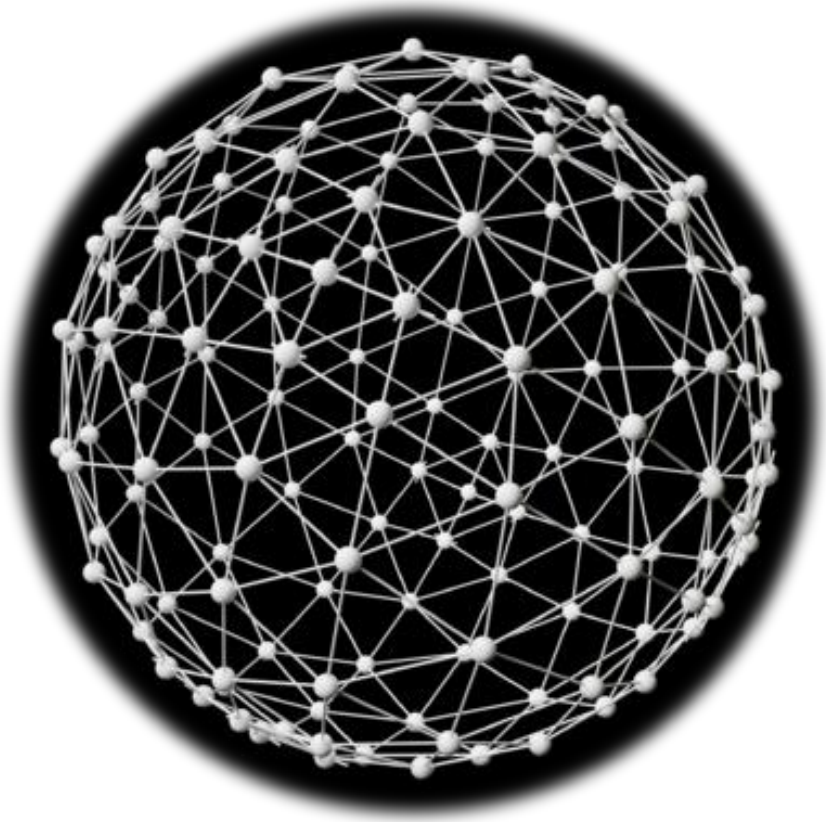
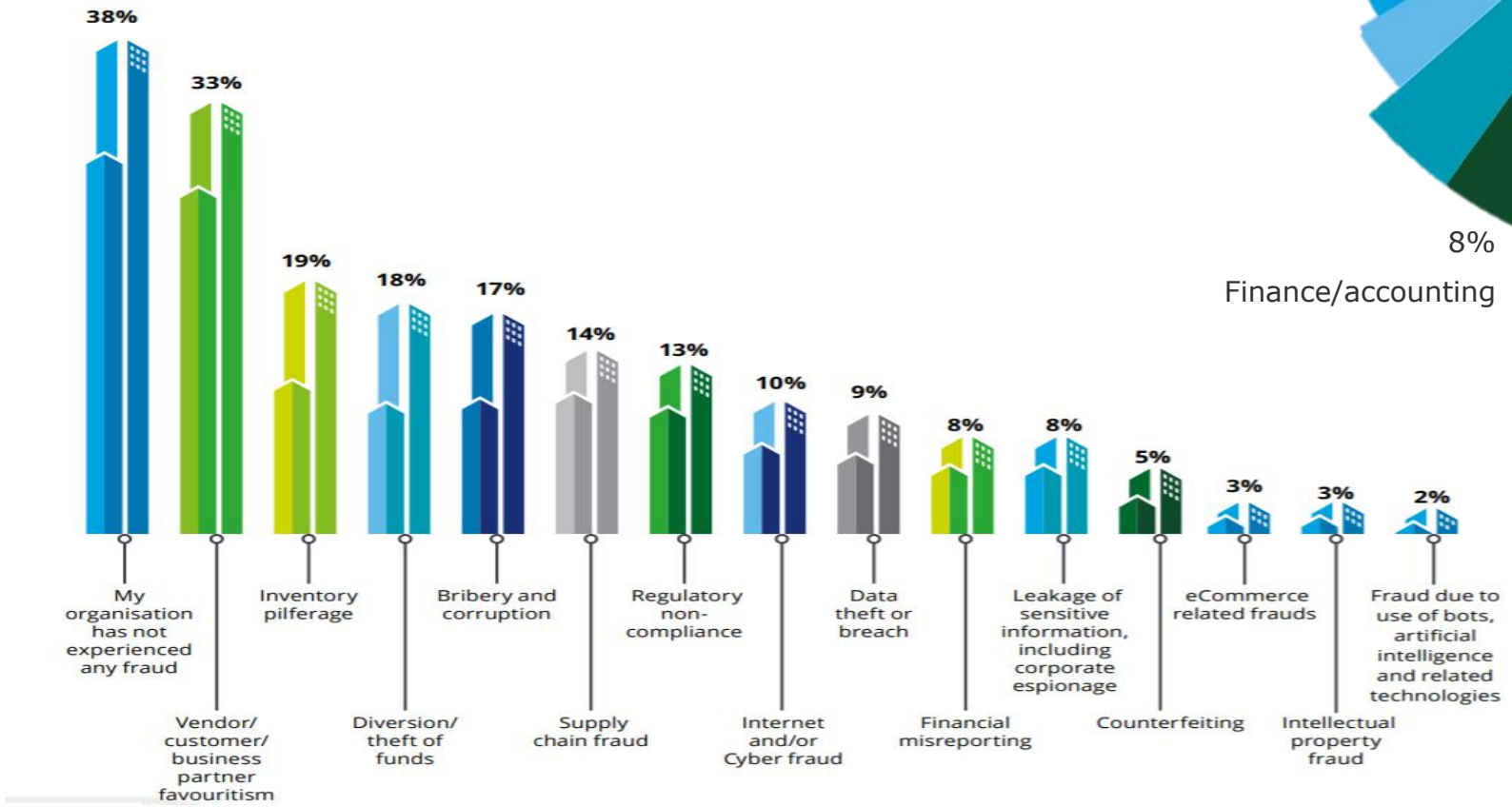


