

Managing the IT Aspects of a Large-scale Divestiture

The new company met design and production objectives during the entire carve-out process, and our experiences enabled us to formalize best practices for similar future program use.

Casey Anselmi
Business Analyst, Intel IT

Jennifer Autry
Program Manager, Intel IT

Executive Overview

To meet the unique needs of Intel's most complex ever corporate divestiture, Intel IT developed new processes and tools that solved substantial challenges in the areas of intellectual property protection, legal compliance, asset transfer, and manufacturing carve-out.

The divestiture was part of a large, complex, international transaction that created a new, independent semiconductor company in collaboration with an industry partner. Intel divested its NOR flash memory business, which was acquired by the new company; the new company also acquired the NOR and NAND businesses of the deal partner. Intel IT's solutions enabled Intel to complete the transaction and facilitated the successful standup of the new company.

During 18 months of co-location until the new company established its own IT systems, the new company shared physical space with Intel and ran its business on Intel IT infrastructure.

This enabled the new company to successfully continue operating and shipping products throughout the carve-out process, while it was in critical start-up phase.

We accomplished a number of major achievements during this project:

- New information security procedures enabled the new company's employees to securely connect to Intel's infrastructure, so the company could operate effectively during carve-out. These and other modifications to security policy also benefit Intel long term.
- Separated three factories in multiple geographies with minimal downtime, while still shipping product.
- Separated and migrated a total of 365 terabytes of data, maintaining data integrity.
- Identified and transferred more than 16,000 assets, and inventoried and evaluated more than 9,000 software applications, transferring 2,547.

The new company met design and production objectives during the carve-out process, and our experiences enabled us to formalize best practices for similar future program use.

Contents

Executive Overview.....	1
Background.....	2
Solution.....	3
Forming the Divestiture Team.....	3
Forming the Program Structure.....	3
Supporting the Enterprise Application Strategy.....	4
Summary of Results and Key Learnings.....	11
Conclusion.....	12
Contributors.....	12
Acronyms.....	12

IT@INTEL

IT@Intel is a resource that enables IT professionals, managers, and executives to engage with peers in the Intel IT organization—and with thousands of other industry IT leaders—so you can gain insights into the tools, methods, strategies, and best practices that are proving most successful in addressing today's tough IT challenges. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

Merger and Acquisition Terminology

Asset transfer agreement (ATA). A legal document stating the assets Intel will transfer to the new company.

Carve-out. The physical separation of the new company's infrastructure, applications, and data from the divesting company.

Day 1. The day after the closing: The new company is the owner of the assets and operates independently. All interaction between the new company and Intel is at arm's length and is considered business to business from this point forward.

Divestiture. Legal transfer of ownership of assets to the new company at closing.

Standup. The final separation of the divested business so that it operates independently and without Intel's support or transition services.

Transition services agreement (TSA). A legal document stating the services Intel will provide to the new company for a defined period following the closing, including costs and terms and conditions.

BACKGROUND

In 2007, Intel engaged in a large, complex, international transaction to create a new, independent semiconductor company in collaboration with an industry partner. The transaction included the divestiture of Intel's NOR flash memory business, which the new company acquired. The new company also acquired the NOR and NAND businesses of the deal partner. Intel transferred associated assets to a new legal entity in exchange for an ownership stake.

Although Intel has divested several businesses over the years, this divestiture was unique in its size, scope, duration, and complexity. The entire transaction took about three years to complete, including a year of planning before the deal closed and 18 months of co-location after the deal closed.

Two critical aspects of this divestiture contributed to the unparalleled complexity:

- **Manufacturing carve-out.** We separated three operational factories in multiple geographies, which impacted end-to-end processes from design engineering to logistics.
- **Extended co-location.** The new company inhabited Intel buildings and used Intel's IT infrastructure for 18 months after the deal closed; however, it was an independent legal entity, and its employees and data needed to be maintained separate from Intel.

Intel IT's main challenge was developing an enterprise application strategy to support the new company; this strategy would subsequently define how we approached all other IT aspects of the divestiture. Because the company was brand new, together with the deal partner, we had to decide whether the new company would clone the enterprise applications of Intel or its deal partner, or build one from scratch. Once that decision was made and implemented, we would then need to migrate Intel data to the new enterprise.

