Xceptional

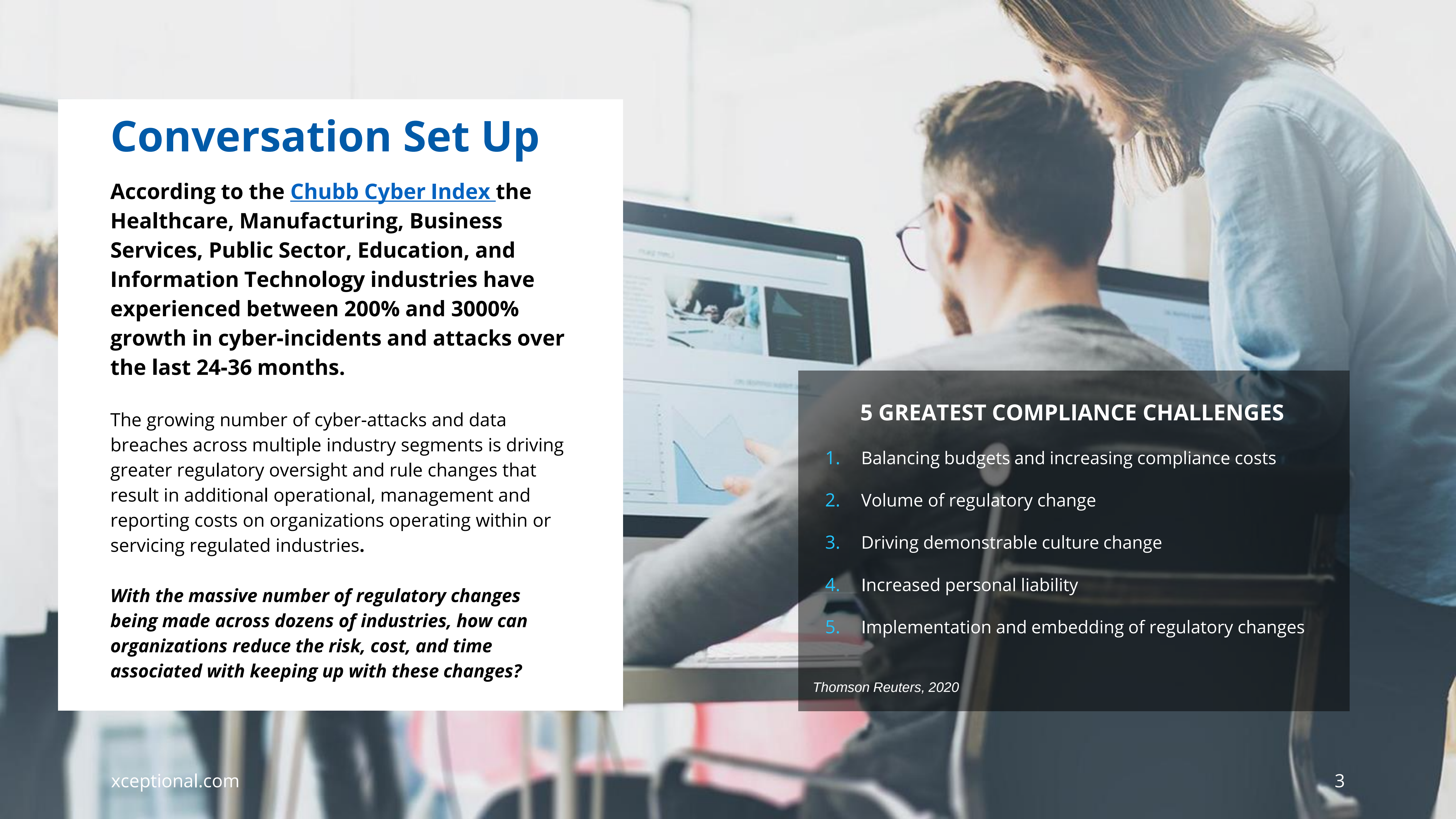
Innovation Webinar Series

COMPLIANCE-AS-A-SERVICE

June 10, 2021

Agenda

- Conversation Set Up
- Market Trends & Research
- Impact of Compliance Demands & Regulatory Actions
- Key Decisions, Options
- Xceptional Innovation: Compliance as a Service



