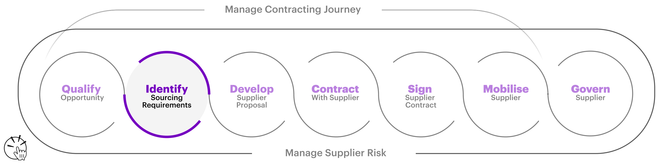
Accenture Way to Supplier-Contract (AWTS)

The Accenture Way to Supplier-Contract (AWTS) is our standard process for qualifying, selecting, approving, contracting with suppliers, and delivering ongoing 360° supplier governance.

About AWTS

AWTS is our new methodology for Supplier-contracting, it creates a common language and framework for all organisations involved in selecting and contracting for products and services from our Ecosystem Partners.

No two supplier contracts are the same, so AWTS provides you with the option to follow the end-to-end process or select a tailored paths, supported by reusable assets and signposts to other valuable content to meet your specific needs.



The AWTS comprises a series of integrated processes, sub-processes and activities, which spans the supplier contracting journey from qualification, through supplier contract signature to ongoing supplier governance with a focus on minimising risk and maximising value.

Objective

As the services we provide to our clients continue to rotate rapidly to the NEW and clients demand ever more innovation, we are required to engage with a larger, more diverse Supplier Ecosystem. Our Supplier Ecosystem plays a crucial role in providing platforms and capabilities that extend the services and value Accenture delivers to our clients, to safely Supplier-Contract for these new services and drive valuable growth we must work with the right Suppliers, obtaining the right services on the best contractual and commercial terms at the lowest risk to Accenture.

The Accenture Way to Supplier-Contract (AWTS) brings all of our best practice into an single end-to-end framework to enable our teams to successfully master Supplier-Contracting in the NEW. AWTS provides the process roadmap, tools and templates needed to balance these competing imperatives and working with our business stakeholders, make the right Supplier-Contracting decisions.

Our experts

Dave Caskie
Client Services Lead
Contact

Pete Henry
Operations & Enablement Lead
Contact

Emil Wuckert
Client Services
Contact

Joel Rocha
Operations & Enablement
Contact

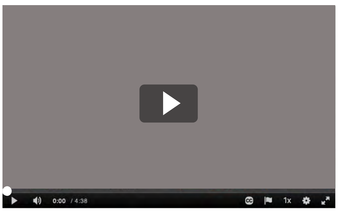
Mark Kuo
Relationship Management
Contact

Ann Parkin
Relationship Management
Contact

Mat Bakley
Strategic Initiatives
Contact

Michael Matias
Operations & Enablement
Contact

Resources



The AWTS Overview video
Brief introduction about the Accenture Way to Supplier-Contract (AWTS) methodology, its main processes and an overview on the AWTS Site structure.

Enhance your skills and knowledge through trainings available for AWTS methodology and its processes by completing the AWTS training.
Posted date: 20 | Jan | 2017
Duration:45 mins
Training Board

This site version was released in February 20th, 2021. For old versions, Release Notes.

Share your thoughts

Manage Supplier Risk

During this process, we focus on the proactive activities required to identify, assess, control and monitor Supplier risks both for internal events and external threats that affect the likelihood of a Supplier's success, such as information security, capability and performance problems.

Process overview

Identify Supplier Risk – There are a number of risk identification processes that can be initiated to assess the potential risks of a given Supplier and Supplier service, each is designed to assess different aspects of the Suppliers capabilities depending on the potential risks associated with the services being provided:

- **Information Security (IS) Assessment** – reviews risks with Supplier's protection/security procedures for access to Accenture and client data
- **Data Privacy for PII Assessment**– work with Legal to include appropriate PII data privacy terms, in addition to Info Sec terms when applicable and required
- **Business Intermediary (BI) Assessment** – legal and financial checks for business corruption and bribery risks
- **SDRA* – Capability and Capacity Assessment** – determination of the confidence of a Supplier's ability to deliver at scale and speed within the given timescales
- **SDRA* – Delivery Contingency Planning** – determination of available contractual, operational, and commercial levers, to mitigate a Supplier's failure to perform
- **SDRA* – Financial Stability Assessment** – evaluates risks with the financial stress of the Supplier
- **SDRA* – Relationship** – determination of risk and needs for management of the Supplier, including reference checks
- **SDRA* – Additional Delivery Assessments** – dependent on the outcome of IS Security review additional security assessments may be required.

Supplier Risk Response – There are a number of responses to identified Supplier risks, including avoiding the risk, transferring some or all of the risk, mitigating the risk to reduce either probability and/or impact, and accepting the risk through appropriate approvals and early notification controls.

