***Series: Adaptive Risk Management for Complex Supply Chains***

Practitioner Guideline Checklist Template for WFA-related Risks

**Practitioners:** This template contains specific risk areas across HR, Security, Privacy, and Control and Maintenance that can be used as a guide to begin tailoring the template to the needs of their own organization and setting. You may brand this checklist for your own use.

Samples of mitigating controls listed in this template are provided as examples only. This is not an exhaustive list but one that should be expanded upon by each organization based on its unique risk and service scope priorities. Each organization should evaluate its processes and tasks from its own standpoint, based on their individual organization’s needs.

**Disclosure:** The content of this series is not intended to convey or constitute legal advice, is not to be acted on as such, and is not a substitute for obtaining legal advice from a qualified attorney. These materials include the strategic and tactical processes deemed the most generally applicable to and useful for most organizations, both outsourcers and third parties. This material is not intended to be inclusive of every case required by statute or regulation for any specific industry, nor those mandated by any industry standard.

**WFA Guideline Checklist Template for HR, Security, Privacy WFA-related Risks and Control and Maintenance**

| **Risks Examined** | **Identify Risks & Controls in Place** | **Gaps Requiring Remediation** | **Mitigating Controls** | **Responsible Party** | **Complete** |
| --- | --- | --- | --- | --- | --- |
| ***Risk Oversight Processes*** |  |  |  |  |  |
| Risk Operations Center (HR, Business Units, IS, InfoSec event management team, other key stakeholders) |  |  |  |  |  |
| Hiring and Outsourcing Processes |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| ***Employees WFA Security & Privacy*** |  |  |  |  |  |
| Network access |  |  | Requiring secure VPN access only |  |  |
| IP Access & Availability/Connectivity | ` |  |  |  |  |
| IoT Device |  |  | Accurate inventory, rules for access to network, other… |  |  |
| Physical Access |  |  |  |  |  |
| Training |  |  | WFA Code of Conduct & Training |  |  |
|  |  |  |  |  |  |
| ***Third and Nth Parties*** |  |  |  |  |  |
| Identify and inventory all potential third parties |  |  |  |  |  |
| Nth party examination rules |  |  |  |  |  |
| Third Party’s WFA requirements/guidelines |  |  |  |  |  |
| ESG (Environmental, Social, and Governance) |  |  |  |  |  |
| Continuous Monitoring for key resilience factors (e.g., M&A, vertical and lines of business, location, financial, regulatory actions, vendor concentration, third party stability, service interruptions, geopolitical, financial, capability/scalability, natural and manmade disasters, etc.) |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| ***HR Employee and Contractor Oversight*** |  |  |  |  |  |
| Employee Well-being & Duty of Care |  |  | Employee hotlines |  |  |
| Regulatory Compliance, including Fraud Prevention |  |  |  |  |  |
| Insurance(s) – Cyber, Worker’s Comp, liability, etc. |  |  |  |  |  |
| Talent Pool (skill levels, training, etc.) |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| ***Infrastructure*** |  |  |  |  |  |
| Location-specific Physical Plant, including electric and communications |  |  |  |  |  |
| Availability of Alternative Sites/Processes/Platforms |  |  |  |  |  |
| Availability of Wi-Fi and associated reliability and “uptime.” |  |  |  |  |  |
| power grid and infrastructure. For example, in a number of critical outsourcing jurisdictions, electrical brownouts and blackouts are routine |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |