

# Incident Response Readiness (IRR) Essentials Package



## STREAMLINE YOUR IR DEVELOPMENT

Simple as 1-2-3. The IRR Essentials Package provides you with all of the elements to develop your company's incident response readiness program quickly plus a consulting team to help you navigate your specific technical questions throughout the process. You receive Incident Response Program components with directions, templates, cyber security training, and advisory services that guide you along the development process.

IRR Essentials enables you to be compliant and "audit-ready".

## ACHIEVE COMPLIANCE WHILE BUILDING UPON YOUR CURRENT APPROACH

The IRR Essentials solution incorporates best practices as well as industry standards and regulations that organizations should address for incident response planning. Our expert team did thorough research to review numerous information security standards and laws and identified more than 200 incident response-related requirements. The content is cited using footnotes to map directly to the original requirement, allowing teams to easily incorporate security goals to build out the IR plan, policy and standard. This cohesive approach ties all standards, policies, requirements together for users and withstands the scrutiny of an audit, as everything is documented.

**All-in-One Solution. Self-Paced with Expert Guidance.**



## Incident Response Plan Template

An incident response plan template complete with references to many security standards, including: NIST, ISO, HIPAA, PCI, CIS, GDPR, DFARS, NERC CIP, 23 NYC 500, and more. The template is a full plan, formatted to accept and integrate any existing materials easily, ready to publish after customization.

### Template Highlights:

- Scope
- Team Framework Suggestions
- Roles and Responsibilities
- Key Definitions, Incident Type Examples
- Incident Response Plan Checklist Framework– Triage, Investigation, Containment, Eradication
- Links to Payment Brand Specific Procedures
- Diagrams for each phase
- **Communications:** Strategies, Plan Framework, “Breach Notification” draft messages – ready for customization
- Recommendations for Recovery, Lessons Learned, Planning and Prevention
- Forms to be completed during an incident

### Features

- Comments for purpose and guidance of each section, and customization options.
- Video Training walks through each section for customization as you go.

## Incident Response Policy Template

- A full incident response management policy template which includes references to all of the aforementioned standards as necessary.
- Turn-Key policy – contains “ready to publish” language – just decide what policy clauses make sense for your organization.
- Change/Remove/Add policy clauses as necessary to support your organization.

## Incident Response Internal Standard Template

A full template which will house all of the rules, tools, technology, process, measurements, objectives, frequencies, and approvals that are needed to support the policy clauses.



## Pre-Recorded Training Videos (17 videos, approximately 180 minutes)

- Covering the customization of the IRR templates.
- Ranging from 6 to 15 minutes – these videos walk the author through the templates in a conversational, helpful manner.

## Live Training Session (2 hours)

- Based on the IR Plan template, your organization can attend a 2-hour training session (online) and it may be recorded.
- Reviewing tabletop scenarios based on real-life security incidents.

## Live IRR expert counseling and advisory services (4 hours)

Assisting with IR Plan creation and more.

## IRR Technology Review

- **An analysis of the current technology in place** that may assist in a cyber security incident response including a documented maturity rating for each area of focus (based on NIST SP 800-61 guidelines).

### Focus Areas

- **Preparation:** Artifacts and processes that can aid in incident response.
- **Detection and Alerting:** Ability to detect and alert on potential incidents.
- **Prevention:** Ability to prevent and/or minimize the extent of damage/propagation of detected incidents.
- **IR technology recommendations** to close gaps and increase maturity scores.
- **Live IRR technical counseling and advisory services** (2 hours) to assist with the creation of a high-level IRR gap remediation plan.