Other significant aspects of this divestiture included:

- **Decision making processes and corporate culture.** We worked with our deal partner to define these for the new company before the deal closed.
- **Business continuity.** The new business ran on Intel's IT infrastructure and Intel shipped product on behalf of the new company during application migration.
- **Geographical diversity.** The business Intel divested was spread across multiple sites and located in several geographical regions. In connection with the divestiture, Intel IT had to take multiple regulations and processes into consideration, requiring a higher level of precision than Intel had previously required in a divestiture.

To complete a transaction and divestiture of this magnitude, we had to create team structure, program structure, and new tools and processes.

SOLUTION

Working with our deal partner, Intel IT formed a team, program structure, and set of tools and processes to support the creation of the new company's enterprise, data migration, and the transition of Intel employees to the new company.

During the divestiture, we aligned our work to four guiding principles:

- Keep Intel aligned with its standard information management policies and guidelines by proactively engaging Intel Internal Audit, Intel Information Security, and Intel Legal to identify and audit key areas of information security and risk.
- Keep the new business running on Intel's IT infrastructure while protecting Intel intellectual property.
- Help the new company's IT organization run successfully without negatively affecting Intel IT operations.

- Focus on simplicity and minimize cost.
- Our processes required the team to test program plans against these principles.

Forming the Divestiture Team

We identified the logical functional areas of the new business—including Design engineering, Office, Manufacturing, and Enterprise (DOME) computing—and formed a team of lead program managers to represent and support each functional area. This multi-lead approach differs significantly from a typical divestiture team, which usually only has one program manager. Figure 1 illustrates the functional areas that comprised the team.

Areas such as human resources (HR), manufacturing, and supply chain aren't usually thought of as IT-related, however IT maintains the applications these organizations use and the networks on which the applications run. It was therefore important for our team to include experts from each of these areas to make the divestiture process as efficient as possible.

The team also included site managers from the different geographies as well as dedicated security, asset management, finance, and communications specialists. Using existing Intel IT employees to form the team enabled us to avoid increased headcount.

The lead program managers acted as chief information officers for their respective functional areas and were assisted by content experts within their domains. This level of expertise enabled Intel IT to discuss specific concerns effectively with the deal partner and enabled faster decision making.

Forming the Program Structure

After closing the deal, we provided services to the new company to assist with planning the program structure—including creating a stand-alone Program Management Office (PMO), defining how decisions would be made, setting up Finance support, and implementing IT customer support for the new company during the carve-out process.

PROGRAM MANAGEMENT

IT merger and acquisition projects at Intel typically follow guidelines from Intel IT's PMO. However, the size, complexity, and need for tighter controls in this divestiture warranted the creation of a self-contained PMO. The program was monitored at the IT staff level by placing our executive sponsor on the IT staff team for the duration of this project.

The program team built a baseline plan spanning all functional groups, which we then incorporated into the overall IT plan of record

