“Integrated Assurance and Risk-based Audit Planning”

Rick Machold, CAE, TSYS
Lillian Scott, VP, Operational Assurance, TSYS
PARTICIPATE IN Q&A

• Download the IIA Conferences App to participate in Q&A during select sessions

• Select the session through the schedule icon

• Submit your questions for the session or to specific presenters by selecting the ASK icon

• Ask a member of the Conference Staff if you need assistance

• You can also go to https://ic.cnf.io/ from your mobile device web browser
LEARNING OBJECTIVES

In this session, participants will:

- Follow the TSYS Integrated Assurance (IA) journey, from initial mandate (late 2011) to present.
- Understand the component parts of the TSYS IA process and how they were developed over time.
- Understand other Assurance Providers, their interactions with Audit Services Group (ASG), and criteria for reliance.
- Discover how IA influences the risk-based audit planning process.
We Keep Money Moving.

**TSYS** is an industry leader in digital payments & software-driven, commerce-enabling solutions.

TSYS helps businesses & individuals make payments, receive payments, and hold & manage their money.
THE “PAIN” STATEMENT

“We are one of the most ‘chronically over-audited’ organizations anywhere.” - TSYS Senior Executive

“Pain” Factors

- **TSYS position within the banking system** as an intermediary service provider to the world’s largest financial institutions.
- Pressure and scrutiny from the **scale** of TSYS operations.
- **Diversity of TSYS business model** – multiple segments with unique assurance/regulatory requirements and implications.
- Pace of change creates a **continuously “moving target”** for assurance coverage.

50+ Client Audits Annually; 16 -20 weeks of on-site regulator visits

Consumer Protection, Data Security & Privacy Regulation

Payment Scheme Compliance

300+ Internal & External Audits
- SOC 1/SOC 2
- SOX
- Internal Audits

“PAIN” STATEMENT

We are one of the most ‘chronically over-audited’ organizations anywhere.” - TSYS Senior Executive

“Pain” Factors

- TSYS position within the banking system as an intermediary service provider to the world’s largest financial institutions.
- Pressure and scrutiny from the scale of TSYS operations.
- Diversity of TSYS business model – multiple segments with unique assurance/regulatory requirements and implications.
- Pace of change creates a continuously “moving target” for assurance coverage.

50+ Client Audits Annually; 16 -20 weeks of on-site regulator visits

Consumer Protection, Data Security & Privacy Regulation

Payment Scheme Compliance

300+ Internal & External Audits
- SOC 1/SOC 2
- SOX
- Internal Audits
CIO asks for a single view and forum to review all findings from all sources across her organization.

Spring 2015
1st draft Integrated Assurance Map created with input from Risk and Compliance leader. Later presented to Audit Committee.

June 2016
CIO asks for a single view and forum to review all findings from all sources across her organization.

2017
Measurable Success!
BISOs removed 13 audits from their assurance schedule; ASG deferred ~3,500 hours from the 2017 Audit plan.

Early 2019
Deployed Enterprise Assurance Request System

October 2011
Initial mandate: “Help us to find the right balance in all these audits!”

Fall 2014
CAE presents on “Combined Assurance” to International Client Assurance Forum

2011 – 2013
Living in the “Pain Cave!”

2016-2017
Develop common processes

Early 2017
“Go Live” of consolidated finding/risk reporting solution

Early 2019
Deployed Enterprise Assurance Request System

2019
We had to go to the highest level detail (audit universe) to truly understand the whole (risk coverage).

We had to struggle through the pain of establishing shared meaning, mutual purpose and common language with the other Assurance Providers.

We have to focus not only on what we should be auditing, but equally on what we should NOT be auditing.

We have to continuously renew and refine our focus on Integrated Assurance applied at the engagement planning level (i.e., not just the audit plan level).
We had to go to the highest level detail (audit universe) to truly understand the whole (risk coverage).

We had to struggle through the pain of establishing shared meaning, mutual purpose and common language with the other Assurance Providers.

We have to focus not only on what we should be auditing, but equally on what we should NOT be auditing.