Digital Forensic and Data Analytics in Forensic Audit

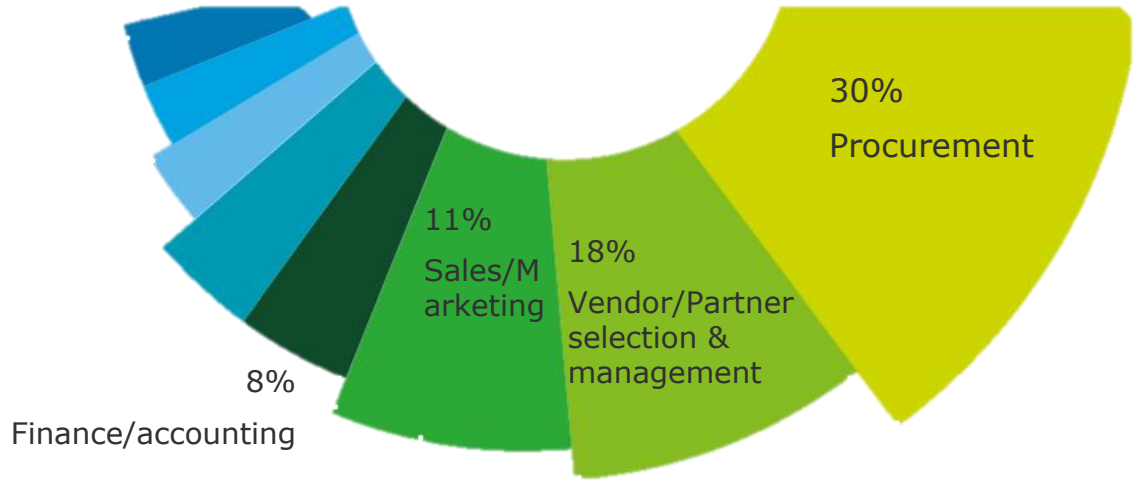
Presented by:
Payal Agarwal,

Perspective of Fraud in India

58% respondent believe that incident of fraud will rise in the next two years



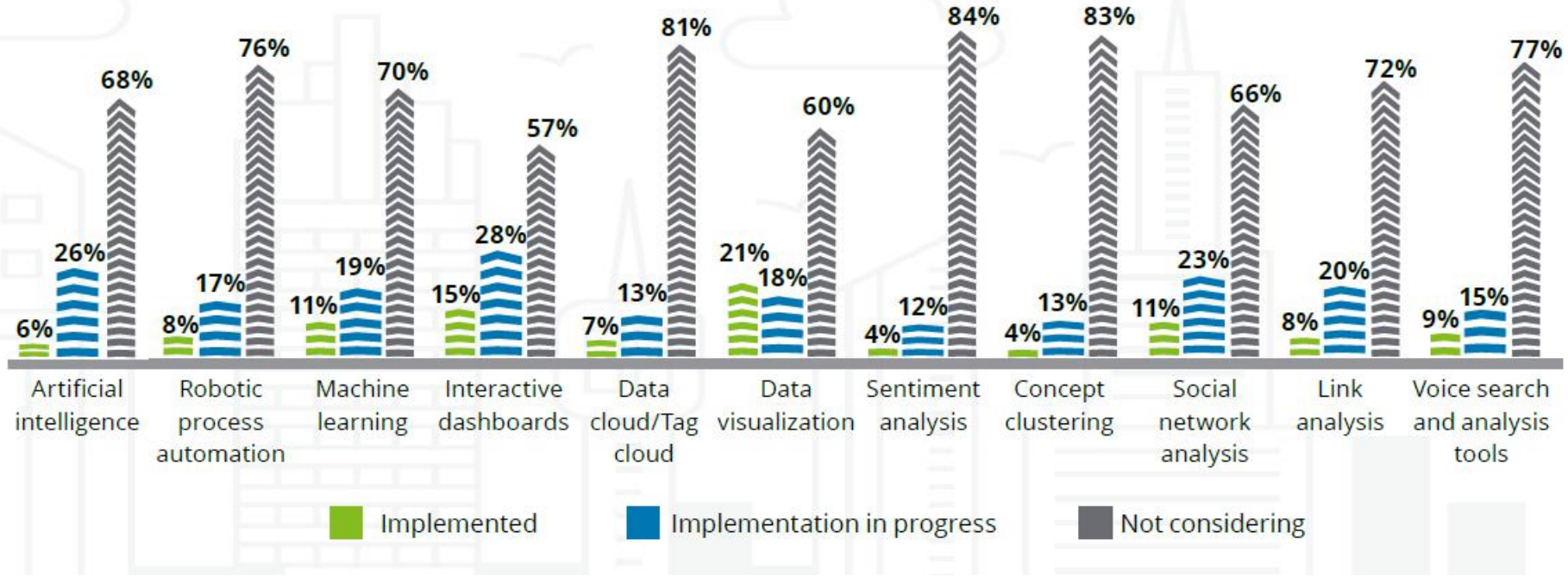
Processes most vulnerable to fraud risk



Source: Deloitte India Fraud Perception Survey 2018

India perspective - usage of technology for fraud detection

Advanced Technology awareness and usage in fraud detection



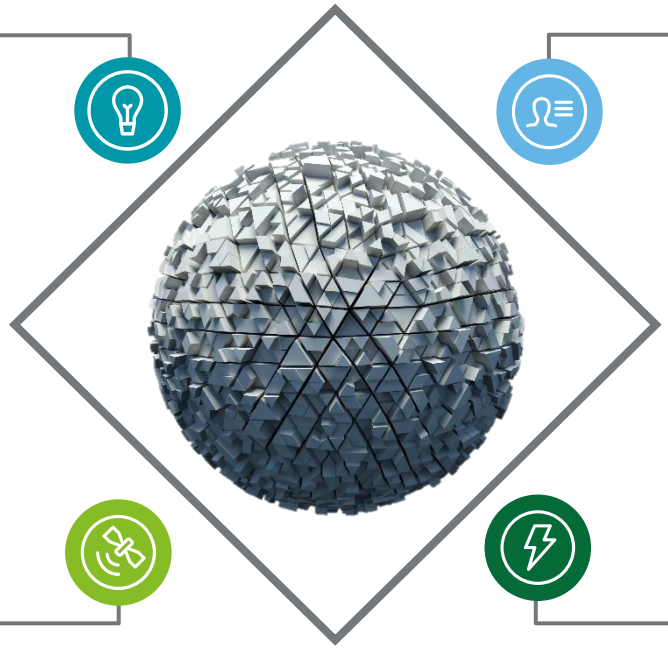
Source: Deloitte India Fraud Perception Survey 2018

Overview of Digital Forensic

Digital Forensic is the application of the scientific principles to the process of discovering information from a digital device

Result Verification:
Result of research need to be validated

Purpose of Research
It is important to define the purpose of research



Test the Hypothesis
Testing helps in fine tuning the results for analysis

Defining the Hypothesis
Defining hypothesis helps in understanding measures to be taken for the research

https://youtu.be/ZUqzcQc_syE

Need for Digital Forensic

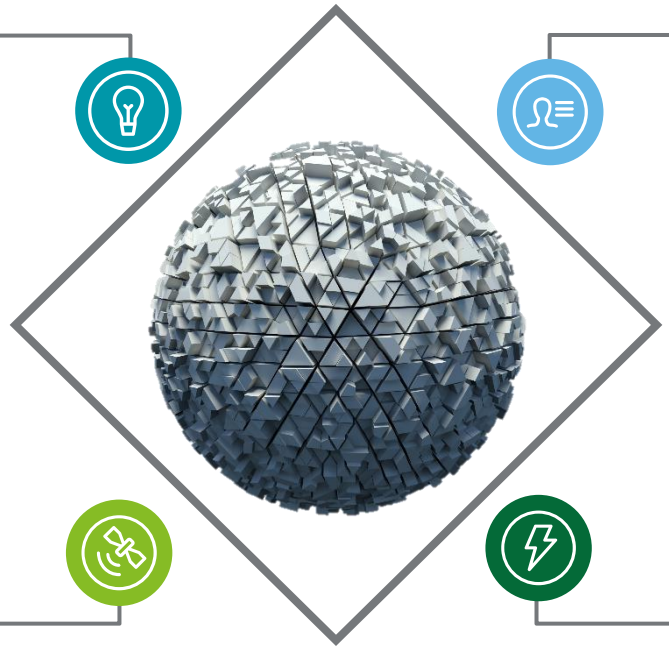
Factors Impeding Fraud Controls

Information Silos :

Can provide an incomplete picture.

Reliance on Rule Based Testing:

Sophisticated schemes can be missed



Can’t always compete with fraudsters:

Reliance on manual processes and ad-hoc data analysis coupled with lack of resources and skills

Unstructured Data :

It is difficult to analyze , access and integrate data.

Digital forensic and its role in fraud risk management

Proactive

- Setting up a forensic lab and/or fraud risk management system
- Evaluating standards of an existing lab/process reviews

Reactive

- Investigations
- Evidence management

Analytics Driven Fraud Investigation

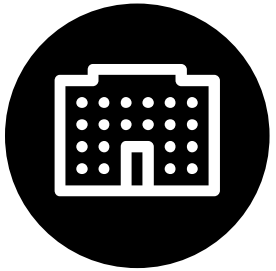
Dimensions for defining analytics driven fraud investigation

Mature Analytics :

Including tools employed, frequency of analysis and whether it is conducted in silos or enterprise manner

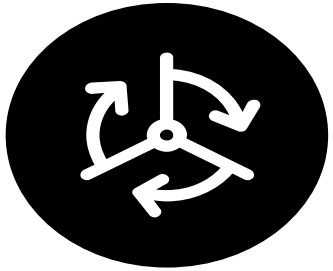
Integrated Data Marts :

Including structured and unstructured data for risk modelling



Risk Scoring at entity rather than transaction :

Transaction don’t commit frauds- employees , vendors, customers and others do..



Advance Analytics :

Including advance analytics such as machine learning, cognitive computing can enable finding associated bad actors

Data considerations during data discovery

Familiarity/Ownership

It is important for senior management to understand the data owners who are fluent at and acquainted with various data systems which are part of their organization's structure

Location

Knowing where the data is stored is as critical as knowing the sensitive nature of different data sets themselves. Data maps help in understanding the landscape of a firm's digital storage infrastructure.

Data type of discovery

Regulatory requirements do not permit cracking passwords to documents or personal email accounts that may be identified as part of the review. Open documents can be reviewed.

Volume

The amount of data that a firm holds must be in line with the understanding of the senior management as well as aligned with the applicable regulatory requirements.

Preservation requirements

Regulatory requirements on retention and preservation schedules of data sets are significant to the firm in times of litigation, and for geographical and jurisdictional privacy compliance.

