White Paper
Data Center
July 2023

IT@Intel: Data Center Facilities Risk Management

By performing a deep-dive data center audit and applying Information Technology Infrastructure Library (ITIL) principles to data center components, Intel IT is optimizing investment and lowering risk of data center incidents and downtime

Authors

Raj Kambar
Data Center Manager, Intel IT

Aengus Nolan
Data Center Manager, Intel IT

John Reggio
Facility Engineering Manager, Corporate Services

Peter Sullivan
Data Center Manager, Intel IT

Michelle Vincenti Urpi
Global Data Center Facilities Principal Engineer, Intel IT

Table of Contents

Executive Summary 1
Business Challenge 2
Solution 2
Using ITIL to Inform the Data Center System of Record 2
Conducting a Street-to-Server Audit 3
Results 6
Next Steps 7
Conclusion 7
Related Content 7
Appendix: Excerpt from Data Center Street-to-Server Audit Report 8

Executive Summary

Intel IT Intel's 54 data center modules located around the globe power Intel's design, office, manufacturing and enterprise business domains—they are the heartbeat of Intel's continued innovation. Intel IT has recently improved how we approach data center facilities risk management, using a unique combination of processes, data and visibility:

- We adopted the Information Technology Infrastructure Library (ITIL) for incident, problem and change management.
- We developed and conducted a global data center audit that probed every aspect of every data center.
- We designed a custom dashboard that provides us with a data center heat map of data center incidents.

Using these processes, data and tools enables us to intelligently prioritize data center risk mitigation efforts and focus investments on problems with the most business impact. Over the last four years, these efforts have enabled us to lower overall data center risk by 50%. We hope that by sharing our best practices, we can help other IT departments take a fresh look at data center risk management.

Intel IT Contributors

John Pereira, Director, Data Centers & Hosting
Jeff Sedayao, Domain Engagement Manager
Mario Villalta, Domain Engagement Manager

Acronyms

EPO	emergency power-off
ITIL	Information Technology Infrastructure Library
RPN	risk priority number
UPS	uninterruptible power supply

Business Challenge

Intel has 54 data center modules located globally, with nearly 400,000 servers to support the needs of Intel's design, office, manufacturing and enterprise users. Keeping Intel's data centers running with maximum uptime to support Intel's business is one of Intel IT's most important jobs. But of course, we also want to optimize our investment decisions to manage infrastructure costs. We also need to ensure that we maintain a close relationship between global Intel IT and the Corporate Services organization (which manages electrical and mechanical facilities) to successfully manage uptime of data centers, including incident response time and driving strategic improvements.[1]

Nearly a decade ago, we adopted the Information Technology Infrastructure Library (ITIL) framework's change management, incident management and problem management modules for tracking data center issues. Our data center system of record contains thousands of entries relating to data center health. However, in 2016 and 2017, instability in data center facilities showed that there was an opportunity to understand potential risks within our data centers at a much deeper level. Even though we had a good framework, we needed to be less reactive and more proactive. We required even more data to inform data center investment decisions.

Intel IT works in tandem with Intel's facilities management group, called Corporate Services, to maintain Intel's data centers. Intel IT is responsible for keeping the hardware (such as servers and networks) up to date and aligned to Intel's business needs across the design, office, manufacturing and enterprise domains. Corporate Services maintains cooling equipment, power distribution, generators and uninterruptible power supply (UPS) systems, and other facility equipment. Roles and responsibilities are governed by an operational-level agreement between the two organizations.

Solution

We have taken a unique approach to reducing the risk of severe data center incidents and downtime by:

- Developing a detailed technical facilities infrastructure audit that can determine possible design and maintenance gaps. This included:
  - Auditing all Intel data centers worldwide with a standardized procedure.
  - Comparing findings for all sites to identify commonalities and highest priority issues.
  - Presenting top priority issues to management for funding approval and implementation of recommended solutions.
- Using the ITIL problem management module on our IT system of record so we can incorporate data center audit findings within a single system and enable easy overall analysis.

