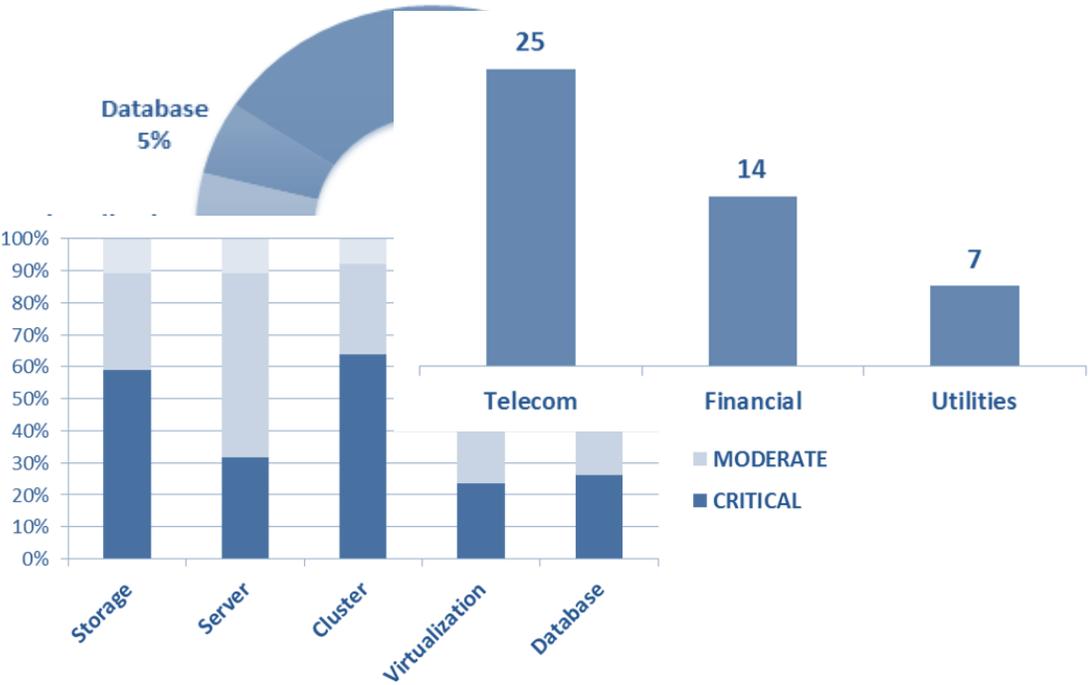


2012 IT Continuity Risk Benchmarks

Presented by



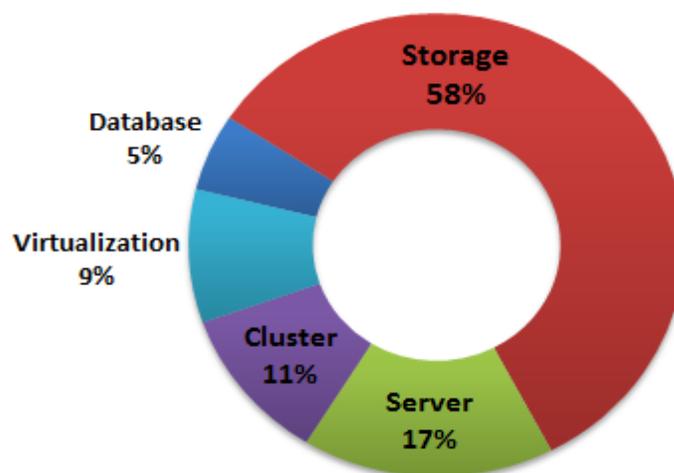
About This Study

The statistics presented in this study are based on data collected using Continuity Software's AvailabilityGuard™, an automated vulnerability detection and monitoring software that scans the entire IT infrastructure and identifies potential downtime, data loss, and performance risks before they impact business operations.

Where Are Risks Found?

Overall, risks to IT business continuity and service availability are most prevalent in the storage layer, followed by the server and cluster layers. The number of HA/DR risks identified in the virtualization layer is relatively low, since most organizations are still shying away from running business-critical application in a virtual environment. As organizations gain more confidence in their cloud implementations, we can expect an increase in the number of applications running in the virtual environment as well as the risks associated with the virtualization layer.

