Simplified Security & Compliance

Compliance-as-a-Service Guidebook

Xceptional Networks
10089 Willow Creek Road, STE 100
San Diego, CA 92131
(858) 225-6230
info@Xceptional.com

"Xceptional's team impressed us with their thoroughness, attention to detail, and level of commitment. They went above and beyond, providing key solutions at every turn with a can-do attitude."

- Michael Limber, Project Manager, Secura Bio

© 2021 Xceptional Networks, Inc. All Rights Reserved.

Increasing Compliance, Cost, and Complexity

According to the Chubb Cyber Index the Healthcare, Manufacturing, Business Services, Public Sector, Education, and Information Technology industries have all experienced between 200% and 3000% growth in cyber-incidents and attacks over the last 24-36 months.

The growing number of cyber-attacks and data breaches across multiple industry segments is driving greater regulatory oversight and rule changes that result in additional operational, management and reporting costs on organizations operating within or servicing regulated industries.

As of May 2021, there were over 58 regulatory actions under review by the U.S. Federal Government according to The Office of Information and Regulatory Affairs website. Once these new actions are implemented, organizations across multiple industries will be required to invest more time, money, energy, and effort to adhere to these new actions.

Healthcare is a heavily regulated industry, yet over the last 5 years hundreds of Healthcare providers have fallen victim to malware, hacking, ransomware, social engineering, and other malicious cyber attacks, so it should be no surprise that 11 of the 51 open regulatory actions that are under review are related to the U.S. Department of Health and Human Services.

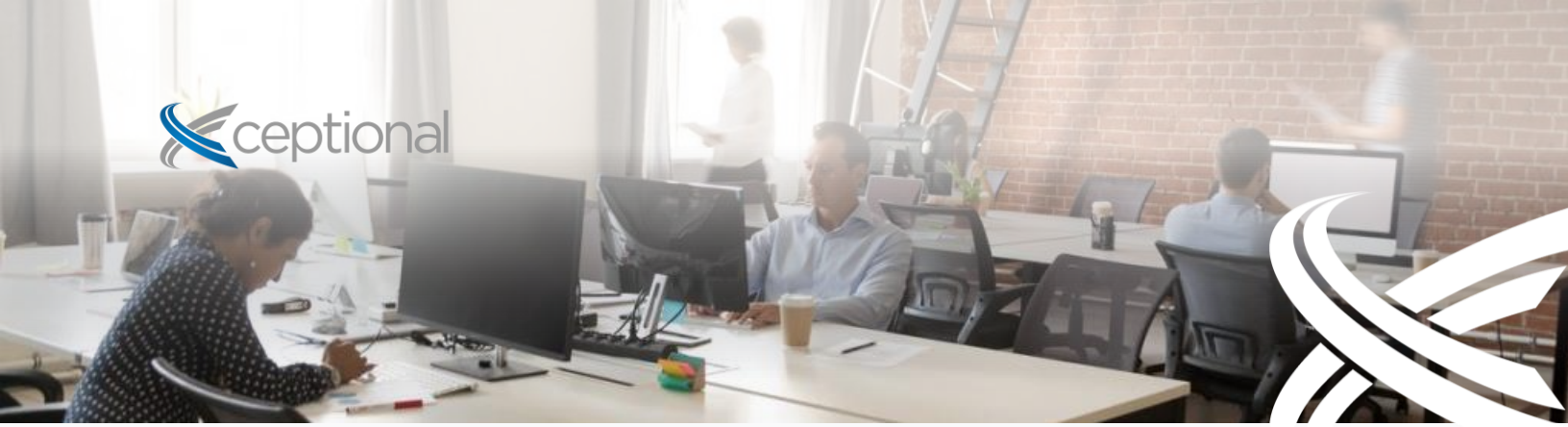
> ***"Managing regulatory change was reported as the top compliance challenge in 2020. 34% of companies report outsourcing some or all of their compliance, up from 28% in 2019.***
>
> *- Thomson Reuters Cost of Compliance 2020 Report.*

The complexity of federal, state, and international regulatory systems have created a significant cost burden on small and medium sized businesses, which account for 99.7% of U.S. companies and over half of private-sector workers.