Together, these advances in our approach to data center risk management inform rational, data-driven decisions about what to upgrade and when.

Using ITIL to Inform the Data Center System of Record

ITIL is an IT service management framework that outlines best practices for delivering IT services. It is usually used for large-scale IT asset and service management (such as managing software upgrades and client devices). Intel IT DevOps teams have used the ITIL framework for many years, reaping the following benefits:

- Transparency
- Standardization
- Cost-efficiency
- Strategic alignment with the business
- Organization change management

About 10 years ago, we adapted portions of the ITIL framework for data center risk management—an innovative way to manage facilities. We applied the change management, incident management and problem management ITIL modules to cooling units, generators, UPS systems, servers, cables and so on. In ITIL parlance, these would be called Configuration Items—the individual units or components that we are tracking. This ITIL-inspired approach enabled us to think about incident management as "data center as a service." It also enabled us to speak the same language as the rest of IT by translating electrical/mechanical engineering terms into more familiar language.

The remainder of this section describes how we use ITIL for data center management.

[1] The scope of this paper focuses on managing risk in data center facilities. Information security, such as dealing with risks associated with software applications, is out of scope for this paper.

Change Management Module in the Data Center

ITIL defines the change management module as information for tracking "the addition, modification or removal of any authorized, planned or supported service or service component that could affect IT services."[2] In the data center system of record, we use the change management module to track and record everything that is happening in, or to, the data center Configuration Items.

In the data center context, "changes" include the following:

- Scheduled maintenance (regular, based on a schedule), such as refreshing servers or regular preventative maintenance on cooling units
- Corrective maintenance (something has broken), such as repairing a UPS
- All changes occurring to the Configuration Items that we have defined (cooling units, UPS, cables and so on), such as adding new cabling

All changes are reviewed and approved in advance, so we know what is happening, when it is happening and that it is happening in the right way, with the right procedures and the right personnel performing the change.

Incident Management Module in the Data Center

ITIL defines the incident management module as information for tracking "an unplanned interruption to a service, or reduction in the quality of a service."[3] In the data center system of record, we use the incident management module to track any event that occurs in our data center facilities that we are not expecting. For instance, a cooling unit could fail, causing several servers to overheat. As another example, a UPS system could fail, leading to a loss of power or transfer to utility power for IT systems.

We categorize incidents depending on their severity (business impact):

- Minor impact: No impact to the end customer (for example, redundancy has prevented any servers from failing)
- Major impact: There is some level end-user impact (for example, one or more servers has crashed, or even the entire data center has gone offline)

We use a severity scale that scores the business impact so we can see the actual impact to our end users and to Intel's business (see Table 1).

Table 1. Business Impact Score

Score	Level of Severity
4	Entire data center facility
3	Cabinet row, group of cabinets; damage to critical equipment
2	Single cabinet, or single server within cabinet; slight annoyance
1	No impact

Problem Management Module in the Data Center

ITIL defines the problem management module as information for tracking "a cause, or potential cause, of one or more incidents."[4] When we originally adopted ITIL for data center risk management, we informed our problem management module only with data and risks that arose out of incidents—meaning that the risks were being identified retrospectively following incidents. Subsequently, as we continued to develop our processes, we began to use the problem management module for both reactive and proactive information:

- Reactive records: We determine the root cause of an incident and what actions are needed to ensure it doesn't reoccur.
- Proactive records: Findings from a data center audit (see the next section), where something is wrong but has not yet caused an incident. Examples of these types of problems in the data center include equipment that has reached end of life, a UPS battery monitoring system is not working or fire extinguishers are not charged.

Adopting the ITIL framework—including all three management modules—was foundational to allowing us to move on to more proactive data gathering. It enabled us to capture, track and act on data in a structured way.