Conversation Set Up

According to the Chubb Cyber Index the Healthcare, Manufacturing, Business Services, Public Sector, Education, and Information Technology industries have 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**.**

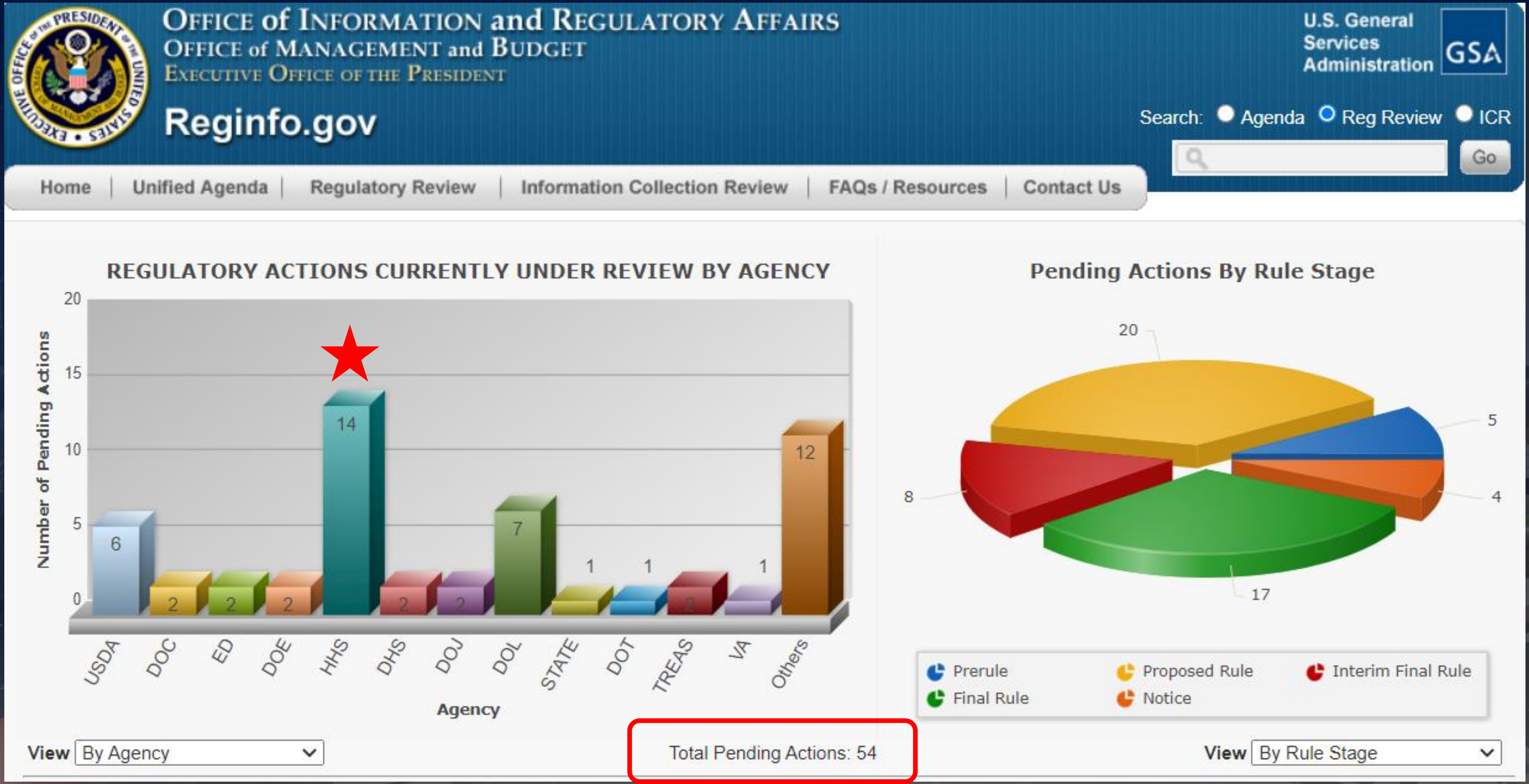
With the massive number of regulatory changes being made across dozens of industries, how can organizations reduce the risk, cost, and time associated with keeping up with these changes?