Reactive Digital forensic: Investigation and data management

- Assessment of complaint and problem at hand
- Stakeholders involved
- Accused involved
- Permission levels
- Access strategy
- Doability assessment

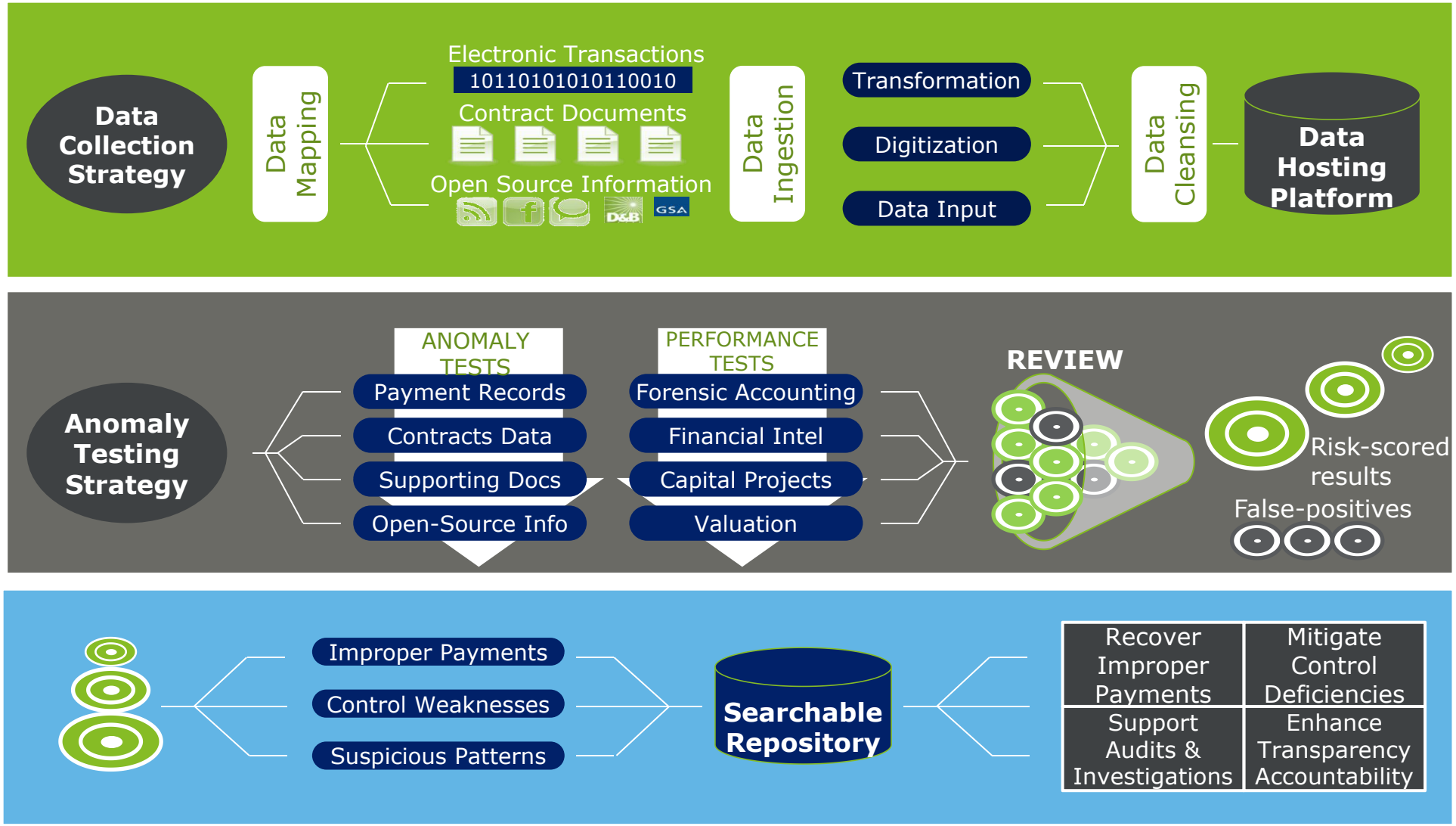
- Nature of IT assets to be reviewed
- Server data + on-asset data identification for each user

- Imaging assets
- 4-24 hour timeframe per asset depending on the security level of asset and type
- Chain of custody procedures
- Raw data collection and storage on hard drives

- Data processing
- Indexing
- Keyword identification based on scope
- Run queries
- Review number of size of results
- Index and transfer data for review

- Review data using review tools like Relativity
- Identify hot, medium, low hits
- Level 1,2,3 reviews for story construct
- Evidence arrangement as per scope and delivery
- Data storage per investigation for 5-7 years as per regulatory requirement

Stages in Advanced Fraud Analytics



Information Processing

Multiple data sources are considered for collection, including electronic records, paper documents, and open-source research.

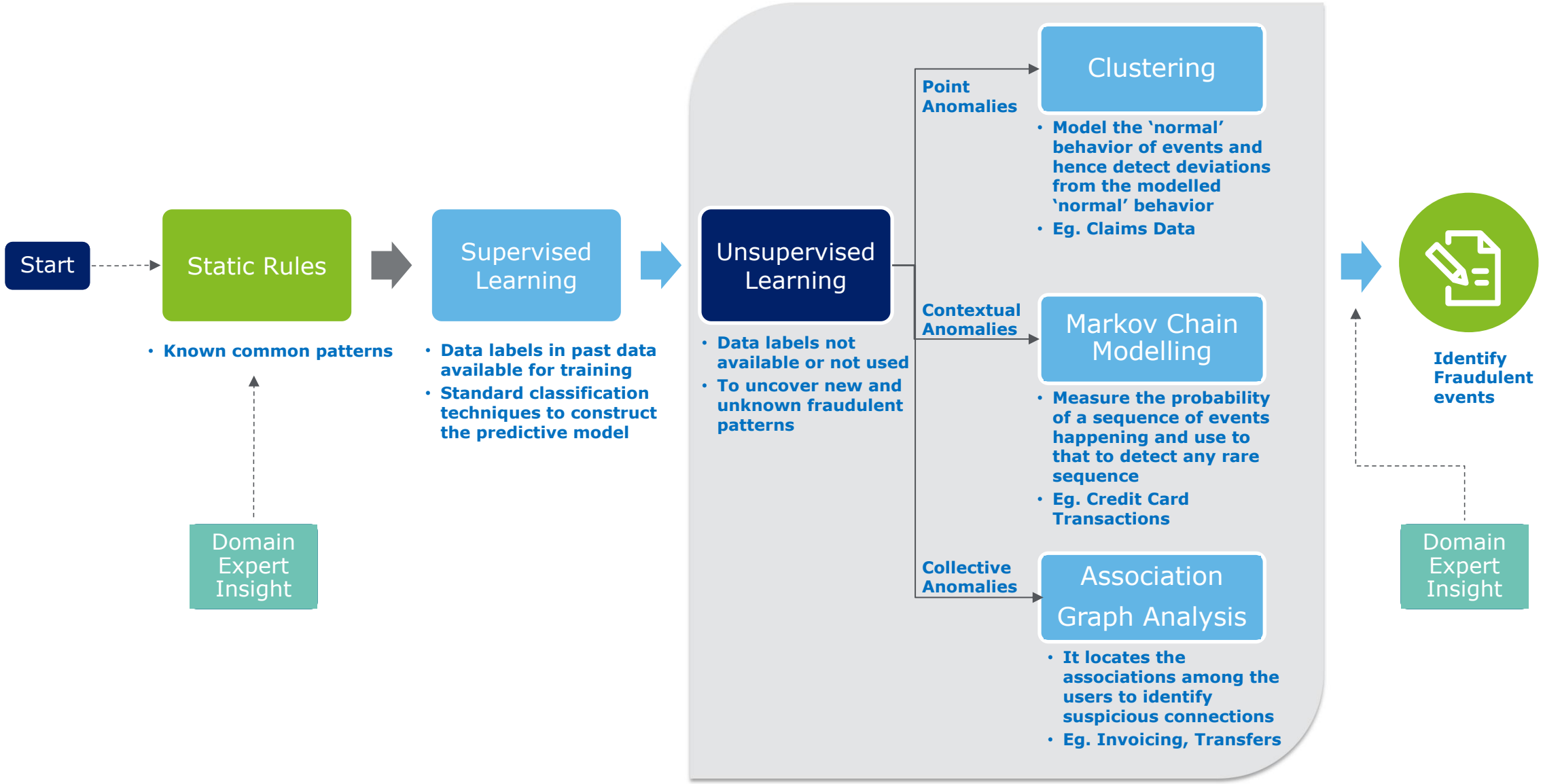
Advance Analytics

Review may be performed on payment data to risk-score potentially anomalous behavior.

Result Management

#The methodology helps to provide the **ACTIONABLE RESULTS** that will provide enhanced transparency and accountability.