We have to continuously renew and refine our focus on Integrated Assurance applied at the engagement planning level (i.e., not just the audit plan level).
**ORIGINAL “CONCEPTUAL” ASSURANCE MAP**

<table>
<thead>
<tr>
<th>Provider Assessment</th>
<th>Overall provision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mgt Assurance</td>
<td>Assurance Gap</td>
</tr>
<tr>
<td>Medium Assurance</td>
<td>Opportunity to Remove / Refocus Effort</td>
</tr>
<tr>
<td>High Assurance</td>
<td>Maintain Current Plan</td>
</tr>
</tbody>
</table>

**Performance Provider**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Management 1st Line**

<table>
<thead>
<tr>
<th>Management 1st Line</th>
<th>Assurance Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Functional Oversight 2nd Line**

<table>
<thead>
<tr>
<th>Functional Oversight 2nd Line</th>
<th>Assurance Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Independent 3rd Line**

<table>
<thead>
<tr>
<th>Independent 3rd Line</th>
<th>Assurance Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Regulatory Oversight 4th Line**

<table>
<thead>
<tr>
<th>Regulatory Oversight 4th Line</th>
<th>Assurance Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Corrective Action**

<table>
<thead>
<tr>
<th>Corrective Action</th>
<th>Assurance Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Source:** PriceWaterhouseCoopers
# ASG’s 2019 Assurance Map

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6300XX</td>
<td>Medium</td>
<td>Intellectual Property</td>
<td>CM</td>
<td>Q</td>
<td>P</td>
<td>A</td>
<td>Q</td>
<td>P</td>
<td>A</td>
<td>A</td>
<td>Yes</td>
<td>Yes</td>
<td>High</td>
<td>Low</td>
<td>G</td>
<td>Y</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8213XX</td>
<td>Medium</td>
<td>Unauthorized, Authorize, Capture &amp; Process</td>
<td>Q</td>
<td>Q</td>
<td>P</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>Yes</td>
<td>Yes</td>
<td>Medium</td>
<td>Yes</td>
<td>High</td>
<td>Low</td>
<td>Y</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100NSXX</td>
<td>Medium</td>
<td>Contract Development, Negotiation &amp; Maintenance</td>
<td>CM</td>
<td>P</td>
<td>A</td>
<td>Q</td>
<td>Q</td>
<td>Q</td>
<td>Y</td>
<td>Yes</td>
<td>Medium</td>
<td>Yes</td>
<td>Medium</td>
<td>Medium</td>
<td>G</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6100XX</td>
<td>Medium</td>
<td>Contract Development, Negotiation &amp; Maintenance</td>
<td>P</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>Yes</td>
<td>Yes</td>
<td>Medium</td>
<td>Yes</td>
<td>Medium</td>
<td>Medium</td>
<td>G</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7110NSXX</td>
<td>High</td>
<td>McAfee Logical Security Administration</td>
<td>P</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>Yes</td>
<td>Yes</td>
<td>Medium</td>
<td>Yes</td>
<td>High</td>
<td>Low</td>
<td>G</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7212XX</td>
<td>Medium</td>
<td>McAfee Distributed Technologies Operating</td>
<td>P</td>
<td>CM</td>
<td>P</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>Yes</td>
<td>Yes</td>
<td>Medium</td>
<td>Yes</td>
<td>Medium</td>
<td>Medium</td>
<td>G</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7420XX</td>
<td>Medium</td>
<td>Network Resources &amp; Management</td>
<td>P</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>Yes</td>
<td>Yes</td>
<td>Medium</td>
<td>Yes</td>
<td>Medium</td>
<td>Medium</td>
<td>G</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G30XX</td>
<td>Medium</td>
<td>Active Directory</td>
<td>P</td>
<td>Q</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>Yes</td>
<td>Yes</td>
<td>Medium</td>
<td>Yes</td>
<td>Medium</td>
<td>Medium</td>
<td>G</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legend:**
- A = Annually
- Q = Quarterly
- P = Periodically (Risk-based)
- CM = Continuous Monitoring
We had to go to the highest level detail (audit universe) to truly understand the whole (risk coverage).

We had to struggle through the pain of establishing shared meaning, mutual purpose and common language with the other Assurance Providers.

We have to focus not only on what we should be auditing, but equally on what we should NOT be auditing.

We have to continuously renew and refine our focus on Integrated Assurance applied at the engagement planning level (i.e., not just the audit plan level).
Assurance - Objective examinations of evidence for the purpose of providing an independent assessment on governance, risk management and control processes for the organization.

