DISASTER RECOVERY / BUSINESS CONTINUITY

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

TO REQUEST A DOCUMENT FROM THIS TOOLKIT, NOTE THE TITLE / NUMBER AND ADD THEM TO THE COMMENTS AREA ON THE REQUEST FORM HERE.

Business Continuity

BACKUP AND RESTORATION POLICY This policy provides a means to actively manage risks associated with data loss by defining a sound backup regime for all data services. 6 Pages (20-1283)

BUSINESS CONTINUITY AND DISASTER RECOVERY POLICY This document defines policy directive on business continuity activities, including planning for all critical business processes and service activities. 7 Pages (20-1282)

BUSINESS CONTINUITY PLAN SIMULATION REPORT This template demonstrates the outcome of annual simulation exercises as part of ongoing maintenance of Business Continuity Plans (BCP). 10 Pages (20-1281)

BUSINESS CONTINUITY PLAN TABLETOP PREPARATION This document is a template of the procedures used during a Business Continuity Plan (BCP) tabletop exercise. 13 Pages (20-1280)

BUSINESS CONTINUITY PLANNING Goals and objectives discussed in this business continuity plan include emergency management, safety plans, property protection, and restoration after an emergency or event. 12 Pages (20-1161)

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)

IT DISASTER NOTIFICATION This is an example of a message used to notify employees of a data center outage. 1 Page (50-389)

Business Impact Analysis

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)

BIA QUESTIONNAIRE The Business Impact Analysis identifies financial and operational impacts to the overall organization resulting from an unexpected outage of critical applications.6 Pages (50-446)

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

BIA QUESTIONNAIRE This questionnaire identifies financial and operational impacts to the overall organization that would result from an unexpected outage of critical applications. 10 Pages (50-429)

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)

APPLICATION RUNBOOK Application description, tech environment, responsible teams, downtime, and recovery are described using a medical application as an example. 6 Pages (50-447)

ENTERPRISE SQL CLUSTER RUNBOOK This runbook describes the Enterprise SQL Cluster application, its technical environment, downtime procedures, recovery plan, and responsible areas. 6 Pages (50-428)

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)

IT DISASTER NOTIFICATION This is an example of a message used to notify employees of a data center outage. 1 Page (50-389)

Incident Management

RANSOMHUB RANSOMWARE PRESENTATION This presentation was given during a NOREX session and is published with the author's permission. 7 Pages (20-1404)

CONTINGENCY PLANNING PROCEDURE The contingency procedure includes what must be done to recover key hardware components that business software and applications require. 3 Pages (20-1300)

INCIDENT RESPONSE PROCEDURE The incident response defined plan will address the seven stages of incident response: preparation, detection, analysis, containment, eradication, recovery, post-incident activity. 4 Pages (20-1299)

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)

Pandemic Plans

COVID-19 PANDEMIC GUIDE This guide provides COVID-19 health and hygiene information and summarizes related policies. 13 Pages (20-940)

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)

COVID-19 RESPONSE TELEWORK SURGE CHECKLIST This document is designed as a quick reference for considering important factors in a teleworking strategy that minimizes downtime and latency. 10 Pages (20- 877)

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)

PANDEMIC BUSINESS CONTINUITY PLANNING STRATEGY This document describes a strategy for sustaining utility operations in the event of an influenza pandemic, based upon previous world pandemic events. This strategy can be updated and applied to potentially pandemic situations. 36 Pages (47-494)

IT PANDEMIC BUSINESS CONTINUITY PLAN This document serves as protection for employees, customers, assets & information, and will minimize restoration time in the event of a pandemic. 28 Pages (47-493)

Safety Guidelines

VISITOR SCREENING TOOL This questionnaire is completed to gain entrance to facilities. It can be kept on file for contract tracing requirements. 1 Page (20-946)

RETURN-TO-WORK GUIDE This guide lists steps and practices for reducing the risk of spreading COVID-19 after returning to the office. 4 Pages (20-945)

RETURN-TO-WORK ORIENTATION This checklist covers health and safety guidelines for returning staff that have been home since the start of the pandemic. 1 Page (20-944)

RETURN-TO-WORK SCREENING To minimize risk of spreading COVID-19, use this questionnaire prior to returning after any absence from work. 2 Pages (20-943)

CERTIFICATION LETTER FOR WORKFORCE TRAVEL This letter certifies the classification of an essential business during the COVID-19 pandemic. 1 Page (20-942)

NOTIFICATION OF INFECTED EMPLOYEE PROCEDURE This policy addresses steps to take in the event that an employee tests positive for COVID-19 and has been in the workplace within 14 days prior to being tested. 5 Pages (20-941)

