The Extended Enterprise
The extended enterprise is the concept that an organization does not operate in isolation, because its success is dependent upon a complex network of third-party relationships.
Evolution of outsourcing

There is a current trend in higher market demand for outsourced services and functions

Outsourcing has transformed from a value protector to a value creator; companies are increasingly looking to third parties for the management of business and IT processes.

What is driving this growth? Simply put, companies must embrace outsourcing to compete globally, grow in the marketplace, and thrive.

- Deloitte Consulting LLP 2014 Outsourcing Survey

Technology will reduce geographic barriers, encouraging companies to constantly reassess service delivery options.
Ever-increasing extended enterprise risk profile

Through the evolution of outsourcing, a new risk focus has developed in the marketplace. The appetite for accepting third-party risk and relationships has grown, and the associated regulatory and monitoring activities have grown with it. To fully understand this new environment, it's important to consider all risks exposed through outsourcing and regulatory requirements:

### Risks in the Outsourcing Domain

- Contractual risk
- Financial risk
- Credit risk
- Compliance/legal risk
- Cyber risk
- Intellectual property risk
- Business continuity risk
- Operations risk
- Reputational risk
- Geopolitical risk
- Strategic risk
- Quality risk

### Governance and Regulatory Expectations

- Board of Governors of the Federal Reserve System (FRB)
- Consumer Financial Protection Bureau (CFPB)
- Federal Deposit Insurance Corporation (FDIC)
- Gramm-Leach-Bliley Act (GLBA)
- Office of the Comptroller of the Currency (OCC)
- Federal Information Security Management Act (FISMA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Public Company Accounting Oversight Board (PCAOB)
- Committee of Sponsoring Organizations (COSO)
- Board of director expectations
In the extended enterprise, third-party assurance has taken center stage

Third-party assurance (TPA) reporting facilitates the efficient exchange of data within the outsourcing marketplace and a company’s extended enterprise. Currently, many companies struggle with how to manage their reporting responsibilities as well as the methods in which assurance is gained from their own providers – this has led to a shift in third-party assurance activities and reporting vehicles.

**Dissonance in the TPA marketplace**

**Users**
- Inconsistent vendor selection processes
- Pressure from regulators
- Too much time sunk into monitoring providers

**Providers**
- Struggling to meet user demand
- Duplicative and unnecessary effort related to security questionnaires

**Evolution**
- Historically SOC (Service Organization Control) 1 reports met provider and user needs
- Increased third party risk has led to other types of reports (SOC 2, AT101, etc.)
- Providers leveraging SOC 2 for reports mapped to industry and regulatory requirements

**The Future**
- Integrated requirements
- Analytics
- Control automation
- Cyber assurance
- Custom reporting

Total number of TPA reports increasing 10% year over year.

SOC 2 reports make up approximately 25% of all reports issued/reviewed

– Deloitte Advisory “Service Auditor Review” Database
The Future of Third Party Assurance

Adaptability, industry-focus, and efficiency

Given the challenges associated with managing and reporting on third party risk within the extended enterprise, and the evolution of how third party assurance is utilized in the marketplace, the approach and mindset is changing.

Integrated Requirements
- Mapping of third party assurance reporting to user and industry requirements (regulatory, security questionnaires, operational areas in additional to financial)
- Common control frameworks can be utilized to facilitate more efficient exchange of compliance data

Analytics and Automation
- Automated control execution and continuous monitoring can streamline efforts of service providers and auditors
- Utilization of analytics continues to drive efficiency within third party assurance reporting efforts

Cyber
- SOC 2 has established itself in the marketplace as the primary reporting vehicle for operational compliance, including security, availability, processing integrity, confidentiality, and privacy
- Cyber assurance will continue to grow and develop within the context of AT101 and SOC 2 standards

Custom Reporting
- Automated report writing
- Customized reports for large user organizations
- Industry and regulatory requirement mapping based on user need
- Prospective user reporting
- New and enhanced report delivery mechanisms
Management challenges could be both internal and external. Some of the key challenges and questions we are hearing in the marketplace regarding the Extended Enterprise include:

- Where are the breakpoints in our third-party relationships? How do we assess and stay ahead of them?
- How do we bridge the gap between those in the business and our compliance and risk staff?
- How can we turn this program into one that evaluates value and does so on a recurring basis?
- What tools and technologies should we leverage to make informed decisions about our third-party relationships?
- What data do we already have access to? What should we be monitoring and analyzing to make real time decisions?
- How do we determine whether to outsource or insource, build or buy? What delivery models should we take advantage of?
- How will evolving technologies, market trends, or disruptive forces present opportunities and challenges to our third-party relationships?
- How do we keep up with the emerging regulatory requirements? Are our third parties keeping up?
- How do we ensure that appropriate contracts are in place with third parties, that they are meeting expectations, and complying with contractual commitments?
The Extended Enterprise

Three lines of defense

A well-structured risk management approach incorporating the three lines of defense can help the organization achieve efficiency and enables the right level of management involvement based on the Extended Enterprise’s risk and performance impact to the organization.

Board: Is aware of the sourcing strategy and risk the strategy brings, and confirms that the risk is sufficiently managed

Second line of defense: Centralized extended enterprise risk management governance program that

- Establishes and enforces policies/processes to ensure that third parties are managed consistently by the business
- Supports the business through provision of tools and templates to enable standard practices and reporting
- Performs independent monitoring, and evaluation of performance and compliance
- Oversees the program broadly across the enterprise to ensure that it is in line with strategy and the appropriate extended enterprise risks are being managed at an enterprise and geographic level

First line of defense: Business unit

- Owns the third-party relationship and is accountable for managing the risk in alignment with policies and procedures

Third line of defense: Internal Audit

Robust internal audit program aligned to the most critical extended enterprise risks and controls and performs independent assessments
The Extended Enterprise maturity model below is designed to help you understand where you are today, your ideal future state, the value the future state can bring to your organization.

The Extended Enterprise maturity model below is designed to help you understand where you are today, your ideal future state, the value the future state can bring to your organization.

**Strategy and Governance**
- No formal governance
- Risk taking for quick fix benefits
- Individual effort
- Little management input
- Lack of training

**People**
- Few activities defined
- Fire fighting mode
- Simple and least expensive tools used ad-hoc

**Process**
- Minimal effort in reducing risk
- Risk taking for short term benefits
- Responsibilities built into existing roles
- Increased input from management
- Defined processes in siloes
- Functional, reactive problem solving
- Off the shelf tools used for problem solving
- Limited access to third-party data

**Technology**
- Focus on preventing issues
- Risk aligns with medium-term enterprise-wide benefits
- Dedicated roles
- Invested executives within each silo
- Some training offered
- Coordinated processes across the business
- Monitoring and alerting leveraging dashboards, with some proactive issue resolution
- Adapted tools used for reporting and monitoring

---

**Integrated**
- Focus on preventing issues and creating value
- Intelligent risk taking, aligned with enterprise strategy
- Awareness of value of extended enterprise across the organization
- Enterprise wide roles
- Executive ownership at the enterprise level
- Fully standardized processes, integrated with tools and data
- Proactive decision making using analytics, improving bottom-line and performance
- Customized tools, used for tactical decision making
- Value additive tools
- Internal data centralized and easily accessible

---

**Optimized**
- State of the art practices, linked to value drivers
- Extended enterprise embedded in strategic planning and decision making
- Trained professionals with defined roles throughout the lifecycle
- Executive champions on both sides, aligning service delivery to strategic objectives
- Processes aligned with strategy, integrated into third parties
- Continuous improvement and proactive responsiveness
- Leveraging predictive and sensing analytics, tools and dashboards
- Highly-customized decision support tools
- Integrated external data sources that enhance insights
- Tools and analytics are key value driver and differentiator
Third Party Attestation (TPA) Reports
What are SOC reports and what do they assess?