Integrated Assurance - A model of assurance that aims to optimize the assurance coverage obtained from management, internal assurance providers and external assurance providers on the risk areas affecting the organization.

Source: Combined Assurance – Case Studies on a Holistic Approach to Organizational Governance, Institute of Internal Auditors Research Foundation
**Establishing a Shared Meaning: Key Definitions**

**Assurance Provider** – A person or group that performs independent testing/verification activities to help ensure that the controls, designed by management, are functioning adequately and comply with regulatory/legal requirements, guidelines and/or control frameworks.

**Risk Leaders** – A group within a business unit responsible for “self-identifying” and managing operational risks and findings.

**Finding** – A gap resulting from an independent assurance engagement.

**Self-reported / Self-identified Issue Identification** – This practice empowers management to raise issues and track remediation to advance corrective action. Auditors gain comfort when management promptly address root causes related to the self-reported issues.
**INTEGRATED ASSURANCE TEAM**

**Authority:** The TSYS IA Team conducts its activities under the auspices of the CAE, whose direct functional reporting line is to the Audit Committee and whose administrative reporting line is to the Chairman and CEO.

<table>
<thead>
<tr>
<th>Host Assurance Providers</th>
<th>Assurance Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CIO Risk Management “Risk Leaders” <em>(Self-report risks/issues)</em></td>
<td>• Audit Services (SOC1, SOC2, SOX, Operational Assurance)</td>
</tr>
<tr>
<td>• North America Client Assurance</td>
<td>• Enterprise Business Compliance</td>
</tr>
<tr>
<td>• Operational Risk and Client Assurance</td>
<td>• Segment-level Compliance</td>
</tr>
<tr>
<td>• Output Services (e.g., PCI DSS, MasterCard)</td>
<td>• External Assessors &amp; Co-Sourcing Partners</td>
</tr>
<tr>
<td>• Encryption Services</td>
<td>(e.g., PCI, BSA/AML)</td>
</tr>
<tr>
<td>• Info Sec (PCI)</td>
<td>• Business Continuity / Disaster Recovery</td>
</tr>
<tr>
<td>• Regulatory Affairs</td>
<td>• Business Information Security Officers</td>
</tr>
<tr>
<td></td>
<td>(Critical Supplier Reviews)</td>
</tr>
</tbody>
</table>
Under the IIA’s guidance, an **approach for relying on the work** undertaken by other assurance providers must be based upon **five criteria**.
KEY DECISIONS MADE BY ASSURANCE PROVIDERS

✓ Determine if findings and ‘self-identified’ risks will be tracked together in the system of record.

✓ Agree on a ‘Risk Acceptance’ form and process.

✓ Adopt the spirit of a single risk rating scale of: VH, H, M, L, and VL (understanding the need to apply professional judgment).
<table>
<thead>
<tr>
<th>Rating</th>
<th>Legal Compliance</th>
<th>Financial Impact</th>
<th>Operational Impact</th>
<th>Reputation Impact</th>
<th>Control Effectiveness</th>
</tr>
</thead>
</table>
| Very Low   | • Not reportable to regulator.  
  • No regulatory sanctions/fines                                                   | Less than $1 million      | • Loss of less than 1% of operational income  
  • No operational disruptions                                                    | • Little to no impact on reputation  
  • Little to no media exposure  
  • No clients impacted.                                                             | • Controls properly designed and operating as intended                            |
| Low        | • Reportable incident to regulator, no follow up.  
  • Regulatory  
  • Warning                                                                   | $1 - $2 million            | • Loss of 2% - 5% of operational income  
  • Disruption in operations for up to one day                                   | • Minor impact on reputation  
  • Minor media exposure  
  • Small number of clients, users and/or systems involved.                        | • Controls properly designed and operating; no significant deficiencies          |
| Medium     | • Case reported but dismissed                                                      | $2 - $10 million           | • Loss of 3%8% of operational income  
  • Disruption in operations for one to two days  
  • Direct impact at a department or division.                                     | • Significant impact on reputation  
  • Visible local or national media exposure  
  • Moderate number of clients, users and/or systems affected.                   | • Controls in place; some deficiencies                                          |
| High       | • Case/incident reported to regulator requiring major project for corrective action.  
  • Moderate sanctions / fines and/or contractual penalties expected.             | $10 - $25 million          | • Loss of 8% - 11% of operational income  
  • Disruption in operations for two to three days  
  • A repeat finding.                                                            | • Significant impact on reputation  
  • Significant international media and/or social media exposure  
  • Significant number of clients, users, or systems affected.                   | • Limited controls, high level of risk remains; significant deficiencies         |
| Very High  | • Case/incident reported and sanctions/fines threaten Operations  
  • Company at risk of losing certifications; potential regulatory downgrade.   | Greater than $25 million   | • Loss of more than 11% of operational income  
  • Disruption in operations for more than three days  
  • Direct material impact on multiple LOBs, or the corporation as whole at the regulatory, association, or client level. | • Very significant impact on reputation  
  • Very significant international media and/or social media exposure  
  • Most/all clients affected or a top 10 client impacted and complaints expected. | • Controls nonexistent or have major deficiencies and do not operate as intended |
INTEGRATED ASSURANCE COLLABORATION MEETINGS