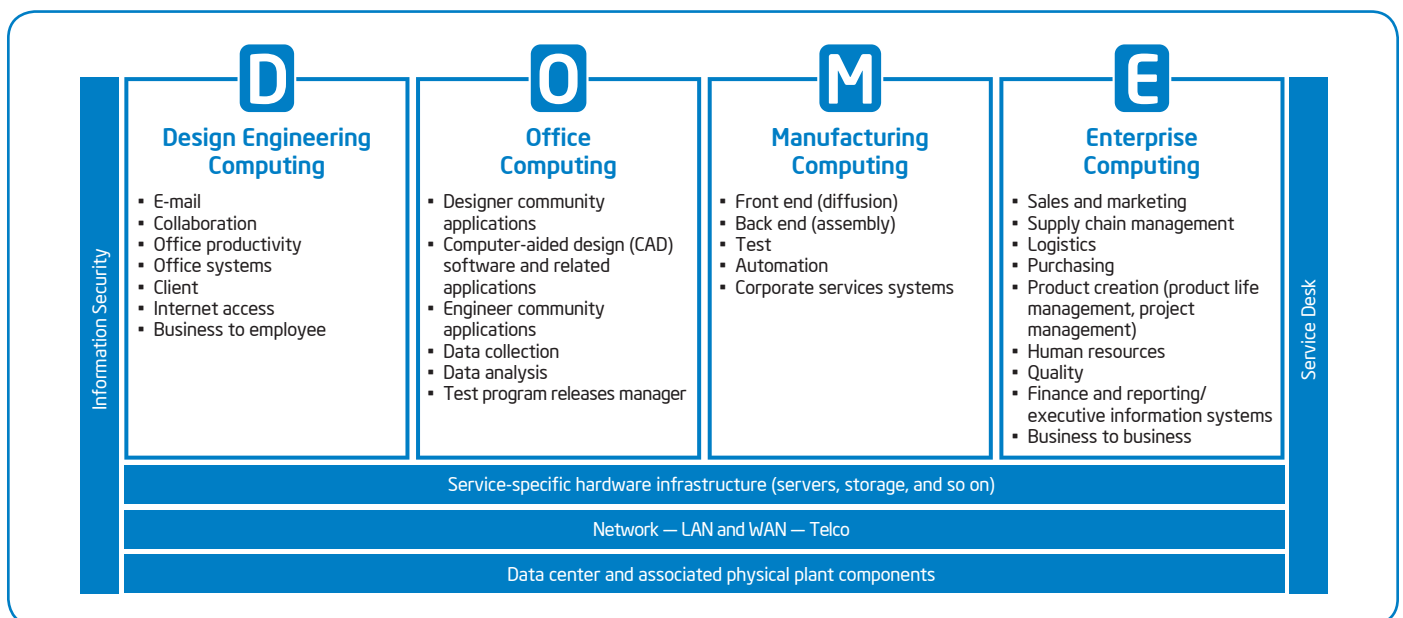


Figure 1. Our divestiture team included experts from four main functional business areas: Design engineering, Office, Manufacturing, and Enterprise (DOME) computing.

(POR). We held several planning sessions in which we refined plans and milestones. The functional leads then developed their own detailed project plans, which were rolled up to upper-level program milestones, alleviating the need to track individual deliverables at the program level. We used a one-page “Matrix of Metrics” to help track key milestones and keep the program on schedule.

The size of this program highlighted the need to clearly document decisions; we maintained a repository, capturing new processes for future reference. This approach helped us formalize IT best-known methods (BKMs) for future divestiture projects.

An important aspect of program management was providing recognition to team members to acknowledge their hard work and embodiment of corporate values. Recognizing employees who exemplified Intel values strengthened the team and built commitment to the program. Recognition could be as simple as a commendation to the employee’s manager or as significant as a monetary award.

DECISION MAKING AND CORPORATE CULTURE

The Intel IT divestiture team and the deal partner worked with the proposed executive management team of the new company to determine the decision making processes that would be used in preparation for Day 1. The proposed executive management team also decided it would be beneficial to adopt a new culture and organizational structure to support an ultra low-cost flash memory business, rather than keep the culture and structure of a full-spectrum chip manufacturer. These two decisions affected the way Intel IT interacted with the new company and at times forced us to change our ways of thinking and doing business.

FINANCE SUPPORT

The divestiture involved not only complex business and technical issues, but also had a significant financial component. Specifically, the team removed thousands of assets from Intel’s financial systems; developed and tracked multiple budgets, including an adaptable contingent workforce model; costed internal services provided to the new

company; and reflected those internal cost reductions within Intel’s own managerial costing processes.

Spending categories

Budgeting entailed defining and forecasting several unique spending categories:

- **Standup cost.** Expenses necessary to prepare the new company for being an operational business on Day 1, incurred before closing the deal. Initial standup costs were borne by Intel and the deal partner, and later billed to the new company when it had systems in place to process the payments.
- **Carve-out cost.** Intel’s cost to separate the NOR flash business from Intel systems and processes.
- **Transition services agreement (TSA) cost.** Ongoing charges to the new company for services provided by Intel.

