Software Asset Management - Security & Cloud Generation

George Arezina – Head of Global Software Asset Management
F.Hoffman La Roche AG

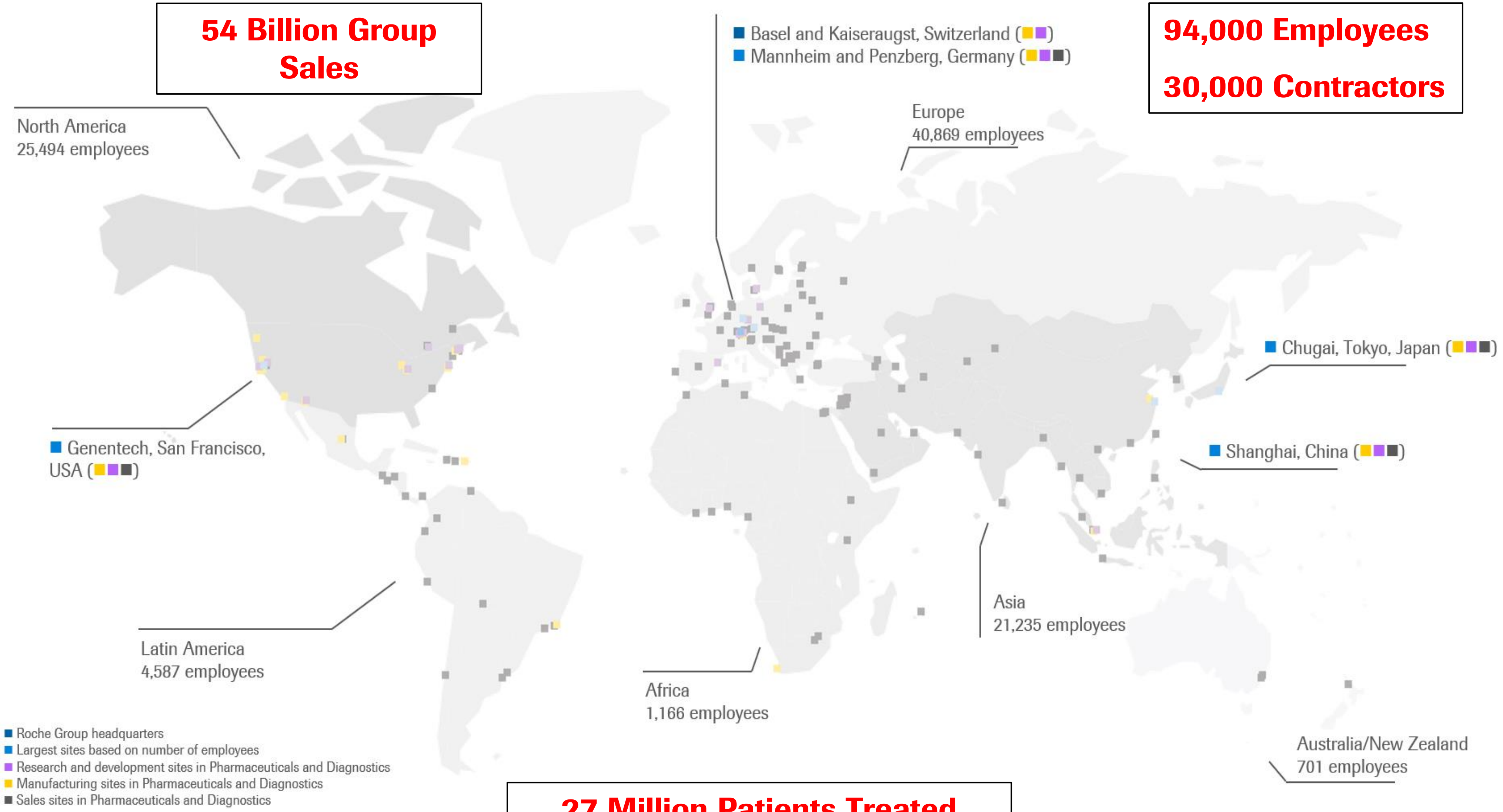
Roche's Global Presence

Leading Biotechnology Pharmaceutical Company in World

54 Billion Group Sales

94,000 Employees

30,000 Contractors



🟦 Basel and Kaiseraugst, Switzerland (🟨🟪)
🟦 Mannheim and Penzberg, Germany (🟨🟪⬛)

Europe
40,869 employees

North America
25,494 employees

🟦 Genentech, San Francisco, USA (🟨🟪⬛)

🟦 Chugai, Tokyo, Japan (🟨🟪⬛)

🟦 Shanghai, China (🟨🟪⬛)