Conducting a Street-to-Server Audit

Operational data center audits are not new for Intel and have been carried out many times in the past. However, these audits tended to be high-level. The data center instability we witnessed prompted us to revamp our approach to data center audits in 2017. We needed a more proactive investigation, so that we weren't just waiting for something to happen. We determined that a global "street-to-server" audit of every Intel data center was necessary—scrutinizing everything from the electrical feed coming into a facility to the components in every server in every rack, and everything in between. We conducted the audit in four phases. When the COVID-19 pandemic restricted travel in 2020, we had already completed three phases of audits. For the fourth phase of audits, our specialist auditors interfaced with local technicians using video cameras during live sessions to emulate a physical inspection, since the auditors could not travel.

The audit was not limited to just the actual data center. We also audited key infrastructural areas that make up the data center facilities ecosystem, including:

- Power supply to all cooling equipment, including chillers and cooling room units that serve the data hall
- All electrical equipment support rooms (such as UPS and battery rooms)
- Mechanical rooms
- Telecommunication rooms

[2] Definition obtained from https://www.knowledgehut.com/blog/it-service-management/change-management-in-itil.

[3] Definition obtained from https://www.knowledgehut.com/blog/it-service-management/incident-management-in-itil.

[4] Definition obtained from https://www.globalknowledge.com/us-en/resources/resource-library/articles/how-itil-differentiates-problems-and-incidents/.

If a facilities room supported any aspect of the data center, even if it was physically separate, we audited it. This innovative approach represents a radical departure from the traditional data center audit process.

We formed an internal multi-organizational team of technical experts to perform the audit. The "One Intel" approach helped uncover numerous previously undiscovered issues that came to light because of the team's open, transparent, detailed and forthcoming approach. Once we had completed the first phase of audits, we verified that our actions aligned with industry best practices. A third-party vendor completed a few data center audits; when we reviewed the third-party vendor's results, it was clear that we were auditing at a far more detailed level. Therefore, we decided to continue conducting our own audits.

"Think globally, act locally" was a key factor. We knew that implementing standardized changes across all our data centers around the world was essential for operational consistency. Conversely, enabling local IT managers with autonomy to work with local facilities teams was also important. Finding a balance was challenging, but with everyone working toward a common goal, it was possible.

Experienced auditors familiar with the global portfolio were able to gather and share experiences from previous incidents with all local teams, which helped identify issues in other locations across the world and avoid repeated incidents. Most audits were performed by the same team to ensure standardization across all sites.

The following sections provide more detail on what we audited, how we prioritized findings, and how we collaborated with Corporate Services to implement solutions.

What We Audited

To ensure a comprehensive assessment of our data center risks, the audit team included professionals with backgrounds in the electrical, mechanical, infrastructure and operations domains. They were subject matter experts on security, infrastructure monitoring, power, cooling and telecommunications. Their aim was to act as a unified team to identify as many risks as possible. They were also expected to understand the types, frequency and root causes of the issues. Finally, their goal was to address each factor by implementing strategies to mitigate the risks. Their main initial goals were to deliver:

- Standardized audits with a consistent level of quality
- Comprehensive audit results across global data centers
- Solutions to all findings

The audit was built based on the logic of power distribution going from the lowest level (120/208V/415V) to the highest on-site power distribution on the medium voltage side.

Auditing for Technical Debt: Many of the issues included in our audit represented technical debt, such as controls for single points of failure or equipment redundancy that were not used as designed. Therefore, the street-to-server audit aligned well with Intel IT's technical debt management framework.

A non-exhaustive list of things we looked for included the following:

- Single points of failure
- Expected lifetime of equipment
- Systems overdue for replacement
- Systems that were not optimally configured
- Systems that weren't using redundant components
- Alerting system functionality
- Setpoints, monitoring and control
- Power quality of the site

Auditing for Plan of Record and Tier Classification: We also observed systems that didn't adhere to the plan of record or the data center's tier classification. Post-audit, we updated the data center's tier classification to align with the audit findings. Here are examples of what we examined:

- How does the load compare to the capacity of every component?
- Have studies and training for electrical issues been conducted (such as for arc flash, short circuit and coordination)?
- Does the equipment manufacturer provide adequate support?
- Are there emergency support contracts?
- Does major maintenance of any component require a load shutdown?
- Does the cooling capacity match the power capacity?
- Are temperature sensors installed at the right locations?
- Is the correct fire suppression equipment available?
- Is the emergency power-off (EPO) labeled properly and has it been tested?
- Can EPO be eliminated?
- Are circuit breakers the right size for the application?
- Is there redundancy for control systems?
- Are the alarms setpoints correct?
- Is the correct metering and monitoring in place?
- What is the state of grounding and bonding?
- How is the site power quality?