IT finance analysts worked with their counterparts in operations to forecast and track these budget categories throughout the program.

Costing techniques

For TSA-related charge-backs, IT finance and operations calculated the cost for IT services provided to the new company to help it run its business. We provided services in each of the DOME areas as well as for the supply chain.

In some cases, we applied managerial costing techniques to create a fully burdened estimate; in other cases, we used Intel’s own internal IT allocation methodology as a starting point. In the end, we realized that using the IT allocation as a basis for external costing efforts was not an optimal decision because the IT allocation does not fully burden the cost of the services it charges to Intel internal business units.

IT CUSTOMER SUPPORT

We created a team to provide IT customer support for employees transitioning to the new company. This team provided software training for any applications that were migrated.

We also provided a transitional Service Desk (TSD) to support the new company. Contingent workers were hired to fill this role for 12 months while the new company’s Service Desk

evolved. Even after the new company’s Service Desk was functional, we provided Level 2 and Level 3 support specialists until the new company’s employees became proficient in their jobs. This helped the new company’s employees learn faster and contributed to the success of the new company.

Supporting the Enterprise Application Strategy

Creating the new company’s enterprise required us to substantially supplement or replace existing processes and technologies. Because there was no stand-alone acquiring company, Intel and its deal partner worked together to determine whether to clone either parties’ enterprise applications or build new applications.

After evaluating each functional area, we decided to clone the deal partner’s enterprise to minimize start up time and the learning curve for employees of the new company. The deal partner’s transitioning employees were familiar with the applications and supporting business processes and could assist and train Intel’s transitioning employees.

Until the new company’s enterprise was functional and ready for data migration, it continued to use Intel’s network and enterprise applications. Maintaining legal separation while both companies used the same infrastructure was a constant focus. We addressed several important areas—such as HR, information security, and DOME functions—and developed new technical solutions to support the program.

HUMAN RESOURCES

Access to the Intel’s infrastructure and facilities is predicated on a person’s employment status within the Intel HR system. There are three systems of record for employees and contract workers. HR SYS-A stores Intel employees’ employment status and determines eligibility for compensation and benefits. HR SYS-C stores the contract status of contingent workers, and HR SYS-B validates active employment or contingent worker status for access to infrastructure and facilities. These systems are illustrated in Figure 2.

Transitioning employees to the new company

Typically, employees who are no longer active in HR SYS-A also become inactive in HR SYS-B. For the divestiture, we created new “reason codes” that identified employees as inactive in HR SYS-A, thus stopping compensation and benefits, but active in HR SYS-B so they could retain infrastructure and building access.

Managing contingent workers

The next challenge was granting the new company’s new hires limited access to Intel facilities and enterprise applications. We used the contingent worker tool, HR SYS-C, to address this requirement. However, we needed to make modifications to this tool and add a new category to support mergers, acquisitions, and divestitures.

The standard business process for bringing in a contingent worker is that there must be a contract or purchase order in place, so the supplier can be paid. In this transaction, the new company was not considered a supplier,

nor was Intel providing any compensation to the worker. The addition of the new category allowed us to bypass the contract or purchase order requirement and show new hires as active contingent workers in our systems. Although we created the new category specifically to support this large-scale divestiture, Intel is using this category for other merger and acquisition activities.

Managing exiting employees

The new company’s employees were no longer active in Intel HR systems, as they were employed by the new company. However, we had to create a new business process to remove an employee’s access to infrastructure and facilities when that employee exited the new company.

Our standard process uses an application to start several automated tasks for various groups and systems. Figure 3 represents the tools and tasks that are part of this process.

