application managers maintaining solutions but becomes a must-have during major changes.

Metadata is more than the data dictionary extracted from physical databases or models in a data modeling tool. It is an amalgamation of technical and business understanding of what data is required for the organization to function. There are no boundaries dictating the “right amount” of metadata and it all depends on case by case. The amount of technical and business information about data elements should be proportional to its importance within an organization. Metadata may be comprised of business, operational, technical, process or stewardship metadata.

Independent organizations may not have the resources to invest in researching and implementing best practices, policies, and procedures in this area. This is one area where collaborative work may be of most help, City wide. It may be noted, however, that though organizations have recognized the importance of maintaining metadata, the success rate, historically, is low indicating that it may be a difficult program to implement.

- ***Strategy:*** *A metadata group to develop the metadata strategy should be among the first areas addressed though data governance.*
- ***Strategy:*** *Focus on the governance of metadata toward high quality metadata, the most important aspect for the success of any metadata program.*
- ***Strategy:*** *Start small (but scalable) at the local level with the most critical business elements.*

- ***Strategy:*** *For every effort, articulate the problem and/or risk driving the metadata management effort.*
- ***Strategy:*** *Explore suitable tools for metadata management whether in-house or commercial, for ease of integration, accessibility, and maintainability of metadata.*

32.1.12 Data Quality Management:

Definition: Data quality management is the planning, implementation, and control activities that apply data quality management techniques to measure, assess, improve, and ensure the fitness of data for use.

Central to the concept of data quality management is the specification of the data needs, determination of the optimal methods to measure and monitor it, agreement of acceptable levels and root cause corrections when there is a deviation from the acceptable levels. The threshold of acceptable quality for the business is to be carefully determined and not be pegged at a level so stringent that is too costly and hence not viable for the organization. Data quality management is not a one-time effort but a continuous program of monitoring and corrections. With a goal of continuous improvement, the acceptable threshold ofdata quality should always be a moving target. The surfacing of master and reference data management initiatives within organizations has furthered the need for data quality management and the usage of COTS data quality tools. The City should promote the awareness of data quality management and the tools that help in the process.

- ***Strategy:*** *Develop and maintain inventory of data quality tools in the City with*
- *usage licensing and cost.*
- ***Strategy:*** *Promote awareness by educating on the data quality tool functions, City government success stories, the need for address standardization and quality.*
- ***Strategy:*** *Seek to arrest the proliferation of multiple vendor offerings in the interest*
- *of reducing overall costs.*
- ***Strategy:*** *Whenever possible, follow industry and federal data standards.*

32.1.13 Tactical Implementation of the Data Management and Data Governance

- Build a clear vision and scope for the data governance initiative, so you can ensure that the organization can meet its expectations.
- Define standards and assign business rationale as to why each exists. Outline the benefits that can be achieved and what level of quality should be reached to realize the benefit. Create metrics that show whether benefits are being realized.
- Design a data governance program that is suitable for managing the defined standards. This includes assigning roles and responsibilities for processes used to manage activities, such as change management for standards, and changes to any external process that affect the organization's ability to govern, including the IT project management process.
- Engage a data owner to own standards and to build/oversee the data quality roadmap.
- Build the data quality roadmap and document current quality levels. Measure it against the requirements and propose actions to bridge the gap and/or maintain good quality.
- Populate remaining data governance roles to operate ongoing compliance. Measure and manage activities identified in the data quality roadmap.

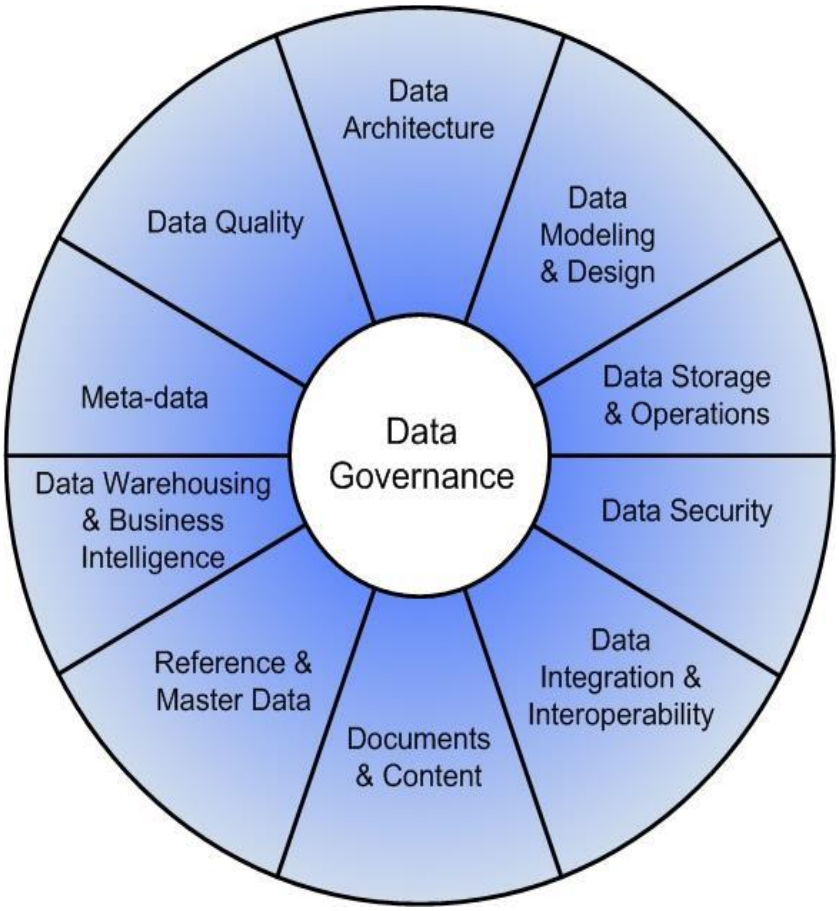
32.2 Data Management Body of Knowledge (DMBOK) Framework

[Primary Source DAMA-DMBOK2 Framework 2014 DAMA International]

Data Management is an overarching term that describes the processes used to plan, specify, enable, create, acquire, maintain, use, archive, retrieve, control and purge data. These processes overlap and interact within each data management knowledge area.

32.2.1 Proposed Framework

DAMA defines 11 Knowledge Areas in the DAMA-DMBOK2 framework for Data Management. These are represented in the figure below:



The 11 Data Management Knowledge Areas are:

- Data Governance – planning, oversight, and control over management of data and the use of data and data-related resources.
- Data Architecture – the overall structure of data and data-related resources as an integral part of the Enterprise Architecture.
- Data Modeling and Design – analysis, design, building, testing and maintenance.
- Data Storage and Operations – structured physical data assets storage deployment and management.
- Data Security – ensuring privacy, confidentiality, and appropriate access.
- Data Integration and Interoperability – a new knowledge area for DMBOK2. Acquisition, extraction, transformation, movement, delivery, replication, federation, virtualization, and operational support of data integration between systems and functional activities.

- Documents and Content – storing, protecting, indexing, and enabling access to data found in unstructured sources, and making this data available for integration and interoperability with structured (database) data.
- Reference and Master Data – managing shared data to reduce redundancy and ensure better data quality through standardized definition and the use of data values.
- Data Warehousing, and Business Intelligence – managing analytical data processing and enabling access to decision support data for reporting and analysis
- Metadata – collecting, categorizing, maintaining, integrating, controlling, managing, and delivering metadata.
- Data Quality – defining, monitoring, maintaining data integrity, and improving data quality.

32.2.2 Summary

In summary, the goal of this section has been to introduce and provide a high-level overview of the DMBOK2 Data Management Framework and the associated knowledge areas. The framework is a flexible guideline to allow entities to work within their internal data management requirements to provide an industry approved common set of areas to create policies, standards and procedures for Data Governance and implementation.

33 Appendix B – IT Service Management

IT service management is an approach to the management of information technology by focusing on the delivery of business value through services.

The City of Dallas has adopted ITILv3 as its IT service management (ITSM) framework. ITILv3 is comprised of 26 processes that support the delivery of IT services to achieve desired business outcomes. Presently, ITS only partially operates three of the 26 available processes.

33.1 Services

Services are a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks. Services facilitate outcomes by enhancing the performance of associated tasks and reducing the effect of constraints. These constraints may include regulation, lack of funding or capacity, or technology limitation. The result is an increase in the probability of desired outcomes. While some services enhance performance of tasks, others have a more direct impact – they perform the task itself. [ITILv3]

ITILv3 has defined an outcome as the result of carrying out an activity, following a process, or delivering an IT Service. The term is used to refer to intended results, as well as to actual results.

