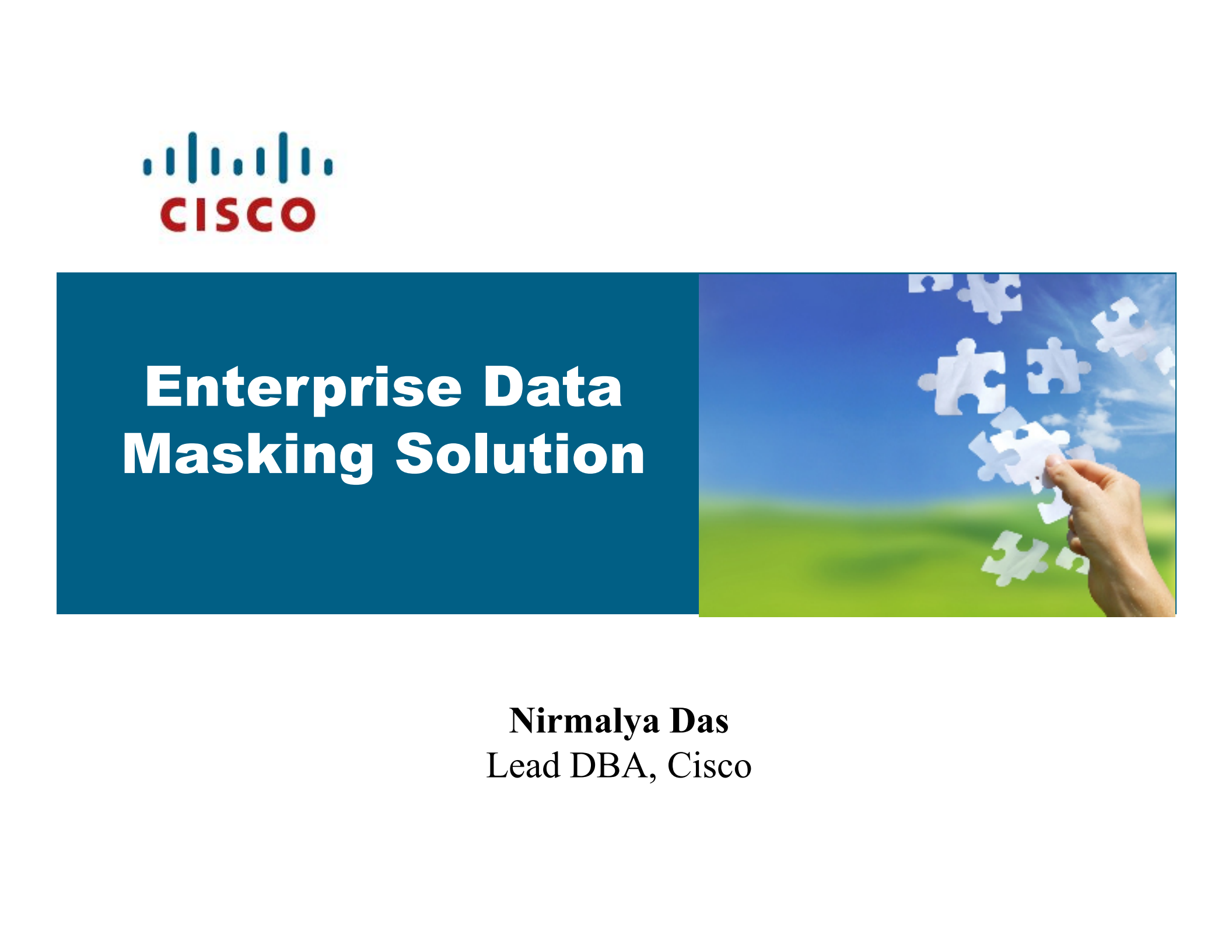


Nirmalya Das
Lead DBA, Cisco

Business Drivers

- Cisco data is required to keep private to be in compliance with external Privacy Laws and Regulations. For example, SOX, Payment Card Industry(PCI), Health Insurance Portability and Accountability Act (HIPAA).
  - Visit Cisco privacy central for in-depth view of Privacy http://www.cisco.com/web/siteassets/legal/privacy.html
  - Privacy policies and guidelines

- All other business data considered sensitive by Cisco e.g. credit card numbers, financial data, engineering data, personnel and customer data (Personally Identifiable Information (PII)).

Current Challenges

- Cisco did not have a uniform, standardized process or tool where private data, data classified as confidential or restricted, is disguised in the supporting instances to production.
- Cisco could not ensure that all private data is disguised and no exposure exists with regards to this data
- Risk to Cisco involving fraudulent activities, loss of customer trust, damage to brand, expensive notification, remediation efforts, and violations of various regulatory and statutory requirements resulting fines and penalties.