SDRA* : Supplier Delivery Risk Assessment

Outcomes

Qualified and Quantified Supplier Risks

How sub-processes apply to service requests

Internal buy	Internal renewal	Offering	Client facing		
✓	✓	✓	✓	Information Security (IS) Assessment	Pre-contract
✓	✓	✓	✓	Data Privacy for PII Assessment	
✗	✗	✗	✗	Responsible Business Assessment	
✗	✓	✓	✓	Business Intermediary (BI) Assessment	
✓	✗	✓	✓	SDRA* – Capability and Capacity Assessment	
✓	✗	✓	✓	SDRA* – Delivery Contingency Planning	
✓	✓	✓	✓	SDRA* – Financial Stability Assessment	
✓	✗	✓	✓	SDRA* – Relationship	
✓	✓	✓	✓	SDRA* – Additional Delivery Assessments	
✓	✓	✓	✓	Information Security (IS) Assessment	Post-contract
✓	✓	✓	✓	Data Privacy for PII Assessment	
✗	✗	✗	✗	Responsible Business Audit	
✗	✓	✓	✓	Global Legal Review (GLR)	
✓	✗	✓	✓	ADRA - Financial Stability Assessment	
✓	✗	✓	✓	Risk Controls Compliance Evaluation	

Pre-contract | Post-contract

Sub-process RACIs | Roles & Responsibilities | Tools & Templates | Accenture polices | Process Alignments

Legend:
Responsible – Individual(s) who completes the task/deliverable. Responsible for the action/implementation plans.
Accountable – The single owner of the task(s), who is answerable for the correct and thorough completion of the deliverable or task(s), person who delegates the work to those Responsible and must sign-of
Consult – Individual(s) to be consulted prior to a final decision or action; two-way communication.
Inform – Individual(s) who needs to be informed after a decision is made or action is taken; one-way communication.

Identify Supplier Risk - Information Security (IS) Assessment

Policy required review of risks with Supplier's protection/security procedures for access to Accenture and client data, via the Protecting Accenture – Supplier IS (Information Security) Risk Profiling.

Roles	RACI	Description	Current Deliverables & Outcomes
Project/Deal Owner	C, I	Ensures IS assessment was completed	
Pilot	R	Ensure that the Supplier 'Data Privacy&InfoSec Risk Profiling Evaluation' is conducted for each Supplier by • completing the questionnaire linked from the IS Portal, • arranging any further IS review meetings needed, and • receiving various IS guidance, including varying IS contract language and/or other actions	Internal or Offering Requests: • 'Supplier Activity' entries updated Client Facing Requests: • 'Risk&Issue Log'updated
Co-Pilot	C, I	Ensures IS assessment was completed	
Legal	C	Provide current information Security schedules applicable based on IS risk rating	IS Contract Exhibits
Information Security	C	Based on 'IS Risk Rating', specify/develop the appropriate risk mitigations	IS Portal 'IS Risk Rating' and recommendations
CIO Operations, Solution Architect and/or Delivery	A	Accountable for completing the questionnaire linked from the IS Portal	

You are in Pre-contract tab
Scroll up to menu

Identify Supplier Risk - Data Privacy for PII Assessment

In addition to the required IS Security approval, it is required to work with Legal to include appropriate Regulated and PII Data privacy terms when applicable and required by GDPR requirements. As per Policy 0090-Data Privacy, this process is followed to determine if additional actions are required whenever a new Supplier/Subcontractor is onboarded, or new services are added to an existing Supplier, and execute the instructions for the corresponding Supplier to be GDPR compliant. See policy document for full details.

Roles	RACI	Description	Current Deliverables & Outcomes
Project/Deal Owner	C, I	Ensures IS assessment was completed	
Pilot	R	Ensure that the Supplier 'Data Privacy&InfoSec Risk Profiling Evaluation' is conducted for each Supplier by • completing the questionnaire linked from the IS Portal, • arranging any further IS review meetings needed, and • receiving various IS guidance, including varying IS contract language and/or other actions	Internal or Offering Requests: • 'Supplier Activity' entries updated Client Facing Requests: • 'Risk&Issue Log'updated
Co-Pilot	C, I	Ensures IS assessment was completed	
Legal	C	Provide current information Security schedules applicable based on IS risk rating	IS Contract Exhibits
Information Security	C	Based on 'IS Risk Rating', specify/develop the appropriate risk mitigations	IS Portal 'IS Risk Rating' and recommendations
CIO Operations, Solution Architect and/or Delivery	A	Accountable for completing the questionnaire linked from the IS Portal	

Responsible Business Assessment

...