The Integrated Assurance Team (now) convenes quarterly, and is chaired by VP of Operational Assurance (Internal Audit)

Representative topics include:

- Enterprise Strategic Initiatives (guest speakers)
- Current and upcoming reviews that may impact scope or timing of other groups
- Noteworthy updates from each group
- Thematic findings and emerging risks
- **Tool enhancements** & change management (e.g. Keylight GRC tool and External Assurance Request System)
We had to go to the highest level detail (audit universe) to truly understand the whole (risk coverage).

We had to struggle through the pain of establishing shared meaning, mutual purpose and common language with the other Assurance Providers.

We have to focus not only on what *we should* be auditing, but equally on *what we should NOT* be auditing.

We have to continuously renew and refine our focus on Integrated Assurance applied at the engagement planning level (i.e., not just the audit plan level).
STRATEGIC DIRECTION: REAL-TIME ASSURANCE

We are here…

ERAS OF AUDIT
Changing Characteristics of Audit Work

Cyclical Auditing
Risk-Based Auditing
Enterprise Risk-Based Auditing
Real-Time Assurance

Set number and type of audits performed each year to execute a cyclical plan with a fixed refresh process.

Annual audit plan that prioritizes elements of audit universe based on an annual risk assessment.

Annual audit plan (with quarterly updates) that prioritizes risk universe with input from all three lines of defense.

Just-in-time allocation of audit and other assurance resources based on up-to-date analysis of diverse risk information.

Tolerance for Volatility

Source: CEB analysis.
AUDIT PLANNING PROCESS

- **Update and Refine Audit Universe**
  Adjust Risk Assessment Approach

- **Complete Risk Assessment and Preliminary Audit Plan**

- **Analyze Integrated Assurance Coverage and Resource Capacity**

- **Validate and Publish Risk-based Audit Plan**
  (after Audit Committee approval in late January)

- **Conduct Engagement-Level IA Analysis**
  Real-time Assurance: Sensing & Responding to changes in internal and external environment
Risk Assessment with Assurance Providers

Year-end Workshop Topics

1. Repeat findings from independent reviews
2. Implementations that improved the control environment
3. Risk Themes
4. Emerging Risks
5. Ideas to improve communication and collaboration across Assurance Providers

Follow-up Meeting: Share planned audits for upcoming year

~ 30 participants in the room and on the phone.
What factors could cause changes to the risk-based audit plan?
We had to go to the highest level detail (audit universe) to truly understand the whole (risk coverage).

We had to struggle through the pain of establishing shared meaning, mutual purpose and common language with the other Assurance Providers.

We have to focus not only on what we should be auditing, but equally on what we should NOT be auditing.

We have to continuously renew and refine our focus on Integrated Assurance applied at the engagement planning level (i.e., not just the audit plan level).
### Project Overview

**Audit Objective:** The objective of this review is to evaluate the effectiveness of the overall risk assessment process, including roles and responsibilities, and awareness of risks presented by third party partners/distributors within the distributor due diligence and oversight program.

**Audit Type:** Operational Assurance Review

#### Audit Scope

**Integrated Assurance:**
- Understand/review results of coverage from new assurance providers, including actions taken to address findings. See table below.

**Distributor Population:**
- Assess the completeness and accuracy of the distributor population, including required state information (e.g., gross transaction volume, type of services, etc.)