Project goals

- Facilitate the compliance of worldwide Data Privacy rules and regulations at Cisco
- Reduce the amount of individual manual analysis and effort required to manage and duplicate masked data among different functional areas
- Implement an enterprise-wide solution that standardizes a repeatable data-masking process and capabilities for non production environments
- Ensure masked data is ‘fit for use’
- Provide reliable assurance that private data will not be exposed in non-production environments
- Leverage investments in existing tools where possible

RFP-based Evaluation

- 5 Vendors shortlisted through RFP process
- 2 selected for final evaluation
  - Technical proof of concept to demonstrate 5 Cisco-specified use cases
  - Other criteria: Customer references and total cost of ownership

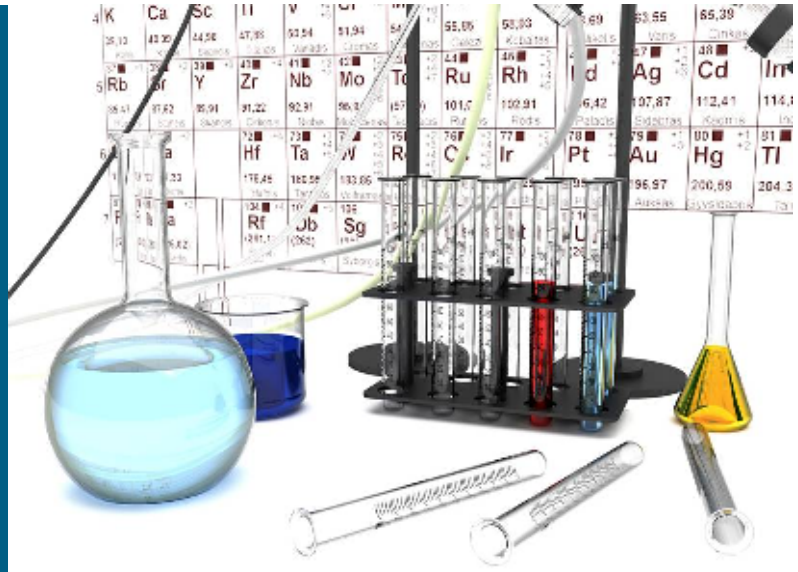
Vendor	Use Case (60%)	Cost (30%)	Customer References (10%)	TOTAL[1] (100%)
Vendor X	**3.75 / 6**	**1.5 / 3**	**0.79 / 1**	**6.04**
ORACLE	**4.50 / 6**	**3 / 3**	**0.5[2] /1**	**8.00**

Notes

[1] **Total possible score for each vendor is 10.**

[2] **Oracle customers were not able to provide the quantitative scoring. However, the customer reference checks have satisfactory results and therefore warrant Oracle with 0.5 of 1 score.**