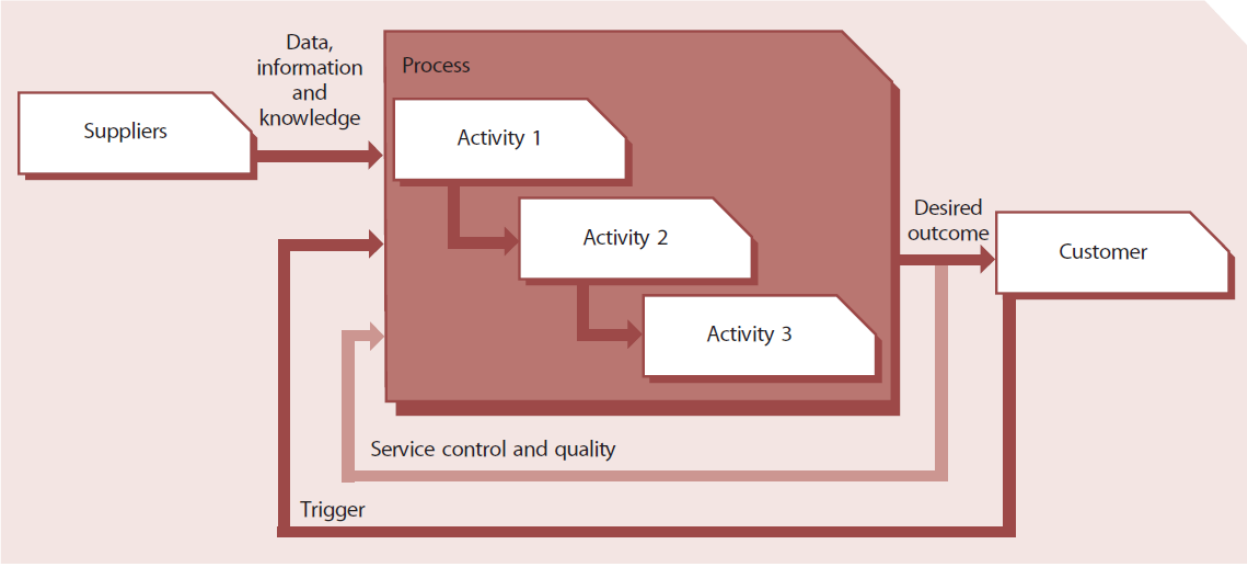


Figure 3 ITILv3 Basic Process Diagram

33.2 Service Management

Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services. The capabilities take the form of functions and processes for managing services over a lifecycle, with specializations in strategy, design, transition, operation, and continual improvement. The capabilities represent a service organization's capacity, competency, and confidence for action. The act of transforming resources into valuable services is at the core of Service Management. Without these capabilities, a service organization is merely a bundle of resources that by itself has relatively low intrinsic value for customers. [ITILv3]

Organizational capabilities are shaped by the challenges they are expected to overcome. An example of this is how in the 1950s Toyota developed unique capabilities to overcome the challenge of smaller scale and financial capital compared to its American rivals. Toyota developed new capabilities in production engineering, operations management and managing suppliers to compensate for its inability to afford large inventories, make components, produce raw materials, or own the companies that produced them. Service Management capabilities are similarly influenced by the following challenges that distinguish services from other systems of value creation such as manufacturing, mining, and agriculture: [ITILv3]

- The intangible nature of the output and intermediate products of service processes; this is difficult to measure, control and validate (or prove). [ITILv3]
- Demand is tightly coupled with customer's assets; users and other customer assets such as processes, applications, documents, and transactions arrive with demand and stimulate service production. [ITILv3]
- High level of contact for producers and consumers of services; there is little or no buffer between the customer, the front-office and back-office. [ITILv3]
- The perishable nature of service output and service capacity; there is value for the customer from assurance on the continued supply of consistent quality. Providers need to secure a steady supply of demand from customers. [ITILv3]

Service Management, however, is more than just a set of capabilities. It is also a professional practice supported by an extensive body of knowledge, experience, and skills. A global community of individuals and organizations in the public and private sectors fosters its growth and maturity. Formal schemes exist for the education, training and certification of practicing organizations and individuals influence its

quality. Industry best practices, academic research and formal standards contribute to its intellectual capital and draw from it. [ITILv3]

The origins of Service Management are in traditional service businesses such as airlines, banks, hotels and phone companies. Its practice has grown with the adoption by IT organizations of a service-oriented approach to managing IT applications, infrastructure and processes. Solutions to business problems and support for business models, strategies and operations are increasingly in the form of services. The popularity of shared services and outsourcing has contributed to the increase in the number of organizations that are service providers, including internal organizational units. This in turn has strengthened the practice of Service Management and at the same time imposed greater challenges on it. [ITILv3]

33.3 Functions and Processes Across the Lifecycle

33.3.1 Functions

Functions are units of organizations specialized to perform certain types of work and responsible for specific outcomes. They are self-contained with capabilities and resources necessary to their performance and outcomes. Capabilities include work methods internal to the functions. Functions have their own body of knowledge, which accumulates from experience. They provide structure and stability to organizations. [ITILv3]

Functions are means to structure organizations to implement the specialization principle. Functions typically define roles and the associated authority and responsibility for a specific performance and outcomes. Coordination between functions through shared processes is a common pattern in organization design. Functions tend to optimize their work methods locally to focus on assigned outcomes. Poor coordination between functions combined with an inward focus leads to functional silos that hinder alignment and feedback critical to the success of the organization as a whole. Process models help avoid this problem with functional hierarchies by improving cross functional coordination and control. Well-defined processes can improve productivity within and across functions. [ITILv3]

33.3.2 Processes

Processes are examples of closed-loop systems because they provide change and transformation towards a goal and use feedback for self-reinforcing and self-corrective action (ITILv3 Basic Process Diagram above). It is important to consider the entire process or how one process fits into another. [ITILv3]

Process definitions describe actions, dependencies, and sequence. Processes have the following characteristics: [ITILv3]

- They are measurable. Organizations are able to measure the process in a relevant manner. It is performance driven. Managers want to measure cost, quality and other variables while practitioners are concerned with duration and productivity. [ITILv3]
- They have specific results. The reason a process exists is to deliver a specific result. This result must be individually identifiable and countable. While we can count changes, it is impossible to count how many service desks were completed. [ITILv3]
- They deliver to customers. Every process delivers its primary results to a customer or stakeholder. They may be internal or external to the organization, but the process must meet their expectations. [ITILv3]
- They respond to a specific event. While a process may be ongoing or iterative, it should be traceable to a specific trigger. [ITILv3]

Functions are often mistaken for processes. For example, there are misconceptions about capacity management being a Service Management process. First, capacity management is an organizational capability with specialized processes and work methods. Whether or not it is a function, or a process depends entirely on organization design. It is a mistake to assume that capacity management can only be a process. It is possible to measure and control capacity and to determine whether it is adequate for a given purpose. Assuming that is always a process with discrete countable outcomes can be an error. [ITILv3]

33.4 Specialization and coordination across the lifecycle

Specialization and coordination are necessary in the lifecycle approach. Feedback and control between the functions and processes within and across the elements of the lifecycle make this possible. The dominant pattern in the lifecycle is the sequential progress starting from Service Strategy (SS) through Service Delivery (SD)–Service Transition (ST)–Service Operation (SO) and back to SS through Continual Service Improvement (CSI). That, however, is not the only pattern of action. Every element of the lifecycle provides points for feedback and control. [ITILv3]

The combination of multiple perspectives allows greater flexibility and control across environments and situations. The lifecycle approach mimics the reality of most organizations where effective management requires the use of multiple control perspectives. Those responsible for the design, development, and

improvement of processes for Service Management can adopt a process-based control perspective. For those responsible for managing agreements, contracts and services may be better served by a lifecycle-based control perspective with distinct phases. Both these control perspectives benefit from systems thinking. Each control perspective can reveal patterns that may not be apparent from the other. [ITILv3]

33.5 A Historical Perspective of IT Service Management and the Origins of ITIL

IT service management (ITSM) evolved naturally as services became underpinned in time by the developing technology. In its early years, IT was mainly focused on application development – all the new possibilities seeming to be ends in themselves. Harnessing the apparent benefits of these new technologies meant concentrating on delivering the created applications as a part of a larger service offering, supporting the business itself. [ITILv3]

During the 1980s, as the practice of service management grew, so too did the dependency of the business. Meeting the business need called for a more radical refocus for an IT service approach and the 'IT help desk' emerged to deal with the frequency of issues suffered by those trying to use IT services in delivery of their business. [ITILv3]

At the same time, the UK government, fueled by a need for finding efficiencies, set out to document how the best and most successful organizations approached service management. By the late 1980s and early 1990s, they had produced a series of books documenting an approach to the IT service management needed to support business users. This library of practice was entitled the IT Infrastructure Library – ITIL to its friends. [ITILv3]

The original Library grew to over 40 books and started a chain reaction of interest in the UK IT service community. The term 'IT service management' had not been coined at this point but became a common term around the mid-1990s as the popularity of ITIL grew. In 1991, a user forum, the IT Information Management Forum (ITIMF), was created to bring ITIL users together to exchange ideas and learn from each other and would eventually change its name to the IT Service Management Forum (itSMF). Today, the itSMF has members worldwide as ITIL's popularity continues to grow. [ITILv3]

A formal standard for ITSM, The British Standard 15000, largely based on ITIL practices, was established and followed by various national standards in numerous countries. Since then, the ISO 20000:2005 Standard was introduced and gained rapid recognition globally. [ITILv3]

ITIL's next revision began in the mid-1990s, until 2004. Version 2 of ITIL, as it is commonly referred to, was a more targeted product – with nine books – explicitly bridging the gap between technology and business, and with guidance focused strongly on the processes required to deliver effective services to the business customer. [ITILv3]

33.6 ITIL Today

In 2004, the OGC began the second major refresh initiative of ITIL, in recognition of the massive advancements in technology and emerging challenges for IT service providers. New technology architectures, virtualization and outsourcing became a mainstay of IT and the process-based approach of ITIL needed to be revamped to address service management challenges. [ITILv3]