Latin America
4,587 employees

Africa
1,166 employees

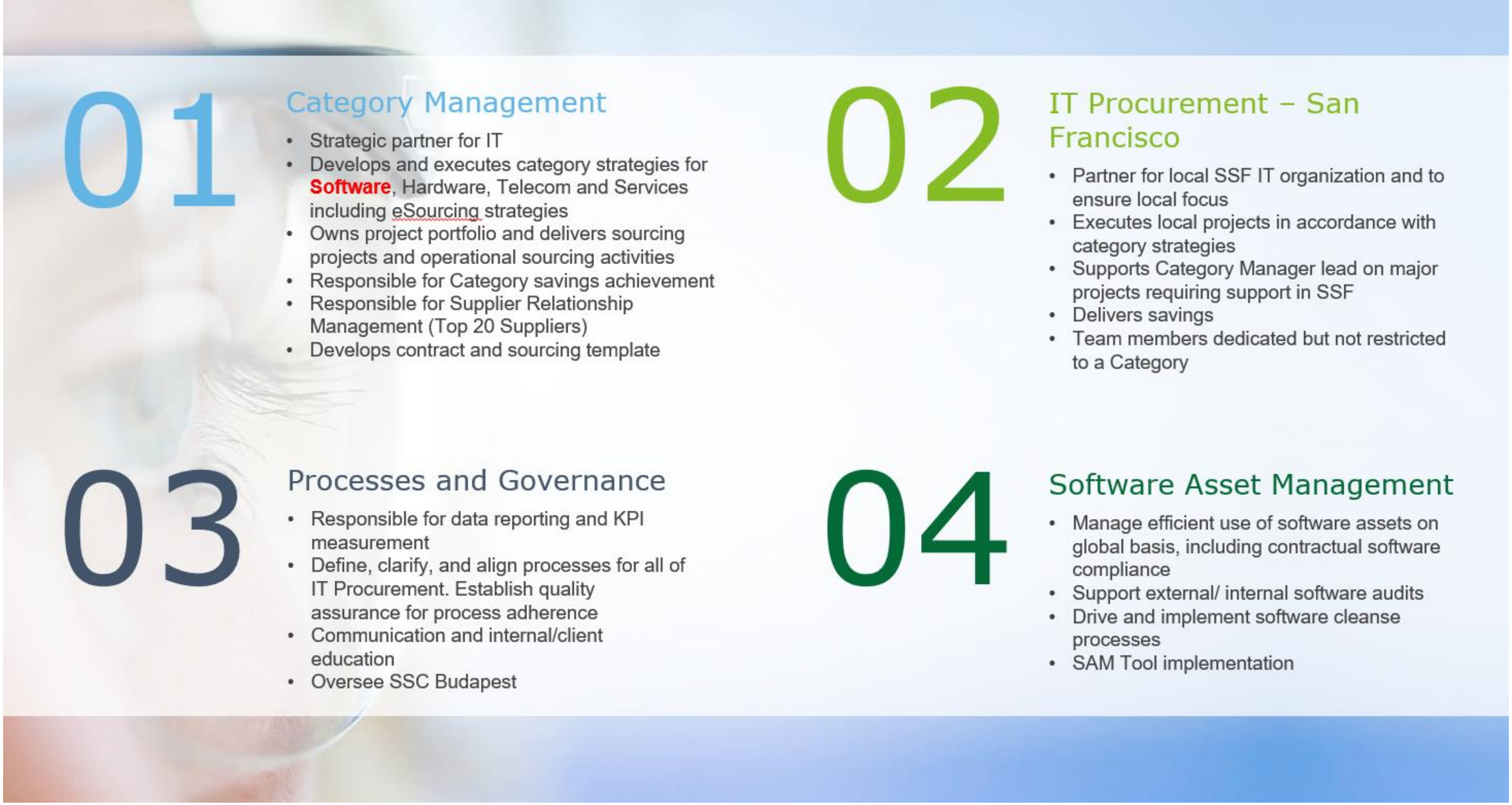
Asia
21,235 employees

Australia/New Zealand
701 employees

- 🟦 Roche Group headquarters
- 🟦 Largest sites based on number of employees
- 🟪 Research and development sites in Pharmaceuticals and Diagnostics
- 🟨 Manufacturing sites in Pharmaceuticals and Diagnostics
- ⬛ Sales sites in Pharmaceuticals and Diagnostics

27 Million Patients Treated

Group IT Procurement



01

Category Management

- Strategic partner for IT
- Develops and executes category strategies for **Software**, Hardware, Telecom and Services including eSourcing strategies
- Owns project portfolio and delivers sourcing projects and operational sourcing activities
- Responsible for Category savings achievement
- Responsible for Supplier Relationship Management (Top 20 Suppliers)
- Develops contract and sourcing template

02

IT Procurement – San Francisco

- Partner for local SSF IT organization and to ensure local focus
- Executes local projects in accordance with category strategies
- Supports Category Manager lead on major projects requiring support in SSF
- Delivers savings
- Team members dedicated but not restricted to a Category

03

Processes and Governance

- Responsible for data reporting and KPI measurement
- Define, clarify, and align processes for all of IT Procurement. Establish quality assurance for process adherence
- Communication and internal/client education
- Oversee SSC Budapest