#### Risk Assessment and Distributor Oversight:

- Evaluate the distributor risk assessment process, including determination of applicable risk factors, strategic designation, frequency, and overall risk/tier ratings.
- Map out roles and responsibilities within the overall distributor due diligence oversight program and assess awareness of responsibilities.
- Assess ongoing distributor oversight and monitoring in accordance with risk ratings, including:
  - Review of the Mystery Shopper Program, results of assessments, management’s review, follow up, and associated reporting to leadership.
  - Analysis of compliance guidelines/training distributed to store locations.

#### Risk Rationale

- Large distributor population
- Third party risk exposure (e.g., data breach, revenue, business continuity, reputation)
- NY Department of Financial Services 2016 report of examination (Issued in October 2017) raised a finding regarding insufficient audit coverage of agent on-boarding and oversight. Testing performed on agents as part of the annual AML/BSA audit was not considered sufficient.
- [Segment] Legal agreed with focus area for 2018 audit plan; audit was approved for deferral to 2019.
- Agent/partner oversight was mentioned as an audit area for consideration in the December 2018 [Segment] risk workshop.

**Risk Breakdown:**

- [Segment] Distributor population
- Third party risk exposure (e.g., data breach, revenue, business continuity, reputation)
- NY Department of Financial Services 2016 report of examination (Issued in October 2017) raised a finding regarding insufficient audit coverage of agent on-boarding and oversight. Testing performed on agents as part of the annual AML/BSA audit was not considered sufficient.
- [Segment] Legal agreed with focus area for 2018 audit plan; audit was approved for deferral to 2019.
- Agent/partner oversight was mentioned as an audit area for consideration in the December 2018 [Segment] risk workshop.

**Out-of-Scope:**

- Sales leads, identification, and sourcing
- Contract negotiation, management, and compliance
- Office of Foreign Assets Control (OFAC) screening
- Anti-money laundering (AML) compliance monitoring
- Suspicious Activity Reporting (SAR) filing
### Example Project Charter (Page 2 of 2)

#### Project Team

**Executive Owners:**
- Senior EVP and President, Netspend
- General Counsel

**Process Owners:**
- Chief Compliance Officer
- Senior Manager, Distributor Due Diligence and Oversight

**ASG Team:**
- Vice President
- Project Manager
- Lead Auditor
- Auditor
- Auditor

#### Integrated Assurance Coverage

**2016 New York State Department of Financial Services (NYDFS) Exam:** Testing included distributor files, risk assessment process, termination policy/procedures, and comprehensiveness of agent list.

**2017 NYDFS 500 Cybersecurity Readiness Assessment:** Cybersecurity risk and rankings based on risk exposure associated with access to nonpublic personal information is not considered in the distributor due diligence process. ASG is tracking this issue separately.

**Annual BSA/AML Audit:** Scope includes BSA/AML and OFC policies/procedures, risk assessments, governance, currency transaction reporting, suspicious activity investigations and reporting, know your customer, transaction monitoring, record training, and record keeping.

**[Segment] Compliance:**
- Performed a review of Q1 2018 of due diligence policies and procedures, and testing of 40 distributor files to assess adequacy of documentation and approval decisions made to onboard a partner.
- *Other:* The distributor due diligence files is subject to quarterly quality assurance reviews by management of application completeness within service level agreements, due diligence files, proper system record updates, and adherence to procedures. The team is also subject to continual State Money Transmitter License Reviews, Issuing Bank Audits, and periodic Federal Banking Agency Exams. Typical scope includes onsite reviews of partner locations.

#### Communication Plan

**Status Update Frequency:** As requested

**Expected First Status Update:** TBD

#### Deliverables

A formal written communication will be issued describing the objectives and scope of the engagement, key risks/issues noted, and agreed upon remediation actions.

#### Timeline

| Month   | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| Planning |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Fieldwork |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Fieldwork |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
| Reporting |   |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
We had to go to the highest level detail (audit universe) to truly understand the whole (risk coverage).

We had to struggle through the pain of establishing shared meaning, mutual purpose and common language with the other Assurance Providers.

We have to focus not only on what we should be auditing, but equally on what we should NOT be auditing.

We have to continuously renew and refine our focus on Integrated Assurance applied at the engagement planning level (i.e., not just the audit plan level).
THANK YOU
TELL US WHAT YOU THINK!

