|  |
| --- |
| ITSecurityConsultant.com |
| Compliance Roadmap For IT Companies, MSPs and VARs |
| The Path To Compliance Starts Here |
|  |
| **Raj Goel, CISSP** |
| **[Pick the date]** |

|  |
| --- |
| This tool designed to determine what regulations clients are subject to, their most common questions, pain points and opportunities. Also assesses self-readiness to provide compliance & security services. |

|  |  |
| --- | --- |
| Your Name: |  |
| Email: |  |
| Phone/Cell: |  |
| LinkedIN profile: |  |
| Company Name: |  |
| Company URL: |  |
| # of employees: |  |
| Any CISSPs on staff? |  |
| Annual Revenues: |  |
| States served:  (e.g. NY, NJ, PA) |  |

|  |  |
| --- | --- |
| Which Regulations are my clients subject to: |  |
| Number of clients subject to compliance:  (please list industry or regulation and # of clients, % of your client list)  e.g. HIPAA, 13 clients, 28% revenue  PCI, 2 clients, 18% revenue  GLBA, 0, 0 |  |
| Average Revenue per client: |  |
| Average Revenue per compliance oriented client: |  |
| Do you handle/support compliance clients different from non-compliance clients?  If yes, please list the differences |  |
| Has your firm signed any BAAs within the past 36 months? |  |
| Has your firm offered any BAAs within past 36 months? |  |
| Are you a QSA , PA-QSA, ASV or other? |  |
|  |  |
| List your top 3 Compliance questions:  1 |  |
| 2 |  |
| 3 |  |
|  |  |
| List your top 3 compliance challenges:  1  2 |  |
| 3 |  |

Please complete the checklist on the next 3 pages.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  | Y/N | Notes |
| 1 | My staff has been trained in HIPAA Compliance |  |  |
| 2 | PCI-DSS |  |  |
| 3 | State Breach Law |  |  |
| 4 | Knows our local Records Retention laws |  |  |
| 5 | We have a designated CPO |  |  |
| 6 | I know who my CSO is (and I know the difference between CPO and CSO) |  |  |
| 7 | Our healthcare attorney is different from contracts & litigation attorney |  |  |
| 8 | We have been audited by a security & compliance expert within the past 18 months |  |  |
| 9 | I know who in my company is authorized to use Social Media |  |  |
| 10 | NOT authorized to use Social Media |  |  |
| 11 | Our network clock skew is under 1 second |  |  |
| 12 | Our client network’s clock skew is known and documented |  |  |
| 13 | We conduct regular compliance training exercises |  |  |
| 14 | We have a written DR plan |  |  |
| 15 | We have TESTED our Business Continuity Plan |  |  |
| 16 | I know who my MEDIA Liaison is |  |  |
| 17 | My staff is trained in handling reporters |  |  |
| 18 | My employees are diligent about reporting access to PHI |  |  |
| 19 | I am comfortable sanctioning employees for documented policy violations |  |  |
| 20 | Our CEO, CSO and staff are in agreement on our cloud-use policies |  |  |
| 21 | We read and review ALL BAAs |  |  |
| 22 | We’ve harmonized BAAs in the past 18 months |  |  |
| 23 | Our documentation and procedures were revised after the Omnibus rules |  |  |
| 24 | I know the difference between TPO and non-TPO activities |  |  |
| 25 | I can certify, under oath, that all systems that can be patched, have been patched and updated within past 30 days |  |  |
| 26 | My staff can testify which systems have patching exemptions, and why |  |  |
| 27 | We can implement the AusCERT TOP 4 |  |  |
| 28 | SANS 20 |  |  |
| 29 | In case of a breach or a hack, I know which law enforcement agency to contact, and am on good relations with them |  |  |
| 30 | I am comfortable having the CE’s security team test my defenses |  |  |
| 31 | Audit my systems |  |  |
|  | Audit my documentation |  |  |
| 32 | When I have a compliance or security question, I know who to call |  |  |