Auditing for Process and People Issues: Beyond simply inspecting physical items (technology), we also considered the risks associated with processes and people. This category of audit items includes the following, among others:

- Checking the step-by-step procedures (job plans) for maintaining critical systems
- Verifying that new technicians are onboarded correctly and know the data center rules and processes
- Identifying insufficient or incorrect signage
- Inspecting housekeeping activities
- Talking with local site teams and maintenance owners to determine technical knowledge

The above examples are a small portion of everything we audited. In fact, the full street-to-server audit report checked nearly 900 line items (see the Appendix for an excerpt).

Prioritizing Audit Findings

Data center uptime is crucial to Intel's business success. However, our data center investment budget is not unlimited—we cannot fix everything at once, and some problems pose a greater risk than others. With the large number of previously undiscovered issues coming to light, it would have been easy to lose focus and work on low-hanging fruit that required little or no funding. Instead, we ranked every problem using a risk priority number (RPN) based on problem severity, occurrence frequency, detectability and recovery time (see Table 2), to enable a data-driven investment decision system. We also assigned a remediation cost to each problem (not shown in the table). The use of RPNs was supported by all stakeholders and made the subsequent investment process quick and smooth.

Table 2. Calculating the Risk Priority Number (RPN)

	Rating	Description
Severity (S)	4	Entire data center facility
	3	Cabinet row, group of cabinets; damage to critical equipment
	2	Single cabinet, or single server within cabinet; slight annoyance
	1	No impact
Occurrence (O)	4	Regular (>1 per month) or almost certain
	3	Periodical (1 per year) or highly likely
	2	Infrequent (1 per 5 years) or moderate failure rate
	1	Never or rare (<1 per 10 year) or remotely likely
Protection/ Detection (P/D)	4	No detection until resulting damage/ evacuation; unacceptable level
	3	Customer detects via monitoring; improvement required; below industrial standard
	2	Operations and maintenance inspection; improvement possible to make "fail-safe"
	1	Facility monitoring system or otherwise monitored via 24-hour monitoring; "state of the art"
Recovery Time (RT)	4	RT > 4 hour
	3	RT => 1 hour
	2	RT > 30 min
	1	RT < 30 min

To calculate the RPN, we considered the level of severity (S), likelihood of occurrence (O), the level of detection/ protection (PD) and recovery time (RT). Each of these categories were ranked from 1 (lowest) to 4 (highest). The RPN is determined by the following equation:

$$RPN = S \times O \times P/D \times RT$$

Figure 1 shows how we rank implementation priority. For example, a problem with an RPN greater than 128 is critical to fix.

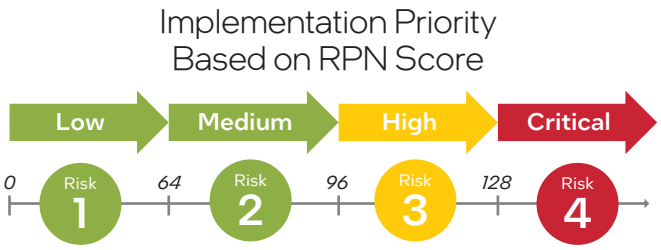

Figure 1. The risk priority number (RPN) enables us to prioritize which problems we need to fix immediately and identifies problems that can be categorized as "acceptable risk."

The RPNs enabled us to develop a roadmap for data center investment by identifying which risks needed immediate investment versus those that were "acceptable risks" that could wait. Now, when a new incident occurs, we evaluate what the business impacts could have been (or avoided entirely) if we had decided to not take this risk (that is, if we had applied budget to eliminate the risk). This, in turn, allows us to gauge if we are taking too much risk, or maybe we can safely increase our risk tolerance and lower our spending levels. The combination of the ITIL framework, the street-to-server audit and the RPN approach helps us make informed risk-taking decisions, as illustrated in Figure 2.

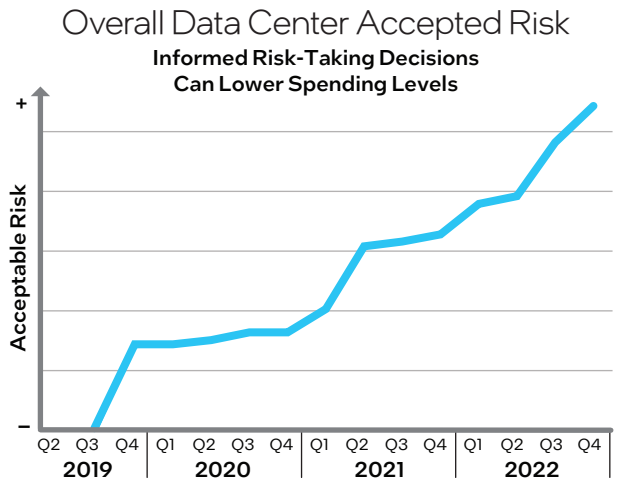

Figure 2. Our level of acceptable risk has increased over time as we fine-tune our use of risk priority numbers (RPNs) and risk analysis, enabling us to reduce spending.

Working with Corporate Services to Better Manage Risk

The street-to-server audit and subsequent investment prioritization strengthened the connection between Intel IT and Corporate Services. In some companies a separation of responsibilities may exist between the people who handle Real Estate and Building and Facilities Management and the people who do IT. In contrast, Intel IT and Corporate Services have a long-established relationship that is structured with a Management Review Committee at the top and global and regional meeting structures to track and discuss issues. The relationship is supported with a formal organizational-level agreement document.

Our ITIL approach, where IT personnel are tracking facilities issues, enabled IT and facilities personnel to speak the same language, translating electrical and mechanical terminology into ITIL service model terminology. Using ITIL and RPNs, we examine the risks together: IT assesses the business impact of problems/incidents and Corporate Services handles funding and project management. The approach also demonstrates to the facilities teams that we are deeply engaged in the workings of the data center and ensures that the facilities teams are fully aware of the needs and concerns of the IT customers.

It is important to note that we are not taking over the facilities management role of the data center, but rather we are managing the risk within our data center environment. So, whether it is change management (where we monitor and control the risks associated with scheduled maintenance), or incident management (where we help to track how our environment is behaving), or problem management (where we highlight where there are issues in the environment), it is important to work closely with the team that owns the facilities ecosystem and who can also work with us on improving the overall customer experience.

Increasing Visibility with a Data Center Heat Map

We developed a custom, live dashboard that tracks ongoing risks—a data center risk heat map (see Figure 3). The street-to-server audit was foundational to the development of the dashboard, but we continue to add functionality. For example, the dashboard includes more than the street-to-server audit results. It tracks all sorts of risks, including storms and risks that have been discovered from incidents. It also includes changes because they can introduce risk. If changes are overdue, then this adds to the risk. The dashboard is integrated into our overall Data Center Management System. In Figure 3, the following risk types are shown:

- **Accepted risk.** An identified risk that we know about and understand, but decided not to fix.
- **External event.** A risk that is outside our control, such as a utility power outage or a severe weather event.
- **Active incident.** An incident that is still ongoing or "live" and has not yet been resolved.
- **Resolution requested.** Ready to fix the risk but waiting for funding approval or downtime to fix the problem.
- **Scheduled change.** Approved change activities, including preventative and corrective maintenance.

These risk types also exist but are not shown in the figure:

- **Decision pending.** Risk is yet to be reviewed for an "invest" or "acceptable risk" decision.
- **Deferred maintenance.** Scheduled changes that have missed planned implementation dates.

The heat map has provided greater visibility into the underlying data center risk, allowing us to make investment decisions, implement cost-saving maintenance practices (such as replacing aging equipment before it causes an incident) and lower the business impact of data center incidents.