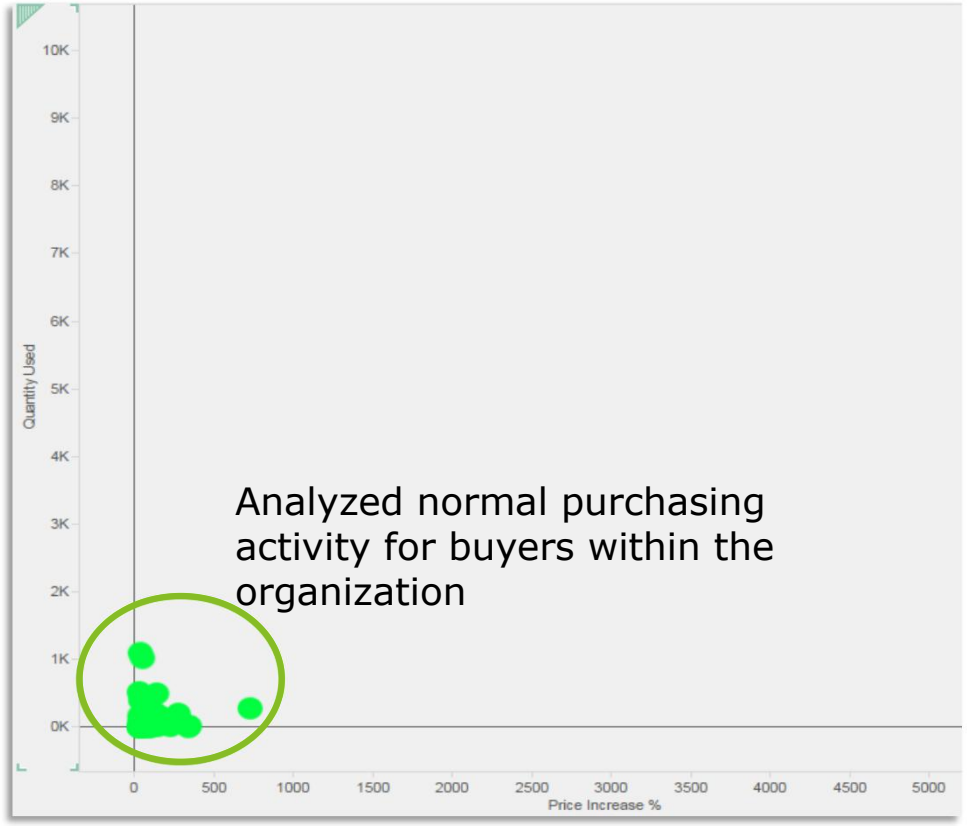
Fraud Detection – Advanced Analytics Solution Approach



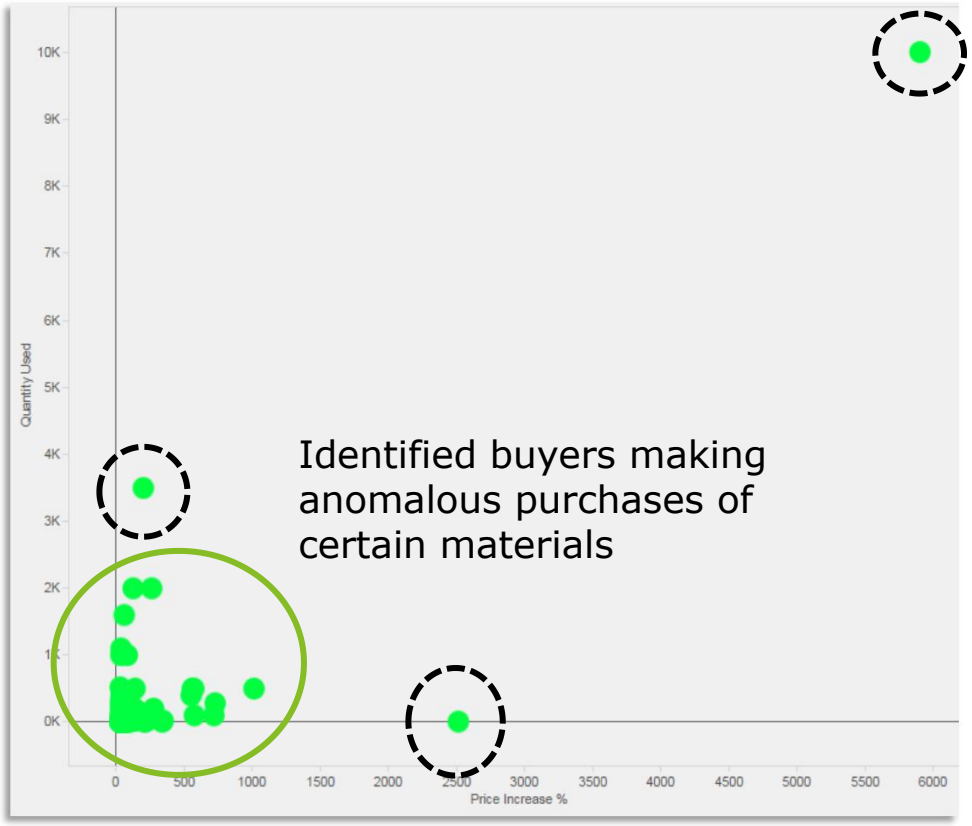
Anomaly Detection

Unsupervised Learning to identify new or emerging fraud patterns, such as buyers that are behaving very differently from their peers.

Buyer A – Normal Behavior



Buyer B – Outliers Identified



Illustrative Sample : Invoice Keywords (Anti-Bribery and Corruption Perspective)

Invoice Keywords
The objective is to identify activites related to bribery or corruption based on keywords
Currency : INR

Summary by Vendor

Vendor ID	Invoice Count	Invoice Line Amount	Number of Keywords
2100005715	5	138,239	3
2100003614	2	8,316	2
2100003738	2	79,380	2
2100006198	4	202,828	2
1000000010	7	391,512	1
1000000027	9	1,188,888	1
1000000032	1	14,904	1
1000000039	1	5,361	1
1000000051	4	92,521	1
1000000056	3	107,855	1
1000000061	9	55,454	1
1000000063	4	83,348	1
1000000079	1	6,270	1
1000000088	3	132,666	1
1000000095	33	1,165,459	1

Summary by Keyword

Keywords			
penal	565	38,399,204	96
dept	16	1,847,812	12
gift	9	1,356,381	8
Award	5	355,886	5
govt	6	148,153	3
agency	1	4,277	1
bonus	1	96,875	1
gratuity	1	500,345	1
police	2		
Proj	1		
Trust	1		

Posting date
3/2/2016 12:00:00 AM to 3/..

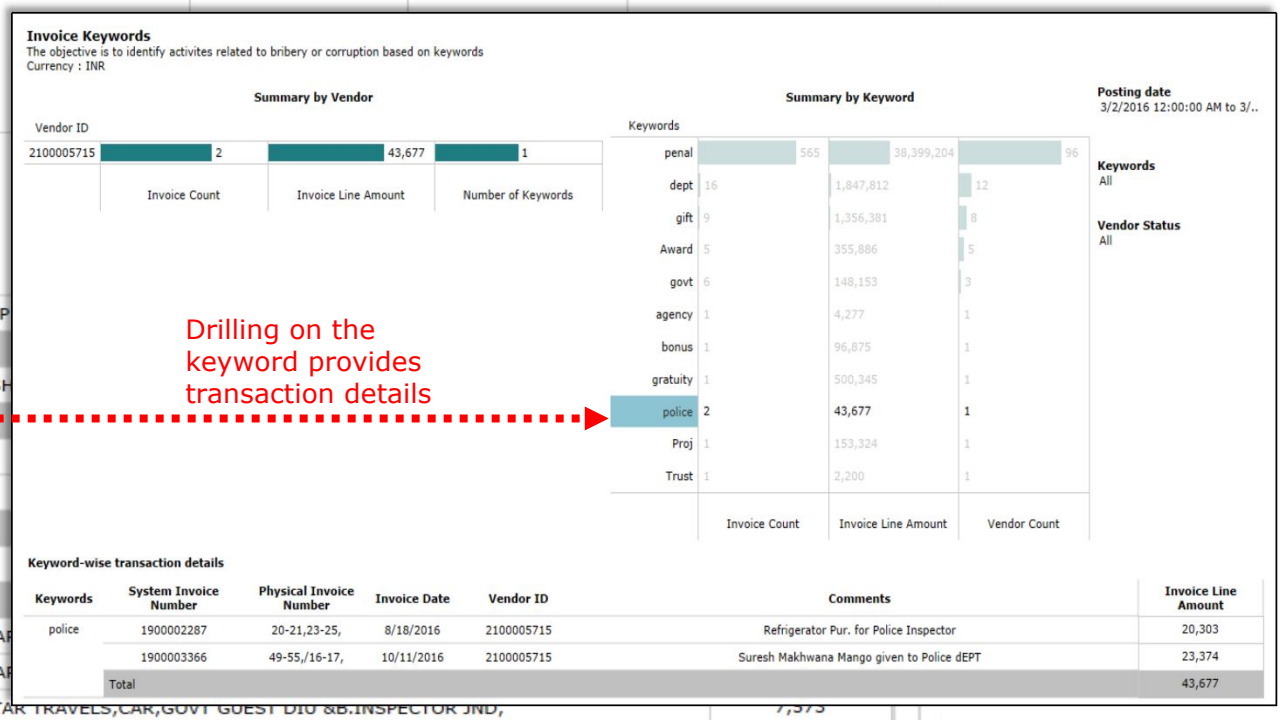
Keywords
All

Vendor Status
All

Keyword-wise transaction details

Keywords	System Invoice Number	Physical Invoice Number	Invoice Date	Vendor ID	
Trust	1900005111	140654,	1/7/2017	EVR020731	R P
	Total				
agency	1900002480	1390,	8/2/2016	2100006026	DISH
	Total				
police	1900002287	20-21,23-25,	8/18/2016	2100005715	
	1900003366	49-55,/16-17,	10/11/2016	2100005715	
	Total				
bonus	5109000895	BONUS	4/27/2016	2100003188	
	Total				
govt	1900002562	26,28,32-35,	8/31/2016	2100005715	STAR
	1900003193	43-48,	9/24/2016	2100005715	STAR
	1900005272	96-97/16-17,	1/29/2017	2100005715	STAR TRAVELS,CAR,GOVT GUEST DIO &B.INSPECTOR JND,
	5109016274	20-23/ESTATE,	11/8/2016	2100005303	ANAND PUSHP BHANDAR,BOUQUETS,GOVT+ABMCPL+G ALORIA

