# CYBERSECURITY INTRO

## CYBERSECURITY: AN INTRODUCTION FOR BROKER DEALERS AND INVESTMENT ADVISORS

*A RISK-BASED APPROACH LEVERAGING REGULATORY GUIDANCE*

STRATEGY BASECAMP

# CYBERSECURITY - THE REGULATION: WHAT ARE BD / IAs REQUIRED TO DO?

**NASD (n/k/a FINRA) Rules of Fair Practice always required confidential treatment of customer information. Regulation S-P strengthened this requirement specifically with Section 30. BDs / IAs Are Required To:**

1. Adopt reasonably designed written policies and procedures addressing administrative, technical and physical safeguards for the protection of customer information and records; and

2. Protect against any anticipated threats or hazards to the security or integrity of customer records and information, and against unauthorized access to or use of customer records or information.

# CYBERSECURITY: WHAT REGULATORS SUGGEST BDs / IAs DO?

## FINRA and the SEC Recommend that Firms:

1. **Document Your Technology Environment and Your Cybersecurity Program.**
2. **Perform a Risk Assessment.**
3. **Implement Cybersecurity Controls.**
4. **Develop, Implement and Test Incident Response Plans.**
5. **Perform 3rd Party Vendor Due Diligence and Manage Related Cybersecurity Risks.**
6. **Train Your Staff to Identify and Mitigate Cybersecurity Risks.**

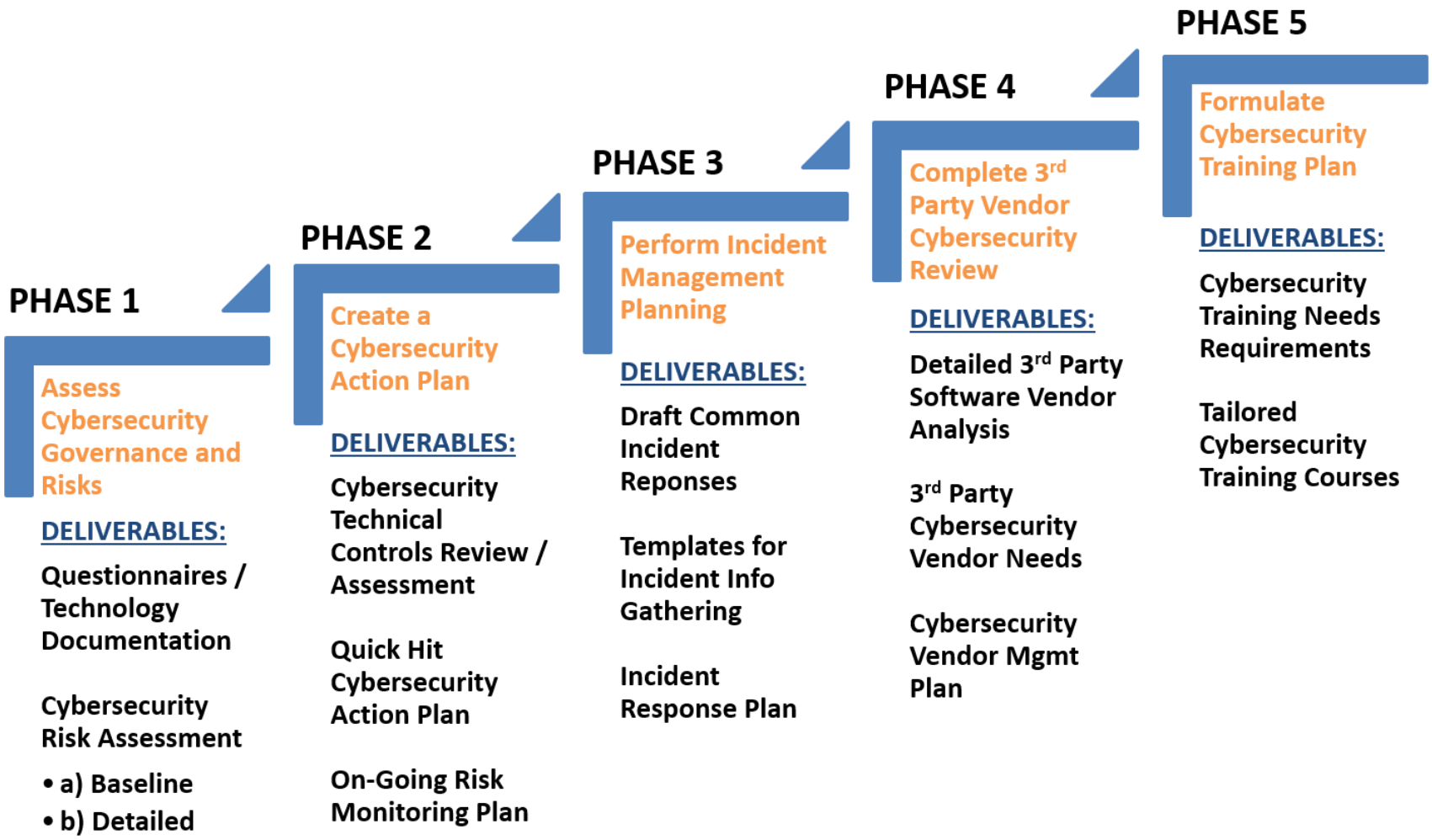
**We recommend all firms start by: 1) Documenting Your Technology / Cybersecurity Program and by 2) Performing a Risk Assessment**

# CYBERSECURITY PROGRAM DEVELOPMENT: A RISK BASED APPROACH


**Your cybersecurity program should be aspirational, yet attainable. Each firm should adopt a framework tailored to the risks inherent to their environment.**

# CYBERSECURITY PROJECT TOOLKIT: COMPREHENSIVE LIST OF DELIVERABLES

**Strategy Basecamp can manage all work. The first steps include performing a cybersecurity risk assessment and reviewing your technical controls.**



# STRATEGY BASECAMP: WAYS TO ENGAGE US

**OPTION 1:**

1. Questionnaires & Technology Documentation
2. High-Level Risk Assessment
3. Cybersecurity Technical Controls Review / Assessment

**OPTION 2:**

1. Option 1 Deliverables Plus:
2. Detailed Risk Assessment
3. Quick Hit Cybersecurity Action Plan
4. On-Going Risk Monitoring Plan