VISITOR HEALTH QUESTIONNAIRE For employee safety, and in the interest of ensuring a safe and healthy work environment, this questionnaire was developed to help monitor the risk of exposure to COVID-19.
1 Page (20-939)

INTERIM TRAVEL POLICY This policy, created during the COVID-19 pandemic, provides guidance for business travelers to limit exposure and risk. 2 Pages (20-914)

SAFE WORK ACTION MANUAL The Safe Work Action Manual includes practical recommendations, based on guidelines from the Centers for Disease Control and Prevention and World Health Organization, that could be tailored to address various scenarios you may face when returning to work. 32 Pages (20-910)

WORKPLACE PROTECTION AFTER COVID-19 These reminders provide information on cleaning, sanitizing, distancing, and other precautions when returning to the office after the COVID-19 pandemic. 3 Pages (20-907)

SOCIAL DISTANCING HANDOUT These slides provide a definition of social distancing and how it can impact the workplace. 2 Pages (20-906)

CLEANING METHODS This guide discusses the differences between cleaning, disinfecting, and sterilizing materials. 1 Page (20-905)

HEALTH ASSESSMENT POLICY This policy explains one organization's plan for doing temperature scans and health screening for employees entering the office. 2 Pages (50-341)

EMPLOYEE TRAVEL PROTOCOL In response to recommendations by the World Health Organization (WHO) and the U.S. Centers for Disease Control and Prevention (CDC), in addition to recent guidance from government officials, updates have been made to this Travel and Visitors Policy. 2 Pages (50-333)

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)

Transcripts & Polls

CONSTRUCTION INDUSTRY TRANSCRIPT NOREX Members discussed emerging technologies; digital twins; IT / OT; securing Teams; project management; tracking resources; staff availability / time tracking; chargebacks; and budget trends. 16 Pages (NV2556)

DISASTER RECOVERY / BUSINESS CONTINUITY TRANSCRIPT NOREX Members discussed homegrown system vs purchased software / service for DR planning; maintaining a dynamic DR plan; use of the Cloud in DR / BC strategies; documenting system recovery; cybersecurity considerations; Dell Cyber Vault and Veeam; Halcyon and Morphisec; climate change and DR planning; and Nutanix AHV vs VMware. 17 Pages (NV2551)

DOCUMENT MANAGEMENT TRANSCRIPT NOREX Members discussed SharePoint alternatives; OneDrive; MS Power Apps; ChatGPT and Copilot; Cloud options; sending files externally; integrating an in-house ChatGPT; end user documentation; Azure DevOps; incorporating updates into multiple documents; monitoring document access; tracking document changes; and long-term file preservation. 21 Pages (NV2550)

MICROSOFT TEAMS ROOMS TRANSCRIPT NOREX Members discussed Teams Rooms usage and licensing; MTR pricing; transitioning from other platforms; Webex to Teams Rooms; Teams on Windows vs Android; domain vs no-domain join; remote hardware support; general MTR support; hardware recommendations; security considerations; room scheduling; Microsoft Places usage; and reading room hardware. 18 Pages (NV2548)

HEALTHCARE INDUSTRY IT TOPICS TRANSCRIPT NOREX Members discussed the usage of AI; security considerations; Electronic Heath Systems (EHS); use of AI for transcription; utilizing generative AI; dealing with physicians; securing PHI and HIPAA data; and the Heath Insurance Security and Accountability Act (HISAA). 16 Pages (NV2546)

MANUFACTURING INDUSTRY: SECURING OPERATIONAL TECHNOLOGY TRANSCRIPT NOREX Members discussed converting IT and OT; network segmentation; vulnerability tools; patching challenges; vendor control; unmanaged devices; integrating ERP software; data exchange security; and defining operational technology. 18 Pages (NV2541)

FRAUD PREVENTION TRANSCRIPT NOREX Members discussed fraud experiences; fraud incident response plans; strategies for introducing prevention techniques to those outside of finance; new fraud detection tools; validating photo IDs; monitoring tools; hosting providers and standards; managing externally hosted sites; and AI risk prevention tools. 18 Pages (NV2538)

ENDPOINT DETECTION & RESPONSE TRANSCRIPT NOREX Members discussed lessons learned from the CrowdStrike outage; EDR tool requirements and performance; Windows Defender; additional security controls; utilizing multiple EDR tools; Arctic Wolf usage; SIEM usage; security control validation; remote device considerations; and Always On VPN. 19 Pages (NV2528)

RANSOMWARE RESPONSE PLANS TRANSCRIPT NOREX Members discussed ransomware playbooks as a part of or separate from incident response; creating a playbook internally vs outsourcing; testing the playbook; tabletop exercises; and Recovery Time Objective (RTO). 15 Pages (NV2525)