After twenty years ITIL remains the most recognized framework for ITSM in the world. While it has evolved and changed its breadth and depth, it preserves the fundamental concepts of leading practice. [ITILv3]

33.7 Why is ITIL so successful?

ITIL is intentionally composed of a common-sense approach to service management – do what works. And what works is adapting a common framework of practices that unite all areas of IT service provision toward a single aim – delivering value to the business. The following list defines the key characteristics of ITIL that contribute to its global success: [ITILv3]

- Non-proprietary – ITIL service management practices are applicable in any IT organization because they are not based on any particular technology platform, or industry type. ITIL is owned by the UK government and not tied to any commercial proprietary practice or solution. [ITILv3]
- Non-prescriptive – ITIL offers robust, mature and time-tested practices that have applicability to all types of service organizations. It continues to be useful and relevant in public and private sectors, internal and external service providers, small, medium and large enterprise, and within any technical environment. [ITILv3]
- Best practice – ITIL service management practices represent the learning experiences and thought leadership of the world's best in class service providers. [ITILv3]
- Good practice – Not every practice in ITIL can be considered 'best practice', and for good reason. For many, a blend of common, good and best practices are what give meaning and achievability

to ITSM. In some respects, best practices are the flavor of the day. All best practices become common practices over time, being replaced by new best practices. [ITILv3]

33.8 The ITIL Value Proposition

All high-performing service providers share similar characteristics. This is not coincidence. There are specific capabilities inherent in their success that they demonstrate consistently. A core capability is their strategy. If you were to ask a high-achieving service provider what makes them distinctive from their competitors, they would tell you that it is their intrinsic understanding of how they provide value to their customers. They understand the customer's business objectives and the role they play in enabling those objectives to be met. A closer look would reveal that their ability to do this does not come from reacting to customer needs, but from predicting them through preparation, analysis and examining customer usage patterns. [ITILv3]

The next significant characteristic is the systematic use of service management practices that are responsive, consistent, and measurable, and define the provider's quality in the eyes of their customers. These practices provide stability and predictability and permeate the service provider's culture. [ITILv3]

The final characteristic is the provider's ability to continuously analyze and fine tune service provision to maintain stable, reliable yet adaptive and responsive services that allow the customer to focus on their business without concern for IT service reliability. [ITILv3]

In these situations, you see a trusted partnership between the customer and the service provider. They share risk and reward and evolve together. Each knows they play a role in the success of the other. [ITILv3]

As a service provider, this is what you want to achieve. As a customer, this is what you want in a service provider. [ITILv3]

Take a moment look around at the industry high-performing service providers. You'll see that most use ITIL Service Management practices. This isn't coincidence at all. [ITILv3]

33.9 The ITIL Service Management Practices

When we turn on a water tap, we expect to see water flow from it. When we press down a light switch, we expect to see light fill the room. Not so many years ago these very basic things were not as reliable as they are today. We know instinctively that the advances in technology have made them reliable

enough to be considered a utility. But it isn't just the technology that makes the services reliable. It is how they are managed. This is service management! [ITILv3]

The use of IT today has become the utility of business. Simply having the best technology will not ensure it provides utility-like reliability. Professional, responsive, value-driven service management is what brings this quality of service to the business. [ITILv3]

The objective of the ITIL Service Management practice framework is to provide services to business customers that are fit for purpose, stable and that are so reliable, the business views them as a trusted utility. [ITILv3]

ITIL offers best practice guidance applicable to all types of organizations who provide services to a business. Each publication addresses capabilities having direct impact on a service provider's performance. The structure of the core practice takes form in a Service Lifecycle. It is iterative and multidimensional. It ensures organizations are set up to leverage capabilities in one area for learning and improvements in others. The core is expected to provide structure, stability, and strength to service management capabilities with durable principles, methods and tools. This serves to protect investments and provide the necessary basis for measurement, learning and improvement. [ITILv3]

The guidance in ITIL can be adapted for use in various business environments and organizational strategies. The complementary guidance provides flexibility to implement the core in a diverse range of environments. Practitioners can select complementary guidance as needed to provide traction for the core in a given business context, much like tires are selected based on the type of automobile, purpose and road conditions. This is to increase the durability and portability of knowledge assets and to protect investments in service management capabilities. [ITILv3]

33.10 Navigating the ITIL Service Management Lifecycle

Before discussing the principles of ITIL service management practices, it is helpful to understand the overall content structure and how topics areas are organized within each of the books that together comprise the practices. [ITILv3]

The ITIL service management practices are comprised of three main sets of products and services: [ITILv3]

- ITIL service management practices – core guidance. [ITILv3]
- ITIL service management practices – complementary guidance. [ITILv3]

- ITIL web support services. [ITILv3]

The City's discussion of ITIL service management will only focus on the core guidance practice areas.

ITIL Service Management Practices – Core Guidance

The core set consists of six publications: [ITILv3]

- Introduction to ITIL Service Management Practices
- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement.

A common structure across all the core guidance publications helps to easily find references between volumes and where to look for similar guidance topics within each stage of the lifecycle: [ITILv3]

Practice fundamentals

This section of each core publication sets out the business case argument of the need for viewing service management in a lifecycle context and an overview of the practices in that stage of the lifecycle that contributes to it. It briefly outlines the context for the practices that follow and how they contribute to business value. [ITILv3]

Practice principles

Practice principles are the policies and governance aspects of that lifecycle stage that anchor the tactical processes and activities to achieving their objectives. [ITILv3]

Lifecycle processes and activities

The Service Lifecycle stages rely on processes to execute each element of the practice in a consistent, measurable, repeatable way. Each core publication identifies the processes it makes use of, how they integrate with the other stages of the lifecycle, and the activities needed to carry them out. [ITILv3]

Supporting organization structures and roles

Each publication identifies the organizational roles and responsibilities that should be considered to manage the Service Lifecycle. These roles are provided as a guideline and can be combined to fit into a

variety of organization structures. Suggestions for optimal organization structures are also provided. [ITILv3]

Technology considerations

ITIL service management practices gain momentum when the right type of technical automation is applied. Each lifecycle publication makes recommendations on the areas to focus technology automation on, and the basic requirements a service provider will want to consider when choosing service management tools. [ITILv3]

Practice implementation

For organizations new to ITIL, or those wishing to improve their practice maturity and service capability, each publication outlines the best ways to implement the ITIL Service Lifecycle stage. [ITILv3]

Challenges, risks, and critical success factors These are always present in any organization. Each publication highlights the common challenges, risks, and success factors that most organizations experience and how to overcome them. [ITILv3]

Complementary guidance

There are many external methods, practices and frameworks that align well to ITIL practices. Each publication provides a list of these and how they integrate into the ITIL Service Lifecycle, when they are useful and how. [ITILv3]

Examples and templates

Each publication provides working templates and examples of how the practices can be applied. They are provided to help you capitalize on the industry experience and expertise already in use. Each can be adapted within your particular organizational context. [ITILv3]

33.11 Core Guidance Topics – Service Strategy

At the core of the Service Lifecycle is Service Strategy. [ITILv3]

Service Strategy provides guidance on how to view service management not only as an organizational capability but as a strategic asset. Guidance is provided on the principles underpinning the practice of service management which are useful for developing service management policies, guidelines and processes across the ITIL Service Lifecycle. [ITILv3]

Topics covered in Service Strategy include the development of service markets, characteristics of internal and external provider types, service assets, the service portfolio and implementation of strategy through the Service Lifecycle. Financial Management, Demand Management, Organizational Development and Strategic Risks are among other major topics. [ITILv3]

Organizations should use Service Strategy guidance to set objectives and expectations of performance towards serving customers and market spaces, and to identify, select and prioritize opportunities. Service Strategy is about ensuring that organizations are in position to handle the costs and risks associated with their service portfolios and are set up not just for operational effectiveness but for distinctive performance. [ITILv3]

Organizations already practicing ITIL use Service Strategy to guide a strategic review of their ITIL-based service management capabilities and to improve the alignment between those capabilities and their business strategies. This ITIL volume encourages readers to stop and think about why something is to be done before thinking of how. [ITILv3]

33.12 Core Guidance Topics – Service Design

'If you build it, they will come' is a saying from a famous 1989 Hollywood movie, Field of Dreams. But if you build it and it doesn't provide value, they will soon leave! [ITILv3]

For services to provide true value to the business, they must be designed with the business objectives in mind. Service Design is the stage in the lifecycle that turns Service Strategy into the blueprint for delivering the business objectives. [ITILv3]

Service Design provides guidance for the design and development of services and service management practices. It covers design principles and methods for converting strategic objectives into portfolios of services and service assets. The scope of Service Design is not limited to new services. It includes the changes and improvements necessary to increase or maintain value to customers over the lifecycle of services, the continuity of services, achievement of service levels, and conformance to standards and regulations. It guides organizations on how to develop design capabilities for service management. [ITILv3]

Among the key topics in Service Design are Service Catalogue, Availability, Capacity, Continuity and Service Level Management. [ITILv3]

33.13 Core Guidance Topics – Service Transition

Transition – Movement, passage, or change from one position, state, stage, subject, concept, etc., to another; change: the transition from adolescence to adulthood. [ITILv3]

Service Transition provides guidance for the development and improvement of capabilities for transitioning new and changed services into live service operation. This publication provides guidance on how the requirements of Service Strategy encoded in Service Design are effectively realized in Service Operation while controlling the risks of failure and disruption. [ITILv3]