Evaluate this session right in the IIA Conference App!

Not using the conference app?

Visit: ic.cnf.io to complete your session evaluations.
INTEGRATED ASSURANCE TEAM

Purpose

This charter formally inaugurates the Integrated Assurance Team (IAT), formed to establish and support the delivery of integrated assurance across the enterprise through information sharing, coordination, and a focus on the continuous improvement of assurance activities within TSYS.

Integrated Assurance Expected Benefits

- Promotes efficiency
- Enables greater cross-functional focus on TSYS risk areas
- Avoids duplication of effort
- Reduces “audit fatigue”
- Enables consolidated reporting of assurance activities
- Provides greater understanding of the extent of assurance
- Enables extended coverage of audit universe

Authority

The Integrated Assurance Team will conduct its activities under the auspices of the TSYS Chief Audit Executive, whose direct functional reporting line is to the TSYS Audit Committee and whose functional reporting line is to the Chairman and CEO.
## INTEGRATED ASSURANCE CHARTER

### Integrated Assurance Team*

<table>
<thead>
<tr>
<th>Groups that host Assurance Providers and/or self-report risks/I issues</th>
<th>Organizations that P\perform independent assessments (Assurance Providers)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CIO Risk Management</td>
<td>• Audit Services (SOC1, SOC2, SOX, Operational Assurance)</td>
</tr>
<tr>
<td>• North America Client Assurance</td>
<td>• Enterprise Business Compliance</td>
</tr>
<tr>
<td>• Operational Risk and Client Assurance</td>
<td>• Segment-level Compliance</td>
</tr>
<tr>
<td>• Output Services (e.g., PCI DSS, MasterCard)</td>
<td>• External Professional Services (e.g., PCI Assessor, Protiviti, PwC, KPMG, others)</td>
</tr>
<tr>
<td>• Encryption Services</td>
<td>• Business Continuity / Disaster Recovery</td>
</tr>
<tr>
<td>• Info Sec (PCI)</td>
<td>• Business Information Security Officers (Critical Supplier Reviews)</td>
</tr>
</tbody>
</table>

*Others added as needed*
INTEGRATED ASSURANCE CHARTER

Integrated Assurance Team Meeting

The Integrated Assurance Team will convene periodically, usually on a quarterly basis, and will be chaired by a representative of Audit Services Group.

• Agenda topics to be agreed upon by participants. Representative topics to include:
  • Current and upcoming reviews scheduled
  • Emerging risk issues
  • Thematic findings
  • Interdependencies across assurance providers (e.g., findings whose remediation requires coordination and cooperation of multiple groups)
  • Change management on shared tools (e.g., Keylight, Enterprise Assurance Request Solution)
  • Strategic initiatives
  • Major production incidents/knowledge sharing
Integrated Assurance Team Responsibilities

The IAT will have responsibility for the following:

- Attending scheduled meetings.
- Meeting to review and discuss standing agenda items and any other such agenda items as have been submitted.
- Reviewing and discussing any other audit and assurance related concerns as appropriate.
- Fostering cross-team collaboration and coordination of efforts with any other control and monitoring functions to share information and avoid duplication of effort. Examples of coordinating activities include:
  - Synchronizing the nature, extent, and timing of planned audit/assurance work.
  - Ensuring a common understanding of assurance techniques, methods, and terminology.
  - Providing access to one another’s work programs, workpapers, and reports, as appropriate.
  - Placing reliance on each other’s work, where appropriate, to minimize duplication of effort.
  - Meeting intermittently outside of quarterly meetings to determine whether it is necessary to adjust the timing of planned work, based on the results of work that has been completed.
- Maintaining adequate documentation and tracking processes to facilitate successful collaboration.
- Using the Integrated Assurance Tracking workflow in Keylight’s Audit Module for tracking findings and self-identified risks.
Appendix A: Glossary

**Appropriate Evidence** – Any piece or collection of evidence gained during an engagement that provides relevant and reliable support for the judgments and conclusions reached during the engagement.

**Assurance** – A positive declaration, intended to give comfort and confidence, following an objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.

**Assurance Provider** – A person or group that performs independent testing/verification activities to help ensure that the controls, designed by management, are functioning adequately and comply with regulatory/legal requirements, guidelines and/or control frameworks.