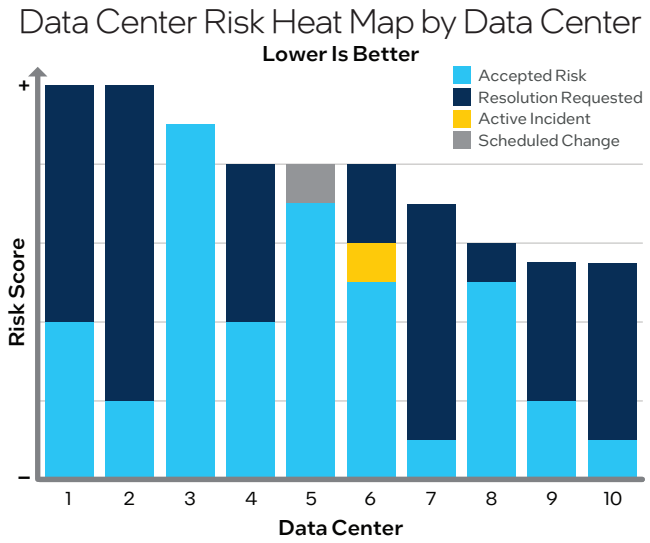

Figure 3. A comprehensive data center risk heat map enables us to track and manage risk.

Results

Over almost four years, we have reduced the overall data center risk score by a little over 50% (see Figure 4). Notable results include:

- We have reduced the occurrence and impact/severity of data center mega-events.
- Both incidents and business impacts are trending down.
- We now make better risk decisions about where to direct our resources.

We have also implemented new maintenance practices and updated our documentation. We expect these efforts to create an increasing return on investment as we measure long-term savings on a revolving five-year basis. Going forward, the team will continue rolling out actions derived from this project, including multi-year construction projects.

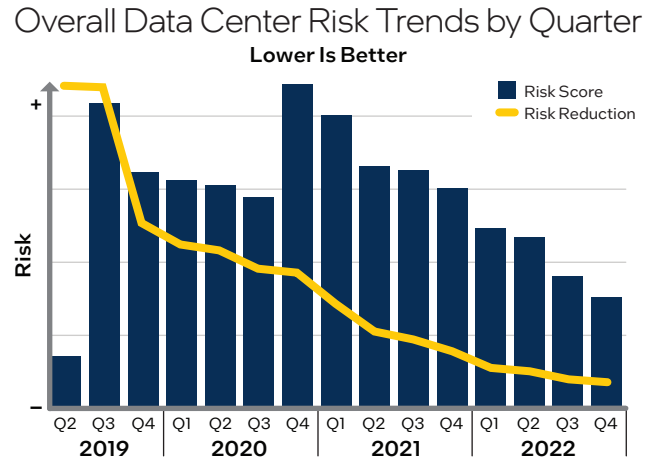

Figure 4. Our ITIL-based risk management approach has decreased the overall data center risk score by about 50%.

As a result of reduced risks, our data center environment is more stable, which reduces business impact. Figure 5 illustrates business impact from all relevant data center incidents. The data in the figure shows that the overall number of incidents has declined and the number of incidents with business impact (black bar) dropped to nearly zero by the end of 2022. Also, the red and yellow lines representing risk-taking and no risk-taking, respectively, were closely aligned by the middle of 2019, indicating that our informed risk-taking decisions were accurate. Note that the data in the figure does not include outlier events, which were unusual occurrences unrelated to our audit and risk-reduction practices; including these events would have incorrectly skewed the data and obscured the real trends.