5 GREATEST COMPLIANCE CHALLENGES

1. Balancing budgets and increasing compliance costs
2. Volume of regulatory change
3. Driving demonstrable culture change
4. Increased personal liability
5. Implementation and embedding of regulatory changes

Thomson Reuters, 2020

The Rate of Change: Reginfo.gov



OFFICE of INFORMATION and REGULATORY AFFAIRS
OFFICE of MANAGEMENT and BUDGET
EXECUTIVE OFFICE OF THE PRESIDENT
Reginfo.gov
U.S. General Services Administration
GSA
Go
Home
Unified Agenda
Regulatory Review
Information Collection Review
FAQs / Resources
Contact Us
REGULATORY ACTIONS CURRENTLY UNDER REVIEW BY AGENCY
Number of Pending Actions
20
15
10
5
0
6
2
2
2
14
2
2
7
1
1
2
1
12
USDA
DOC
ED
DOE
HHS
DHS
DOJ
DOL
STATE
DOT
TREAS
VA
Others
Agency
Pending Actions By Rule Stage
20
5
4
17
8
Prerule
Proposed Rule
Interim Final Rule
Final Rule
Notice

Search: ○ Agenda ● Reg Review ○ ICR

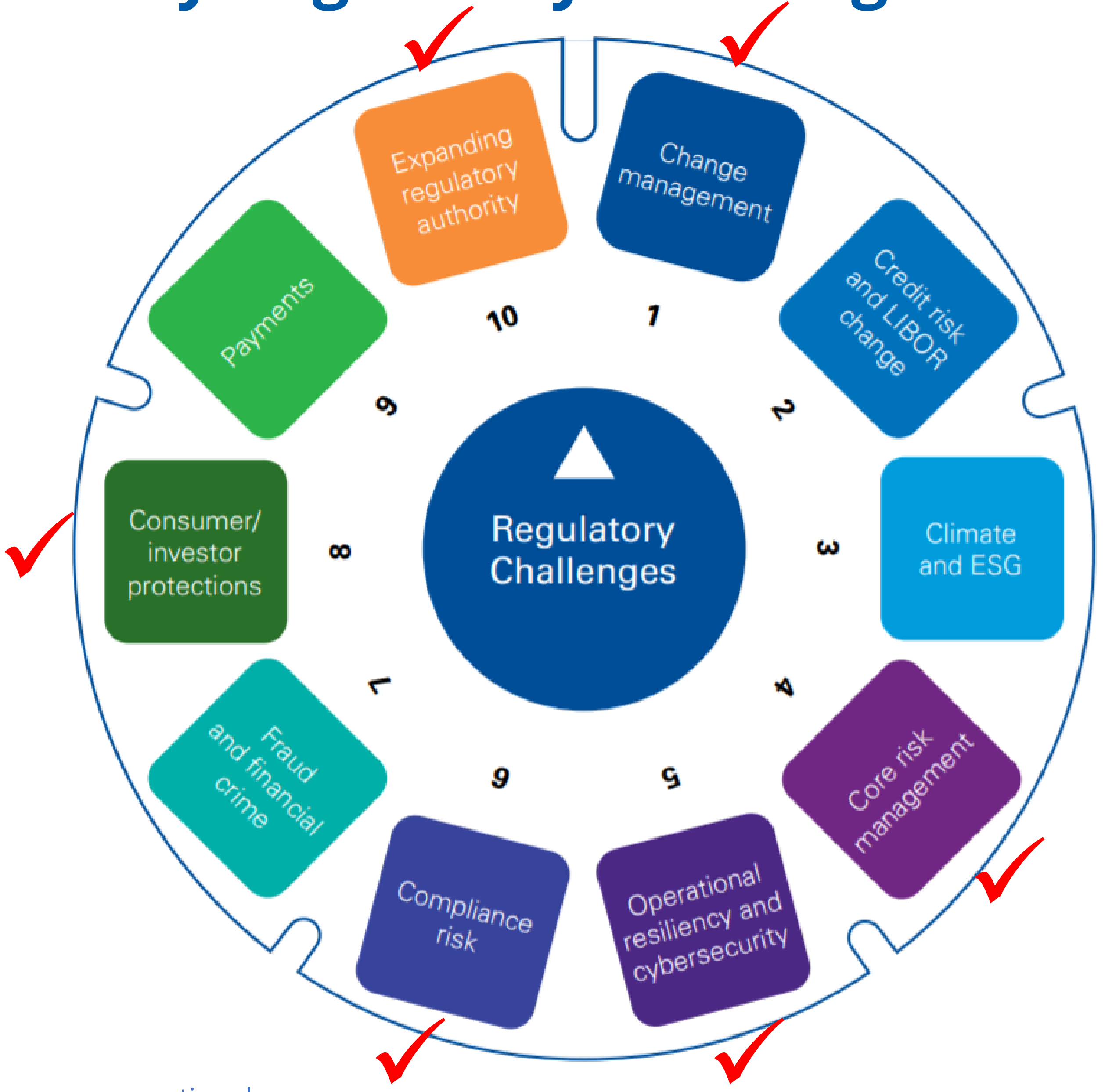
View By Agency

Total Pending Actions: 54

View By Rule Stage

June 9, 2021

10 Key Regulatory Challenges 2021


Regulatory Challenges
1
Change management
2
Credit risk and LIBOR change
3
Climate and ESG
4
Core risk management
5
Operational resiliency and cybersecurity
6
Compliance risk
7
Fraud and financial crime
8
Consumer/ investor protections
9
Payments
10
Expanding regulatory authority
✓
✓
✓
✓
✓
✓

TAKE AWAYS

1. Change management around compliance
2. Volume of regulatory change
3. Driving demonstrable culture change
4. Increased personal liability
5. Implementation and embedding of regulatory changes

KPMG, 2020

Average loss per ransomware attack reported on SARs increased from

$417,000

in 2018 to

$783,000

in 2020. (FinCEN / FBI)

Regulatory Pressure Points:

1. Increased integration and improved operational resiliency, including cyber risk management
2. Outdated risk assessment and resiliency frameworks
3. Closer partnership between the board and business functions to strategically align initiatives
4. Focus on modern technology resilience across platforms, data and applications
5. Expanded cyber and vulnerability threats resulting from increased use of digital platforms, including rapid cloud adoption and software deployment
6. Regulatory focus on proprietary data, customer data, core processes, and exposure from third party vendors and partners
7. Availability of new technologies and tooling; increased focus on IT asset management and the need for a complete and accurate view of IT assets
8. Enhanced integration of cyber risk management with enterprise risk management

Victory Media Research 2021

Top Technology risks to manage

- Software development
- Obsolete technology
- Security of systems and data
- People and skills
- Third party technology and services
- Failed technology strategy
- Services and availability
- Emerging technology
- Data quality and management
- Regulations and compliance

Impact of Compliance Demands & Regulatory Actions on Business

SMBs pay $11,700 per year, per employee on average in regulatory costs.

The costs of regulation on businesses with less than 50 FTEs are nearly 20% higher than larger companies.

The costs of federal regulations on SMBs is estimated to total over $40B annually.

73% of firms believe regulatory changes will increase the personal liability of senior managers.

More than 67% of organizations expect regulatory compliance costs to increase over the next 12 months.

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

https://www.uschamberfoundation.org/smallbizregs/
https://corporate.thomsonreuters.com/Cost-of-Compliance-2020

xceptional.com

> *“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.*

Victory Media Research, Surveys 2020-2021

Compliance Realities on Businesses

30% of financial services firms expect to spend between 5% and 25% of revenues toward regulatory compliance in 2021.

Hospitals with 161 beds pay on average $7.6 million in compliance administrative costs per year.

88% of companies expect to spend more than $1M to achieve & maintain GDPR compliant.

NSBA survey respondents expect to spend $83,019 in the first year of business on compliance.

A report by the Ponemon Institute found that the average cost of compliance for an organization was $5.5 million.

Meanwhile, the average cost of noncompliance was over $14.5 million.

CCPA

The California Consumer Privacy Act is a state statute intended to enhance privacy rights and consumer protection for residents of California.

Growing Enforcement, Penalties (HIPAA, PCI Examples)

HIPAA Violation Type	Civil Penalty (MIN)	Civil Penalty (MAX)
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	**$100 - $50,000** per violation, with an annual maximum of $25,000 for repeat violations	**$59,522** per violation, with an annual maximum of $1,789,651
HIPAA violation due to reasonable cause and not due to willful neglect	**$1,000 - $50,000** per violation, with an annual maximum of $100,000 for repeat violations	**$59,522** per violation, with an annual maximum of $1,789,651
HIPAA violation due to willful neglect but violation is corrected within the required time period	**$10,000 - $50,000** per violation, with an annual maximum of $250,000 for repeat violations	**$59,522** per violation, with an annual maximum of $1,789,651
HIPAA violation is due to willful neglect and is not corrected	**$59,522** per violation, with an annual maximum of **$1,789,651**	**$59,522** per violation, with an annual maximum of **$1,789,651**

https://www.govinfo.gov/content/pkg/FR-2020-01-17/pdf/2020-00738.pdf

https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement#:~:text=Civil%20violations&text=The%20secretary%20is%20prohibited%20from,extended%20at%20HHS'%20discretion).

PCI Violation Month	Merchant Level 1	Merchant Level 2
1 to 3	**$10,000 monthly**	**$5,000 monthly**
4 to 6	**$50,000 monthly**	**$25,000 monthly**
7 and on	**$100,000 monthly**	**$50,000 monthly**

Where and How to Begin…?

1. NIST 800-53: (256 Controls / 18 Families) C
2. NIST CSF: (5 Sections / 22 Categories (Functions) / 98 Subcategories (Outcomes) B
3. CIS 20/CIS RAM: (1-6 Basic / 7-16 Foundational / 17-20 Organizational) A
4. CCPA
5. CMMC (NIST 800-171)
6. FFIEC
7. FINRA
8. GDPR
9. ISO/IEC 27001
10. NCUA/ASET/AIRES
11. NERC-CIP
12. NY Regulation
13. PCI DSS: (6 Sections / 12 Requirements) B
14. HIPAA: (3 Security Safeguard Sections / 18 Categories / 245 Controls) A
15. HITRUST
16. SSAE-18 (16)
17. SOX

Key Decisions, Options

Delay & Denial:
The Highest Risk Option

Templates & Tool Kits:
Confusion, Gaps, Corrective Action

Deflect, Defer:
Proof of Compliance is Still on You

Baby Steps:
Find an Advisor, Get Some Advice

Begin to Act:
Assessments, Gap Analysis, Remediation

Find Cost Effective Solutions:
Find a Partner & Outsource

Victory Media Research, Surveys 2020-2021

Introducing: Compliance Manager

> *"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

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 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
- ✓ 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.

