Toolkit

The Vendor-Free IT Community.

DISASTER RECOVERY & BUSINESS CONTINUITY

These NOREX Member-contributed documents include vendor tools & requirements, RFP, BIA, emergency response, incident management, disaster recovery, business continuity, testing, co-location, discussions, and polls. | TK003

The NOREX Document Library is continually updated for the benefit of our Members. Please consider contributing documents from your organization. Thank you!

Business Continuity

BUSINESS CONTINUITY POLICY. This policy includes details on data backup, retention, destruction, colocation, and disaster recovery. 4 Pages (20-1062)

BUSINESS CONTINUITY DISCLOSURE STATEMENT. This comprehensive statement describes there is a business continuity plan in place and describes its purpose. 1 Page (20-1039)

BUSINESS CONTINUITY PLAN. This plan outlines procedures to take in the event of a serious business disruption affecting business functions, to ensure employee safety and provide a framework to ensure business continuity. 27 Pages (20-963)

CONTINGENCY PLANNING PROCEDURE. This document outlines a contingency planning procedure that applies to all information systems and components. It includes what must be done to recover key hardware components that all business software and applications require in order to run. 2 Pages (20-925)

CRISIS MANAGEMENT INTRODUCTION. This document is an introductory plan for enabling fast and effective recovery from an unforeseen disaster or emergency which interrupts normal business operations. 28 Pages (20-895)

COVID-19 CONTINUITY PLAN. This plan outlines the coordinated preparation and personnel response to ensure critical services are maintained during a COVID-19 or other pandemic outbreak. 3 Pages (20-893)

HEALTHCARE BUSINESS CONTINUITY PLAN. This template details a healthcare business continuity program including disaster recovery strategy and service prioritization. 13 Pages (20-890)

CENTRAL SCHEDULING BCP. This Business Continuity Plan template focuses on a central scheduling concierge program in a healthcare setting. 8 Pages (20-889)

BUSINESS CONTINUITY MANAGEMENT POLICY. Effective contingency planning can minimize the impact of a disaster or threat. This document provides planning and program guidance for implementing a Business Continuity Plan (BCP). 17 Pages (20-685)

BUSINESS CONTINUITY PLAN. The following BCP template is a guide for creating your own continuity plan to preserve critical processes and operations. 14 Pages (20-684)

BUSINESS CONTINUITY MANAGEMENT. Included in this Business Continuity Plan are policies, procedures, and organization charts for crisis management and disaster recovery. 93 Pages (20-682)

BUSINESS CONTINUITY PLAN. This document provides planning and program guidance for implementing the company's Business Continuity Plan. 32 Pages (20-057)

Business Impact Analysis

BIA TEMPLATE. This Business Impact Analysis template includes timeline, impact, process, data records, and more. 30 Pages (50-371)

BUSINESS IMPACT ANALYSIS QUESTIONNAIRE. The following BIA evaluation is designed to collect the information necessary to support development of alternative processing strategies and solutions. 14 Pages (20-842)

CASH MANAGEMENT BIA. The following is an asset management & cash management Business Impact Analysis process. 5 Pages (20-681)

DRP QUESTIONNAIRE & BIA TEMPLATE. A Disaster Recovery Plan questionnaire and Business Impact Analysis template helps prepare site specific information for unexpected occurrences. 15 Pages (20-321)

PCI REQUIREMENTS KEY. Payment Card Industry (PCI) requirements regarding security, development, and firewall/router configurations are outlined in this key. 19 Pages (20-281)

BUSINESS IMPACT ANALYSIS QUESTIONNAIRE. A BIA will help to estimate financial impacts as well as intangible or operational impacts of a disaster situation. 3 Pages (50-312)

Colocation

IT DATA CENTER AND COLOCATION POLICY. Guidelines for proper maintenance and protection of the data center, whether hosted in-house or offsite, are provided in this policy. 3 Pages (20-1068)

Disaster Recovery

RECOVERY RUN BOOK. This template logs business system service restoration processes for disaster recovery. 2 Pages (20-993)

SERVER LIST BY TIER. This worksheet illustrates a method of listing servers, function, operating system, and other details. 4 Pages (20-680)

SYSTEM CLASSIFICATION BY TIER. Systems & applications and their impact and dependencies are arranged according to tiered classification in this sample document. 2 Pages (20-679)