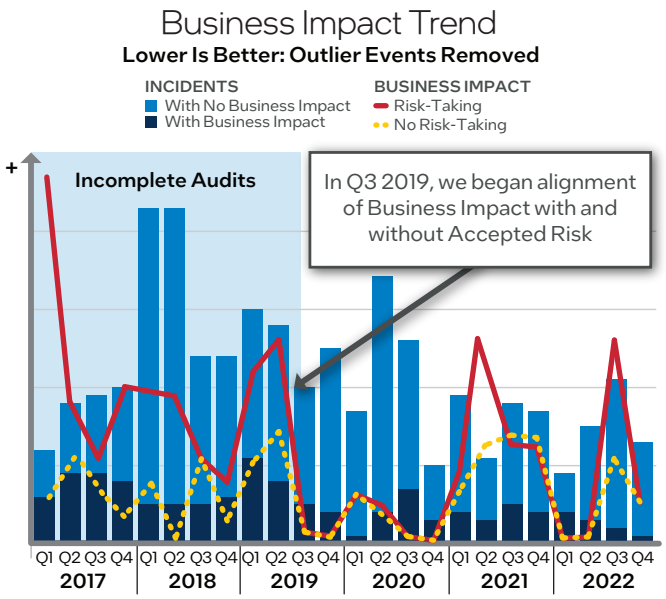

Figure 5. Prioritized risk management reduces overall business impact from all data center incidents (excluding outlier events).

Next Steps

Risk management is an ongoing process, and the risk list can grow and change over time. We will continue to manage equipment, such as UPS or generators, and replace them as they reach end of life stage. We will not need to do another global full street-to-server audit any time soon. Although if a facility has a major change like a construction project, we may fully audit that data center when the project is complete. If Intel acquires an additional data center through the merger and acquisition process, we have a ready-made audit that helps us assess the quality of the data center and integrate it into the Intel data center fleet.

We will also continue to use and evolve our dashboards to proactively manage data center risk. For example, we will continue to add new risks as they are discovered (such as when an incident occurs) and will investigate if the incident is likely to happen in other data centers, potentially leading to a mini-audit on that specific risk to see if it exists elsewhere.

Conclusion

We have learned that not investing in our data centers can introduce risk through technical debt. Adoption of the ITIL change, incident and problem management modules—combined with a highly detailed global data center audit over nearly four years and a close working relationship with Corporate Services—has enabled us to lower overall data center risk score by 50%. Key lessons include:

- The ITIL processes gave us the right methodology.
- The street-to-server audit presented us with the necessary data.
- The dashboards and heat map provided us with the necessary visibility.

We can now make data-driven data center investment decisions so we can focus our investments on areas that matter most and that will deliver the best return on investment.

Related Content

If you liked this paper, you may also be interested in these related stories:

- Data Center Strategy Leading Intel's Business Transformation white paper
- Enterprise Technical Debt Strategy and Framework white paper
- Scaling Intel's Data Centers with Software-Defined Networking and Automation white paper
- Fuel Cells – An Alternative Energy Source for Intel's Data Centers white paper
- Affordably Increase Network Bandwidth at 100 Gbps and Beyond white paper
- Disaggregated Servers Drive Data Center Efficiency and Innovation white paper

For more information on Intel IT best practices, visit intel.com/IT.

IT@Intel

We connect IT professionals with their IT peers inside Intel. Our IT department solves some of today's most demanding and complex technology issues, and we want to share these lessons directly with our fellow IT professionals in an open peer-to-peer forum.

Our goal is simple: improve efficiency throughout the organization and enhance the business value of IT investments.

Follow us and join the conversation on **Twitter** or **LinkedIn**. Visit us today at **intel.com/IT** if you would like to learn more.

Appendix: Excerpt from Data Center Street-to-Server Audit Report

#	Data Center	DC Tier	Audit Tier	Issue	Impact of Failure	Solution	Post Implementation Risk	Impact to Implementation	Severity	Occurrence	Detect	Recovery	Before RPN	Severity2	Occurrence2	Detect2	Recovery2	After RPN	Finding Type
1	R3	3	2	**Normal power DC 480V:** Switchgear retrofit required. No feeder breaker monitoring, acrylic covers or remote rack in/out device. No remote operator available. Label missing. **Major Maintenance/Code compliance.**	If switchgear fails, DC will lose power. Breaker failure, arc flash safety, no equipment monitoring, no proper power quality metering.	Perform 480V switchgear retrofit. Replace obsolete power meters with 7650/PM9000. Implement PML meters to track incidents, alarms and loading. Acquire remote ON/OFF and racking equipment.	Switchgear failure won't cause normal power for cooling shutdown.	Partial DC cooling shutdown	4	3	4	1	**48**	3	2	1	1	**6**	Other
2	R3	3	2	**BCR ATS:** ATS are open transition and don't have ext. bypass. **Maintenance requires shutdown of load. ATS EOL.**	ATS failure during power outage. IF ATS fails or needs maintenance, shut down BCR SCR.	Replace ATS with new one with close transition, remote monitoring and external bypass. Exercise ATS annually.	ATS can be maintained without DC downtime, and failure of 1 component won't impact DC operation.	Partial DC cooling shutdown	2	4	3	2	**48**	1	2	1	1	**2**	End of life critical components
3	R3	3	2	**EPO SOO, testing and labeling:** Ensure proper maintenance, testing, and monitoring of EPO. EPO needs label and identify impact if activated **EPO. SPOF.**	DC shutdown	Update master EPO drawings and SOO. Label/identify EPO and add associated impact. Test EPO during next site MM. Confirm is passive EPO. Or Eliminate EPO: Based on NEC 645.10 (B) this DC is in compliance with the requirements to eliminate the EPO.	No DC shutdown due to EPO malfunction.	Site shutdown	4	1	3	3	**36**	3	1	1	1	**3**	Other
4	R3	3	2	**Electrical documentation:** Update electrical studies. Replace dated/missing panel schedules and labels. Arc Flash Labeling on MV gear, HVAC disconnects, Distribution Boards and Busways End feeds missing. Labeling on field doesn't match elect drawings on ACU-05/06. Replace CU labeling outdoors.	Code compliance and safety	Perform electrical studies every 5 years and update information on the field. Make electrical equipment labeling consistent in the field, in PME and on drawings. Calculate and place Arc Flash labels on electrical equipment.	Updated drawings and electrical studies. Code compliance.	No impact	2	2	3	3	**36**	2	1	2	2	**8**	Electrical studies and drawings

#	Data Center	DC Tier	Audit Tier	Issue	Impact of Failure	Solution	Post Implementation Risk	Impact to Implementation	Severity	Occurrence	Detect	Recovery	Before RPN	Severity2	Occurrence2	Detect2	Recovery2	After RPN	Finding Type
5	R3	3	2	**Gen:** Generators don't have double/redundant battery charger. Gen has wet batteries.	No emergency power during utility power outage.	Replace batteries with maintenance-free batteries ASAP. Add 2 redundant battery chargers as approved on spec.	Generator will run as expected during a power outage.	No impact	3	3	2	2	36	1	1	2	1	2	Critical updates per historical MIs
6	R3	3	2	**Needs attention:** UPS room has water pipes on top of UPS/ batteries. UPS room has ext. door. Entrance doesn't have water retention/contention. No water leak detection system on floor.	UPS room water leak/ floated	Build a retention barrier/ bump to avoid water intrusion into the room. Install water leak-detection system.	No water inside UPS room.	No impact	3	1	2	4	24	1	1	2	1	2	Redundancy: Enable maintenance without downtime and eliminate SPOF
7	R3	3	2	**Grounding/Bonding:** Network racks don't have appropriate grounding/bonding.	Code compliance and safety	Provide appropriate grounding/bonding for all racks. All grounding lugs on ground bar to be double-barrel 2 holes compression lugs.	Equipment is property grounded.	No impact	2	2	3	2	24	2	1	1	1	2	Other
8	R3	3	2	**DC power to MV SWGR:** DC control power in MV equipment not compliant with latest specs.	In case of power outage, MV equipment can operate.	Upgrade DC control power to MV SWGR per spec. Provide 2 battery chargers in parallel for each SWGR. 2 battery strings. Alarms to FMS for each battery charger. Alber on each battery bank.	MV equipment operation during power outage.	No impact	3	1	2	4	24	3	1	2	1	6	Redundancy: Enable maintenance without downtime and eliminate SPOF