FILE SHARING TRANSCRIPT NOREX Members discussed file sharing options; moving away from local file servers; Azure file shares; hybrid Azure; using multiple vendors; ShareFile usage; backup considerations; Teams guest access; external sharing; VPN alternatives; Google usage; integrating with workflows; and migrating on-prem to Cloud-based SharePoint. 17 Pages (NV2523)

KNOWLEDGE MANAGEMENT TRANSCRIPT NOREX Members discussed effective KM procedures; establishing governance; lifecycle management; creating a KM program; managing a number of knowledge bases; SharePoint Usage; tools; incentivizing employee usage; identifying SMEs; usage of Scribe; and data retention. 15 Pages (NV2521)

IMPACT OF GENERATIVE AI ON THE WORKFORCE TRANSCRIPT NOREX Members discussed introducing GenAI to the organization; where and how GenAI is being piloted and used; Copilot; linking AI products to strategic business goals; build or buy AI solutions; technology setup; Microsoft Purview; projecting proprietary data; AI reshaping / enhancing job roles; AI in data science; and AI in higher education. 18 Pages (NV2516)

MICROSOFT TEAMS ROOMS TRANSCRIPT NOREX Members discussed challenges or limitations encountered; Teams Rooms reliability; equipment experiences and recommendations; domain join vs no-domain join; remote access tools; lag issues; audio issues; echo cancellation; Teams Rooms and Zoom; OneDrive file management; user training; camera policies; Teams updates; and overall satisfaction. 21 Pages (NV2514)

CYBER INSURANCE TRANSCRIPT NOREX Members discussed policy features; cyber insurance landscape; SOC requirements; penetration testing; insurance providers; changing providers; pooled insurance; damage to partner organizations; staffing considerations; merger and acquisition issues; risk analysis; future changes; informational resources; provider questionnaires; and lessons learned. 24 Pages (NV2513)

ENTERPRISE ARCHITECTURE TRANSCRIPT NOREX Members discussed where EA fits organizationally; the role of governance in EA; purchasing / procurement departments; EA related to GenAI; SaaS solutions / contracts; technology reviews; management tools; and EA success metrics. 16 Pages (NV2510)

SERVICE MAPPING FUNDAMENTALS TRANSCRIPT NOREX Members discussed service mapping vs configuration management; implementation experiences; mapping tools; mapping across shared technologies; ServiceNow partners; tag-based mapping; microservices; issues with low-code platforms; working with ServiceNow; differentiating between CIs, services, and dependencies; and integrating with ITSM processes. 13 Pages (NV2506)

DISASTER RECOVERY / BUSINESS CONTINUITY TRANSCRIPT NOREX Members discussed developing DR / BC strategies; DR for VPN / firewall / secure monitoring; on-prem data backups and a Cloud-based copy; DR / BC drills; events at Cloud Service Providers (CSP); BC software; outage events at a SaaS provider; and tools and procedures for stakeholder communication / coordination. 17 Pages (NV2504)

BANKING / FINANCIAL INDUSTRY IT ISSUES TRANSCRIPT NOREX Members discussed compliance issues; regulatory trends; onboarding / offboarding software; AI usage; AI / ML for enhanced customer service; Cloud usage; IT staffing trends; remote work trends; and the impact of AI on IT careers. 15 Pages (NV2503)

DATA ENCRYPTION TRANSCRIPT NOREX Members discussed data encryption pros and cons; implementations; encouraging the use of data encryption in the enterprise; standards; file sharing considerations; encryption in a hyperconverged environment; BitLocker recovery; tools; emerging technologies; encryption issues in China; and USB encryption. 14 Pages (NV2501)

GOVERNMENT IT ISSUES TRANSCRIPT NOREX Members discussed prioritization and budgeting; centralized, decentralized, or hybrid IT departments; out of state FTE positions; publishing the application catalog innovation and new capabilities; M365 governance and communication; managing AI; impact of emerging technologies; Cloud strategy; and disaster recovery and continuity of operations (COOP). 14 Pages (NV2500)

MANAGING TECHNICAL DEBT TRANSCRIPT NOREX Members discussed the definition of technical debt; problems that occur; cleaning up a ServiceNow database; upper-level support; cyber attack risks; strategies to remediate technical debt; budget considerations; security risks; project delivery considerations; and Cloud vs on-prem technical debt. 18 Pages (NV2496)

SECURITY INCIDENT RESPONSE TRANSCRIPT NOREX Members discussed executive support for IR; MDR and cyber insurance vendors; business continuity's role in IR; communication of an event across teams; timing for tabletop exercises; methodology to write an IR playbook; email incident response; and AI and cybersecurity. 14 Pages (NV2491)