DISASTER RECOVERY PROCEDURE OUTLINE. The following is a basic outline of disaster recovery site procedures. 1 Page (20-678)

DISASTER RECOVERY & BUSINESS CONTINUITY POLICY TEMPLATE. A disaster recovery & business continuity policy includes processes for recovering critical technology systems and data. 3 Pages (20-667)

DISASTER RECOVERY RECORDS RETENTION. This policy provides step-by-step procedures for reducing the risk of service disruption in order to ensure continuity of operations. 2 Pages (20-639)

DISASTER RECOVERY & BUSINESS CONTINUITY STANDARD. In order to quickly restore critical business systems in the event of a disaster, Business Impact and Risk Assessment tools can be used to determine dependencies, strategies, and safeguards. 17 Pages (20-352)

DRP QUESTIONNAIRE & BIA TEMPLATE. A Disaster Recovery Plan questionnaire and Business Impact Analysis template helps prepare site specific information for unexpected occurrences. 15 Pages (20-321)

IT RISK ASSESSMENT. This is a worksheet detailing external and internal threats as well as disaster risk factors. 3 Pages (20-250)

UNPLANNED OUTAGE PROTOCOL. This document establishes communication protocols for staff (and their outside business partners) in the event of an unplanned outage. 5 Pages (20-080)

DISASTER RECOVERY EXECUTIVE SUMMARY. The plan documents the necessary steps to take regardless of the type of disaster that has been declared. 4 Pages (20-004)

IT DISASTER RECOVERY PLAN. Included are organization charts, sample incident reporting responses, infrastructure, and data protection procedures. 22 Pages (10-1646)

Discussions & Polls

SD-WAN TRANSCRIPT. NOREX Members discussed drivers to SD-WAN, reliability of their solution, negative experiences when implementing SD-WAN, recommendations for design and deployment, solutions evaluated for SD-WAN, utilizing providers with their own backbone vs. providers like CATO and Velo, access to all internet / Cloud services routed through NGFWaaS, and use of a managed service provider for SD-WAN. 22 Pages (NV2389)

FOOD & BEVERAGE MANUFACTURING: IT SECURITY TRANSCRIPT. NOREX Members discussed recommended IT Security initiatives, cybersecurity insurance and renewals, segregation of the IT network, communication to the outside world from the OT network, solutions used for 2FA on VPN connections, Artic Wolf, Red Canary, and documented recovery and response plans. 15 Pages (NV2386)

POST-COVID HYBRID WORK STRATEGIES TRANSCRIPT. NOREX Members discussed how best to manage a hybrid work environment, provisions for home offices, hardware support and budget, internet connectivity issues, cash allowances and potential legal concerns, achieving equity amongst in-office and at-home staff, best tools for building out conference rooms, and security. 30 Pages (NV2385)

POWER BI TRANSCRIPT. NOREX Members discussed getting started with Power BI, experiences with building and executing, visualization services, mining capabilities, dashboard viewing, licensing agreements, backup and recovery strategies, deliverables, and alternative products. 15 Pages (NV2383)

RANSOMWARE TRANSCRIPT. NOREX Members discussed Ransomware attacks and what to do once infected, restoring LAN shares and rebuilding workstations, warnings against paying ransom, counter measures and mitigation, backups and patching, cybercriminal activity detection, MDR vs. MSSP, endpoint protection, and the use of an MDM application. 30 Pages (NV2381)

DISASTER RECOVERY / BUSINESS CONTINUITY TRANSCRIPT. NOREX Members discussed best practices conducting Business Impact Analysis, addressing cyber-resilience for DR and BC, determining appropriate recovery time objectives and recovery point objectives, testing and training users, testing disaster recovery plans, and the use of vendors for DR. 16 Pages (NV2379)

CONSTRUCTION INDUSTRY – IT PROJECT MANAGEMENT TRANSCRIPT. NOREX Members discussed how best to elevate the presence of IT project management in the Construction Industry, community of practice standardization, master service integrators, Construction Management software, credential harvesting, and security. 14 Pages (NV2375)

SECURITY FRAMEWORKS TRANSCRIPT. NOREX Members discussed the hierarchy of security frameworks; most commonly used frameworks; categorization of control, platform, and risk frameworks; and active threat hunting. 14 Pages (NV2374)

