Below is a **Third-Party Risk Assessment Checklist** aligned with **ServiceNow IRM / Vendor Risk Management (VRM)** best practices and common governance guidelines. You can use this as a template for onboarding, evaluating, or monitoring vendors within ServiceNow.

ServiceNow-Aligned Third-Party Risk Assessment Checklist

---

1. Vendor Profile & Classification

☐ Vendor name, ownership, and registration details captured

☐ Services/products clearly defined

☐ Vendor tiering completed (Critical / High / Medium / Low)

☐ Data sensitivity classification applied (PII, PHI, PCI, Confidential, Public, etc.)

☐ Regulatory impact assessed (HIPAA, GDPR, SOX, ISO, FFIEC, etc.)

☐ Contract type, duration, and renewal dates documented

---

2. Governance & Compliance

☐ Vendor has documented Information Security policies

☐ Policies reviewed within last 12 months

☐ Governance framework followed (ISO 27001, SOC 2, NIST CSF, etc.)

☐ Evidence of compliance certifications uploaded (SOC reports, ISO certs, audits)

☐ Non-compliance or exceptions recorded and tracked in ServiceNow

☐ Third-party subcontractor list provided and assessed

3. Data Protection & Privacy

☐ Data handling procedures documented

☐ Encryption in transit & at rest verified

☐ Data retention & deletion policies validated

☐ Access controls and least-privilege applied

☐ Data transfer mechanisms compliant (GDPR SCC, HIPAA, etc.)

☐ Breach notification process in place

☐ Privacy Impact Assessment (PIA) completed (if applicable)

---

4. Security Controls & Technical Safeguards

Identity & Access Management

☐ MFA enabled

☐ Role-based access (RBAC) implemented

☐ User provisioning & de-provisioning controls

Network & Infrastructure Security

☐ Firewalls, IDS/IPS implemented

☐ Patch management program validated

☐ Vulnerability scans performed regularly

☐ Penetration test reports available

Application Security

☐ SDL / secure coding practices followed

☐ API security & authentication controls evaluated

☐ OWASP compliance verified

5. Business Continuity & Resilience

☐ Business Continuity Plan (BCP) available

☐ Disaster Recovery (DR) plan validated

☐ RTO/RPO meets business needs

☐ Evidence of DR testing in last 12 months

☐ Service uptime SLA documented

☐ Incident response plan shared

---

6. Financial & Operational Stability

☐ Financial health assessment performed

☐ Recent audited financial statements available

☐ Vendor bankruptcy/insolvency risk assessed

☐ Key personnel competency validated

☐ Operational maturity reviewed

---

7. Ethical, Legal & Contractual Requirements

☐ Non-disclosure agreements (NDAs) signed

☐ Data Processing Agreement (DPA) in place

☐ Intellectual property protection confirmed

☐ Vendor adheres to anti-bribery and ethical policies

☐ Legal disputes or litigations disclosed

---

8. Continuous Monitoring (as per ServiceNow VRM)

☐ Risk indicators (KRIs) configured in ServiceNow

☐ Automated vendor scorecards enabled

☐ Evidence & documents stored in Vendor Engagement record

☐ Automated reassessment cycle scheduled

☐ Risk acceptance, mitigation, or transfer decisions recorded

☐ Issues logged and tracked to closure

---

9. Onboarding & Off-boarding Controls

Onboarding

☐ Due diligence completed

☐ Contract signed and stored

☐ Risks evaluated and accepted/mitigated

Off-boarding

☐ Access revoked and accounts disabled

☐ Data retrieval or deletion confirmed

☐ Final audit and compliance review completed

---

10. Overall Risk Determination

☐ Inherent risk assessment completed

☐ Residual risk scoring verified

☐ Final risk rating assigned (Low/Med/High/Critical)

☐ Approvals captured in workflow (Business Owner, Compliance, Security)