Drilling on the keyword provides transaction details

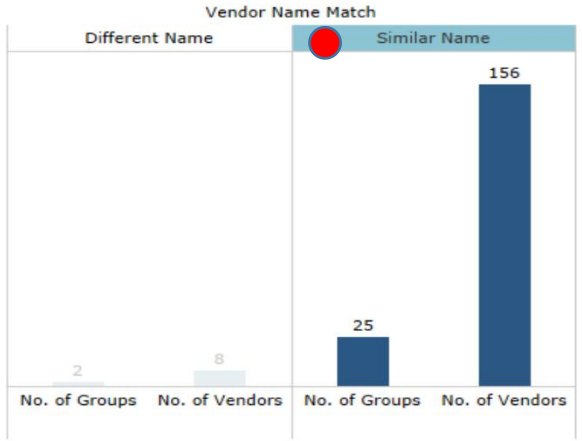


Private and Confidential

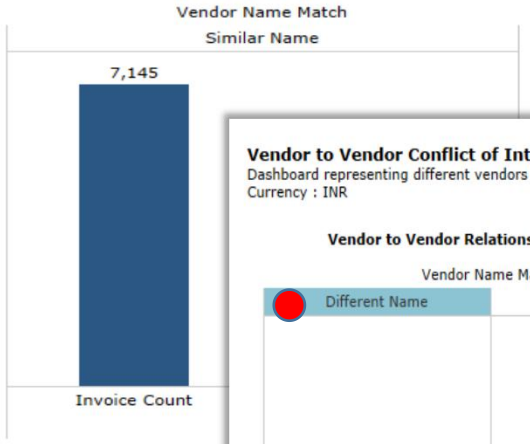
Illustrative Sample : Conflict of Interest Amongst Vendors

Vendor to Vendor Conflict of Interest
Dashboard representing different vendors having the same Account Number, PAN and telephone numbers
Currency : INR

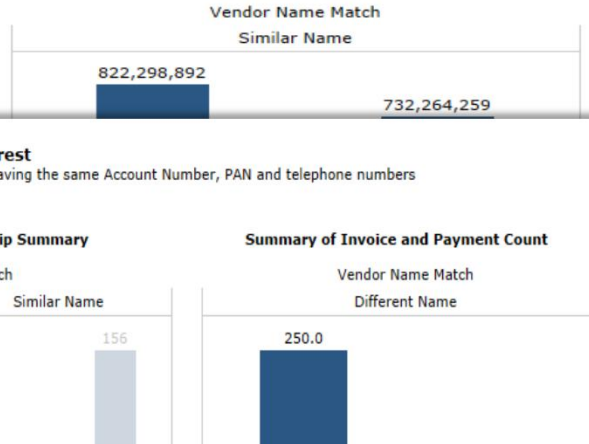
Vendor to Vendor Relationship Summary



Summary of Invoice and Payment Count



Summary of Invoice and Payment Amount



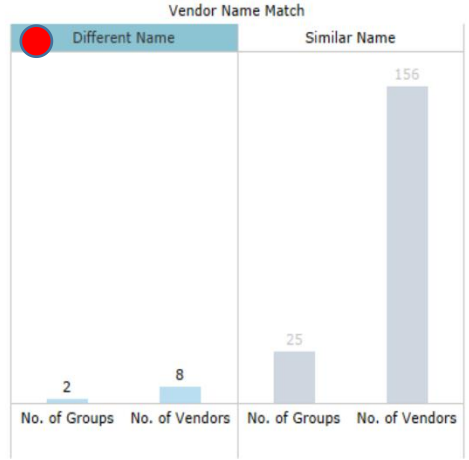
Status
ACTIVE
INACTIVE

Vendor to Vendor demographic details

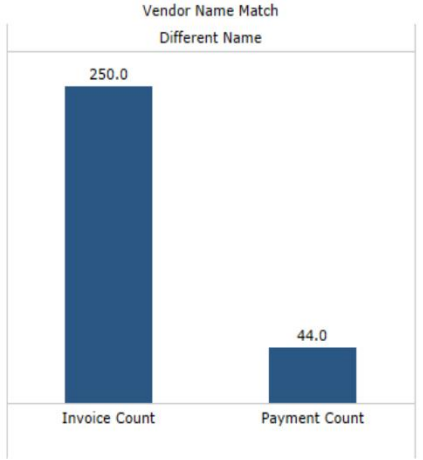
Group Id	Vendor Id	Vendor Name	Account
26	1000000041	ULHASPRABHAS GRAPHITE INC	00640110
			00640110
	2100001405	ULHASPRABHAS GRAPHITE INC	00640110
	Total		
1	0000100307	TECHNOPLAST TIME INC. UNIT- PANOLI	00010330
	0000100308	TECHNOPLAST TIME INC. UNIT -	00010330
	2100008851	TECHNOPLAST TIME INC	2563983
			34337300
			00010330
	2100015083	TECHNOPLAST TIME M/S	00010330
	2100016421	TECHNOPLAST TIME INC.	00010330
	2110000189	TECHNOPLAST TIME INC.	00010330
	Total		
42	1100000131	COM QUEST2TRAVEL ULHASPRABHAS PVT INC	05412560
	2100002592	ULHASPRABHAS QUEST2TRAVEL.COM PVT INC	05412560
	2100006340	ULHASPRABHAS QUEST2TRAVELCOM PVT INC	05412560
	Total		

Vendor to Vendor Conflict of Interest
Dashboard representing different vendors having the same Account Number, PAN and telephone numbers
Currency : INR

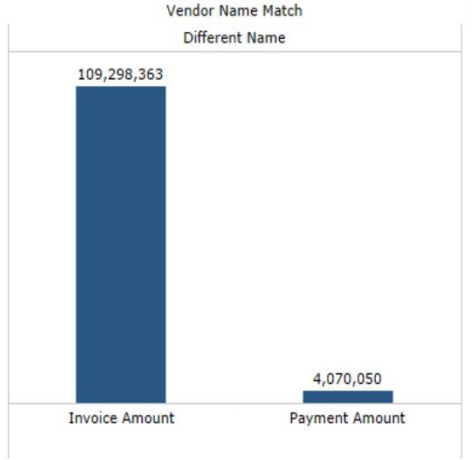
Vendor to Vendor Relationship Summary



Summary of Invoice and Payment Count



Summary of Invoice and Payment Amount



Status
ACTIVE
INACTIVE

Vendor to Vendor demographic details

Group Id	Vendor Id	Vendor Name	Account Number	Pan No	Phone No	Invoice Count	Invoice Amount	Payment Count	Payment Amount
19	2100001081	NARAYAN RAM RAWANI	01430110006917	AADCP1019J	0120-4273453	67	4,647,766	17	2,764,380
	2100001089	RAWANI SANGEETA	01430110006917	AADCP1019J	0120-4273450	0	0	0	0
	Total					67	4,647,766	17	2,764,380
39	1100000132	NEW THE ULHASPRABHAS ASSURANCE CO.,INC	22205443806	AKLPP4722H	01732-307368	42	9,685,975	11	960,397
	2100002194	NEW THE ULHASPRABHAS ASSURANCE CO.	22205443806	AKLPP4722H	01732-250250	93	69,159,783	9	4,620
	2100007854	ULHASPRABHAS NEW ASSURANCE CO.,INC	22205443806	AKLPP4722H	098960-48709	26	6,073,287	3	10,279
	2100009147	ULHASPRABHAS NEW ASSURANCE COMPANY I..	22205443806	AKLPP4722H	01732-250250	22	19,731,552	4	330,374
	Total					183	104,650,597	27	1,305,670

Private and Confidential

Illustrative Sample : Vendor Risk Profile

Executive Summary

Currency : INR

Risk
- [x] HIGH RISK
- [x] LOW RISK
- [x] MEDIUM RISK

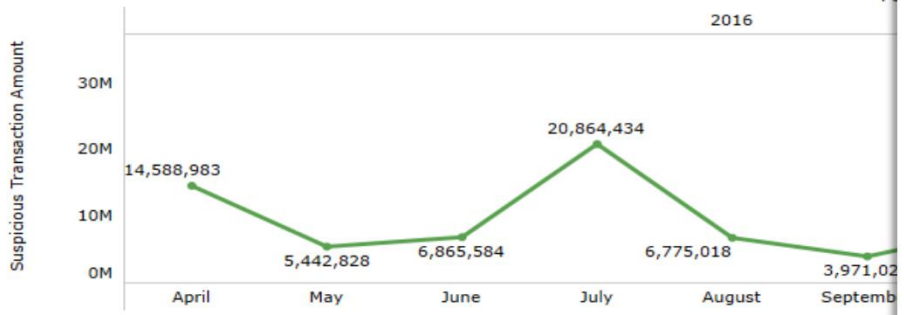
Vendor Risk Classification

Top 10 High Risk Vendors by Exposure Amount

Vendor Id	Exposure Amount	Suspicious Transaction Count
2100005259	10,954,338	2
2100004173	7,180,011	20
2100003211	5,969,085	2
2000000390	3,883,893	3
21000		
21000		
21000		
21000		
20000		
21000		