GLOBAL IT ISSUES TRANSCRIPT. NOREX Members discussed the biggest issues they and their organizations are facing with a global footprint in today's business climate. The expectations with employees able to return to the office, IT talent recruiting and hiring internationally, standardization of processes, cybersecurity, procuring equipment globally, keyboard sourcing, and in-country IT support were challenges shared by all Member participants. 17 Pages (NV2371)

MICROSOFT TEAMS BEST PRACTICES TRANSCRIPT. NOREX Members discussed the implementation of Microsoft Teams within an organization, Teams' members as part of the infrastructure or collaboration teams, the use of the exploratory license program, promoting adoption and usage of the platform, and VoIP integrations. 49 Pages (NV2369)

CLOUD-BASED STORAGE TRANSCRIPT. NOREX Members discussed the lessons learned, and difficulties experienced, when transitioning from on-prem storage to Cloud. The discussion covered the pros and cons of various Cloud platforms, security, policy and practices, and the dangers of accessibility. 17 Pages (NV2368)

HYPERCONVERGED INFRASTRUCTURE TRANSCRIPT. NOREX members share experiences adopting a Hyperconverged Infrastructure including performance expectations, vendor options, and back-up strategies during this April 2021 WebForum. 16 Pages (NV2365)

IT CHANGE MANAGEMENT TRANSCRIPT. NOREX members discuss IT Change Management processes including recommended tools, governance approaches and communication protocols during this April 2021 session. 25 Pages (NV2363)

ENTERPRISE STORAGE SOLUTIONS TRANSCRIPT. Member organizations discuss a variety of enterprise storage technology, trends, vendor solutions, and more during this March 2021 WebForum. Several polls are included. 24 Pages (NV2362)

RISK MANAGEMENT TRANSCRIPT. NOREX members share strategies for identifying, managing and reporting risks during this February 2021 session. 21 Pages (NV2358)

SECURITY INITIATIVES FOR 2021 TRANSCRIPT. NOREX members share 2021 IT security plans including budgets, initiatives and tools during this January 2021 session. 34 Pages (NV2354)

PLANNING FOR 2021 TRANSCRIPT. NOREX members share their expectations for IT budgets, staffing levels, security initiatives, user support trends and other 2021 issues during this December 2020 session. 19 Pages (NV2351)

BACKUP / RECOVERY TRANSCRIPT. Assuring that lost data can be accessed is a key factor to assuring businesses run smoothly. This discussion on this important task includes strong conversations around Veeam as a tool and its role in backing up Exchange. 10 Pages (NV2344)

BUSINESS CONTINUITY TRANSCRIPT. Planning for the unexpected, business continuity is a perpetual challenge for business and often falls on the shoulders of IT. With a pandemic forcing entire workforces home, NOREX members share how their plans stood up against the very unusual situation we all find ourselves in and share strategies and tools to consider as plans continue. It includes a long discussion around vendors and tools members have found successful. 19 Pages (NV2336)

CYBERSECURITY TRANSCRIPT. NOREX Members share cybersecurity best practices and tool recommendations during this July 2020 WebForum. 19 Pages (NV2331)

AZURE / AWS / GOOGLE ENTERPRISE CLOUD USAGE TRANSCRIPT. NOREX Members discuss the usage of Microsoft, Amazon and Google cloud services during this June 2020 WebForum. 20 Pages (NV2325)

ASSET MANAGEMENT / PROCUREMENT FOLLOWING COVID-19 TRANSCRIPT. NOREX Members discuss ITAM strategies and tools in light of the COVID-19 Pandemic during this May 2020 WebForum. 20 Pages (NV2323)

COVID-19: BRINGING WORKFORCE BACK TRANSCRIPT. Organizations are currently working on how and when to move staff back to the office after the COVID-19 pandemic shutdown. Among the decisions to be made are whether to return the full or partial staff to the office. During this WebForum, NOREX Members and guests discussed options, resources, and lessons learned regarding equipment returns, social distancing in the office, government requirements and guidelines, stipends for employees, work prioritization, remote work tools, sanitizing, restrictions, and temperature scanning in the workplace. This transcript includes discussion about keeping the workforce safe after returning to the office, as well as a robust chat log conversation. 53 Pages (NV2321)

COVID-19 PANDEMIC: RESPONSE, LESSONS LEARNED, WHAT'S NEXT? TRANSCRIPT. Members discuss how the organization has responded to the impact to the pandemic crisis. Lessons learned on supporting WFH from a technical, hardware, security and team engagement / collaboration, and what is next perspective are shared. Polls, links, and a lively chat section are included in this April, 2020 transcript. 28 Pages (NV2315)

PREPARATION FOR A REMOTE WORKFORCE TRANSCRIPT. With the onset of COVID-19 and the need for distancing, aggressive remote workforce processes are in place for most NOREX Member organizations. NOREX hosted this discussion on March 17, 2020 with over 200 participants. This transcript includes a very active chat log conversation, results from polls taken, and the takeaways we received from those who completed an evaluation. 48 Pages (NV2313)

ENDPOINT DETECTION / PREVENTION / RESPONSE TRANSCRIPT. Member organizations discuss Endpoint Detection / Prevention / Response during this March, 2020 WebForum. Several polls and a variety of products / solutions in use are included. 19 Pages (NV2310)

PANDEMIC CRISIS PREPAREDNESS TRANSCRIPT. NOREX members discuss business continuity, disaster recovery and updated policies to prepare for the possibility of a pandemic. 12 Pages (NV2307)

VDI TRANSCRIPT. NOREX Members discuss the selection, implementation and operation of various Virtual Desktop Infrastructure platforms during this February 2020 WebForum. 16 Pages (NV2306)

2020 IT SECURITY INITIATIVES TRANSCRIPT. What are member organizations top IT security initiatives for 2020? This January 2020 discussion is packed with security plans, strategies, polls, links to solutions / tools, a lively chat section, and much more. 27 Pages (NV2303)

DISASTER RECOVERY / BUSINESS CONTINUITY TRANSCRIPT. This December 2019 discussion begins with best practices in conducting the Business Impact Analysis (BIA) and continues with a variety of DR and BC topics, solutions, polls, chats, and more. 17 Pages (NV2301)

PATCH MANAGEMENT TRANSCRIPT. NOREX Members share their patching schedules for routine and critical system patching and discuss tools used for applying patches during this November 2019 WebForum. 15 Pages (NV2298)

HELP DESK / SERVICE DESK TRANSCRIPT. NOREX Members discuss Help Desk / Service Desk procedures and recommended tracking tools during this November 2019 WebForum. 14 Pages (NV2296)

ENTERPRISE STORAGE SOLUTIONS TRANSCRIPT. NOREX members discuss current storage trends including usage of flash, cloud options, modern data protection, automation and artificial intelligence during this September 2019 WebForum. 10 Pages (NV2289)

VULNERABILITY MANAGEMENT TRANSCRIPT. NOREX members share recommendations on processes and tools to manage IT vulnerabilities and risks during this September 2019 WebForum. 20 Pages (NV2288)

DOCUMENT MANAGEMENT TRANSCRIPT. NOREX members share experiences selecting, implementing and managing Document Management systems during this September 2019 WebForum. 18 Pages (NV2286)

DATA GOVERNANCE / GDPR / US PRIVACY LAWS TRANSCRIPT. NOREX members share recommendations on achieving compliance with various privacy regulations during this August 2019 WebForum. 25 Pages (NV2283)

CYBERSECURITY TRANSCRIPT. This August, 2019 discussion is filled with member best practices, product experiences, and lessons learned on all aspects of cybersecurity. Several polls are included. 24 Pages (NV2281)

PRIVILEGED ACCESS MANAGEMENT TRANSCRIPT. NOREX members discuss the implementation and of Privileged Access Management procedures and tools during this July 2019 WebForum. 14 Pages (NV2278)

O365 NEW FEATURES / INITIATIVES TRANSCRIPT. Members share experiences with the implementation of various Microsoft Office 365 services and features including PowerBI, SharePoint, Skype for Business and Teams during this June 2019 WebForum. 32 Pages (NV2275)

BACKUP/RECOVERY TRANSCRIPT. Members share experiences with the leading backup and recovery tools during this May 2019 WebForum. 12 Pages (NV2270)

DISASTER RECOVERY TRANSCRIPT. Topics of this March 2019 session include recovery approaches such as on- prem vs. DR-as-a-Service, backup and recovery tools, testing strategies and Business Continuity considerations. 20 Pages (NV2264)

DATA LOSS PREVENTION (DLP) TRANSCRIPT. Getting started with DLP, DLP attributes, solutions used, cloud impact, data classification, and more are discussed during this March 2019 WebForum. 17 Pages (NV2263)

CLOUD-BASED STORAGE TRANSCRIPT. NOREX members discuss the pros and cons of moving from on-prem to cloud-based storage during this January 2019 session. 16 Pages (NV2254)

SECURITY INITIATIVES FOR 2019 TRANSCRIPT. This January, 2019 security discussion covers a wide range of member security initiatives planned for this year and/or already implemented. Many links, polls and multiple chat discussions are included. 33 Pages (NV2253)

MEMBER VENDOR RATINGS: ENDPOINT SECURITY. This Endpoint Security Tools and Solutions poll resulted in 50 products being rated. 5 Pages (NR008)

MEMBER VENDOR RATINGS: NETWORK SECURITY. This Network Security Tools and Solutions poll resulted in 65 products being rated. 5 Pages (NR007)

MEMBER VENDOR RATINGS: BACKUP / STORAGE. This Backup and Storage Tools and Solutions poll resulted in 51 products being rated. One hundred and thirty members responded. 6 Pages (NR004)

QUICK POLL RESULTS: COVID-19: WORKFORCE NEXT STEPS. In April 2020, over 200 NOREX members responded to a poll on workforce next steps in relation to the COVID-19 pandemic. Topics covered are when to bring employees back to the office, what measures will you deploy, and lessons learned and best practices implemented during the pandemic. 20 Pages (NP2319)

QUICK POLL RESULTS: TECHNOLOGY & BUDGET TRENDS 2019. Member organizations participated in our Technology & Budget Trends poll in December 2018. This poll includes deployment plans, technology plans, cloud solutions, desktops/laptops, IT staffing/salaries, new technologies or applications implemented in 2018 and projects planned for 2019. 12 Pages (NP2252)

REAL-WORLD IT TRENDS. The IT professionals that make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. Real-World IT Trends is a collection of the NOREX Member input captured in the first quarter of 2021 from Virtual Roundtable and WebForum polls. 55 Pages (DT2021-1)

YOUR DATA: 2020 REAL-WORLD IT TRENDS. The IT professionals that make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. Real-World IT Trends is a collection of the NOREX Member input captured in the first half of 2020 from Virtual Roundtables and WebForum polls. 61 Pages (DT2020-1)

YOUR DATA: 2019 REAL WORLD IT TRENDS. The IT professionals that make up NOREX realize the benefits of no vendor bias when analyzing IT polls and trends. Your Data is a collection of the real world member input captured in the second half of 2019 WebForum polls. 36 Pages (DT2019-2)

YOUR DATA: 2019 REAL WORLD IT TRENDS. The IT professionals that make up NOREX realize the benefits of no vendor bias when analyzing IT polls and trends. Your Data is a collection of the real world member input captured in the first seven months of 2019 WebForum polls. 25 Pages (DT2019-1)

CIO: ROLE / JOB DESCRIPTION OF THE CIO TRANSCRIPT. Senior IT leaders discuss the evolution of the Chief Information Officer role during this October 2020 session. 17 Pages (CV076)

CIO: IT'S ROLE IN BUSINESS SUCCESS TRANSCRIPT. Senior IT leaders share strategies for aligning IT with business objectives during this July 2020 WebForum. Topics include cloud computing, staffing, project prioritization and Business Intelligence tool recommendations. 20 Pages (CV075)

CIO: NAVIGATING INTERNATIONAL / GLOBAL IT ISSUES DURING A PANDEMIC TRANSCRIPT. During this CIO call, NOREX Members and guests shared experience and ideas on global office management, particularly in Asia. They discussed differences in products, regulations, firewalls, long distance connectivity, and collaboration tools. 21 Pages (CV074)

CIO: REMOTE WORKFORCE / WORK-FROM-HOME TRANSCRIPT. The benefits and concerns of supporting a remote workforce and a work-from-home program are a hot topic for IT executives. In December 2019, NOREX members discuss experiences, recommendations, policy, tools to support, and general consideration when offering employee remote workforce / WFH programs. 26 Pages (CV073)

CIO: IT TRANSFORMATION TRANSCRIPT. This March 2019 session featured strategic-level discussion on starting the transformation process, gaining executive support, involving business units and developing roadmaps for cloud usage and mobile device management. 19 Pages (CV071)

Emergency Response / Crisis Management

PANDEMIC PREPAREDNESS PLAN. Here is a flexible guide for responding to the problems associated with a pandemic influenza outbreak. 31 Pages (20-859)

