

## Phase I - Preparation

- ☐ Develop and maintain AI incident response plan with:
  - ☐ Clear definition of AI incident
  - ☐ Severity schema (high, medium, low etc.)
  - ☐ Clear roles and responsibilities for response activities
  - ☐ Overview of:
    - ☐ Existing security standards as applied to AI
    - ☐ Privacy and data usage restrictions
    - ☐ Warranties associated with models
    - ☐ Related consumer expectations
    - ☐ Role of contractors and vendors
    - ☐ Existing sensitive data assets
  - ☐ Clear relation to existing information security plans (standalone vs. addendum)
  - ☐ Communications strategy (internal, PR, legal, etc.)
- ☐ Allocate in-house resources and/or select third parties for:
  - ☐ AI liability assessment
  - ☐ AI forensic investigation
  - ☐ Legal assessment and response
  - ☐ Public and media relations
- ☐ Communicate potential for AI failures and attacks to:
  - ☐ Senior management
  - ☐ Data scientists
  - ☐ Information security
  - ☐ IT personnel
- ☐ Confirm authorization to respond to AI incidents across all information technology (IT) systems
- ☐ Establish a clear understanding of containment strategies:
  - ☐ “Watch and Learn” vs. “Disrupt and Disconnect” standard operating procedures (SOP)
  - ☐ Processes for necessary departures from SOPs

---

**Disclaimer:** bnh.ai leverages a unique blend of legal and technical expertise to protect and advance clients’ data, analytics, and AI investments. Not all firm personnel, including named partners, are authorized to practice law.

## Phase I - Preparation (Cont.)

- ☐ Standardize model documentation, to include:
  - ☐ Applicable regulatory requirements
  - ☐ Anticipated litigation or reputational risks
  - ☐ Baseline operational data for a model
  - ☐ Estimated business impact of disconnecting a model
  - ☐ IT and business contacts for a model
  - ☐ Technical specifications for a model
  - ☐ Sensitivity of data involved (input or output data)
  - ☐ Other key assumptions
- ☐ Backup and secure model documentation against integrity attacks
- ☐ Implement critical response capabilities, including:
  - ☐ Appeal of model-based decisions
  - ☐ Model “kill switch”
  - ☐ Processes for model monitoring
  - ☐ Override of model-based decisions
- ☐ Inventory and backup models in offline storage

---

**Disclaimer:** bnh.ai leverages a unique blend of legal and technical expertise to protect and advance clients' data, analytics, and AI investments. Not all firm personnel, including named partners, are authorized to practice law.