The Service Transition combines practices in Change, Configuration, Asset, Release and Deployment, Program and Risk Management and places them in the practical context of service management. It provides guidance on managing the complexity related to changes to services and service management processes, preventing undesired consequences while allowing for innovation. Guidance is provided on transferring the control of services between customers and service providers. [ITILv3]

Service Transition introduces the Service Knowledge Management System, which builds upon the current data and information within Configuration, Capacity, Known Error, Definitive Media, and Assets systems and broadens the use of service information into knowledge capability for decision and management of services. [ITILv3]

33.14 Core Guidance Topics – Service Operation

Service Operation embodies practices in the management of the day-to-day operation of services. It includes guidance on achieving effectiveness and efficiency in the delivery and support of services to ensure value for the customer and the service provider. Strategic objectives are ultimately realized through Service Operation, therefore making it a critical capability. Guidance is provided on how to maintain stability in service operations, allowing for changes in design, scale, scope, and service levels. Organizations are provided with detailed process guidelines, methods, and tools for use in two major control perspectives: reactive and proactive. Managers and practitioners are provided with knowledge allowing them to make better decisions in areas such as managing the availability of services, controlling demand, optimizing capacity utilization, scheduling of operations, and fixing problems. Guidance is provided on supporting operations through new models and architectures such as shared services, utility computing, web services and mobile commerce. [ITILv3]

Among the topics presented in this Service Operations are Event, Incident, Problem, Request, Application and Technical Management practices. This book discusses some of the newer industry practices to manage virtual and service-oriented architectures. [ITILv3]

33.15 Core Guidance Topics – Continual Service Improvement

Continual Service Improvement provides instrumental guidance in creating and maintaining value for customers through better design, transition and operation of services. It combines principles, practices and methods from quality management, change management and capability improvement. Organizations learn to realize incremental and large-scale improvements in service quality, operational efficiency and business continuity. Guidance is provided for linking improvement efforts and outcomes with service strategy, design and transition. A closed-loop feedback system, based on the Deming Plan-Do-Check-Act (PDCA) model, is established and capable of receiving inputs for improvements from any planning perspective. [ITILv3]

Guidance on Service Measurement, demonstrating value with metrics, developing baselines and maturity assessments are among the key topics. [ITILv3]

34 Appendix C – National Institute of Science and Technology

The National Institute of Science and Technology (NIST) promulgates cybersecurity standards for use by federal government agencies and others wishing to securely operate information systems and Industrial Control Systems (ICS).

The current version of NIST cybersecurity standards can be found here:

https://csrc.nist.gov/publications/final-pubs

35 Appendix D – Criminal Justice Information Systems (CJIS)

Criminal Justice Information Systems (CJIS) are a network of law enforcement systems, managed nationally by the Federal Bureau of Investigation (FBI). In operating CJIS, the FBI works collaboratively with state, local, and tribal governments to share criminal-justice-related information and publishes standards with which law enforcement agencies must comply for managing and storing Criminal Justice Information (CJI). [FBI]

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. [CJIS Security Policy]

The City of Dallas, in managing CJIS data is required to comply with both federal and state policies and standards governing CJIS. As previously stated, the FBI maintains its federal CJIS Security Policy, while the Texas Department of Public Safety (DPS) publishes a Requirements Companion Document and a Texas CJIS Security Policy that accompanies the FBI CJIS Security Policy. The Texas DPS is also responsible for auditing municipalities' compliance with federal and state CJIS requirements.

The federal CJIS Security Policy requires that agencies shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for CJIS Security Policy areas can be developed for the security program in general, and for a particular information system, when required. [Federal CJIS Security Policy]

The CJIS Security Policy looks at the data (information), services, and protection controls that apply regardless of the implementation architecture. Architectural independence is not intended to lessen the importance of systems but provide for the replacement of one technology with another while ensuring the controls required to protect the information remain constant. [Federal CJIS Security Policy]

The CJIS Security Policy's objective and conceptual focus on security policy areas provide the guidance and standards while avoiding the impact of the constantly changing landscape of technical innovations. The architectural independence of the Policy provides agencies with the flexibility for tuning their information security infrastructure and policies to reflect their own environments. [Federal CJIS Security Policy]

The CJIS Security Policy defines the types of information that comprise CJI. Included in this category is:

- Biometric Data,
- Identity History Data,
- Biographic Data,
- Property Data, and
- Case or Incident History. [Federal CJIS Security Policy]

The Texas DPS embraces the federal CJIS Security Policy as the security policy for the State of Texas, but also publishes the Texas CJIS Security Policy. Consistent with and in addition to the CSP, DPS requires each agency to adhere to the following rules, which shall be followed by all agencies that access Criminal Justice data in the State of Texas:

1. System Updates – All components of IT systems with CJIS connectivity shall be updated with all available Security Hot fixes, Updates and Patches within 30 days of availability. This applies to workstations, servers, laptops, switches, routers, and all other managed IT equipment.
2. End of Life Equipment – All IT systems with CJIS connectivity shall be replaced within 6 months of becoming "end of life", or no longer supported by the manufacturer with Security Hot fixes, Updates and Patches.
3. Physically Secure Location – A physically secure location is a facility, an enclosed police vehicle, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.
4. Compensating Controls for Advanced Authentication – Chief Security Officer approved compensating controls to meet the Advanced Authentication requirement on agency-issued smartphones and tablets with limited feature operating systems are permitted. Compensating controls are temporary control measures that are implemented in lieu of the required Advanced Authentication control measures when an agency cannot meet a requirement due to legitimate technical or business constraints. [Texas CJIS Security Policy]

Finally, the Texas DPS Requirements Companion Document, which outlines changes made to policies. The Texas DPS Requirements Companion Document provides guidance on policy changes, what actor is responsible for ensuring policy implementation, and the prioritization of implementing policy changes. [Texas DPS Requirements Companion Document]

36 General Terms and Acronyms

AD – Administrative Directive (internal policy document) or Assistant Director (position/role)

Archival Data – historical data that is retained for long-term retention reasons. Compliance support is a reason such data may be subject to long-term retention business rules.

BABOK – Business Analyst Body of Knowledge

Backup Data – current or recent data maintained to restore operational data to information systems in the event of a service outage or service incident related to operational data.

CIO – Chief Information Officer

CISO – Chief Information Security Officer

CJIS – Criminal Justice Information System

DAMA – Data Management (DAMA) International

DMBOK – Data Management Body of Knowledge

DHS – The Department of Homeland Security

DOJ – The Department of Justice

DPS – Department of Public Safety (generally refers to the State of Texas Department of Public Safety)

FBI – Federal Bureau of Investigation

GB - Gigabyte

HIPAA – Health Insurance Portability and Accountability Act

IAM – Identity and Access Management

IT – Information Technology

ITIL – Information Technology Infrastructure Library

NIST – National Institute of Standards and Technology

PMBOK – Project Management Body of Knowledge

TB - Terabyte

37 IT Service Management Acronyms

BC – Business Continuity

DR – Disaster Recovery

IAM – Identity and Access Management

ITBC – IT Business Continuity

ITIL – Information Technology Infrastructure Library

38 Solution Acronyms

AMS – American Management Solutions (refers to the CGI Advantage Government Accounting Solution)

CAD – Computer Aided Dispatch (used by City Public Safety elements)

CAPERS – Crimes Against Persons

GIS – Geographical Information System

RMS – Records Management System

39 Department Codes/Acronyms

ATT – City Attorney's Office

AUD – Office of the City Auditor

AVI – Department of Aviation

CIS – Department of Communications and Information Services (former designation for ITS)

DFR – Dallas Fire-Rescue

DPD – Dallas Police Department

DSV – Data Services (accounting code for ITS)

DWU – Dallas Water Utilities

ITS – Department of Information and Technology Services

PBW – Department of Public Works

PKR – Department of Park and Recreation

40 Glossary (ITILv3 Terms of Interest)

Account Manager - A Role that is very similar to Business Relationship Manager but includes more commercial aspects. Most used when dealing with External Customers.

Application – Software that provides Functions that are required by an IT Service. Each Application may be part of more than one IT Service. An application runs on one or more Servers or Clients. See also Application Management.

Application Management - The Function responsible for managing Applications throughout their Lifecycle.

Assembly – A Configuration Item (CI) that is made up of a number of other CIs. For example, a Server CI may contain CIs for CPUs, Disks, Memory, etc.; an IT Service CI may contain many Hardware, Software and other CIs. See also Build.

Assessment – Inspection and analysis to check whether a Standard or set of Guidelines is being followed, that Records are accurate, or that Efficiency and Effectiveness targets are being met. See also Audit.

Asset – Any Resource or Capability. Assets of a Service Provider including anything that could contribute to the delivery of a Service. Assets can be one of the following types: Management, Organization, Process, Knowledge, People, Information, Applications, Infrastructure, and Financial Capital.

Asset Management – Asset Management is the Process responsible for tracking and reporting the value and ownership of financial Assets throughout their Lifecycle. Asset Management is part of an overall Service Asset and Configuration Management Process. See also Asset Register.

Asset Register – A list of Assets that includes their ownership and value. Asset Management maintains the Asset Register.

Audit – Formal inspection and verification to check whether a Standard or set of Guidelines is being followed, that Records are accurate, or that Efficiency and Effectiveness targets are being met. An Audit may be carried out by internal or external groups. See also Certification, Assessment.