RANSOMWARE TRANSCRIPT NOREX Members discussed lessons learned; paying or not paying the ransom; ethical and legal considerations regarding payment; engaging outside assistance; ransomware plan vs cybersecurity plan, immutable backup; early detection; reporting an attack; security and vulnerability assessments; and cybersecurity insurance considerations. 16 Pages (NV2488)

TRANSPORTATION INDUSTRY IT ISSUES TRANSCRIPT NOREX Members discussed cybersecurity practices and tools; automating cybersecurity processes; user training videos; Azure Sentinel; securing personal messenger apps; WhatsApp security considerations; vendor flow; deploying MFA for all types of access; applying security certificates; black box device security; predictive ETA tools; and capturing real-time vehicle data. 14 Pages (NV2486)

SD-WAN TRANSCRIPT NOREX Members discussed SD-WAN pros and cons; deployment; the complexity of SD-WAN; public vs private internet connections; backup strategies; cost considerations; quality-of-service experiences; firewall positioning; P2P traffic performance; VPN connections; vendor selection; Fortinet usage; Cisco vs Meraki; utilizing multiple vendor solutions; Palo Alto; managed services options; SASE; WAN acceleration; and Always On VPN. 19 Pages (NV2483)

MANUFACTURING INDUSTRY IT ISSUES TRANSCRIPT NOREX Members discussed aligning IT with manufacturing processes; the "walkabout" model; implementing an enterprise-wide approach; network segmentation strategies; patching floor systems; Manufacturing Execution Systems (MES); ERP integration with manufacturing processes; authentication for frontline workers; Microsoft Dynamics; and dedicated operational technology. 18 Pages (NV2482)

DISASTER RECOVERY / BUSINESS CONTINUITY TRANSCRIPT NOREX Members discussed where to start with DR / BC; engaging the business and getting business continuity out of IT; raising awareness and participation from the business; mitigating risk for SaaS solutions; multiple backup solutions on prem and in the Cloud; mass communication options; frequency to review and test a plan; COVID's impact on DR / BC planning; and tools to back up network devices. 14 Pages (NV2475)

MERGERS & ACQUISITIONS TRANSCRIPT NOREX Members discussed merger and acquisition experiences and recommendations; acquiring executive consideration for technical issues; M&A planning; managing due diligence; identity federation; migrating Active Directory and Microsoft Forms; platform and cross-platform migration tools; ERP migration; domain access; management software / discovery tools to inventory IT asset inventories; and enterprise reporting platforms. 16 Pages (NV2473)

PRIVACY LAWS TRANSCRIPT NOREX Members discussed privacy law compliance; departments best suited to manage privacy; sources consulted to measure compliance against; developing and keeping current a Record of Processing Activities (ROPA); Privacy Impact Assessments (PIA) tools; NIST CSF core functions; Chief Privacy Officer or Chief Compliance Officer; audit frequency of IT tools to ensure privacy law compliance; leveraging internal audits to evaluate privacy programs; and US federal legislation on privacy laws. 13 Pages (NV2471)

MFA & IDENTITY ACCESS MANAGEMENT FOR ADMINISTRATORS TRANSCRIPT NOREX Members discussed the definitions of MFA, IAM, and PAM; cyber insurance requirements; MFA tools; MFA usage trends; enforcing MFA with M365; MFA for non-admins; MFA for non-service accounts; threat detection and response; automated detection tools; passwordless authentication; phishing resistant MFA; and password vault usage. 21 Pages (NV2468)

GOVERNMENT: CYBERSECURITY TRANSCRIPT NOREX Members discussed significant changes to the cybersecurity program considering the current threat landscape; optimizing the organizational structure; cybersecurity priorities for leadership; AI considerations; accommodating business needs while maintaining effective security; recommended cybersecurity tools; Microsoft tools utilized; G3 M365 licensing experiences; and security frameworks. 14 Pages (NV2463)

CLOUD PHONE SYSTEMS TRANSCRIPT NOREX Members discussed initial cost per user for a Cloud phone system vs VoIP system; Cloud phone providers and moving from a Cisco Unified Communication Manager (CUCM) VoIP system; Teams integration (8x8 vs RingCentral vs others); direct routing vs Cloud-hosted / managed; replacing an older on-prem Mitel system; Dialpad usage; issues with Teams; Operator Connect or direct routing integration with Teams; Vonage Premier unified communications with mobility; all-in-one VoIP / chat / video / mobile solutions for call routing workflows and SMS user requirements; devices on desktop vs softphones; Kari's Law and RAY BAUM'S Act compliance with regard to Cloud Phone Systems; and data ownership and PCI considerations. 23 Pages (NV2460)

IT GOVERNANCE TRANSCRIPT NOREX Members discussed defining and initiating IT Governance; lessons learned; data governance; pain points when starting IT governance; ensuring effective governance; where IT governance sits in the organization; authority to accept or reject proposed governance policies; promoting governance as a value-add; producing policies and guidelines; governing "citizen development"; governance tools; and securing vulnerable legacy systems. 18 Pages (NV2457)

BACKUP / RECOVERY TRANSCRIPT NOREX Members discussed tools used for backup / recovery; issues getting Veeam backups on tape; backing up to the Cloud; cost savings backing up to the Cloud; backup strategies; software / hardware for Linux Ubuntu servers; securing backups from ransomware attacks; testing recovery environments after daily backup; people responsible for overseeing backup / recovery; use of an MSP to perform backups; Recovery Point Objective (RPO) and Recovery Time Objective (RTO); cyber recovery / vault to protect against ransomware; and exercising / updating the cyberattack incident playbook. 17 Pages (NV2453)

HEALTHCARE INDUSTRY IT SECURITY TRANSCRIPT NOREX Members discussed when risk outweighs an operational mandate; managing comprehensive security; successful tool and processes for centralized or almost-centralized security management; state of cybersecurity infrastructure; routine tests to measure cybersecurity readiness; managing outside access requests such as VPN connections, vendor contract workers, etc.; Cloud-hosted EMRs; responding to natural disasters or other emergencies; and best practices for recruiting and retaining talent. 14 Pages (NV2447)

PATCH MANAGEMENT TRANSCRIPT NOREX Members discussed the best tools other than WSUS for patching servers and the time to report after the patch is installed; the level of automation when patching servers; automation tools for patching 3rd-party software besides SCCM; process for manually patching servers / software; enforcing or forcing workstation reboots to ensure updates and patches are applied; efficient patching and vulnerability scan frequency; VDI patching; Linux patching; Ivanti with Intune; and updating hardware drivers. 13 Pages (NV2444)

DISASTER RECOVERY / BUSINESS CONTINUITY TRANSCRIPT NOREX Members practicing / simulating DR and on what schedule; process to determine critical systems for restoration; DR strategy moving from on- prem to Cloud; separating backups from production to protect against ransomware events; steps to review suitability of DR plans for a ransomware attack; mass communications systems in use to notify stakeholders of major incidents; prioritizing processes / applications; and ultimate accountability for DR / BC. 19 Pages (NV2443)

LICENSING / CONTRACT NEGOTIATIONS TRANSCRIPT NOREX Members discussed IT Contract Management vs IT License Management and who should manage each; negotiating renewals and strategies to keep price increases at a minimum; questions to ask a vendor to determine a good deal; 3rd-party services to support negotiations; handling Managed Service Contracts; Service Level Agreements; tools for License and Contract Management; and Non-Disclosure Agreements. 21 Pages (NV2441)

ERP STRATEGIES TRANSCRIPT NOREX Members discussed managing ERP workload across the organization’s teams; running ERP globally; on-prem vs Cloud-hosted, single vs multi-instance, regional support vs central support teams; running multiple unique ERPs and financial considerations; implementing Electronic Data Interchange (EDI); the value of implementing an EDI solution and ERP solution; Dynamics 365 ERP accessing ERP data through the Dataverse; Asset Management features of Dynamics F&O; implementing a WMS; migrating from EBS to another ERP system; SAP ECC to SAP S/4; and keeping inventory in sync between 3PLs and the ERP. 17 Pages (NV2435)

PASSWORD MANAGEMENT TRANSCRIPT NOREX Members discussed NIST password guidelines; verifying users for password reset without using the last four of SSN or employee ID number; critical steps to be taken before rolling out a Password Management solution; enterprise, end-user password solutions (LastPass, 1Password, Keeper, and Dashlane); user adoption of an Enterprise Password Manager; Windows Hello for Business and Beyond Identity for passwordless authentication; utilizing an MFA security thumb key; requiring two-factor or multi-factor authentication; and secure backup strategy. 21 Pages (NV2434)

MULTI-FACTOR AUTHENTICATION / SINGLE SIGN-ON TRANSCRIPT NOREX Members discussed preventing MFA fatigue; minimizing the impact to registration of the users before enabling MFA; passwordless MFA configured through Microsoft Azure by conditional access; applying MFA for service accounts; handling MFA for admins; utilizing PAM solutions and if this will be a requirement for cyber insurance; white glove configuration of new laptops; startup difficulties to retrofit SSO into the existing environment; and adopting SSO for third-party accounts that employees frequently access. 19 Pages (NV2432)

RISK & VULNERABILITY MANAGEMENT TRANSCRIPT NOREX Members discussed conducting a formal vulnerability assessment; prioritizing which aspects of Risk / Vulnerability Management to be managed internally vs contracted out to a MSS vendor; mitigating human resources risk; reporting to executives / application owners; communicating risk to decision makers; policy to patch zero-day, critical, high, medium, or low vulnerabilities; dynamic Asset Management tools; processes used to discover and track vulnerabilities in IT systems; and measuring progress on remediating vulnerabilities. 21 Pages (NV2422)

DISASTER RECOVERY / BUSINESS CONTINUITY TRANSCRIPT NOREX Members discussed organizational roles, responsibilities, and accountability for DR / BC; defined standards; having DR and BC sites on-prem, Cloud, or colocation; DRaaS vendors; backup solutions such as VEEAM, Acronis, and MS Azure; strategies for having both a DR and a BC site; replication software; Oracle; established reusable patterns; incorporating DR / BC plans in architecture reviews; app tiers / categories corresponding to implementation; meeting business requirements for resiliency and performance; and testing disaster recovery plans. 24 Pages (NV2418)

ENERGY / UTILITY INDUSTRY IT ISSUES TRANSCRIPT NOREX Members discussed IT budget trends, applications used to track compliance requirements, tools to analyze historical meter and weather data to determine the performance of behind-the-meter load control programs, leveraging collaboration tools (MS Teams / Slack) to work with 3rd parties, vendor partners, or stakeholders, use of MS Sentinel as both a SIEM and a SOAR, network tap monitoring tools like CyberX and Darktrace, Identity and Access Management initiatives, maintaining utility-owned communications equipment, partnering with outside Incident Response Services, and capabilities in the area of RPA / Automation. 22 Pages (NV2412)

RUSSIA-UKRAINE IMPACT ON CYBERSECURITY TRANSCRIPT NOREX Members discussed trusting the resiliency of government and infrastructure security, increase in security metrics due to the war, measuring the risk impact of this event, determining dependencies and risks with overseas vendors, important steps of system hardening, email security vendors, utilizing threat intelligence effectively, preparing executives for worst-case scenarios, Honeypot as a security measure, supply chain attacks, securing Operational Technology environments, and the evaluation and address of risks from ransomware. 22 Pages (NV2410)

CLOUD PHONE SYSTEMS TRANSCRIPT NOREX Members discussed when it makes most sense to invest in a Cloud-based phone system, caveats to Cloud phones, implementing a Cloud phone system in the workplace, call center performance in the Cloud, handling contact center outages, using Microsoft Teams as a Cloud phone system, 8x8 offerings, combining Zoom telephony with Teams, call recording capabilities, moving Cisco Call Manager to the Cloud, and Vonage Mobility for desk phones and call forwarding. 28 Pages (NV2406)

IAM: MANAGING INDENTITIES & PROVISIONING TRANSCRIPT NOREX Members discussed lessons learned from implementing an IAM solution, the source of truth for employee information and identity, tools used on MFA privileged accounts, tools for account provisioning for Active Directory / Hybrid 365, IAM tools in use to manage user accounts, staff resources devoted to IAM, and Access Reviews / Certifications. 16 Pages (NV2405)

TRANSPORTATION INDUSTRY IT ISSUES TRANSCRIPT NOREX Members discussed the shortage of drivers, issues with finding and retaining IT workers, addressing cybersecurity risk, types of digital investments being made, managing the 3G February / March sunset dates and asset tracking, implementing Snowflake for a data warehouse solution using Azure Data Factory for ELT / ETL, solutions for source control, data dictionary, glossary of terms while following DevOps best practices, and increased infrastructure and maintenance costs. 16 Pages (NV2403)

SECURITY INITIATIVES FOR 2022 TRANSCRIPT NOREX Members discussed the percentage of the IT budget directed to InfoSec, cyber insurance, top 3 security initiatives, implementing a governance framework for accepting risk, GRC tools, best practices to apply security patches on Windows OS, automating / outsourcing cybersecurity processes, MDR services and pen testing, successful tools to protect from malicious web links and sites, VPN requirements, EDR / AI scanners, security strategies, and providing security dashboards to company officers. 28 Pages (NV2401)

MULTI-FACTOR AUTHENTICATION / SINGLE SIGN-ON TRANSCRIPT NOREX Members discussed struggles setting up users with MFA, conditional access policies, minimizing the impact to registration of the users before enabling 2FA / MFA, experiences implementing Duo 2FA, passwordless MFA configured through Microsoft Azure, integrating with Remote Desktop Connection to servers and / or Terminal Server, MFA products for remote access to network (VPN / RDP) and local login, adopting Single Sign-On for 3rd-party accounts, and pain points with implementing OKTA for MFA and SSO. 19 Pages (NV2396)