**Finding** – A gap resulting from an independent assurance engagement.

**Independence** - The freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner.

**Integrated Assurance** – Aligning various assurance activities within an organization to ensure assurance gaps do not exist and assurance activities minimize duplication and overlap but still manage risk consistent with the board’s and management’s expectations.

**Management Action Plan** – What the audit customer, alone or in collaboration with others, intends to do to address the cause, correct the condition, and — if appropriate — recover from the condition.
Appendix A: Glossary

Management Assurance – The provision of assurance by managers within the First Line of the Three Lines of Defence Model.

Objectivity – An unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they have an honest belief in their work product and that no significant quality compromises are made. Objectivity requires internal auditors not to subordinate their judgment on audit matters to that of others.

Reliance – confident or trustful dependence.

Risk Leaders – A group within a business unit responsible for “self-identifying” and managing operational risks and findings.

Self-reported / Self-identified Issues – This practice empowers management to raise issues and track remediation to advance corrective action. Auditors gain comfort when management promptly address root causes related to the self-reported issues.

Sufficient Evidence – A collection of evidence gained during an engagement that, in its totality, is enough to support the judgments and conclusions made in the engagement.
Appendix B

Institute of Internal Auditors (IIA) International Professional Practice Framework (IPPF) References
INTEGRATED ASSURANCE CHARTER

The Institute of Internal Auditors (IIA) International Professional Practices Framework (IPPF) allows ASG to place reliance on the work of other assurance providers with consideration to five factors:

Placing Reliance On The Work Of Others

Internal audit’s decision to rely on the work of other assurance providers can be made for a variety of reasons, including addressing areas that fall outside the competence of the internal audit activity, to enable knowledge transfer from other assurance providers or to efficiently enhance coverage of risk beyond the internal audit plan.
INTEGRATED ASSURANCE CHARTER

Placing Reliance On The Work Of Others

Under the IIA’s guidance, an approach for relying on the work undertaken by other assurance providers must be based upon the following five principles:

• **Purpose:** When the assurance provider is committed and its purpose is aligned with internal audit’s objectives, auditors will find the work more relevant.

• **Objectivity:** The assurance provider can demonstrate credibility and deliver value to the internal auditor even where independence is lacking. The assurance provider’s competence, elements of practice and impact are key factors in balancing lower objectivity and establishing reliance.

• **Competence:** Assurance providers can bring a high level of expertise relevant to the specific business process while exercising sufficient objectivity. Although internal auditors provide a high degree of objectivity, they may not have the depth of knowledge needed to provide the desired level of assurance in certain organizational processes or technical areas.

• **Elements of Practice:** The external and internal assurance providers’ discipline to practice standard procedures is directly related to their capability for timely and persuasive conclusions. Consistency and rigor in practice should raise the internal auditor’s confidence in the assurance provider’s work.

• **Impact:** Internal assurance providers who are in close proximity to the business process may communicate risk and influence management to remediate control deficiencies quickly, perhaps more quickly than would a traditional internal audit. By monitoring risk and responding promptly, internal assurance providers may shorten the time to management action meetings.
Appendix B: IPPF References

Performance Standard 2050: Coordination and Reliance

The chief audit executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts.

Interpretation:

In coordinating activities, the chief audit executive may rely on the work of other assurance and consulting service providers. A consistent process for the basis of reliance should be established, and the chief audit executive should consider the competency, objectivity, and due professional care of the assurance and consulting service providers. The chief audit executive should also have a clear understanding of the scope, objectives, and results of the work performed by other providers of assurance and consulting services. Where reliance is placed on the work of others, the chief audit executive is still accountable and responsible for ensuring adequate support for conclusions and opinions reached by the internal audit activity.
Appendix B: IPPF References

Implementation Guide 2050: Coordination and Reliance

Provides guidance and advice on implementing Performance Standard 2050. Advises that the CAE may seek to gain an understanding of the scope, objectives, and results of the actual work performed by other assurance providers, to determine the extent of reliance that may be placed on the provider’s work. The CAE typically considers whether the provider’s findings appear reasonable and are based on sufficient, reliable, and relevant audit evidence. The CAE determines whether additional work or testing is needed to obtain sufficient evidence to support or increase the level of reliance desired. If additional work is needed, the internal audit activity may retest the results of the other provider.