Availability – Ability of a Configuration Item or IT Service to perform its agreed Function when required. Availability is determined by Reliability, Maintainability, Serviceability, Performance, and Security. Availability is usually calculated as a percentage. This calculation is often based on Agreed Service Time

and Downtime. It is Best Practice to calculate Availability using measurements of the Business output of the IT Service.

Availability Management – The Process responsible for defining, analyzing, Planning, measuring, and improving all aspects of the Availability of IT services. Availability Management is responsible for ensuring that all IT Infrastructure, Processes, Tools, Roles, etc. are appropriate for the agreed Service Level Targets for Availability.

Back-out - Recovery to a known state after a failed Change or Release.

Back-out Plan – A plan to recover a service to a known state after a failed Change or Release.

Backup - Copying data to protect against loss of Integrity or Availability of the original.

Best Practice – Proven Activities or Processes that have been successfully used by multiple Organizations. ITIL is an example of Best Practice.

Build – The Activity of assembling a number of Configuration Items to create part of an IT Service. The term Build is also used to refer to a Release that is authorized for distribution. For example, Server Build or laptop Build.

Build Environment – A controlled Environment where Applications, IT Services and other Builds are assembled prior to being moved into a Test or Live Environment.

Business – (Service Strategy) An overall corporate entity or Organization formed of a number of Business Units. In the context of ITSM, the term Business includes public sector and not-for-profit organizations, as well as companies. An IT Service Provider provides IT Services to a Customer within a Business. The IT Service Provider may be part of the same Business as its Customer (Internal Service Provider), or part of another Business (External Service Provider).

Business Case – (Service Strategy) Justification for a significant item of expenditure. Includes information about Costs, benefits, options, issues, Risks, and possible problems.

Business Continuity Plan (BCP) – (Service Design) A Plan defining the steps required to Restore Business Processes following a disruption. The Plan will also identify the triggers for Invocation, people to be involved, communications, etc. IT Service Continuity Plans form a significant part of Business Continuity Plans.

Business Customer – A recipient of a product or a Service from the Business. For example, if the Business is a car manufacturer, then the Business Customer is someone who buys a car.

Business Objective – The Objective of a Business Process, or of the Business as a whole. Business Objectives support the Business Vision, provide guidance for the IT Strategy, and are often supported by IT Services.

Business Operations – The day-to-day execution, monitoring and management of Business Processes.

Business Process – A Process that is owned and carried out by the Business. A Business Process contributes to the delivery of a product or Service to a Business Customer. For example, a retailer may have a purchasing Process that helps to deliver Services to its Business Customers. Many Business Processes rely on IT Services.

Business Relationship Management – The Process or Function responsible for maintaining a Relationship with the Business. Business Relationship Management usually includes:

- Managing personal Relationships with Business managers
- Providing input to Service Portfolio Management
- Ensuring that the IT Service Provider is satisfying the Business needs of the Customers.

This Process has strong links with Service Level Management.

Business Service – An IT Service that directly supports a Business Process, as opposed to an Infrastructure Service, which is used internally by the IT Service Provider and is not usually visible to the Business.

The term Business Service is also used to mean a Service that is delivered to Business Customers by Business Units. For example, delivery of financial services to Customers of a bank, or goods to the Customers of a retail store. Successful delivery of Business Services often depends on one or more IT Services.

Business Service Management (BSM) – An approach to the management of IT Services that considers the Business Processes supported and the Business value provided. This term also means the management of Business Services delivered to Business Customers.

Business Unit – A segment of the Business that has its own Plans, Metrics, income and Costs. Each Business Unit owns Assets and uses these to create value for Customers in the form of goods and Services.

Capability – The ability of an Organization, person, Process, Application, Configuration Item or IT Service to carry out an Activity. Capabilities are intangible Assets of an Organization. See also Resource.

Capacity – The maximum Throughput that a Configuration Item or IT Service can deliver whilst meeting agreed Service Level Targets. For some types of CI, Capacity may be the size or volume, for example a disk drive.

Capacity Management – The Process responsible for ensuring that the Capacity of IT Services and the IT Infrastructure is able to deliver agreed Service Level Targets in a Cost Effective and timely manner. Capacity Management considers all Resources required to deliver the IT Service, and plans for short-, medium- and long-term Business Requirements.

Capacity Plan – A Capacity Plan is used to manage the Resources required to deliver IT Services. The Plan contains scenarios for different predictions of Business demand, and costed options to deliver the agreed Service Level Targets.

Category – A named group of things that have something in common. Categories are used to group similar things together. For example, Cost Types are used to group similar types of Cost, Incident Categories are used to group similar types of Incident, CI Types are used to group similar types of Configuration Item.

Change – The addition, modification or removal of anything that could have an effect on IT Services. The Scope should include all IT Services, Configuration Items, Processes, Documentation, etc.

Change Advisory Board (CAB) – A group of people that advises the Change Manager in the Assessment, prioritization and scheduling of Changes. This board is usually made up of representatives from all areas within the IT Service Provider, representatives from the Business and Third Parties such as Suppliers.

Change History – Information about all changes made to a Configuration Item during its life. Change History consists of all those Change Records that apply to the CI.

Change Management – The Process responsible for controlling the Lifecycle of all Changes. The primary objective of Change Management is to enable beneficial Changes to be made, with minimum disruption to IT Services.

Change Model – A repeatable way of dealing with a particular Category of Change. A Change Model defines specific pre-defined steps that will be followed for a change of this Category. Change Models may be very simple, with no requirement for approval (e.g. Password Reset) or may be very complex with many steps that require approval (e.g. major software release). See also Standard Change, Change Advisory Board.

Change Record – A Record containing the details of a Change. Each Change Record documents the Lifecycle of a single Change. A Change Record is created for every Request for Change that is received, even those that are subsequently rejected. Change Records should reference the Configuration Items that are affected by the Change. Change Records are stored in the Configuration Management System.

Change Request – See Request for Change.

Change Schedule – A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented.

Change Window – A regular, agreed time when Changes or Releases may be implemented with minimal impact on Services. Change Windows are usually documented in SLAs.

CI Type – A Category that is used to Classify CIs. The CI Type identifies the required Attributes and Relationships for a Configuration Record. Common CI Types include: Hardware, Document, User, etc.

Classification – The act of assigning a Category to something. Classification is used to ensure consistent management and reporting. CIs, Incidents, Problems, Changes, etc. are usually classified.

Client – A generic term that means a Customer, the Business or a Business Customer. For example, Client Manager may be used as a synonym for Account Manager. The term client is also used to mean:

- A computer that is used directly by a User, for example a PC, Handheld Computer, or Workstation
- The part of a Client-Server Application that the User directly interfaces with. For example, an e-mail Client.

Closed – The final Status in the Lifecycle of an Incident, Problem, Change, etc. When the Status is Closed, no further action is taken.

Closure – The act of changing the Status of an Incident, Problem, Change, etc. to Closed.

Compliance – Ensuring that a Standard or set of Guidelines is followed, or that proper, consistent accounting or other practices are being employed.

Component – A general term that is used to mean one part of something more complex. For example, a computer System may be a component of an IT Service, an Application may be a Component of a Release Unit. Components that need to be managed should be Configuration Items.

Configuration – A generic term, used to describe a group of Configuration Items that work together to deliver an IT Service, or a recognizable part of an IT Service. Configuration is also used to describe the parameter settings for one or more CIs.

Configuration Item (CI) – Any Component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the Configuration Management System and is maintained throughout its Lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT Services, hardware, software, buildings, people, and formal documentation such as Process documentation and SLAs.

Configuration Management – The Process responsible for maintaining information about Configuration Items required to deliver an IT Service, including their Relationships. This information is managed throughout the Lifecycle of the CI. Configuration Management is part of an overall Service Asset and Configuration Management Process.

Configuration Management Database (CMDB) – A database used to store Configuration Records throughout their Lifecycle. The Configuration Management System maintains one or more CMDBs, and each CMDB stores Attributes of CIs, and Relationships with other CIs.

Configuration Management System (CMS) – A set of tools and databases that are used to manage an IT Service Provider's Configuration data. The CMS also includes information about Incidents, Problems, Known Errors, Changes and Releases; and may contain data about employees, Suppliers, locations, Business Units, Customers and Users. The CMS includes tools for collecting, storing, managing, updating, and presenting data about all Configuration Items and their Relationships. The CMS is maintained by

Configuration Management and is used by all IT Service Management Processes. See also Configuration Management Database, Service Knowledge Management System.

Configuration Record – A Record containing the details of a Configuration Item. Each Configuration Record documents the Lifecycle of a single CI. Configuration Records are stored in a Configuration Management Database.

Configuration Structure – The hierarchy and other Relationships between all the Configuration Items that comprise a Configuration.

Continual Service Improvement (CSI) – A stage in the Lifecycle of an IT Service and the title of one of the Core ITIL publications. Continual Service Improvement is responsible for managing improvements to IT Service Management Processes and IT Services. The Performance of the IT Service Provider is continually measured and improvements are made to Processes, IT Services and IT Infrastructure in order to increase Efficiency, Effectiveness, and Cost Effectiveness. See also Plan–Do–Check–Act.