Distribution of Identified Risks by Area



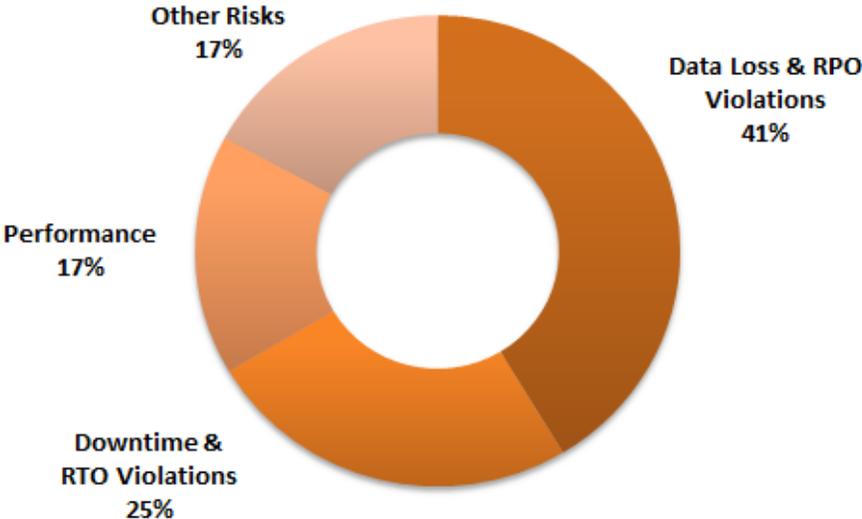
Top 3 Risks by Area

	Storage	Server	Cluster	Virtualization	Database
1	Storage array consistency	Insufficient number of active SAN I/O paths	Cluster components in a bad state	Dead SAN I/O paths	Suboptimal I/O configuration
2	Unauthorized access to storage	Inconsistent HBA configuration	Inconsistent OS properties between cluster nodes	Incorrect storage alignment or tiering	Violation of vendor redundancy best practices
3	RPO SLA violation	Incorrect file system configuration on HA/DR servers	File system management conflicts between the OS and the cluster software	Datstores incorrectly configured on certain cluster nodes	Standby database is out of sync

What Is the Impact of These Risks?

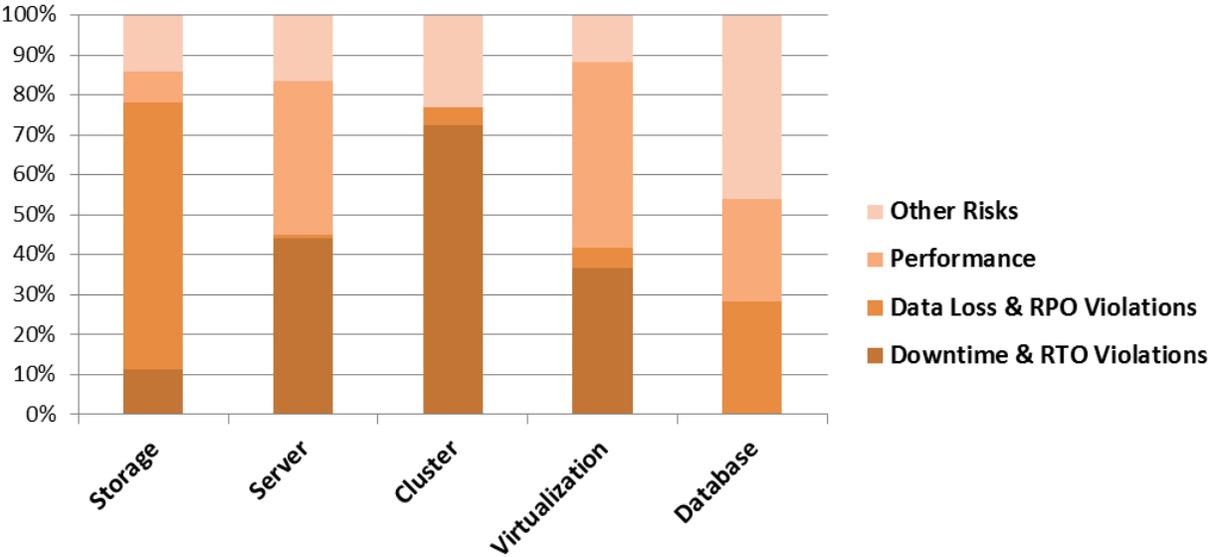
Most issues identified pose a risk of data loss or violation of the company’s RPO (Recovery Point Objective) goals¹, followed by downtime and RTO (Recovery Time Objective) violation risks.