SOC (Service Organization Control) Statement on Standards for Attestation Engagements (SSAE) No. 16 reports are independent assessments on the services provided by a third party, generally covering controls related to internal control over financial reporting (SOC 1) or controls related to privacy, security, availability and regulatory compliance of IT (SOC 2).

**SOC 1**
Issued under AICPA’s SSAE 16 standard, reports on controls at a third party relevant to internal control over financial reporting

**SOC 2**
Report on controls related to compliance or operations related to specific trust principles (security, availability, processing integrity, confidentiality, and privacy)

**SOC 3**
Short report (with same underlying scope as a SOC 2) that can be more generally distributed, with the option of displaying a web site seal; Viewed as marketing material

**Intended Audience/Users**
- Financial statement auditors
- Management of end user and third party
- Third-party management/risk management
- Internal/external auditors
- Useful to a third party’s customers, regulators, business partners
- Publicly available for anyone to view
- Current/prospective clients

Copyright © 2015 Deloitte Development LLC. All rights reserved.
## Third-party assurance—report type snapshot

<table>
<thead>
<tr>
<th></th>
<th>AUP (AT 201)</th>
<th>AT 101, 601</th>
<th>SOC 1</th>
<th>SOC 2</th>
<th>SOC 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope</strong></td>
<td>Fairly open-ended and not limited to Internal Control Over Financial Reporting (ICFR)</td>
<td>Management defined scope based on assertion (AT101 defined as attestation, AT601 defined as compliance)</td>
<td>ICFR</td>
<td>Trust Principles (Security, Availability, Processing Integrity, Confidentiality and/or Privacy)</td>
<td>Trust Principles (Security, Availability, Processing Integrity, Confidentiality and/or Privacy)</td>
</tr>
<tr>
<td><strong>Audience</strong></td>
<td>User entity (customer), their auditors, and the service provider</td>
<td>User entity (customers) and their auditors</td>
<td>User entity (customers) and their auditors</td>
<td>User entity and prospective customers</td>
<td>Anyone interested in the report</td>
</tr>
<tr>
<td><strong>Use</strong></td>
<td>Vendor management and operational audit</td>
<td>Custody Rule, Operational and regulatory audits</td>
<td>Financial and SOX audits</td>
<td>Operational, and regulatory audits</td>
<td>General</td>
</tr>
<tr>
<td><strong>Format</strong></td>
<td>High-level report that includes the auditor opinion related to the agreed-upon-procedures (not a control based report)</td>
<td>A flexible report that can either be high level or have detailed results</td>
<td>A detailed report that includes results of tests performed to obtain assurance of operating effectiveness of controls (Type 2)</td>
<td>A detailed report that includes results of operating effectiveness (Type 2)</td>
<td>A summary report that can be in the form of a Seal displayed on the website</td>
</tr>
<tr>
<td><strong>Report Components</strong></td>
<td>Auditor Opinion and List of Agreed-Upon-Procedures</td>
<td>Service Auditor Opinion, Management Assertion, System Description, and Controls (including tests of operating effectiveness and results) (Type 2)</td>
<td>Service Auditor Opinion, Management Assertion, System Description, and Controls (including tests of operating effectiveness and results) (Type 2)</td>
<td>Service Auditor Opinion, Management Assertion, System Description, and Controls (including tests of operating effectiveness and results) (Type 2)</td>
<td>Service Auditor Opinion, Management Assertion, System Description</td>
</tr>
</tbody>
</table>
## Which SOC report is right for your purpose?