04

Software Asset Management

- Manage efficient use of software assets on global basis, including contractual software compliance
- Support external/ internal software audits
- Drive and implement software cleanse processes
- SAM Tool implementation

SAM & IT Security

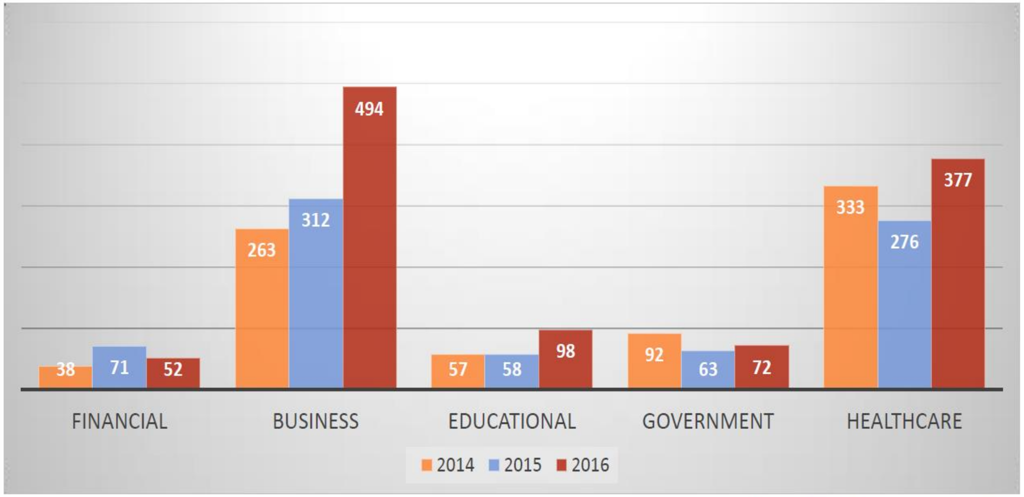
Leveraging Both Organizations at Roche

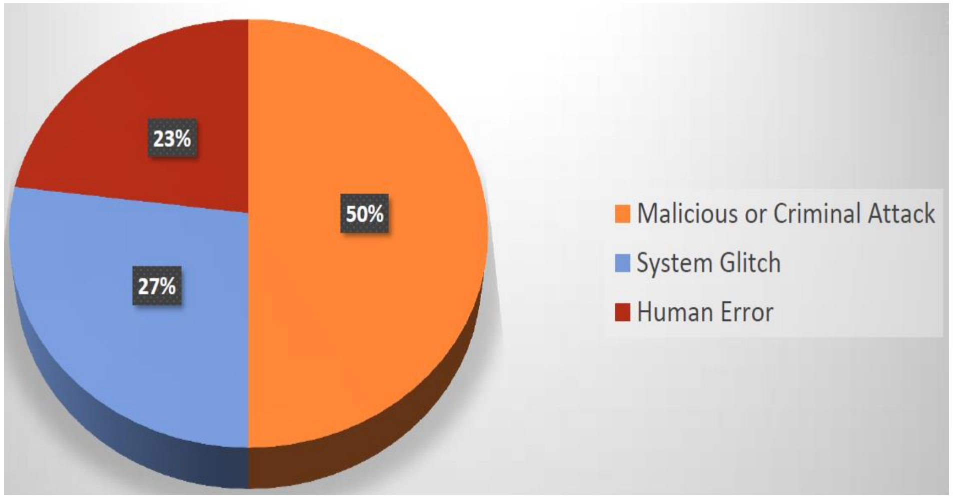
Global Data Breaches 2016

- 4,149 Confirmed Breaches
- 4.2 Billion Records Exposed
- $158 Average Cost Per Record Compromised

Ponemon Institute Research Report

US Breach Statistics 2014 to 2016





Identity Theft Resource Center (ITRC)

Trends Fueling Cybercrime

The Ever-changing Threat Environment…

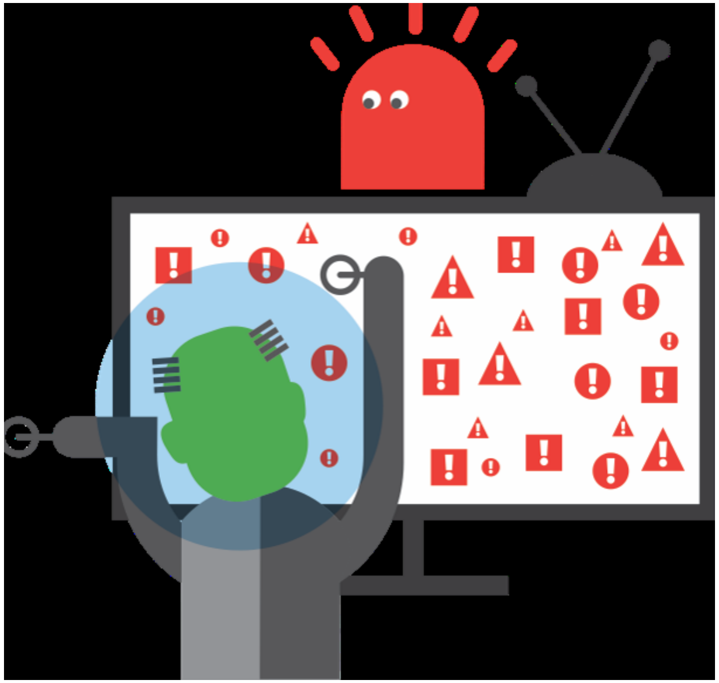
- Heterogeneous corporate environments
- Scattered locations of devices (mobility)
- Bring-Your-Own-Device (BYOD)
- Virtualization
- The Internet of Things (IoT)

