
Contract Language/Vendor Management

A non-legalized look at items to consider when writing vendor contracts for project solutions

Introductions

□ Laura Griffitt – Vendor Management

- A.P.P. (Accredited Purchasing Practitioner)
- PRINCE2 Foundation

□ Bruce Tons – Security Officer

- CISSP
- ITIL
- PMP
- COBIT5

Targets That Impact Projects

- ❑ At times, some projects require outside resources to be utilized.
 - Staff Augmentation
 - ❑ Certain IT Expertise i.e.: DB Admin, Tech. Architecture
 - Customized software to be developed - externally
 - Package Software
 - ❑ Service or Solution
 - 3rd party vendor offerings
 - ❑ Web Applications
 - ❑ Mobile Applications
- ❑ Each item will require some type of contract while others may also require Statement of Work (SOW)



Are you ready to negotiate?



The Usual Language Included

- ❑ Indemnification
- ❑ Insurance Coverage
- ❑ Intellectual Property (IP) protection
- ❑ Scope, Renewal Terms and Notification
- ❑ Assignment – with or without written notice
- ❑ Termination – what are you to do if you need to exit
- ❑ Breach of contract – escalation, ownership, timeframes
- ❑ Processing restrictions – US Only
- ❑ Confidentiality & Ownership
- ❑ Audit (reports, BC/DR plans)
- ❑ Limitation of Liability
- ❑ Cost - T&M or Fixed-Price Project
- ❑ Service Level Agreements (SLA)



Negotiations vs. Due Diligence

- ❑ Regulatory reporting
 - SOC 2 Type 2 Reports or Auditor's Report
 - Review their Disaster Recovery Plans
 - Participation in each others DR exercise
 - Tour the facility(ies) / Right to audit
 - Physical Security – badges, biometrics, gates, cameras
- ❑ Penetration and Vulnerability Tests
 - mobile apps, web apps, thick client
 - Provide results, any patching and remediation plan
 - Provide final/clean report
- ❑ Exit Strategy
 - Ensure there is a way to retrieve your data
 - Degaussing your data from their site – backups?



Due Diligence vs. Negotiations

(continued)

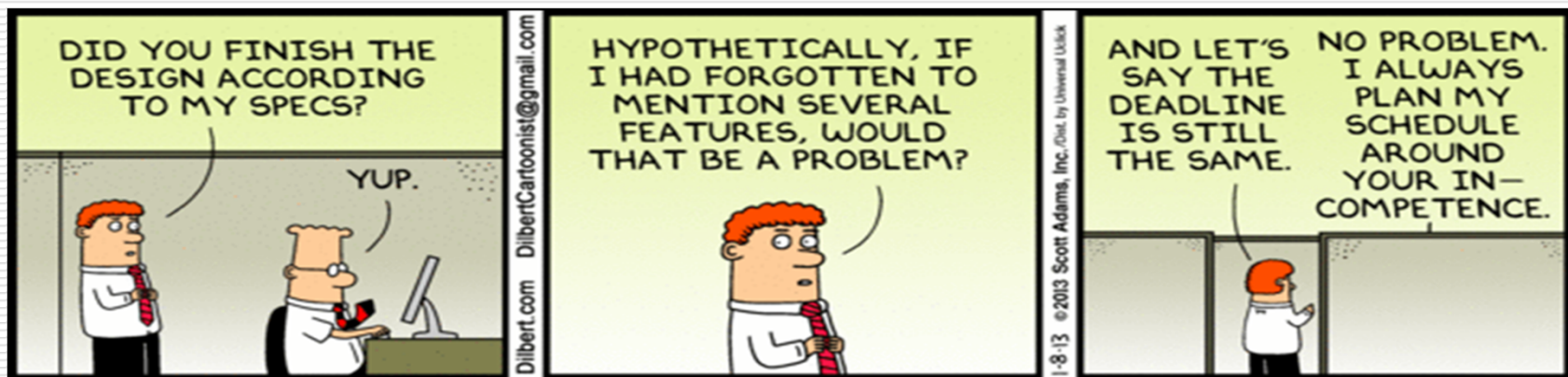
- ❑ What type of due diligence do they do on their contractors and employees
 - Confidentiality Agreement
- ❑ OFAC – anti-money laundry-terrorist watch list
- ❑ SSAE16
- ❑ Background checks
 - Criminal
 - Credit/financial
- ❑ Negative News
 - Company
 - Board of Directors
 - Officers or Ultimate Beneficial Owners (UBO)



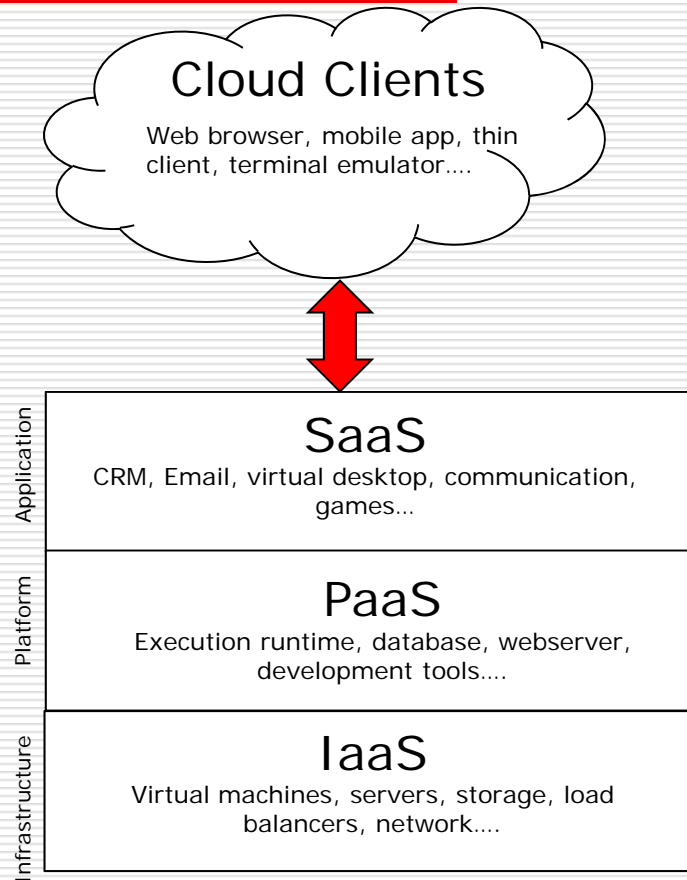
www.shutterstock.com · 271349714

Staff Augmentation

- ❑ Indemnification
- ❑ Data Loss
- ❑ Compliance with Policies
- ❑ Scope and rates
- ❑ Right to Hire
- ❑ Background checks, drug test, etc. – who pays?
- ❑ Non-Disclosure Agreement (NDA)



Service Modules



Project Delays – Conditional Contract Language to Consider

- Internal Staff and vendor service staff terminations
- Delay in contract execution
- Vendor Service delays, schedules
- Illness, vacations, holidays
- Force Majeure (Disasters)
- Arbitration, Lawsuits
- Other competing internal projects
- Equipment/hardware purchases



How to avoid what can go wrong





THANK YOU!!

- Laura Griffitt – Vendor Management
 - A.P.P. (Accredited Purchasing Practitioner)
 - PRINCE2 Foundation

- Bruce Tons – Security Officer
 - CISSP
 - ITIL
 - PMP
 - COBIT5