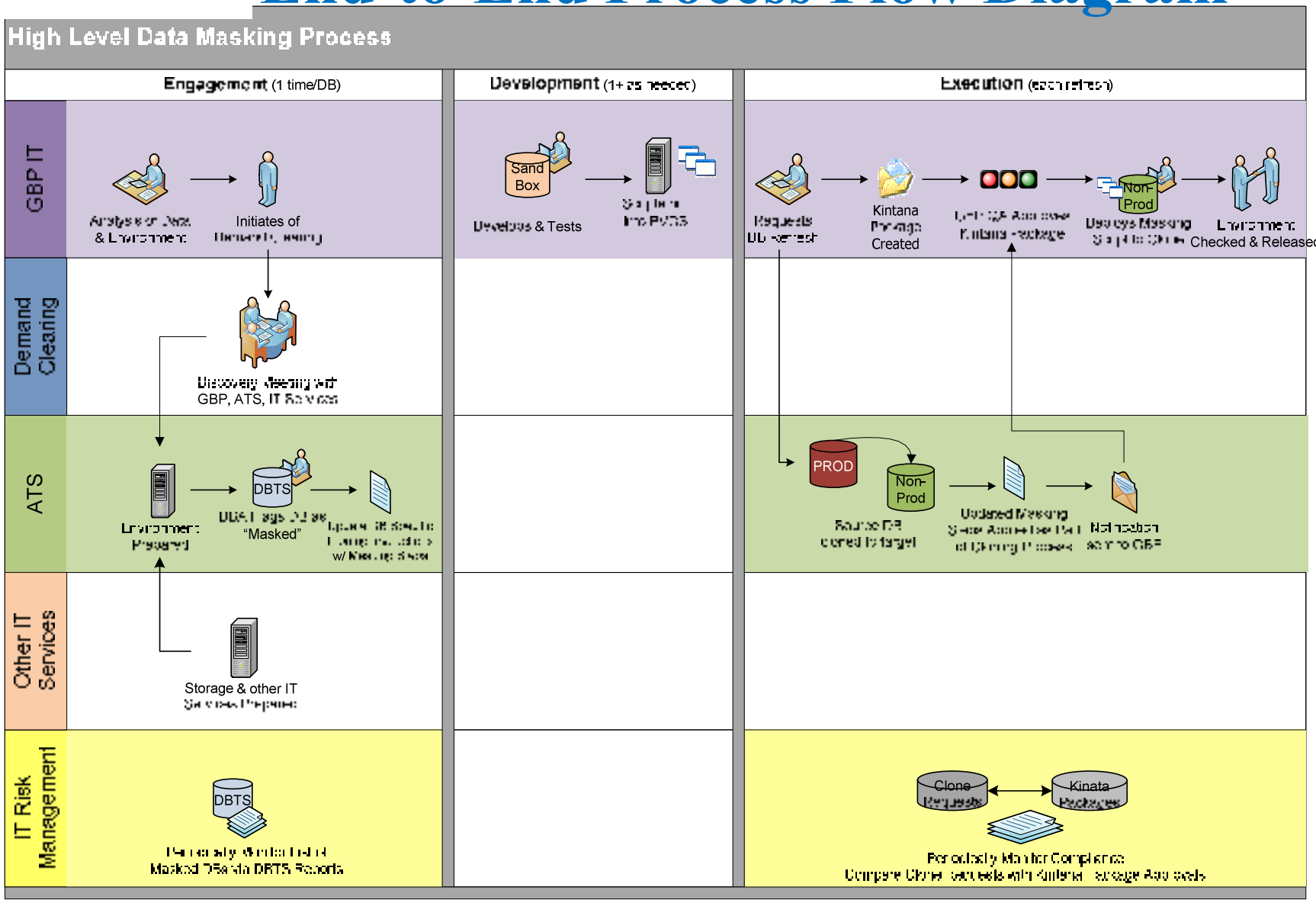
Data Masking Implementation At Cisco



Roles & Responsibilities

Owner	Role	Masking Responsibilities
GBP Business	Data Steward	– Identify & prioritize sensitive data
GBP IT	Data Analyst	– Locate data in databases – Analyze environments – Initiate Demand Clearing – Create & push PVCS & Kintana Packages
	Developer	– Create & test masking scripts
	QA Reviewer	– Review & approve Kintana package
ATS	DBA	– Participate in Demand Clearing – Flag database in DBTS – Update cloning instructions for database – Set up environment – Generate monitoring reports periodically
	WIPRO	– Perform additional cloning instructions
ITRM	Auditor	– Request & inspect compliance w/ process – Identify root cause of issues found – Work with others to resolve systemic issues – Refine process as it matures

End-to-End Process Flow Diagram



Data Masking Solution Features

- Initially an Oracle database solution only.
- Data Masking software tool is a module of Oracle Enterprise Manager, currently used to monitor all Oracle databases at Cisco.
- Masked data cannot be reversed to its original value.
- Data Masking tool provides
  - predetermined masking rules for common sensitive data eg ss#, credit cards
  - Ability to create customized masking rules
- Provides User Access Control to Data Masking tool
- Provides automated Change Control process to deploy production masking rules
- Creates a script which masks data during the existing database refresh processes

Where are we now?

- Oracle data masking solution implemented
- Phase 1 with HR IT and GPSS IT successful
- Playbook created for GBPs to implement masking in Phase 2
- Continue to work with Oracle to resolve software issues - Open

Masked Data Elements in EBS application

Phase 1

GBP	Field to be Masked
Human Resources (HRMS)	Registered Disable Flag Ethnic Origin Termination Reason Code Home Phone Base Salary Bonus/CAP Birth Date Country of Birth National Identifier Address ePM Rating
GPSS	Salary Sales Rep's Annual Target (Local Currency) Sales Rep's Annual Target (US Dollars) Sales Rep's Annual Target by Territory (Local Currency) Sales Rep's Annual Target by Territory (US Dollars) Sales Rep's Quarterly Target (Local Currency) Sales Rep's Quarterly Target (US Dollars)

Phase 2

GBP	Field to be Masked
Finance (P2R, H2R)	Emp. Bank Account # Emp. Corporate Card # Emp. Divorce Status
Human Resources (HRMS)	Emp. Nationality Emp. Citizenship Status Emp. Country Emp. Region Emp. Town of Birth Emp. Veteran Status Emp. Separation Package Type
GGSG	Pay Grade Clearance Level Clearance Bonus
Marketing (MODS, CM, SMCC, SMS, GIST)	Customer & Prospect email
GPSS	Commission Incentive Bonus Plan Code Bonus Status Bonus Description Bonus Type OMF Opportunity $

Phase 2

- Extend the enterprise-wide masking solution to Finance, Marketing, & GGSG
- Mask sensitive data in a risk based, iterative approach
- Provide a framework to enable ongoing enterprise-wide adoption
- ITRM continued monitoring and engagement of GBPs

Life Before and After Data Masking

	Before Masking	After Masking
Process used for masking	Manual	Automated
Data elements protected	Unknown	8 (in Phase 1)
Databases protected	1	8 (in Phase 1)
Divisions using data masking	1	2 (in Phase 1) 5 (in Phase 2)

Business Benefits

- Increase Cisco's assurance that private data is not unnecessarily exposed and exploited
- Reduce exposure risk due to private data leakage
- Reduce the risk of failing an ICS audit or government regulations
- Increased visibility and traceability where private data is stored and masked
- Reduce effort by the project teams during project initiative development and testing, where data masking is required
- Reduce duplicate effort in defining what data needs to be masked
- Increased standardization and uniformity of data masking process Cisco wide
- Financial benefit to Cisco through improved 'value for money' potential and better management of data usage