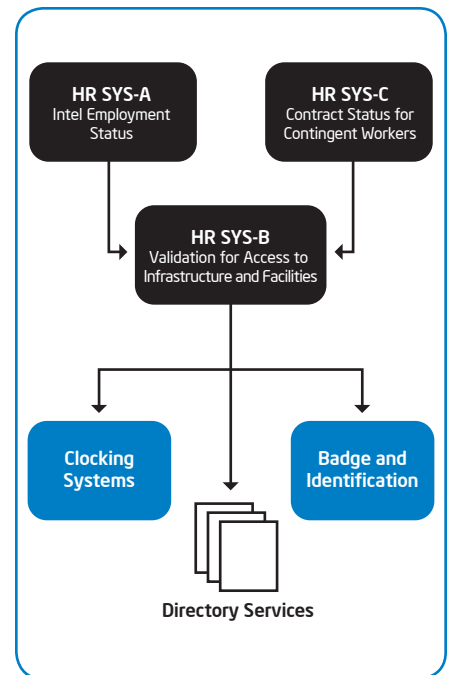


Figure 2. Three separate human resource systems control workers’ access to Intel’s infrastructure and facilities.

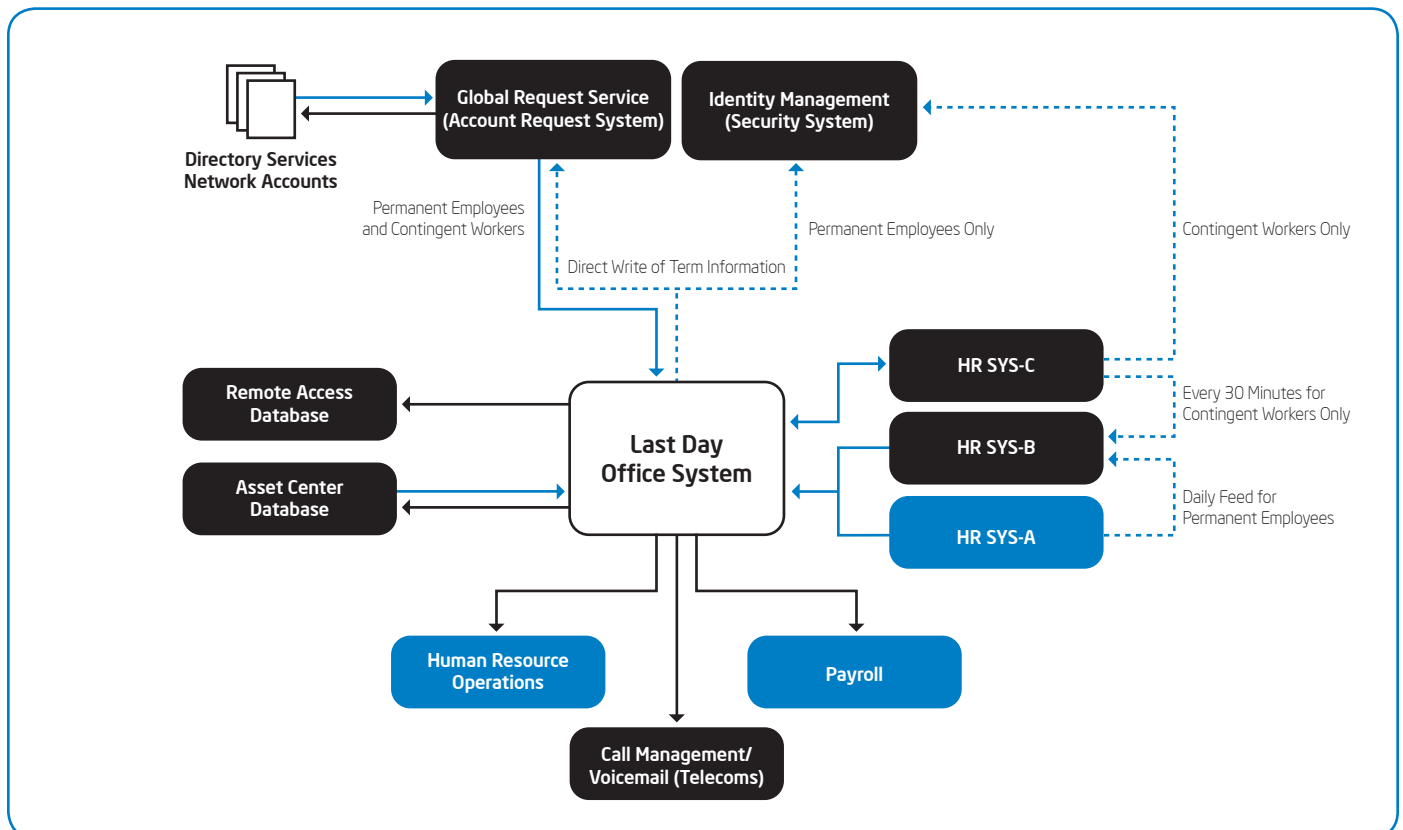


Figure 3. A new business process removed access to Intel infrastructure and facilities when an employee exited the new company.