Control – A means of managing a Risk, ensuring that a Business Objective is achieved, or ensuring that a Process is followed. Example Controls include Policies, Procedures, Roles, RAID, door locks, etc. A control is sometimes called a Countermeasure or safeguard. Control also means to manage the utilization or behavior of a Configuration Item, System, or IT Service.

Control Perspective – An approach to the management of IT Services, Processes, Functions, Assets, etc. There can be several different Control Perspectives on the same IT Service, Process, etc., allowing different individuals or teams to focus on what is important and relevant to their specific Role. Example Control Perspectives include Reactive and Proactive management within IT Operations, or a Lifecycle view for an Application Project team.

Cost – The amount of money spent on a specific Activity, IT Service, or Business Unit. Costs consist of real cost (money), notional cost such as people's time, and Depreciation.

Cost Effectiveness – A measure of the balance between the Effectiveness and Cost of a Service, Process or activity. A Cost-Effective Process is one that achieves its Objectives at minimum Cost. See also KPI, Return on Investment, Value for Money.

Countermeasure – Can be used to refer to any type of Control. The term Countermeasure is most often used when referring to measures that increase Resilience, Fault Tolerance or Reliability of an IT Service.

Crisis Management – Crisis Management is the Process responsible for managing the wider implications of Business Continuity. A Crisis Management team is responsible for Strategic issues such as managing media relations and shareholder confidence and decides when to invoke Business Continuity Plans.

Critical Success Factor (CSF) – Something that must happen if a Process, Project, Plan, or IT Service is to succeed. KPIs are used to measure the achievement of each CSF. For example, a CSF of 'protect IT Services when making Changes' could be measured by KPIs such as 'percentage reduction of unsuccessful Changes', 'percentage reduction in Changes causing Incidents', etc.

Culture – A set of values that is shared by a group of people, including expectations about how people should behave, their ideas, beliefs, and practices. See also Vision. Customer Someone who buys goods or Services. The Customer of an IT Service Provider is the person or group that defines and agrees the Service Level Targets. The term Customers is also sometimes informally used to mean Users, for example 'this is a Customer-focused Organization'.

Data–to–Information–to–Knowledge–to– Wisdom (DIKW) – A way of understanding the relationships between data, information, knowledge, and wisdom. DIKW shows how each of these builds on the others.

Definitive Media Library (DML) – One or more locations in which the definitive and approved versions of all software Configuration Items are securely stored. The DML may also contain associated CIs such as licenses and documentation. The DML is a single logical storage area even if there are multiple locations. All software in the DML is under the control of Change and Release Management and is recorded in the Configuration Management System. Only software from the DML is acceptable for use in a Release.

Deliverable – Something that must be provided to meet a commitment in a Service Level Agreement or a Contract. Deliverable is also used in a more informal way to mean a planned output of any Process.

Demand Management – Activities that understand and influence Customer demand for Services and the provision of Capacity to meet these demands. At a Strategic level Demand Management can involve analysis of Patterns of Business Activity and User Profiles. At a tactical level it can involve use of Differential Charging to encourage Customers to use IT Services at less busy times. See also Capacity Management.

Design – An Activity or Process that identifies Requirements and then defines a solution that is able to meet these Requirements. See also Service Design.

Emergency Change – A Change that must be introduced as soon as possible. For example, to resolve a Major Incident or implement a Security patch. The Change Management Process will normally have a specific Procedure for handling Emergency Changes. See also Emergency Change Advisory Board (ECAB).

Emergency Change Advisory Board (ECAB) – A sub-set of the Change Advisory Board that makes decisions about high-impact Emergency Changes. Membership of the ECAB may be decided at the time a meeting is called and depends on the nature of the Emergency Change.

Environment – A subset of the IT Infrastructure that is used for a particular purpose. For example: Live Environment, Test Environment, Build Environment. It is possible for multiple Environments to share a Configuration Item, for example Test and Live Environments may use different partitions on a single mainframe computer. Also used in the term Physical Environment to mean the accommodation, air conditioning, power system, etc.

Error – A design flaw or malfunction that causes a Failure of one or more Configuration Items or IT Services. A mistake made by a person or a faulty Process that affects a CI or IT Service is also an Error.

Event – A change of state that has significance for the management of a Configuration Item or IT Service.

Failure – Loss of ability to Operate to Specification, or to deliver the required output. The term Failure may be used when referring to IT Services, Processes, Activities, Configuration Items, etc. A Failure often causes an Incident.

Fault – See Error.

Fault Tolerance – The ability of an IT Service or Configuration Item to continue to Operate correctly after Failure of a Component part. See also Resilience, Countermeasure.

Fit for Purpose – An informal term used to describe a Process, Configuration Item, IT Service, etc. that is capable of meeting its objectives or Service Levels. Being Fit for Purpose requires suitable design, implementation, control, and maintenance.

Fulfilment – Performing Activities to meet a need or Requirement. For example, by providing a new IT Service, or meeting a Service Request.

Governance – Ensuring that Policies and Strategy are actually implemented, and that required Processes are correctly followed. Governance includes defining Roles and responsibilities, measuring, and reporting, and taking actions to resolve any issues identified.

Integrity – A security principle that ensures data and Configuration Items are modified only by authorized personnel and Activities. Integrity considers all possible causes of modification, including software and hardware Failure, environmental Events, and human intervention.

IT Infrastructure – All of the hardware, software, networks, facilities, etc. that are required to develop, Test, deliver, Monitor, Control or support IT Services. The term IT Infrastructure includes all of the Information Technology but not the associated people, Processes and documentation.

IT Operations – Activities carried out by IT Operations Control, including Console Management, Job Scheduling, Backup and Restore, and Print and Output Management. IT Operations is also used as a synonym for Service Operation.

IT Operations Management – The Function within an IT Service Provider that performs the daily Activities needed to manage IT Services and the supporting IT Infrastructure. IT Operations Management includes IT Operations Control and Facilities Management.

IT Service – A Service provided to one or more Customers by an IT Service Provider. An IT Service is based on the use of Information Technology and supports the Customer's Business Processes. An IT Service is made up from a combination of people, Processes and technology and should be defined in a Service Level Agreement.

IT Service Continuity Plan – A Plan defining the steps required to Recover one or more IT Services. The Plan will also identify the triggers for Invocation, people to be involved, communications, etc. The IT Service Continuity Plan should be part of a Business Continuity Plan.

IT Service Management (ITSM) – The implementation and management of Quality IT Services that meet the needs of the Business. IT Service Management is performed by IT Service Providers through an appropriate mix of people, Process, and Information Technology. See also Service Management.

ITIL – A set of Best Practice guidance for IT Service Management. ITIL was owned by the UK Office of Government Commerce and consists of a series of publications giving guidance on the provision of Quality IT Services, and on the Processes and facilities needed to support them. See www.itil.co.uk for more information.

Knowledge Management – The Process responsible for gathering, analyzing, storing and sharing knowledge and information within an Organization. The primary purpose of Knowledge Management is

to improve Efficiency by reducing the need to rediscover knowledge. See also Data–to–Information–to–Knowledge–to–Wisdom, Service Knowledge Management System.

Maintainability – A measure of how quickly and Effectively a Configuration Item or IT Service can be restored to normal working after a Failure. Maintainability is often measured and reported as MTRS. Maintainability is also used in the context of Software or IT Service Development to mean ability to be Changed or Repaired easily.

Major Incident – The highest Category of Impact for an Incident. A Major Incident results in significant disruption to the Business.

Management Information – Information that is used to support decision making by managers. Management Information is often generated automatically by tools supporting the various IT Service Management Processes. Management Information often includes the values of KPIs such as 'Percentage of Changes leading to Incidents', or 'first-time fix rate'.

Management System – The framework of Policy, Processes and Functions that ensures an organization can achieve its Objectives.

Maturity – A measure of the Reliability, Efficiency and Effectiveness of a Process, Function, Organization, etc. The most mature Processes and Functions are formally aligned to Business Objectives and Strategy and are supported by a framework for continual improvement.

Objective – The defined purpose or aim of a Process, an Activity or an Organization as a whole. Objectives are usually expressed as measurable targets. The term Objective is also informally used to mean a Requirement. See also Outcome.

Operate – To perform as expected. A Process or Configuration Item is said to Operate if it is delivering the Required outputs. Operate also means to perform one or more Operations. For example, to Operate a computer is to do the day-today Operations needed for it to perform as expected.

Operation – Day-to-day management of an IT Service, System, or other Configuration Item. Operation is also used to mean any pre-defined Activity or Transaction. For example, loading a magnetic tape, accepting money at a point of sale, or reading data from a disk drive.

Operational – The lowest of three levels of Planning and delivery (Strategic, Tactical, Operational). Operational Activities include the day-to-day or short-term Planning or delivery of a Business Process or IT Service Management Process. The term Operational is also a synonym for Live.

Operational Level Agreement (OLA) – An Agreement between an IT Service Provider and another part of the same Organization. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties. For example, there could be an OLA:

- Between the IT Service Provider and a procurement department to obtain hardware in agreed times
- Between the Service Desk and a Support Group to provide Incident Resolution in agreed times. See also Service Level Agreement.

Outcome – The result of carrying out an Activity; following a Process; delivering an IT Service, etc. The term Outcome is used to refer to intended results, as well as to actual results. See also Objective.

Performance – A measure of what is achieved or delivered by a System, person, team, Process, or IT Service.