<table>
<thead>
<tr>
<th>Professional standard used</th>
<th>SOC 1 report</th>
<th>SOC 2 report</th>
<th>SOC 3 report</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT 801</td>
<td>AT 101</td>
<td>AT 101</td>
<td></td>
</tr>
</tbody>
</table>

- **Used by auditors to plan and perform financial audits**
  - Yes
  - No
  - No

- **Used by user entities to gain confidence and place trust in service organization systems**
  - No
  - Yes
  - Yes

- **Obtain details of the processing performed and related controls, the tests performed by the service auditor and results of those tests**
  - Yes
  - Yes
  - No

- **Report generally available — can be freely distributed or posted on a website as a “SysTrust for Service Organizations” seal**
  - No
  - No
  - Yes
Third-party assurance—trend overview

**TPA**

**Traditional Areas: SOC 1, AT101 (or equivalent)**

**SOC 1, AT101 or Equivalent**

Based on statistics from Deloitte’s Service Auditor Review database:

- Increased number of SOC1 report issuances (by about 10%), increases in observed exceptions in attest work
- The total number of reports is increasing by around 10% every year
- Around 70% of the reports are issued by Big 4 audit firms.
- The percentage of qualified reports to total reports increased from 3% in FY14 to 7% in FY15.

**Growth Areas: SOC 2 or Equivalent**

**SOC 2 or Equivalent**

Report on controls related to compliance or operations related to specific trust principles (security, availability, processing integrity, confidentiality, and privacy)

- Significant increase in SOC 2 projects in FY15 as compared to the prior year
- Privacy is emerging as a leading concern for organizations and increased adoption of SOC 2 privacy principle
- SOC 2s are now 1/3 of the reports performed (security, availability & other criteria)

**Emerging Areas: Cyber Assurance**

**Cyber Assurance**

On February 12, 2014, the National Institute of Standards and Technology (NIST) issued a new Framework for Improving Critical Infrastructure Cybersecurity resulting from an Executive Order issued by President Obama

- In light of high-profile and costly cyber attacks at large corporations, Management is more vested in cyber assurance, and audit committees, boards of directors, and investors are asking more questions than ever before.
Third-party assurance—focus on SOC 2

SOC 2 is emerging as a leading standard across industries that can be applied for regulatory or non-regulatory purposes to cover business areas outside of financial reporting.

<table>
<thead>
<tr>
<th>Topic</th>
<th>SOC 2 Guidance</th>
</tr>
</thead>
</table>
| Professional Guidance     | AT 101, Attestation Engagements  
AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy |
| Scope                     | Controls at a service organization intended to mitigate risks related to security, availability, processing integrity, confidentiality, or privacy (trust services principles) |
| Application of SOC 2      | • SOC 2 can be applied for regulatory or non-regulatory purposes to cover business areas outside of financial reporting.                          
• The report can be distributed to customers and other stakeholders to demonstrate a focus on system and processing controls to meet their requirements.  
• SOC 2 can be applied to virtually every industry and business sector. SOC 2 will allow service organizations to provide assurance to customers and other stakeholders that effective internal controls are in place. |

SOC 2—Security

Trust Principle- Security relates to the authorization of transactions and protection of the integrity of those transactions throughout the system and also protecting personal and other information from unauthorized use or disclosure from the time it is collected until the time it is disposed of.

SOC 2—How it improves System Security

• Adoption of leading information security practices/controls during the attestation process  
• Year on year service auditor assessments improve the security posture of the organization
For large, complex service organizations, a thoughtful approach to assurance can save time, money, and lead to more satisfied clients and prospects.

### TPA Optimization

<table>
<thead>
<tr>
<th>Understand</th>
<th>Integrate</th>
<th>Rationalize</th>
<th>Implement and Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify reporting requirements – internal and external</td>
<td>Integrate control testing requirements across the enterprise to reduce work effort</td>
<td>Level set scope and report type requirements</td>
<td>Streamline overall TPA approach to better respond to customer queries</td>
</tr>
<tr>
<td>Report definition and inventory</td>
<td>Regulatory requirement mapping</td>
<td>Identification of redundant controls</td>
<td>Implement salesforce training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Identification of control gaps and areas of improvement</td>
<td>Implement regular optimization activities related to TPA trends and industry</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Execute on-going monitoring activities related to third-party assurance requirements, testing, and reporting including common approach</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Establish continuous monitoring techniques and technology</td>
</tr>
</tbody>
</table>