IT Security & SAM

- Security wants to ensure assets are secured and being used properly
- SAM wants to ensure infrastructure and processes necessary for the effective management, control and protection of software assets within an organization
- How do these Groups Work Together?

SAM Has Data IT Security Can Use

- Software Installation
- Version & Edition
- Contract Information
- Owner
- Location
- License Entitlements
- Connections between Assets and CI’s
- Financial value

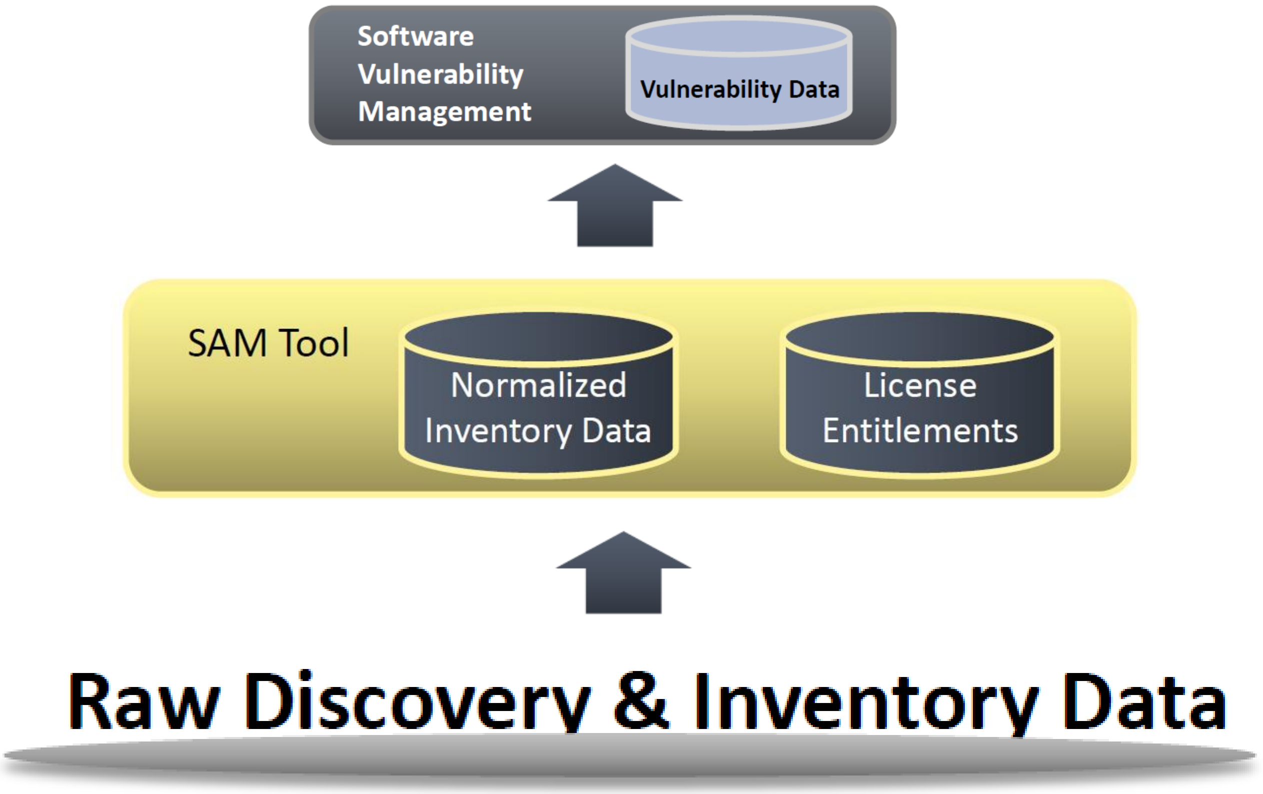


SAM Helps Reduce IT Security Risk

Visibility; Reduction in Unlicensed and Unauthorized Apps; Rationalization and Consolidation of the Software Portfolio

Inventory Data is the Foundation

Drives SAM and Software Vulnerability Management Processes


Software Vulnerability Management
Vulnerability Data
SAM Tool
Normalized Inventory Data
License Entitlements
Raw Discovery & Inventory Data

IT Security Has Data SAM Can Use

- Software Black List
- Software White List
- Last Time User Logged On

How do these teams work together

- Building policies that include both IT security and SAM interests
  - Craft policy language that ensures interests of IT Security & SAM are addressed (eg. Acceptable use, lost/missing asset reporting, SW installation