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 Session. 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 Session. 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 Session. 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 Session. 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 Session. 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 Session, 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 Session. 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 Session. 16 Pages (NV2306)

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 Session. 15 Pages (NV2298)

HELP DESK / SERVICE DESK TRANSCRIPT NOREX Members discuss Help Desk / Service Desk procedures and recommended tracking tools during this November 2019 Session. 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 Session. 10 Pages (NV2289)

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

DOCUMENT MANAGEMENT TRANSCRIPT NOREX members share experiences selecting, implementing and managing Document Management systems during this September 2019 Session. 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 Session. 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 Session. 14 Pages (NV2278)

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

BACKUP/RECOVERY TRANSCRIPT Members share experiences with the leading backup and recovery tools during this May 2019 Session. 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 Session. 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)

SELECT: SERVICENOW TRANSCRIPT NOREX Select Members from Fortune / Forbes 1000 organizations discussed module usage; managing and communicating features and releases; staffing requirements; customization impact; requests requiring multiple organizational pillars; APM considerations; CMDB and CSDM interaction; usage of Automated Test Framework; Release Management Module; use of the employee portal; integration with Microsoft Teams; data extraction tips; usage of archive function; incident response functionality; backup options; ServiceNow Impact Squad; and citizen development implementation. 19 Pages (NS253)

SELECT: BUSINESS CONTINUITY & RESILIENCY TRANSCRIPT NOREX Select Members from Fortune / Forbes 1000 organizations discussed establishing business continuity tiers; defining and measuring application resiliency; processes to add / remove applications from the DR plan; applications with SaaS dependencies; frequency to perform DR / failover exercises; strategies to strengthen application operational resiliency; and dedicated remote business continuity sites. 14 Pages (NS251)

SELECT: RISK & VULNERABILITY MANAGEMENT TRANSCRIPT NOREX Select Members from Fortune / Forbes 1000 organizations discussed including SLAs in a strategic approach; prioritizing vulnerabilities; tracking tools; identifying shadow IT; measuring program effectiveness; internal communication; emerging threats; and communicating risk to senior management. 12 Pages (NS250)

SELECT: MANAGING TECHNICAL DEBT TRANSCRIPT NOREX Select Members from Fortune / Forbes 1000 organizations discussed the definition, management, and communication of technical debt; how to identify, surface, and prioritize TD; risk as an assessment; using employee retention as leverage; management in the Cloud vs on-prem; IT in the enterprise hierarchy; and balancing TD and product development. 15 Pages (NS247)

SELECT: SECURITY INCIDENT RESPONSE TRANSCRIPT NOREX Select Members from Fortune / Forbes 1000 organizations discussed developing an incident response plan; incident communication tips; tabletop exercise recommendations; usage of an incident response service provider; business continuity tool recommendations; post-breach activity; third-party security monitoring; and incident response playbooks.
13 Pages (NS243)

SELECT: IT GOVERNANCE TRANSCRIPT NOREX Select Members from Fortune / Forbes 1000 organizations discussed initiating a governance process; the scope of IT Governance; defining IT Governance; decision makers and how decisions are made; establishing governance standards; IT Governance tools; Change Management considerations; maintaining process; and dealing with a less-rigid planning cycle. 13 Pages (NS238)

SELECT: DISASTER RECOVERY / BUSINESS CONTINUITY TRANSCRIPT NOREX Select Members from Fortune / Forbes 1000 organizations discussed raising awareness and participation on BCM and IT DRP; integrated or separate DR / BC plans; DR strategy when moving from on-prem to the Cloud; leveraging BIAs for funding and support; validating BIAs to ensure system restoration and resilience are addressed; maintaining a holistic organizational view on prioritization to determine which systems are critical for restoration; separate backups to protect against ransomware events; air gapping backups from production; mass communications systems in use to notify stakeholders; high-level testing of DR / BC plans; and testing system restoration. 18 Pages (NS229)

QUICK POLL RESULTS: SOFTWARE TOOLS In January 2025, 85 NOREX Member organizations responded to a poll regarding software tools. The categories included Artificial Intelligence, Disaster Recovery / Business Continuity, Document Management, Enterprise Data Storage, IT Service Management, Network Management, Security, and VDI. 6 Pages (NP2557)

