CENSINET®

How Intermountain Health Went From "Managed Chaos" to Strategic Cyber Risk Management

Intermountain Health

About Intermountain Health

Intermountain Health is the largest nonprofit health system in the Intermountain West, with 34 hospitals, 400 clinics, and 3M+ telehealth patients served. Based in Salt Lake City, Intermountain serves patients and communities in Utah, Idaho, Nevada, Colorado, Montana, Wyoming, and Kansas.

Matt Christensen, CISSP, CRISC, CFE

Sr. Director - Governance, Risk, & Compliance
Intermountain Health

Managing Risk with 'Rows & Columns'

Like many healthcare organizations, Intermountain Health did the best they could with the resources they had managing third-party and enterprise risk. With a heavy reliance on spreadsheets and a healthy stack of Post-It Notes®, managing cyber risk was highly manual, time consuming, and simply not scalable. Not surprisingly, risk management efforts were held back by:

- **Subjective risk evaluation –** Managed risk on intuition and what *seemed* risky, which was highly inconsistent across the team.
- **Lack of standardization –** Had no standardization or automation of repeatable processes, creating significant inefficiencies.
- **Data integrity & audit issues –** What happens if the spreadsheet gets lost, cells are locked, or the team is working off an old version?

> **"Managing risk was recognized, acknowledged, and managed chaos."**

Searching for a New Solution

Fed up with this approach, Intermountain sought out a new cyber risk solution. This was more challenging than anticipated, as the vast majority of solutions they encountered forced them to make undesirable trade-offs and fell short of expectations, including:

- **Not healthcare specific –** Pan-industry solutions weren't designed to solve the unique challenges faced by the health sector.
- **Required too much configuration –** Even with training, many solutions made managing cyber risk even more complex and convoluted.
- **Too broad or too technical –** Solutions were either too broad to address specific issues, or were too technical with endless data fields.

> **"Healthcare is the most complex industry...You can't just take a tool and apply it to healthcare if it wasn't built specifically <u>for</u> healthcare."**

Intermountain Health

Why Censinet?

After evaluating many solutions, Intermountain ultimately decided to choose Censinet:

- **Purpose-built for healthcare –** Censinet was the only solution that addressed both Intermountain's needs and healthcare's unique risks and complexities.
- **IRB assessments –** With research representing a large part of the business, Censinet and Intermountain worked together to streamline and automate an assessment process that all stakeholders can collectively benefit from.

"Censinet has been an amazing partner not just to listen, but to act."

HELPING TO SERVE THE BUSINESS AND PATIENTS BETTER

❝ With Censinet, we spend less time 'documenting risk', and more time *actively managing risk* to help the business make better decisions.

— Matt Christensen, Intermountain Health

Censinet's Broad Impact at Intermountain

65% reduction in time to complete third-party risk assessments, and IRB assessments now completed in days, not weeks.

Significantly stronger executive engagement due to benchmarking – How do we compare to peers on enterprise cyber maturity and investment levels?

Tighter collaboration between Cybersecurity and Supply Chain to **simplify vendor procurement and onboarding** powered by a faster risk assessment process.

Leveraging risk tiering (based on vendor's potential impact to the business) to **automatically schedule and complete reassessments.**

Contact Us Today!

To learn more about Intermountain's journey and how Censinet can transform cyber risk management at your organization, please contact info@censinet.com.

Censinet is an American Hospital Association Preferred Cybersecurity Service Provider for Cyber Firm Risk Management and Information Governance and Cyber Risk Assessment, Privacy and HIPAA Compliance.