Small and medium sized businesses pay on average $11,700 per year per employee in regulatory costs, and the costs of regulation on businesses with 50 or less employees are nearly 20% higher than larger companies.

The costs associated with federal regulations on small and medium sized businesses are estimated to total over $40 billion annually according to the US Chamber Foundation.

© 2021 Xceptional Networks, Inc. All Rights Reserved.



Increasing Compliance Demands

According to the 2020 Assent Compliance Report, 88% of companies expect to spend more time on compliance efforts over next three years. This demonstrates companies will require a steady increase in resources to manage compliance programs. At the same time, organizational confidence in meeting compliance demands has dropped from 6.2 to 5.4 (out of 10) over the last 24 months.

Research shows there are 416 million words in state regulations, containing 6.07 million regulatory restrictions. It would take about 23,000 hours, or more than 11.5 years, to read every word of every state regulatory code for the states analyzed.

The average state has 135,000 regulatory restrictions in its administrative rules, but the states vary hugely.

California is the most regulated state, with 395,608 regulatory restrictions; Idaho is the least regulated state, with just 38,961 regulatory restrictions.

The federal code is much larger than any individual state's administrative code, and various industries such as financial services, healthcare, manufacturing, mining, business services, local government, all have multiple industry regulations that must be adhered to.

With the advent of GDPR (an EU regulation that requires businesses to protect the personal data and privacy of EU citizens) and the California Consumer Privacy Act (a state statute intended to enhance privacy rights and consumer protection for residents of California) small and medium sized businesses are under significant scrutiny and pressure to ensure IT systems, applications, and business operations are secure.

Every company is expected to have documented policies and procedures in place, and they must provide evidence that they are handling sensitive customer information according to regulations. Regulations have created a significant burden on organizations, causing a large percentage of companies to outsource compliance related activities, or their compliance program.

© 2021 Xceptional Networks, Inc. All Rights Reserved.

Compliance Manager

Compliance-as-a-Service Introduction

Since 2007 Xceptional has built a reputation as a collaborative, innovative, and proactive Managed IT Services Provider that delivers superior IT, security, and compliance solutions, helping customers to achieve positive business outcomes.

> ***"Xceptional's 'hands-on' approach is ideal for a business with limited or no in-house IT expertise."***
>
> - Julie Barnes, Partner at Jones Barnes LLC

Xceptional's Compliance Manager is a compliance-as-a-service solution that provides quarterly scanning and reporting for various regulations and compliance frameworks such as CMMC, NIST CSF, HIPPA, GDPR, ISO 27001, and Cyber Insurance.

The Compliance Manager solution can be customized to address your unique cybersecurity and compliance requirements, and includes:

- ✓ Annual Subscription for Client
- ✓ Compliance Manager Software Module *(by regulation licensed)*
- ✓ One-time set up support
- ✓ Quarterly Scans
- ✓ Assessment Report
- ✓ 1 Hour Report Review/Recommendations Session
- ✓ Policies, Procedures, Evidence of Compliance Documents *(by regulation licensed)*
- ✓ Additional Supporting Documents and Worksheets

Xceptional Compliance Manager also tracks the implementation of remediation activities and corrective actions, documenting compliance improvements and adherence.

This reduces the risk, cost, and time associated with regulatory compliance management and provides valuable support during the audit process.

© 2021 Xceptional Networks, Inc. All Rights Reserved.

Xceptional Compliance Manager – What's Included

Below is a list of regulations and compliance frameworks that can be included within your Compliance Manager managed services deployment, followed by a summary of what is included within each subscription. **Subscriptions can be purchased ala carte or bundled with another Xceptional Care managed services or Security-as-a-Service solutions.*

Cyber Insurance:

- ✓ Compliance Manager One-time Set Up.
- ✓ Annual Subscription.
- ✓ Cyber Insurance Compliance Manager Software
- ✓ Quarterly Scans
- ✓ Assessment Report Delivery
- ✓ 1 Hour Report Review/Recommendations Session

Reports & Assets Included:

- ✓ Cyber Risk Analysis
- ✓ Cyber Risk Management Plan
- ✓ External Vulnerability Scan Detail by Issue Report
- ✓ Network Assessment Full Detail Report
- ✓ Compensating Control Worksheet
- ✓ Personal Data File Scan Report
- ✓ Response Verification Reports
- ✓ Additional Supporting Documents & Worksheets

GDPR:

- ✓ Compliance Manager GDPR One-time Set Up.
- ✓ Annual Subscription.
- ✓ GDPR Compliance Manager Software
- ✓ Quarterly Scans
- ✓ Assessment Report Delivery
- ✓ 1 Hour Report Review/Recommendations Session

Reports & Assets Included:

- ✓ GDPR Compliance Checklist
- ✓ ISO 27001-213 Auditor Checklist
- ✓ EU GDPR Policies and Procedures
- ✓ ISO 27001 Policies and Procedures
- ✓ Risk Treatment Plan
- ✓ Data Protection Impact Assessment
- ✓ GDPR Evidence of Compliance
- ✓ Additional Supporting Documents & Reports

HIPAA:

- ✓ Compliance Manager HIPAA One-time Set Up.
- ✓ Annual Subscription.
- ✓ HIPAA Compliance Manager Software
- ✓ Quarterly Scans
- ✓ Assessment Report Delivery
- ✓ 1 Hour Report Review/Recommendations Session

Reports & Assets Included:

- ✓ HIPAA Privacy Rule Worksheet
- ✓ HIPAA Breach Notification Rule Worksheet
- ✓ HIPAA Auditor Checklist
- ✓ HIPAA Policies and Procedures
- ✓ HIPAA Management Plan
- ✓ HIPAA Risk Analysis
- ✓ HIPAA Evidence of Compliance
- ✓ HIPAA Risk Analysis Update
- ✓ HIPAA Change Summary Report
- ✓ HIPAA Risk Management Plan Update
- ✓ HIPAA External Vulnerability Scan Detail
- ✓ Additional Supporting Documents & Worksheets

CMMC:

- ✓ Compliance Manager CMMC One-time Set Up.
- ✓ Annual Subscription.
- ✓ CMMC Compliance Manager Software
- ✓ Quarterly Scans
- ✓ Assessment Report Delivery
- ✓ 1 Hour Report Review/Recommendations Session

Reports & Assets Included:

- ✓ NIST 800-171 DoD Assessment
- ✓ Score Report
- ✓ System Security Plan (SSP)
- ✓ Plan of Action and Milestones (POA&M)
- ✓ NIST 800-171 Scoring Supplement Worksheet
- ✓ CMMC Assessor Checklist
- ✓ CMMC Risk Treatment Plan
- ✓ CMMC Risk Analysis
- ✓ CMMC Evidence of Compliance
- ✓ Additional Supporting Documents & Worksheets

NIST CSF:

- ✓ Compliance Manager NIST CSF One-time Set Up.
- ✓ Annual Subscription.
- ✓ NIST CSF Compliance Manager Software
- ✓ Quarterly Scans
- ✓ Assessment Report Delivery
- ✓ 1 Hour Report Review/Recommendations Session

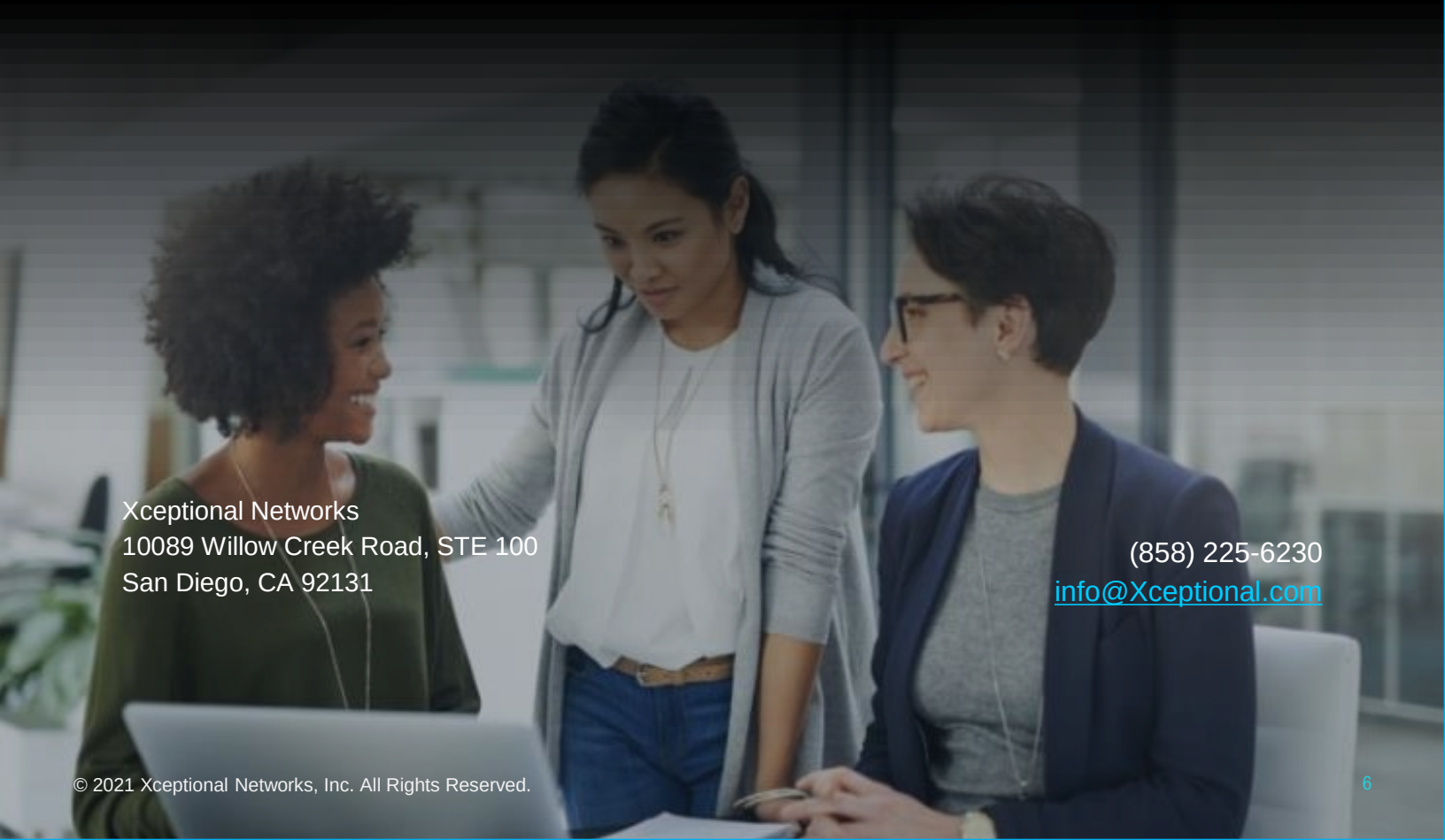
Reports & Assets Included:

- ✓ NIST Auditor Checklist
- ✓ NIST Risk Treatment Plan
- ✓ NIST Risk Analysis
- ✓ Evidence of NIST Compliance
- ✓ NIST Policies and Procedures
- ✓ Additional Supporting Documents & Worksheets

© 2021 Xceptional Networks, Inc. All Rights Reserved.

www.Xceptional.com/managed-it-services/

Contact us today about Compliance Manager or other Compliance-as-a-Service and Security-as-a-Service solutions!



Xceptional Networks
10089 Willow Creek Road, STE 100
San Diego, CA 92131

(858) 225-6230
info@Xceptional.com

© 2021 Xceptional Networks, Inc. All Rights Reserved.