- Sharing data
  - Grant IT Security read access into SAM tool, provide reporting that augments existing data

- Quarterly or Bi-Annually IT Security/SAM Review

- Systems Integrations
  - IT Security may have pieces of information that SAM may want to use (eg. Last logged on user)

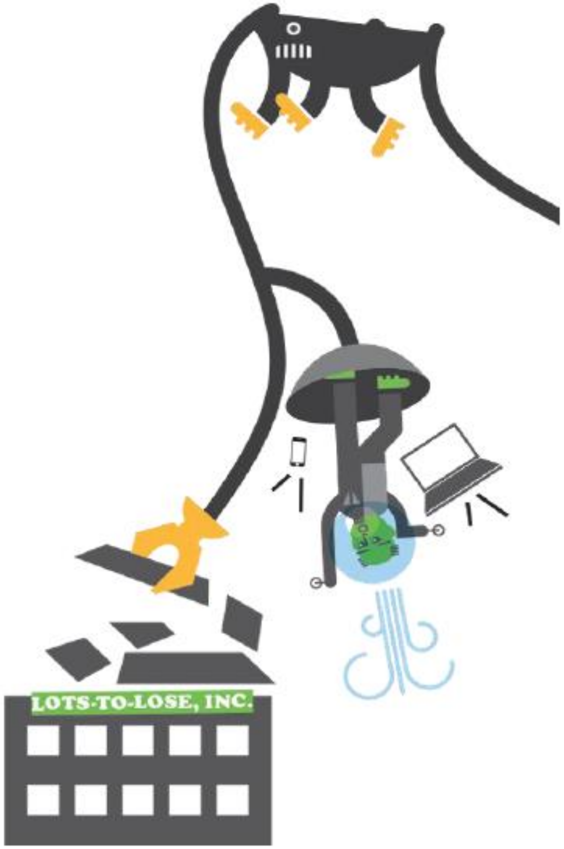
Why Work Together

- Each group has the capability to get the other teams information. Usually in a vary laborious fashion
- By working together information can be provided more quickly and completely
- Automation and/or Access to the data gets us to where we want to be faster.
- Increased reliability of asset and security information

There’s lots at Stake!

Lost/compromised assets = Lots to lose!