Impact of Risks



As expected, storage issues result mostly in data loss and RPO risks, while server and cluster issues lead mostly to downtime and RTO risks.

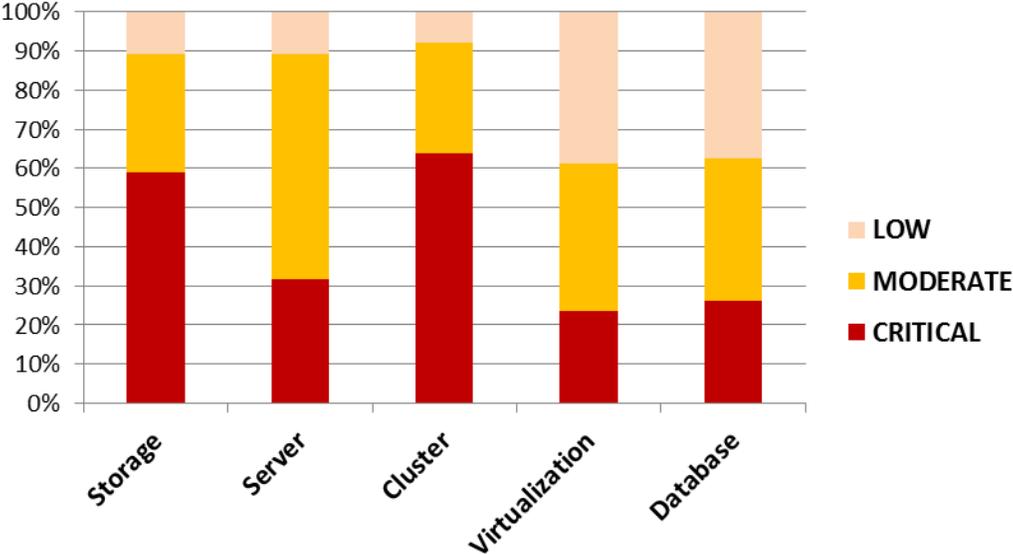
Impact of Risks



¹ The AvailabilityGuard software allows each organization to define and measure compliance with specific RPO goals for each business service.

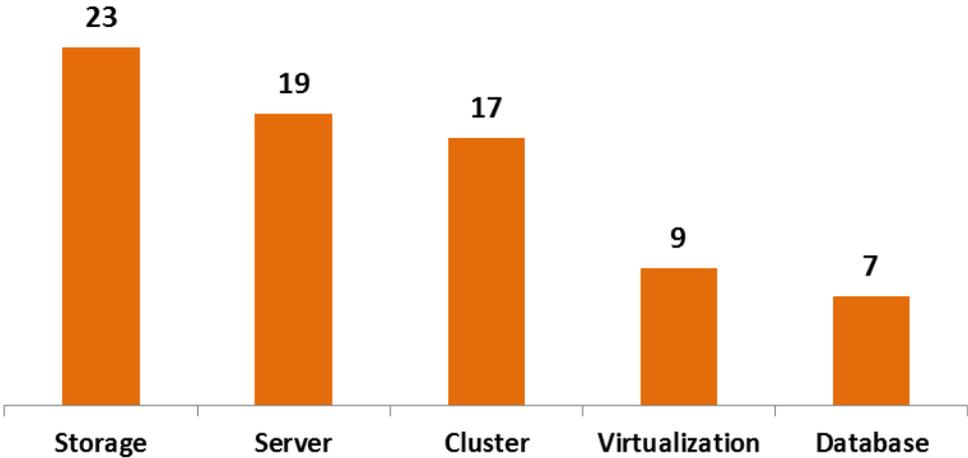
Cluster and storage issues tend to be more critical in nature, while virtualization and database issues tend to have lower levels of risks associated.

Severity of Issues by Area



Storage issues take the longest to resolve, followed by server and cluster issues, while virtualization and database issues are the quickest to resolve.

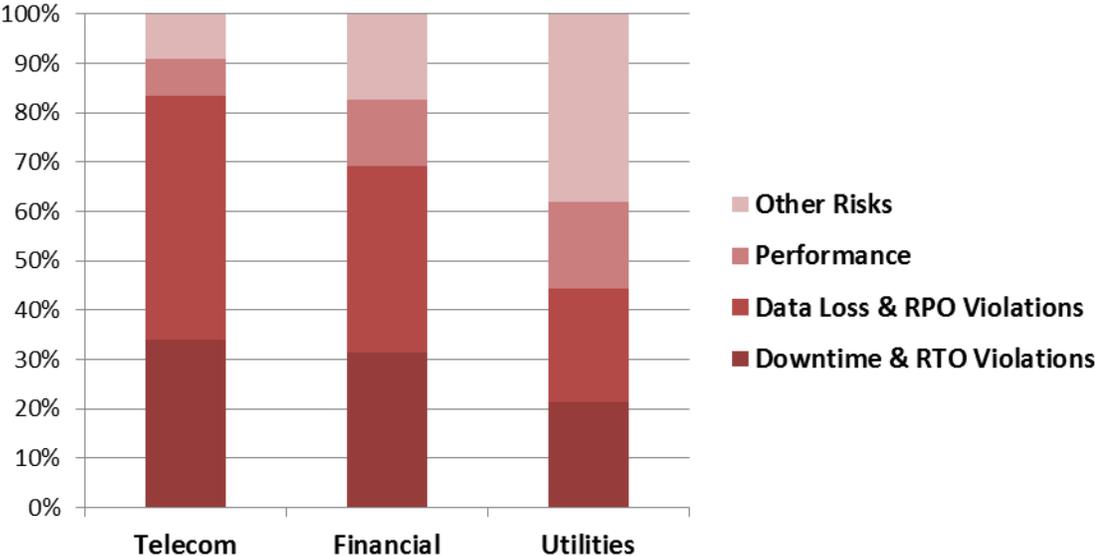
Average Days to Resolution by Area



Which Industries Are Most Impacted?

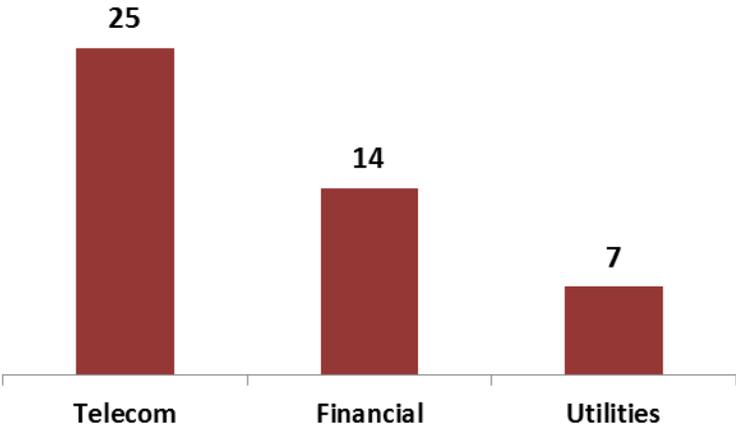
Companies in the telecom and financial services sectors experience more downtime and data loss risks than those in the utilities sector.

Risk Impact by Industry



Even more troublesome is the fact that companies in these sectors take longer to address these critical issues compared to utility providers.

Days to Resolution of Critical Risks by Industry



In Conclusion

Despite ongoing efforts to eliminate IT business continuity and service availability risks, organizations in all sectors still exhibit a significant number of issues that could lead to downtime, data loss, performance degradation, and violations of RPO and RTO.

Maybe even more alarming is the fact that many organizations simply don't know what risks exist in their environment. Lacking the tools to automatically monitor risks on an ongoing basis, these organizations rely on infrequent and incomplete manual tests, limiting their ability to accurately account for and risks that can impact business continuity and service availability goals.

[To see how AvailabilityGuard can help you identify the vulnerabilities that can put your organization at risk, sign up for a 24-hour assessment of your environment.](#)

Disclaimers and notices

The results presented in this publication are based on a limited data set and are not warranted to accurately represent any data beyond the data set used.

This publication is subject to change without notice. While every precaution has been taken in the preparation of this publication, Continuity Software assumes no responsibility for errors or omissions.

No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, photocopying, recording or otherwise, without prior written consent of Continuity Software.

Copyright © Continuity Software Inc. All rights reserved.