Suspicious Transa

Suspicious Transac

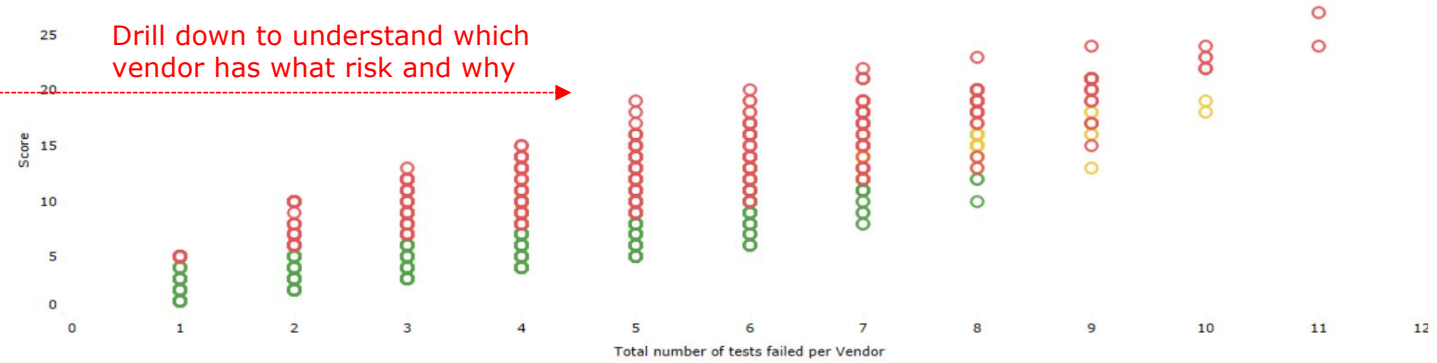


Vendor Profile

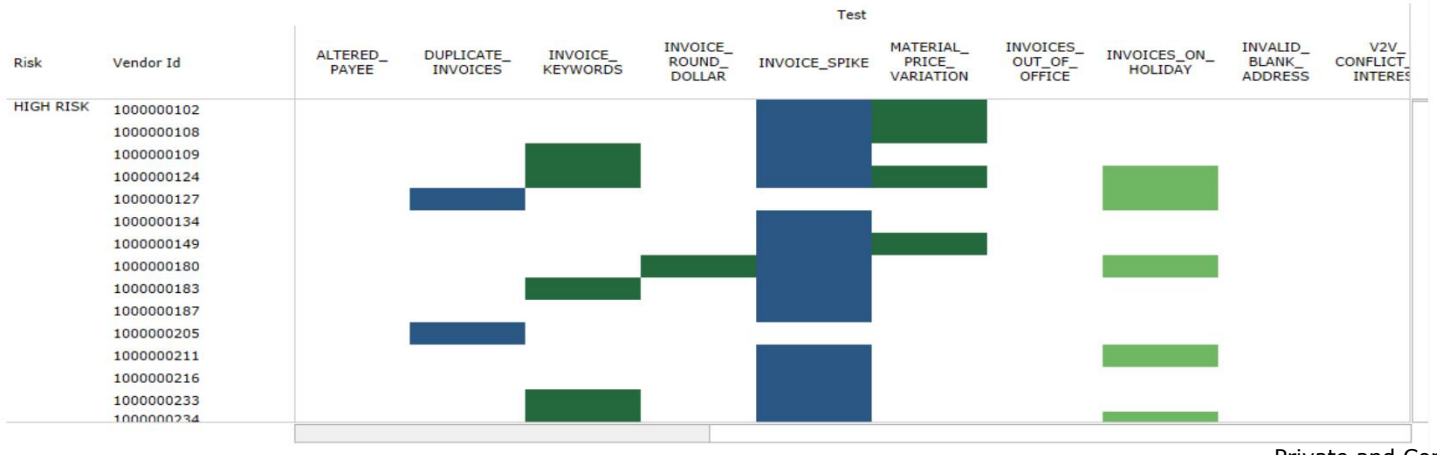
Analysis on demographics and transactional scoring basis vendor

High Risk : > 19 (Also if any of the High Risk Test fails (Score is 5))
Medium Risk : 12-18
Low Risk : 0-11

Drill down to understand which vendor has what risk and why



Vendor-wise test details

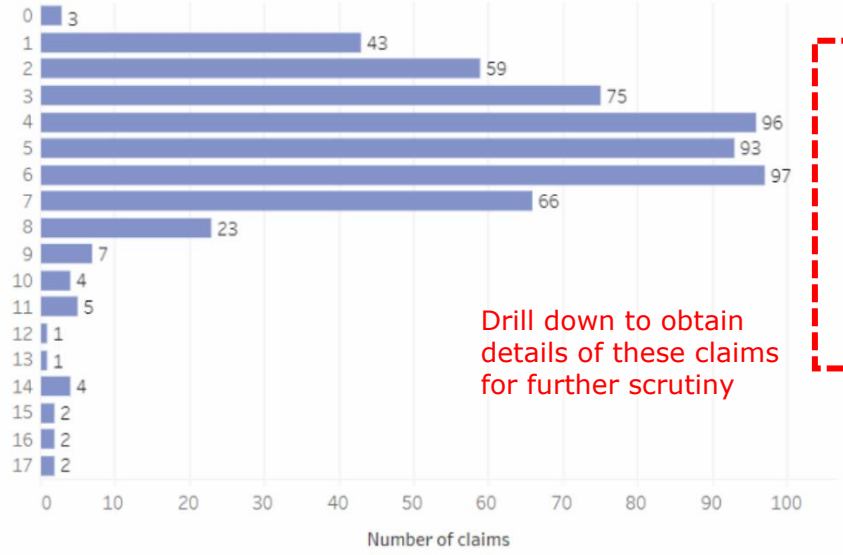


Private and Confidential

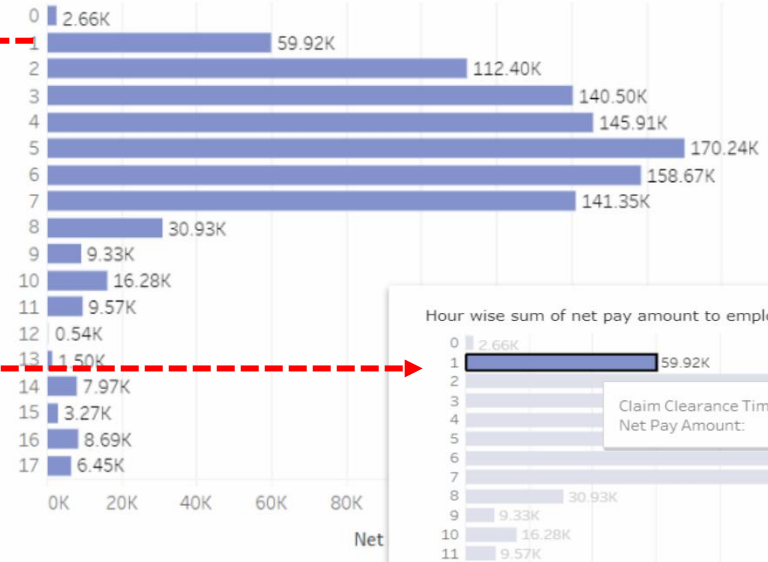
Illustrative Sample :Travel and expense–Claim approved and paid within 24 hours