- Financial
- Organizational IP
- Data Theft
- Identity Theft
- Etc

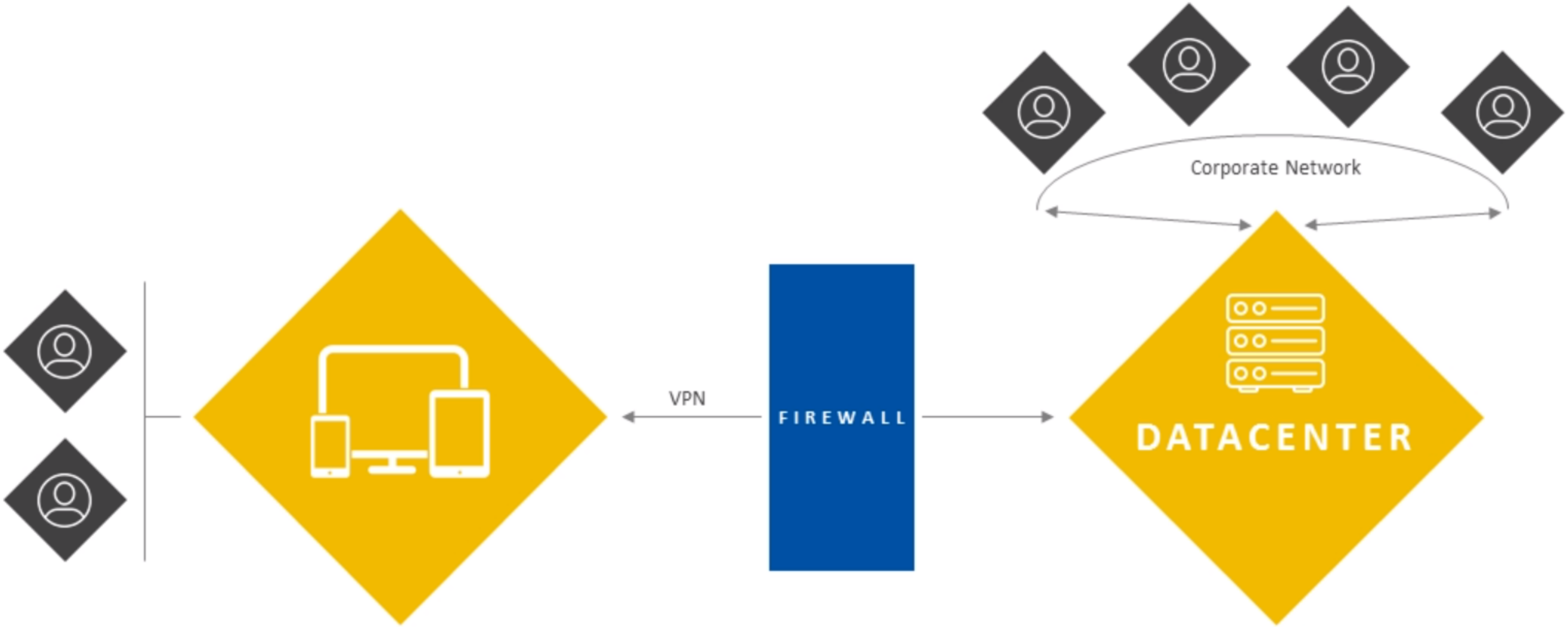


Protect Roche's IT Assets

- Data Discovery – Find IT
- Data Classification – Organize IT
- Policies – Operationalize IT
- Enforcement – Defend IT

Classic versus Cloud SAM

Traditional IT Environment

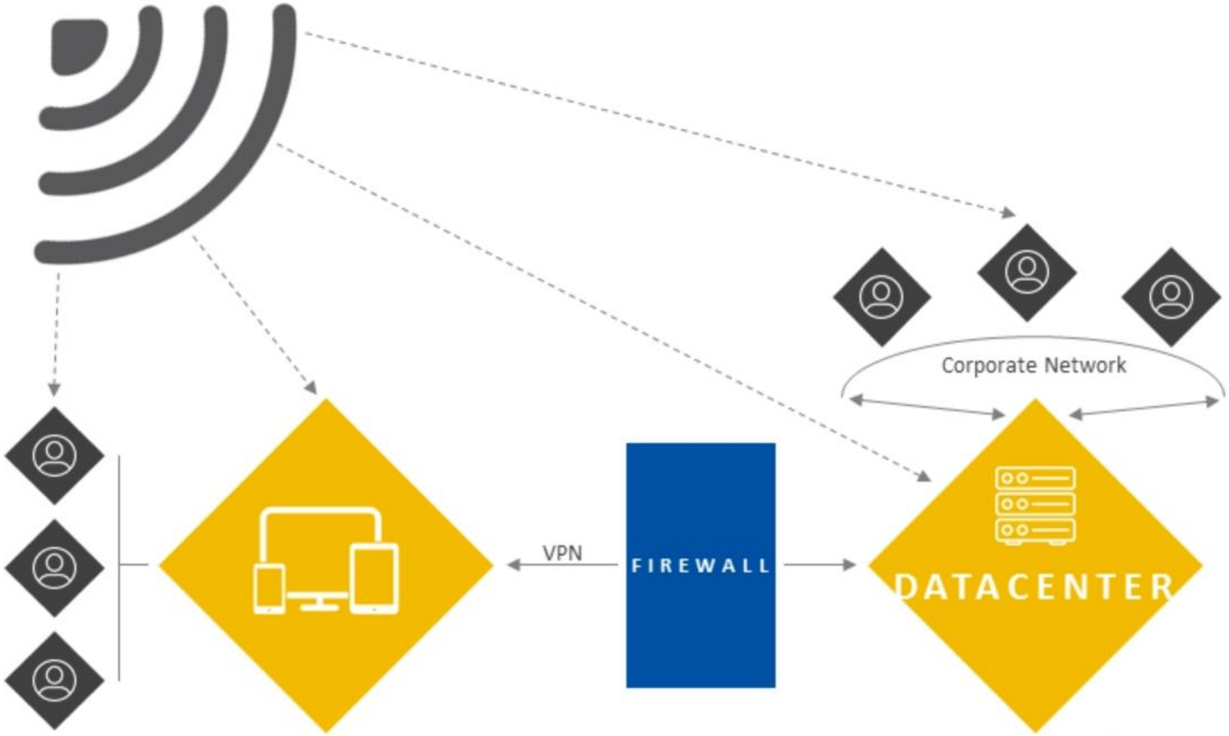


Classic SAM Building blocks for success

What you should be doing already!