Xceptional Compliance Manager: What’s Included

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

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

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

A sample 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.*

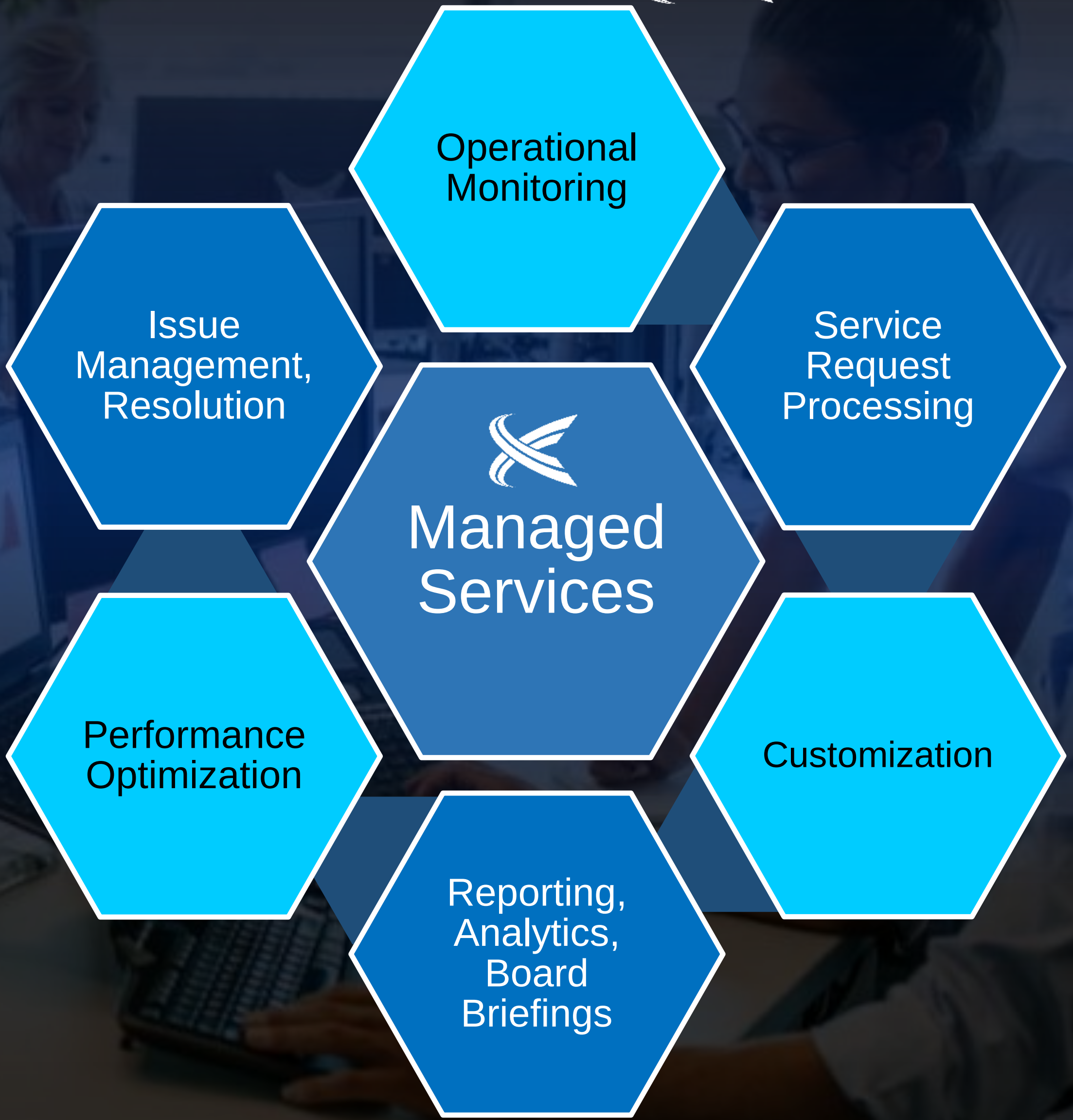
Experience Xceptional Value

Xceptional

Knowledgeable, Proactive, Responsive, Committed

PORTFOLIO OF PROACTIVE MANAGED SERVICES & SUPERIOR IT CONSULTING SERVICES

- Remote and on-site managed services to fit your budget, scheduling, and resource needs: *Managed Desktop, Network, Phones, Applications, Security, Compliance.*
- 24x7 monitoring and support provided by live engineers *that are highly responsive and committed to your business.*
- Virtual CIO: Quarterly Technology Reviews and Reporting Solutions to provide strategic IT planning, *update to current standard levels and ensure specifications are maintained.*
- Advanced IT consulting, advisory, architecture and procurement services to help align IT systems and applications to the business, *or to develop and implement a future IT roadmap and technology strategy that enables business growth.*