Claims approved and paid within 24 hours

Hour wise total number of claim approved

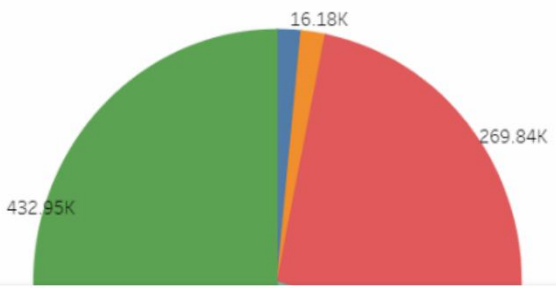


Hour wise sum of net pay amount to employee



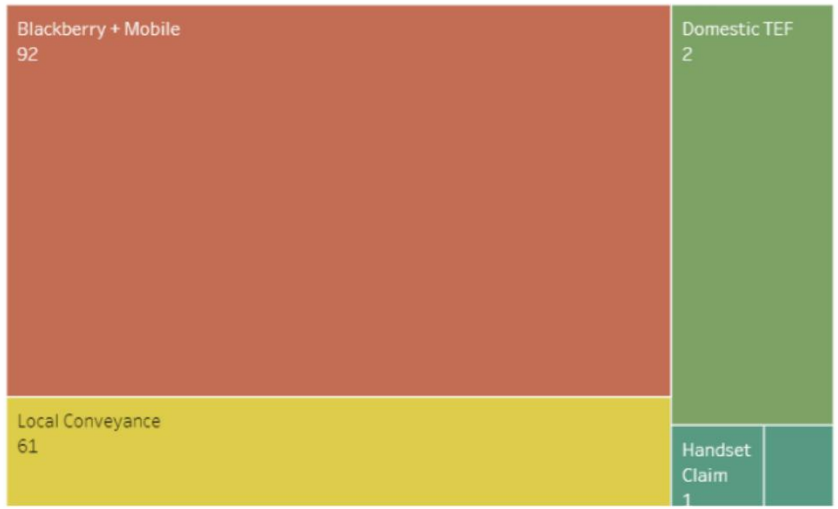
Drill down to obtain details of these claims for further scrutiny

Band wise net paid amount to employee in 24 hours



Claim Clearance Time

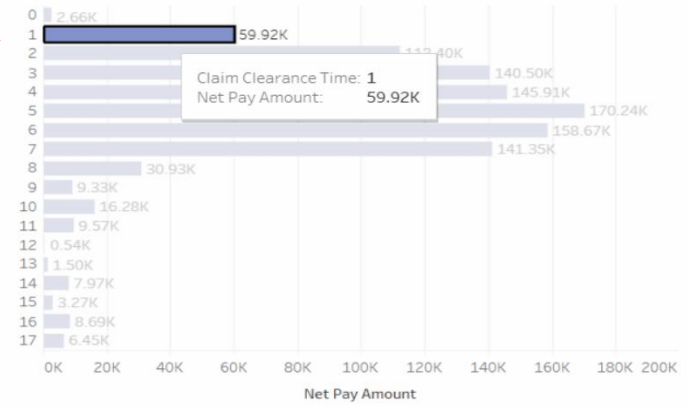
Claim category wise count of claims



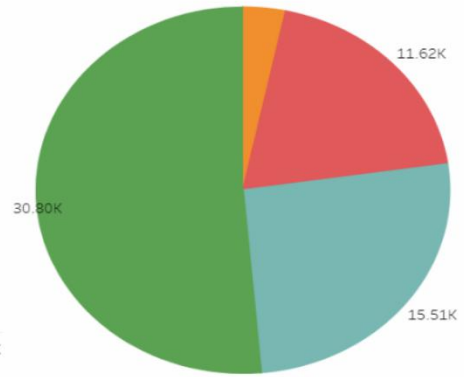
Detail analysis of employees where claim

Claim Id	Employee C..	Employee Name
208128	16943	Santu Paul
220140	18381	Raj Patel
222418	15111	Ashwini Pawar
222870	15208	Pooja Khanna
224773	16319	Jairaj Bisht
224776	16315	Debasis Sasmal
224792	12847	Vikrant Kini
224795	18033	Nitesh Tigga
224796	11871	Parul Sharma
224798	16122	Roshan Panjwani
224802	13129	Rajan Utreja
224816	18015	Gaurav Singh
224817	17253	Rupamanjari Mitr
224825	14537	Harsha Shetty
224830	16894	Sujata Dutta
224831	18223	Moumita Das Roy

Hour wise sum of net pay amount to employee



Band wise net paid amount to employee in 24 hours



Detail analysis of employees where claim approved and paid to employee in 60 Minutes only

Claim Id	Employee C..	Employee Name	Claim clearance time(In Min)	Net Pay Amount
231027	18518	Abhishek Mehta	25	668
233293	17780	Selvaganesh Nadar	31	1,000
226889	18520	Amrit Chopra	32	828
231022	18520	Amrit Chopra	35	732
233292	17780	Selvaganesh Nadar	37	1,000
231024	15111	Ashwini Pawar	40	804
231019	14006	Amit Gupta	43	1,470
270935	14320	Maria Gigool	43	900
230933	15350	Tajinder Bedi	45	578
229028	15412	Pramod Nagdeve	48	2,359
233289	16168	Ashish Harsora	48	534
229029	15412	Pramod Nagdeve	49	2,366
231018	16752	Ravikant Sabnavis	49	1,160
233288	14680	Indranil Dey	51	733
234999	11268	Rajan G. Waingankar	55	517
288366	10037013	Siddharth Taparia	55	177

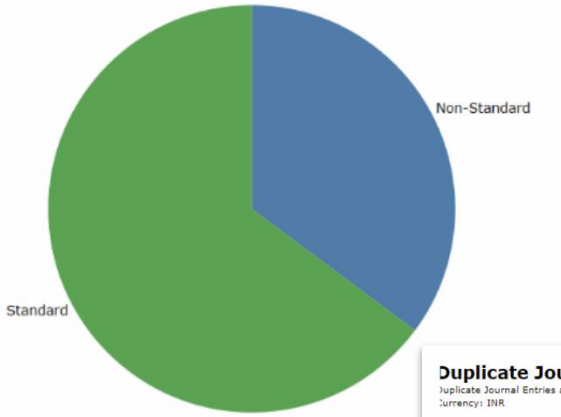
Private and Confidential

Illustrative Sample :Duplicate journal entries

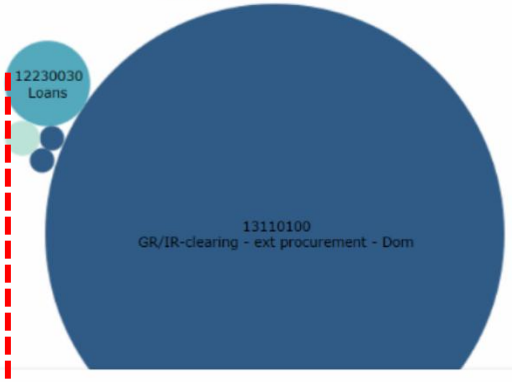
Duplicate Journal Entries

Duplicate Journal Entries are identified basis the Account ID and the absolute General Legder Amount.
Currency: INR

Summary by Entry type



Summary by Account ID



Effective Date
4/12/2013 3/31/2014

Company ID
(All)

General Ledger Amount
1,793,957 8,766,000,000

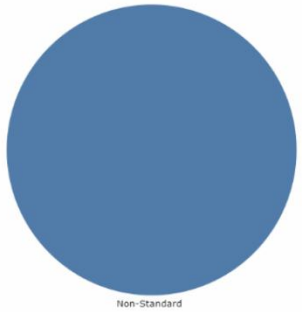
Drill down by account ID for detail breakup

Group ID	Account ID	Account Description	Voucher ID	Line No
9	10200001	Share Application Money (Equity Share)	100002385	1
			100002389	1
8	10200001	Share Application Money (Equity Share)	100002777	1
			100002778	1
64	12230030	Loans Received- Vendors ICD Taken	100002070	1
			100002290	1
58	12230030	Loans Received- Vendors ICD Taken	100000124	1
			100000422	1
			100001478	1
			100001665	1
			100001731	1
			100002021	1
			100002218	1
			100002336	1
			100002474	1
			100003343	1

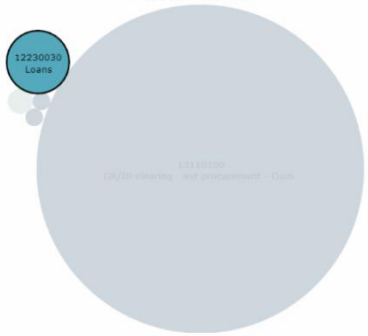
Duplicate Journal Entries

Duplicate Journal Entries are identified basis the Account ID and the absolute General Legder Amount.
Currency: INR

Summary by Entry type



Summary by Account ID



Effective Date
4/12/2013 3/31/20

Company ID
(All)