Performance Management – The Process responsible for day-to-day Capacity Management Activities. These include monitoring, threshold detection, Performance analysis and Tuning, and implementing changes related to Performance and Capacity. Plan A detailed proposal that describes the Activities and Resources needed to achieve an Objective. For example, a Plan to implement a new IT Service or Process. ISO/IEC 20000 requires a Plan for the management of each IT Service Management Process.

Planned Downtime – Agreed time when an IT Service will not be available. Planned Downtime is often used for maintenance, upgrades and testing. See also Downtime.

Policy – Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of Processes, Standards, Roles, Activities, IT Infrastructure, etc.

Post-Implementation Review (PIR) – A Review that takes place after a Change or a Project has been implemented. A PIR determines if the Change or Project was successful and identifies opportunities for improvement.

Practice – A way of working, or a way in which work must be done. Practices can include Activities, Processes, Functions, Standards and Guidelines. See also Best Practice.

Problem – A cause of one or more Incidents. The cause is not usually known at the time a Problem Record is created, and the Problem Management Process is responsible for further investigation.

Problem Management – The Process responsible for managing the Lifecycle of all Problems. The primary objectives of Problem Management are to prevent Incidents from happening, and to minimize the Impact of Incidents that cannot be prevented.

Problem Record – A Record containing the details of a Problem. Each Problem Record documents the Lifecycle of a single Problem.

Procedure – A Document containing steps that specify how to achieve an Activity. Procedures are defined as part of Processes. See also Work Instruction.

Process – A structured set of Activities designed to accomplish a specific Objective. A Process takes one or more defined inputs and turns them into defined outputs. A Process may include any of the Roles, responsibilities, tools, and management Controls required to reliably deliver the outputs. A Process may define Policies, Standards, Guidelines, Activities, and Work Instructions if they are needed.

Process Control – The Activity of planning and regulating a Process, with the Objective of performing the Process in an Effective, Efficient, and consistent manner.

Process Manager – A Role responsible for Operational management of a Process. The Process Manager's responsibilities include Planning and coordination of all Activities required to carry out, monitor and report on the Process. There may be several Process Managers for one Process, for example regional Change Managers or IT Service Continuity Managers for each data center. The Process Manager Role is often assigned to the person who carries out the Process Owner Role, but the two Roles may be separate in larger Organizations.

Process Owner – A Role responsible for ensuring that a Process is Fit for Purpose. The Process Owner's responsibilities include sponsorship, Design, Change Management and continual improvement of the Process and its Metrics. This Role is often assigned to the same person who carries out the Process Manager Role, but the two Roles may be separate in larger Organizations.

Qualification – An Activity that ensures that IT Infrastructure is appropriate, and correctly configured, to support an Application or IT Service. See also Validation.

Quality Assurance (QA) – The Process responsible for ensuring that the Quality of a product, Service or Process will provide its intended Value.

RACI – A Model used to help define Roles and Responsibilities. RACI stands for Responsible, Accountable, Consulted, and Informed. See also Stakeholder.

Record – A Document containing the results or other output from a Process or Activity. Records are evidence of the fact that an activity took place and may be paper or electronic. For example, an Audit report, an Incident Record, or the minutes of a meeting.

Recovery – Returning a Configuration Item or an IT Service to a working state. Recovery of an IT Service often includes recovering data to a known consistent state. After Recovery, further steps may be needed before the IT Service can be made available to the Users (Restoration).

Redundancy – See Fault Tolerance

Relationship – A connection or interaction between two people or things. In Business Relationship Management it is the interaction between the IT Service Provider and the Business. In Configuration Management it is a link between two Configuration Items that identifies a dependency or connection between them. For example, Applications may be linked to the Servers they run on, IT Services have many links to all the CIs that contribute to them.

Remediation – Recovery to a known state after a failed Change or Release.

Request for Change (RFC) – A formal proposal for a Change to be made. An RFC includes details of the proposed Change and may be recorded on paper or electronically. The term RFC is often misused to mean a Change Record, or the Change itself.

Request Fulfilment – The Process responsible for managing the Lifecycle of all Service Requests.

Requirement – A formal statement of what is needed. For example, a Service Level Requirement, a Project Requirement, or the required Deliverables for a Process.

Resilience – The ability of a Configuration Item or IT Service to resist Failure or to Recover quickly following a Failure. For example, an armored cable will resist failure when put under stress. See also Fault Tolerance.

Resolution – Action taken to repair the Root Cause of an Incident or Problem, or to implement a Workaround. In ISO/IEC 20000, Resolution Processes is the Process group that includes Incident and Problem Management.

Responsiveness – A measurement of the time taken to respond to something. This could be Response Time of a Transaction, or the speed with which an IT Service Provider responds to an Incident or Request for Change, etc.

Restore – Taking action to return an IT Service to the Users after Repair and Recovery from an Incident. This is the primary Objective of Incident Management.

Return to Normal – The phase of an IT Service Continuity Plan during which full normal operations are resumed. For example, if an alternate data center has been in use, then this phase will bring the primary data center back into operation and restore the ability to invoke IT Service Continuity Plans again.

Review – An evaluation of a Change, Problem, Process, Project, etc. Reviews are typically carried out at predefined points in the Lifecycle, and especially after Closure. The purpose of a Review is to ensure that all Deliverables have been provided, and to identify opportunities for improvement. See also Post-Implementation Review.

Rights – Entitlements, or permissions, granted to a User or Role. For example, the Right to modify data, or to authorize a Change.

Risk – A possible event that could cause harm or loss or affect the ability to achieve Objectives. A Risk is measured by the probability of a Threat, the Vulnerability of the Asset to that Threat, and the Impact it would have if it occurred.

Risk Assessment – The initial steps of Risk Management. Analyzing the value of Assets to the business, identifying Threats to those Assets, and evaluating how Vulnerable each Asset is to those Threats. Risk Assessment can be quantitative (based on numerical data) or qualitative.

Risk Management – The Process responsible for identifying, assessing and controlling Risks. See also Risk Assessment.

Role – A set of responsibilities, Activities and authorities granted to a person or team. A Role is defined in a Process. One person or team may have multiple Roles, for example the Roles of Configuration Manager and Change Manager may be carried out by a single person.

Root Cause – The underlying or original cause of an Incident or Problem.

Root Cause Analysis (RCA) – An Activity that identifies the Root Cause of an Incident or Problem. RCA typically concentrates on IT Infrastructure failures. See also Service Failure Analysis.

Scope – The boundary, or extent, to which a Process, Procedure, Certification, Contract, etc. applies. For example, the Scope of Change Management may include all Live IT Services and related Configuration Items, the Scope of an ISO/IEC 20000 Certificate may include all IT Services delivered out of a named data center.

Service – A means of delivering value to Customers by facilitating Outcomes Customers want to achieve without the ownership of specific Costs and Risks.

Service Acceptance Criteria (SAC) – A set of criteria used to ensure that an IT Service meets its functionality and Quality Requirements and that the IT Service Provider is ready to Operate the new IT Service when it has been Deployed. See also Acceptance.

Service Asset – Any Capability or Resource of a Service Provider. See also Asset.

Service Asset and Configuration Management (SACM) – The Process responsible for both Configuration Management and Asset Management.

Service Catalog – A database or structured Document with information about all Live IT Services, including those available for Deployment. The Service Catalogue is the only part of the Service Portfolio published to Customers and is used to support the sale and delivery of IT Services. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request Processes. See also Contract Portfolio.

Service Contract – A Contract to deliver one or more IT Services. The term Service Contract is also used to mean any Agreement to deliver IT Services, whether this is a legal Contract or an SLA. See also Contract Portfolio.

Service Culture – A Customer-oriented Culture. The major Objectives of a Service Culture are Customer satisfaction and helping Customers to achieve their Business Objectives.

Service Design – A stage in the Lifecycle of an IT Service. Service Design includes a number of Processes and Functions and is the title of one of the Core ITIL publications. See also Design.

Service Design Package – Document(s) defining all aspects of an IT Service and its Requirements through each stage of its Lifecycle. A Service Design Package is produced for each new IT Service, major Change, or IT Service Retirement.

Service Desk – The Single Point of Contact between the Service Provider and the Users. A typical Service Desk manages Incidents and Service Requests, and also handles communication with the Users.

Service Improvement Plan (SIP) – A formal Plan to implement improvements to a Process or IT Service.

Service Knowledge Management System (SKMS) – A set of tools and databases that are used to manage knowledge and information. The SKMS includes the Configuration Management System, as well as other tools and databases. The SKMS stores, manages, updates, and presents all information that an IT Service Provider needs to manage the full Lifecycle of IT Services.

Service Level – Measured and reported achievement against one or more Service Level Targets. The term Service Level is sometimes used informally to mean Service Level Target.

Service Level Agreement (SLA) – An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple customers. See also Operational Level Agreement.

Service Level Management (SLM) – The Process responsible for negotiating Service Level Agreements and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management Processes, Operational Level Agreements, and Underpinning Contracts, are appropriate for the agreed Service Level Targets. SLM monitors and reports on Service Levels and holds regular Customer reviews.

Service Level Package (SLP) – A defined level of Utility and Warranty for a particular Service Package. Each SLP is designed to meet the needs of a particular Pattern of Business Activity.

Service Level Requirement (SLR) – A Customer Requirement for an aspect of an IT Service. SLRs are based on Business Objectives and are used to negotiate agreed Service Level Targets.