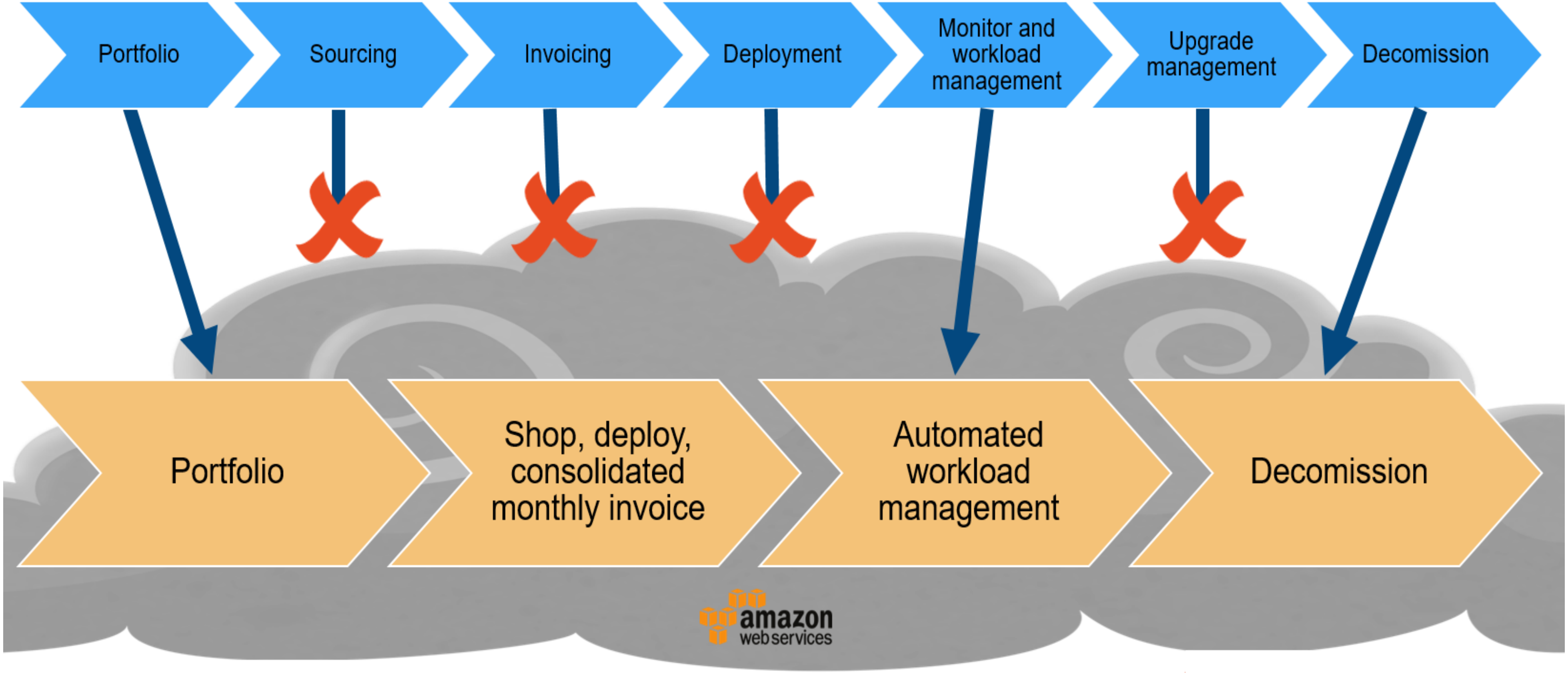
Know what's installed	• Client, Servers, mobile devices • Scan, normalize, report
Know what you purchased	• Spend centralization • Direct relationship with mega vendors • Use global re-sellers • Follow the money and risk
Manage and Optimize	• Draw conclusions • Pooling, metering, reharvesting • Periodic compliance checks • Manage audits
Portfolio Management	• Assign SW to SW classes, manage SW classes • Limit SW versions • Limit number of apps doing the same thing

Modern IT Environment



IaaS, PaaS – The way to consume today

The digital revolution arriving in SAM



Manage your new Cloud Challenges

Important things to consider

SAM must manage SW asset and service

Risk of overspend, manage TCO, be aware of hidden cloud service cost

Accessible from anywhere

BYOD allowed? Additional costs? address security risks

Transfer of licenses to the cloud must be checked prior

May be prohibited, can carry restrictions, pre-approval required?, possibly additional costs

Ability to measure metrics

Does provider allow and enable the measurement of license consumption?

What is the total cost for the service?

Check for hidden costs, migration cost, additional services, renewals, true-ups, Shelf-Ware

SAM in the Cloud

Where does my data reside?

Potential loss of control, data privacy, information security, business continuity exposure, check industry specific regulations

SAM becomes more real time

Services are provisioned and changed in a matter of minutes, governance needed, immediate cost impact

Compliance risks still exist

geographical limitations, sharing user accounts, providing access to non-employees, indirect usage

IaaS or PaaS

Check if virtualization is permitted, cost might increase, sudden price changes (e.g. Oracle) keep track own versus CSP provided SW