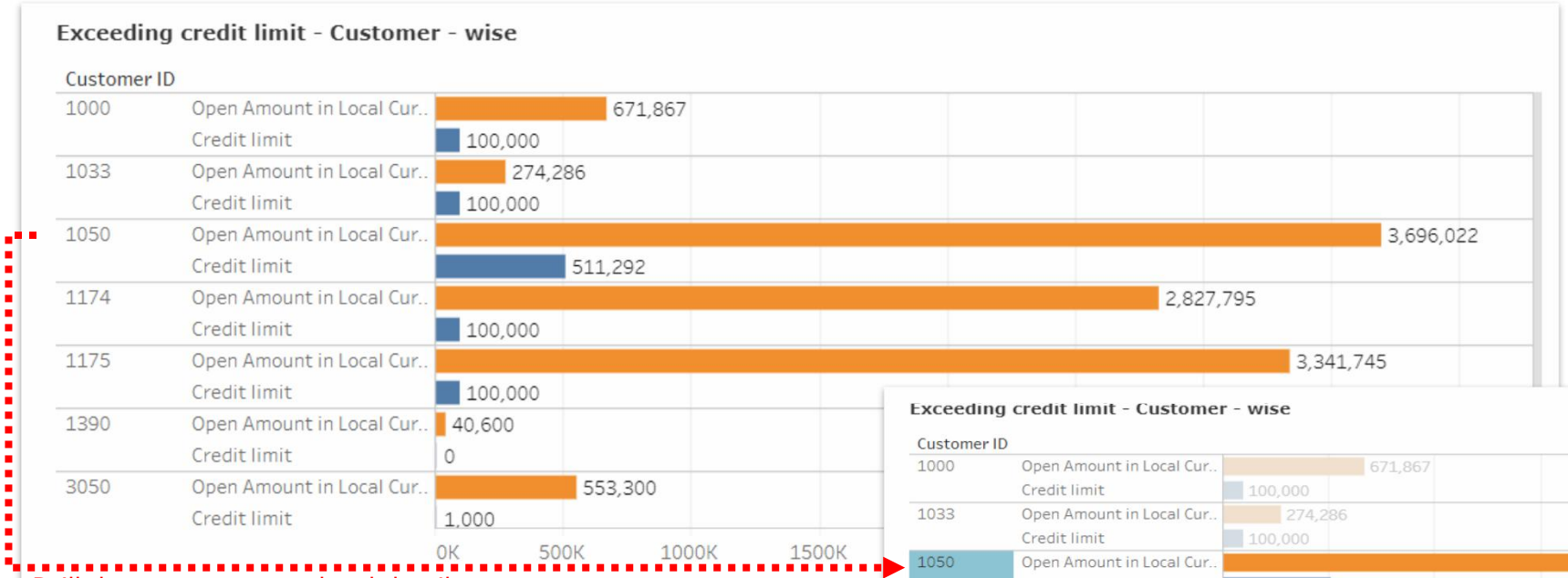
General Ledger Amount
1,793,957 8,766,000,0

Duplicate Journals Analysis

Group ID	Account ID	Account Description	Voucher ID	Line No	Line Description	General Ledger Amount
64	12230030	Loans Received- Vendors ICD Taken	100002070	1	BKTXT: ICD Given Back SGTXT: Bng ICD given back to IPL-35393	1,500,000,000
			100002290	1	BKTXT: ICD GIVEN BACK SGTXT: Bng ICD given back to IPL-35393 from Elena-31007	1,500,000,000
58	12230030	Loans Received- Vendors ICD Taken	100000124	1	BKTXT: SGTXT: bng ICD given back to IPL	75,000,000
			100000422	1	BKTXT: SGTXT: Bng ICD given back to IPL 35393	75,000,000
			100001478	1	BKTXT: SGTXT: Bng ICD given bck to IPL	75,000,000
			100001665	1	BKTXT: ICD GIVEN BACK SGTXT: bng icd given back to IPL from elena-31007	75,000,000
			100001731	1	BKTXT: ICD given back SGTXT: being ICD given baqck to IPL-35393	75,000,000
			100002021	1	BKTXT: ICD Given Back SGTXT: being ICD given back to IPL-35393	75,000,000
			100002218	1	BKTXT: ICD GIVEN BACK SGTXT: Bng ICD given back to IPL-35393	75,000,000
			100002336	1	BKTXT: ICD GIVEN BACK SGTXT: Bng ICD given back to IPL-35393 from Elena-31007	75,000,000
			100002474	1	BKTXT: ICD GIVEN BACK SGTXT: Bng ICD given back to IPL-35393 from Elena-31007	75,000,000
			100003343	1	BKTXT: ICD GIVEN BACK SGTXT: Bng ICD Given back to IPL-35393 from Elena-31007	75,000,000
59	12230030	Loans Received- Vendors ICD Taken	100000870	1	BKTXT: ICD GIVEN SGTXT: BNG ICD GIVEN TO IPL	78,000,000
			100002278	1	BKTXT: ICD Given Back SGTXT: Bng ICD given back to IPL-35393 from Elena-31007	78,000,000
			100002676	1	BKTXT: ICD GIVEN BACK SGTXT: Bng ICD given back to IPL-35393 from Elena-31007	78,000,000
			100002999	1	BKTXT: ICD GIVEN BACK SGTXT: Bng ICD Given back to IPL-35393 from Elena-31007	78,000,000
61	12230030	Loans Received- Vendors ICD Taken	100000040	1	BKTXT: ICD Given Back SGTXT: being ICD given back to IPL-35393	90,000,000

Private and Confidential

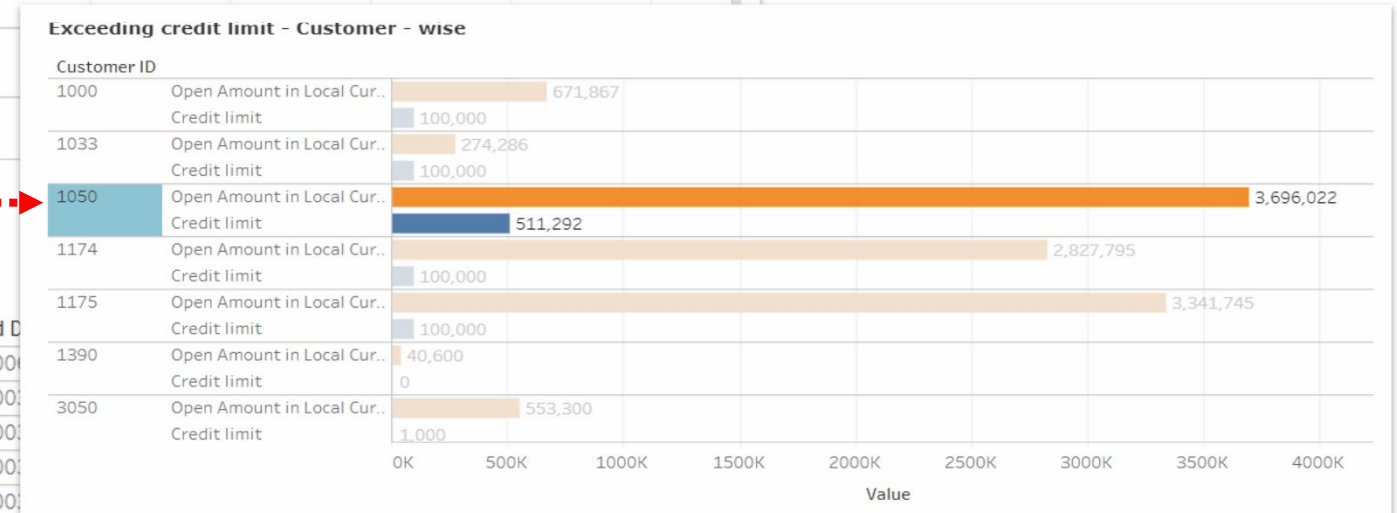
Illustrative Sample : Order to cash- Exceeding credit limit-customer wise



Drill down to customer level details

Exceeding credit limit - Customer - details

Customer ID	Invoice Entere..	Credit limit	Open Amount in Lo..	System Invoic..	Entered D
1000	LYNAM	100000	671866.5	1800000000	8/10/200
	MOELLGAARD	100000	671866.5	1800000032	8/15/200
				1800000031	8/15/200
				1800000030	8/15/200
				1800000029	8/15/200
				1800000028	8/15/200
	ZECHA	100000	671866.5	100000025	5/8/2006
1033	MAASSBERG	100000	274286.14	100006220	2/18/200
	MMUELLER	100000	274286.14	100000015	1/5/2005
				100000245	2/5/2006



Exceeding credit limit - Customer - details

Customer ID	Invoice Ent..	Credit limit	Open Amount in Lo..	System Invoic..	Entered Date	Invoice Date	Gross Amount
1050	MAASSBERG	511291.88	3696022.16	100002680	9/23/2005 4:01:38 AM	9/30/2005 12:00:00 AM	625,133
				100003227	10/26/2005 4:01:22 AM	10/31/2005 12:00:00 AM	623,305
				100002388	8/23/2005 4:01:40 AM	8/31/2005 12:00:00 AM	604,149
				100000608	1/28/2005 4:30:22 PM	1/31/2005 12:00:00 AM	594,557
				100001808	6/23/2005 4:01:35 AM	6/30/2005 12:00:00 AM	544,986
				100002353	7/25/2005 4:02:57 AM	7/31/2005 12:00:00 AM	229,094
				100001252	4/25/2005 4:03:57 AM	4/30/2005 12:00:00 AM	133,639
				100003228	10/26/2005 4:01:50 AM	10/31/2005 12:00:00 AM	127,220
				100000958	3/23/2005 4:02:15 AM	3/31/2005 12:00:00 AM	106,970
				100002389	8/23/2005 4:02:09 AM	8/31/2005 12:00:00 AM	106,970

Private and Confidential

Thank You

Payal Agarwal