QUICK POLL RESULTS: IT STAFFING & BUDGETING 2024 In October 2024, 112 NOREX Member organizations responded to a poll regarding IT staffing & budgeting. Questions included organization's total revenue, IT staff size, IT staff dedicated to cybersecurity, employee and customer end-users supported, 2025 IT staff size, salaries and budget compared to 2024, IT staff size as a percentage of the organization's overall staff size, and 2025 IT budget as a percentage of the organization's overall budget. 7 Pages (NP2537)

QUICK POLL RESULTS: CYBERSECURITY In June 2024, 107 NOREX Member organizations responded to a Cybersecurity poll. Questions included where cybersecurity resides, framework, anticipated IT security budget for 2025, percent of revenue your IT security budget represents, IT staff dedicated to cybersecurity, vendors used for security assessments, MFA / Two-factor authentication requirements, MFA solutions used, status of cybersecurity insurance, phishing test frequency, and security awareness or phishing training modules used. 7 Pages (NP2524)

THE VALUE OF AN INCIDENT RESPONSE PLAN This Member Presentation was given by an IT Project Manager with over 39 years of experience in IT positions, including Developer, Applications Manager, Project Manager, Consultant, and IT Director. He discusses lessons learned as his org recovers from a RansomHub threat actor attack. 23 Pages (MP002)

CYBERSECURITY FRAMEWORKS This Member Presentation describes a cybersecurity framework as an essential tool that helps organizations to better manage, improve, and maintain their cybersecurity systems. 19 Pages (MP001)

IT TRENDS 2024 Q4 IT Trends is a collection of the NOREX Member input captured in the fourth quarter of 2024 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 37 Pages (DT2024-4)

IT TRENDS 2024 Q3 IT Trends is a collection of the NOREX Member input captured in the third quarter of 2024 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 24 Pages (DT2024-3)

IT TRENDS 2024 Q2 IT Trends is a collection of the NOREX Member input captured in the second quarter of 2024 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 28 Pages (DT2024-2)

IT TRENDS 2024 Q1 IT Trends is a collection of the NOREX Member input captured in the first quarter of 2024 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 32 Pages (DT2024-1)

IT TRENDS 2023 Q4 IT Trends is a collection of the NOREX Member input captured in the fourth quarter of 2023 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 25 Pages (DT2023-4)

IT TRENDS 2023 Q3 IT Trends is a collection of the NOREX Member input captured in the third quarter of 2023 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 22 Pages (DT2023-3)

IT TRENDS 2023 Q2 IT Trends is a collection of the NOREX Member input captured in the second quarter of

2023 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 36 Pages (DT2023-2)

IT TRENDS 2023 Q1 IT Trends is a collection of the NOREX Member input captured in the first quarter of 2023 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 45 Pages (DT2023-1)

IT TRENDS 2022 Q4 IT Trends is a collection of the NOREX Member input captured in the fourth quarter of 2022 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 37 Pages (DT2022-4)

IT TRENDS 2022 Q3 IT Trends is a collection of the NOREX Member input captured in the third quarter of 2022 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 44 Pages (DT2022-3)

IT TRENDS 2022 Q2 IT Trends is a collection of the NOREX Member input captured in the second quarter of 2022 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 43 Pages (DT2022-2)

IT TRENDS: 2022 Q1 IT Trends is a collection of the NOREX Member input captured in the first quarter of 2022 from NOREX event polls. The IT professionals who make up NOREX realize the benefits of no-vendor bias when analyzing IT polls and trends. 57 Pages (DT2022-1)

CIO: AI & PREDICTIVE ANALYTICS TRANSCRIPT NOREX Members discussed achieving quick wins; educating the workforce for usage; using AI for planning and IT roadmaps; utilizing AI for predictive analytics for the enterprise; data strategies for usage on smaller IT teams; and bias in modeling. 13 Pages (CV088)

CIO: ALIGNING BUSINESS & TECHNOLOGY PLANNING TRANSCRIPT NOREX Members discussed stakeholder involvement in planning; usage of a steering committee; technology roadmap tools; capability mapping; consultant involvement; organizational considerations; business-led ERP implementation; steps to achieve IT objectives; digital transformation and ChatGPT usage; cyber training for leadership; retaining staff; and transferring IT leadership. 17 Pages (CV083)

CIO: IT BUDGETING & PLANNING FOR 2022 TRANSCRIPT NOREX Members discussed projecting vendor price increases, cybersecurity goals aligning with legal and cyber insurance needs, percentage of IT budget to overall budget, success stories to acquire more funding and staff, the cost to move to the Cloud, software, infrastructure, and platforms when moving to the Cloud, leveraging ARPA funding in 2022, mid-year reviews to analyze spending, determining the optimal size for an IT organization, critical-success criteria, and measuring productivity of software developers in an Agile Scrum environment. 24 Pages (CV078)

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 Session. 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)