Check risk of IP infringement is covered

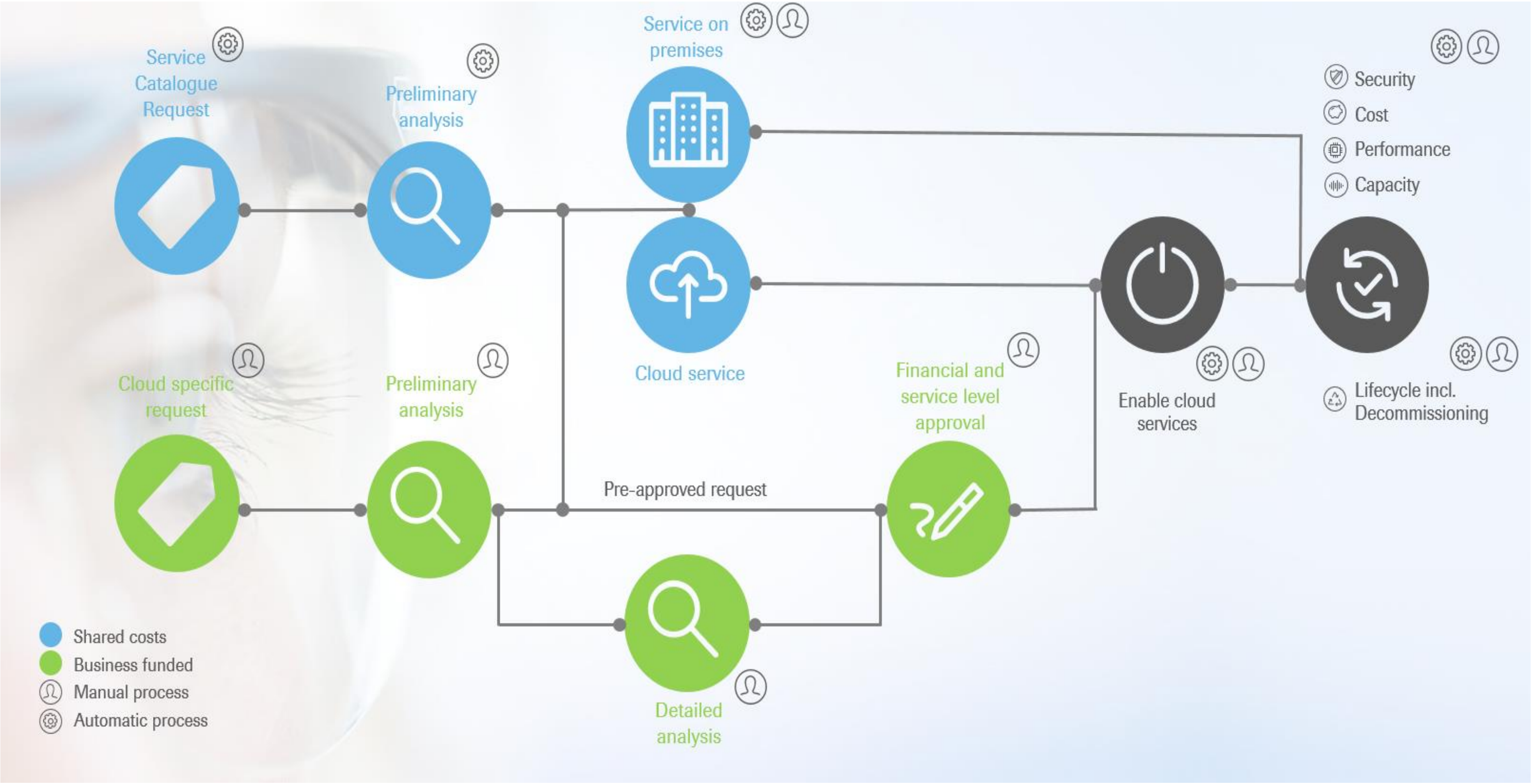
Check CSP contract terms, does the CSP have the legal right to provide the service?

Adapting Classic SAM for the Cloud

Develop Cloud Strategy, add Cloud-SAM Scope

- Develop, agree corporate cloud strategy before moving to the cloud
- Involve SAM in the cloud strategy & management process
- Rework “Classic SAM” to cover/manage new Cloud Risks
- Develop Cloud-SAM Governance (Policies) covering all stages of the cloud life cycle (from contracting, architecture, service execution including security aspects)
- Shift your SAM focus from compliance management to manage your XaaS commitments and costs, manage SW assets and cloud services
- Establish detailed cloud reporting to support stakeholders responsible for Cloud - Services, -budgets and -security aspects
- Impact of cloud changes are instant, therefore establish change processes and increase scanning and reporting frequency

Cloud Governance Model at Roche



Service Catalogue Request

Preliminary analysis

Service on premises

Cloud service

Cloud specific request

Preliminary analysis

Pre-approved request

Detailed analysis

Financial and service level approval

Enable cloud services

Security

Cost

Performance

Capacity

Lifecycle incl. Decommissioning

🔵 Shared costs

🟢 Business funded

👤 Manual process

⚙ Automatic process

Adapting Classic SAM for the Cloud

New Cloud-SAM Scope

- Develop, agree corporate cloud strategy before moving to the cloud
- Involve SAM in the cloud strategy & management process
- Rework “Classic SAM” to cover/manage new Cloud Risks
- Develop Cloud-SAM Governance (Policies) covering all stages of the cloud life cycle (from contracting, architecture, service execution including security aspects)
- Shift your SAM focus from compliance management to manage your XaaS commitments and costs, manage SW assets and cloud services
- Establish detailed cloud reporting to support stakeholders responsible for Cloud -Services, -budgets and -security aspects
- Impact of cloud changes are instant, therefore establish change processes and increase scanning and reporting frequency

Thank You

Roche

Doing now what patients need next