Service Level Target – A commitment that is documented in a Service Level Agreement. Service Level Targets are based on Service Level Requirements and are needed to ensure that the IT Service design is Fit for Purpose. Service Level Targets should be SMART and are usually based on KPIs.

Service Management – a set of specialized organizational capabilities for providing value to Customers in the form of Services.

Service Management Lifecycle – An approach to IT Service Management that emphasizes the importance of coordination and Control across the various Functions, Processes, and Systems necessary to manage the full Lifecycle of IT Services. The Service Management Lifecycle approach considers the Strategy, Design, Transition, Operation and Continuous Improvement of IT Services.

Service Manager – A manager who is responsible for managing the end-to-end Lifecycle of one or more IT Services. The term Service Manager is also used to mean any manager within the IT Service Provider. Most commonly used to refer to a Business Relationship Manager, a Process Manager, an Account Manager or a senior manager with responsibility for IT Services overall.

Service Operation – A stage in the Lifecycle of an IT Service. Service Operation includes a number of Processes and Functions and is the title of one of the Core ITIL publications. See also Operation.

Service Owner – A Role that is accountable for the delivery of a specific IT Service.

Service Package – A detailed description of an IT Service that is available to be delivered to Customers. A Service Package includes a Service Level Package and one or more Core Services and Supporting Services.

Service Pipeline – A database or structured Document listing all IT Services that are under consideration or Development but are not yet available to Customers. The Service Pipeline provides a business view of possible future IT Services and is part of the Service Portfolio that is not normally published to Customers.

Service Portfolio – The complete set of Services that are managed by a Service Provider. The Service Portfolio is used to manage the entire Lifecycle of all Services and includes three Categories: Service Pipeline (proposed or in Development); Service Catalog (Live or available for Deployment); and Retired Services. See also Service Portfolio Management, Contract Portfolio.

Service Portfolio Management (SPM) – The Process responsible for managing the Service Portfolio. Service Portfolio Management considers Services in terms of the Business value that they provide.

Service Reporting – The Process responsible for producing and delivering reports of achievement and trends against Service Levels. Service Reporting should agree the format, content, and frequency of reports with Customers.

Service Strategy – The title of one of the Core ITIL publications. Service Strategy establishes an overall Strategy for IT Services and for IT Service Management.

Service Transition – A stage in the Lifecycle of an IT Service. Service Transition includes a number of Processes and Functions and is the title of one of the Core ITIL publications. See also Transition.

Service Utility – The Functionality of an IT Service from the Customer's perspective. The Business value of an IT Service is created by the combination of Service Utility (what the Service does) and Service Warranty (how well it does it). See also Utility.

Service Warranty – Assurance that an IT Service will meet agreed Requirements. This may be a formal Agreement such as a Service Level Agreement or Contract or may be a marketing message or brand image. The Business value of an IT Service is created by the combination of Service Utility (what the Service does) and Service Warranty (how well it does it). See also Warranty.

Specification – A formal definition of Requirements. A Specification may be used to define technical or Operational Requirements and may be internal or external. Many public Standards consist of a Code of Practice and a Specification. The Specification defines the Standard against which an organization can be Audited.

Stakeholder – All people who have an interest in an Organization, Project, IT Service, etc. Stakeholders may be interested in the Activities, targets, Resources, or Deliverables. Stakeholders may include Customers, Partners, employees, shareholders, owners, etc. See also RACI.

Standard – A mandatory Requirement. Examples include ISO/IEC 20000 (an international Standard), an internal security standard for Unix configuration, or a government standard for how financial Records should be maintained. The term Standard is also used to refer to a Code of Practice or Specification published by a Standards Organization such as ISO or BSI. See also Guideline.

Standard Change – A pre-approved Change that is low Risk, relatively common and follows a Procedure or Work Instruction. For example, password reset or provision of standard equipment to a new employee. RFCs are not required to implement a Standard Change, and they are logged and tracked using a different mechanism, such as a Service Request. See also Change Model.

Strategic – The highest of three levels of Planning and delivery (Strategic, Tactical, Operational). Strategic Activities include Objective setting and long-term Planning to achieve the overall Vision.

Strategy – A Strategic Plan designed to achieve defined Objectives.

Supplier Management – The Process responsible for ensuring that all Contracts with Suppliers support the needs of the Business, and that all Suppliers meet their contractual commitments.

Support Group – A group of people with technical skills. Support Groups provide the Technical Support needed by all of the IT Service Management Processes. See also Technical Management.

Supporting Service – A Service that enables or enhances a Core Service. For example, a Directory Service or a Backup Service. See also Service Package.

System – A number of related things that work together to achieve an overall Objective. For example:

- A computer System including hardware, software and Applications
- A management System, including multiple Processes that are planned and managed together. For example, a Quality Management System
- A Database Management System or Operating System that includes many software modules that are designed to perform a set of related Functions.

Tactical – The middle of three levels of Planning and delivery (Strategic, Tactical, Operational). Tactical Activities include the medium-term Plans required to achieve specific Objectives, typically over a period of weeks to months.

Technical Management – The Function responsible for providing technical skills in support of IT Services and management of the IT Infrastructure. Technical Management defines the Roles of Support Groups, as well as the tools, Processes and Procedures required.

Technical Support – See Technical Management.

Test – An Activity that verifies that a Configuration Item, IT Service, Process, etc. meets its Specification or agreed Requirements. See also Service Validation and Testing, Acceptance.

Test Environment – A controlled Environment used to Test Configuration Items, Builds, IT Services, Processes, etc.

Total Cost of Ownership (TCO) – A methodology used to help make investment decisions. TCO assesses the full Lifecycle Cost of owning a Configuration Item, not just the initial Cost or purchase price. See also Total Cost of Utilization.

Total Cost of Utilization (TCU) – A methodology used to help make investment and Service Sourcing decisions. TCU assesses the full Lifecycle Cost to the Customer of using an IT Service. See also Total Cost of Ownership.

Transition – A change in state, corresponding to a movement of an IT Service or other Configuration Item from one Lifecycle status to the next.

Transition Planning and Support – The Process responsible for Planning all Service Transition Processes and coordinating the resources that they require. These Service Transition Processes are Change Management, Service Asset and Configuration Management, Release and Deployment Management, Service Validation and Testing, Evaluation, and Knowledge Management.

Underpinning Contract (UC) – A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.

Urgency – A measure of how long it will be until an Incident, Problem or Change has a significant Impact on the Business. For example, a high Impact Incident may have low Urgency, if the Impact will not affect the Business until the end of the financial year. Impact and Urgency are used to assign Priority.

Usability – The ease with which an Application, product, or IT Service can be used. Usability Requirements are often included in a Statement of Requirements.

Use Case – A technique used to define required functionality and Objectives, and to design Tests. Use Cases define realistic scenarios that describe interactions between Users and an IT Service or other System. User A person who uses the IT Service on a day-to-day basis. Users are distinct from Customers, as some Customers do not use the IT Service directly.

User Profile (UP) – A pattern of User demand for IT Services. Each User Profile includes one or more Patterns of Business Activity.

Utility – Functionality offered by a Product or Service to meet a particular need. Utility is often summarized as 'what it does'. See also Service Utility.

Validation – An Activity that ensures a new or changed IT Service, Process, Plan, or other Deliverable meets the needs of the Business. Validation ensures that Business Requirements are met even though these may have changed since the original design. See also Verification, Acceptance, Qualification, Service Validation and Testing.

Value for Money – An informal measure of Cost Effectiveness. Value for Money is often based on a comparison with the Cost of alternatives.

Variance – The difference between a planned value and the actual measured value. Commonly used in Financial Management, Capacity Management and Service Level Management, but could apply in any area where Plans are in place.

Verification – An Activity that ensures a new or changed IT Service, Process, Plan, or other Deliverable is complete, accurate, Reliable and matches its design specification. See also Validation, Acceptance, Service Validation and Testing.

Verification and Audit – The Activities responsible for ensuring that information in the CMDB is accurate and that all Configuration Items have been identified and recorded in the CMDB. Verification includes routine checks that are part of other processes. For example, verifying the serial number of a desktop PC when a User logs an Incident. Audit is a periodic, formal check.

Version – A Version is used to identify a specific Baseline of a Configuration Item. Versions typically use a naming convention that enables the sequence or date of each Baseline to be identified. For example, Payroll Application Version 3 contains updated functionality from Version 2.

Vision – A description of what the Organization intends to become in the future. A Vision is created by senior management and is used to help influence Culture and Strategic Planning.

Warranty – A promise or guarantee that a product or Service will meet its agreed Requirements. See also Service Validation and Testing, Service Warranty.

Work Instruction – A Document containing detailed instructions that specify exactly what steps to follow to carry out an Activity. A Work Instruction contains much more detail than a Procedure and is only created if very detailed instructions are needed.

Workaround – Reducing or eliminating the Impact of an Incident or Problem for which a full Resolution is not yet available. For example, by restarting a failed Configuration Item. Workarounds for Problems are documented in Known Error Records. Workarounds for Incidents that do not have associated Problem Records are documented in the Incident Record.

Workload – The Resources required to deliver an identifiable part of an IT Service. Workloads may be Categorized by Users, groups of Users, or Functions within the IT Service. This is used to assist in analyzing and managing the Capacity, Performance and Utilization of Configuration Items and IT Services. The term Workload is sometimes used as a synonym for Throughput.

2021-09-30/001