Managed Services

Operational Monitoring

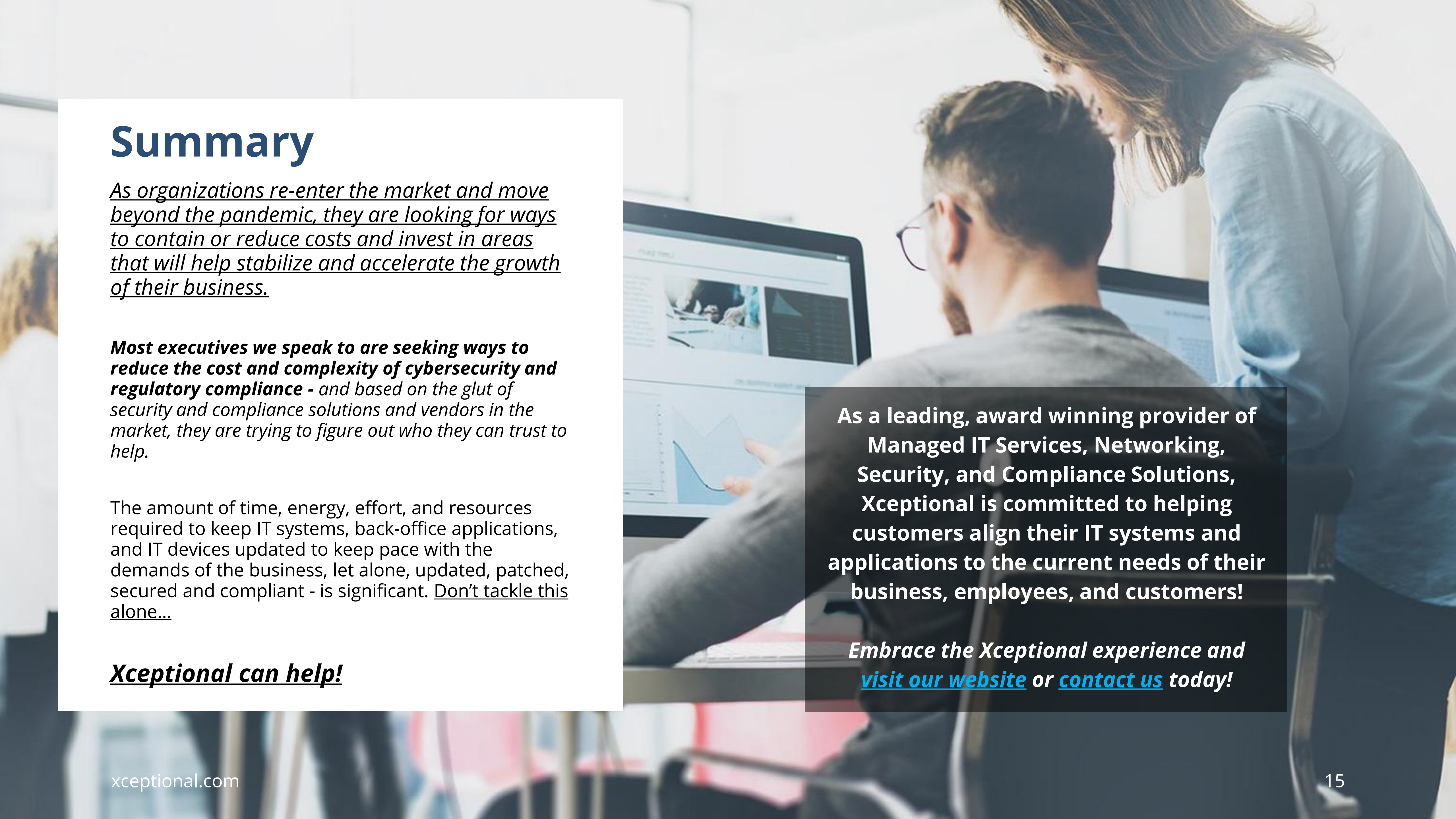
Issue Management, Resolution

Service Request Processing

Performance Optimization

Customization

Reporting, Analytics, Board Briefings



Summary

<u>As organizations re-enter the market and move beyond the pandemic, they are looking for ways to contain or reduce costs and invest in areas that will help stabilize and accelerate the growth of their business.</u>

Most executives we speak to are seeking ways to reduce the cost and complexity of cybersecurity and regulatory compliance - *and based on the glut of security and compliance solutions and vendors in the market, they are trying to figure out who they can trust to help.*

The amount of time, energy, effort, and resources required to keep IT systems, back-office applications, and IT devices updated to keep pace with the demands of the business, let alone, updated, patched, secured and compliant - is significant. <u>Don't tackle this alone…</u>

<u>Xceptional can help!</u>

As a leading, award winning provider of Managed IT Services, Networking, Security, and Compliance Solutions, Xceptional is committed to helping customers align their IT systems and applications to the current needs of their business, employees, and customers!

Embrace the Xceptional experience and <u>visit our website</u> or <u>contact us</u> today!

Xceptional

Thank You!

Visit our **resources page** to access our free eBooks and research!
Request a **complimentary network** or **security assessment**!

xceptional.com | 858-225-6230