PANDEMIC PLAN: ISOLATION GUIDE. This document provides a flexible plan for the isolation of staff in the event of an outbreak of illness such as influenza. 3 Pages (20-858)

SECURITY INCIDENT RESPONSE PLAN. This emergency operations & disaster preparedness plan explores response teams, mitigation, and recovery. 8 Pages (20-732)

INCIDENT REPORT LOG. This document provides the guidelines for the creation, maintenance, management, and secured storage of the Incident Report Log (IRL). 2 Pages (20-350)

INCIDENT RESPONSE POLICY. This document outlines the credit card security incident response policy. 3 Pages (20-280)

CREDIT CARD SECURITY INCIDENT RESPONSE PLAN. The Incident Response Team, comprised of the Controller, the IT Manager, the Facilities Director, the Loss Prevention Supervisor, and the Senior Systems Administrator have established specific guidelines for safeguarding cardholder information. 12 Pages (20-279)

SITUATION MANUAL INSTRUCTIONS. Provided are instructions and tips for customizing each section of the Situation Manual (SitMan) Template. 7 Pages (20-233)

UNPLANNED OUTAGE PROTOCOL. This document establishes communication protocols for staff (and their outside business partners) in the event of an unplanned outage. 5 Pages (20-080)

Incident Management

DISASTER RECOVERY RECORDS RETENTION. This policy provides step-by-step procedures for reducing the risk of service disruption in order to ensure continuity of operations. 2 Pages (20-639)

INCIDENT RESPONSE PLAN. An IRP is a formal roadmap to follow when handling suspected intrusions, system misuse, a cyber incident, or any incident where unauthorized access to confidential information has been detected or suspected. 26 Pages (20-382)

INCIDENT REPORT LOG. This document provides the guidelines for the creation, maintenance, management, and secured storage of the Incident Report Log (IRL). 2 Pages (20-350)

INCIDENT RESPONSE POLICY. This document outlines the credit card security incident response policy. 3 Pages (20-280)

CREDIT CARD SECURITY INCIDENT RESPONSE PLAN. The Incident Response Team, comprised of the Controller, the IT Manager, the Facilities Director, the Loss Prevention Supervisor, and the Senior Systems Administrator have established specific guidelines for safeguarding cardholder information. 12 Pages (20-279)

SYSTEM OUTAGE ROOT CAUSE ANALYSIS. The following is a chart for recording details of a service desk ticket problem and the subsequent Root Cause Analysis (RCA). 2 Pages (20-120)

INCIDENT RESPONSE PLAN. The plan will facilitate the security response and remediation process to ensure the least amount of potential damage to systems, networks, members, and business reputation. 8 Pages (20-098)

UNPLANNED OUTAGE PROTOCOL. This document establishes communication protocols for staff (and their outside business partners) in the event of an unplanned outage. 5 Pages (20-080)

SECURITY INCIDENT RESPONSE PLAN. This response plan describes actions that a company would take after a known or suspected information security incident affecting its technology system(s) and/or data. 18 Pages (20-053)

WEEKLY TREND INCIDENT REPORT. Weekly ITS critical and high incident reports are demonstrated as enterprise-wide and divisional categories. 7 Pages (50-258)

MONTHLY INCIDENT REPORTS. Following are examples of monthly incident reports from various locations for a one to two year period. 15 Pages (50-257)

ITS OUTAGE DASHBOARD. This outage dashboard records critical incidents by count, duration, and cause. 5 Pages (50-256)

INCIDENT RESPONSE PLAN. This document details the procedure to follow when a potential incident is identified. An incident may be a malicious code attack, unauthorized access to systems, unauthorized utilization of services, denial of service attacks, general misuse of systems, or sabotage / theft. 33 Pages (50-252)

Testing

SOW: TESTING. This template logs quality assurance COTS implementation, deliverables, and other aspects of testing. 1 Page (20-506)

TEST TRACKING TEMPLATE. This chart tracks pass/fail and defects when testing. 1 Page (20-497)

MASTER TEST PLAN. The following is a template for a project master test plan, to outline the highlights of all the testing events that will take place during this project. 13 Pages (20-202)

SOW: VULNERABILITY & PENETRATION TESTING. Vulnerability identification and analysis, physical security, authenticated and unauthenticated testing are examined in this SOW. 11 Pages (20-143)

QUALITY CONTROL TEST PLAN. This is a test plan template for a Quality Control (QC) environment. 19 Pages (20-075)