The new company provided Intel with weekly reports detailing former Intel employees exiting the new company. The Intel TSD implemented a manual process to completely remove these employees from all HR systems. Because some of the tasks had already been completed, such as removing the employee from HR SYS A, the manual process addressed only those tasks that remained, such as changing the HR SYS-B status and canceling building, network, and remote access. The process did not have to notify the asset center because laptop assets had been transferred to the new company. This manual process was in place for the entire 18-month co-location period.

INFORMATION SECURITY

This divestiture project posed significant challenges to established Intel information security policies:

- **Decentralized management.** The project was managed in a decentralized fashion, with each functional area making decisions for its domain and each having different ramifications on information security. The Information Security team worked with each area to develop individual tactical plans while maintaining an overall view to control the larger strategic and cumulative risks.
- **Compliance.** Corporate data retention, data destruction, and e-Discovery processes were evolving during the course of this project at both the company policy level as well as at governmental regulation levels. This forced the Information Security team to take a proactive approach to minimize future disruptions.
- **Co-location.** Co-location was a major technical and physical concern for Information Security. The new company inhabited Intel buildings and used Intel's network and enterprise applications for 18 months. Intel IT had never managed a divestiture with co-location of this duration.
- **Standard practices.** Standard risk assessment methodologies didn't scale to take into account extended co-location, nor

did our rigid security policies comprehend the new business models necessary for a successful divestiture of this complexity.

To meet these challenges while still maintaining a high level of information security, a small team of dedicated experts was assigned to and held accountable for managing overall risks in all functional areas. This team proactively established controls and acceptable levels of risk, and contributed to program planning. A new methodology, Threat Agent Risk Assessment (TARA), was very effective at identifying and managing the most critical security exposures.¹

As an example, our normal practice is to immediately remove all accounts and access when an employee leaves the company. However in this case, it was necessary for exiting employees to retain legacy access to buildings and enterprise applications. To help mitigate this risk, we instituted a number of controls, both technical and behavioral. This ongoing access was critical to enabling the new company to bring its products to market during the carve-out period.

Two companies using the same network posed operational challenges. Our solution logically separated the new company using a pocket network and logical domains. We used cables of different colors to identify network usage. Employees of the new company experienced seamless network and e-mail functionality.

We also implemented data segregation. Intel data remained on the Intel portion of the network and was not accessible to the new company. Similarly, any data that belonged to the new company resided on its pocket network, and Intel could not access it. In some cases, Intel rescripted and redesigned applications to restrict data access.

Employees of the new company were located in dedicated spaces inside Intel buildings but needed to enter and leave the building and access common areas such as elevators and

cafeterias. We posted signs to identify where Intel and new company employees were allowed. We also implemented a new badge process that electronically controlled access to sensitive areas.

Continuous auditing from Information Security as well as collaborating with internal and external audit resources helped us address constant changes in regulations pertaining to divestiture and information security. These audits served different purposes:

- Information security audits were continuous and broadly based, covering policies, configurations, systems, physical separation, networks, and clients.
- Internal audits were aligned to the highest risk areas.
- External audits were specific to litigation or areas of regulatory concern.

Based on policy adaptations, ongoing risk assessments, and audit results, we identified areas of concern, ultimately optimizing our processes accordingly. In the end, we successfully mitigated information security risks during the divestiture and also developed a stronger and more flexible security policy that benefits Intel.

DESIGN ENGINEERING COMPUTING

Design engineering computing managed the silicon development environment for approximately 800 engineers who were transitioning to the new company. Because of their expertise, this group was heavily engaged in creating the new company's design infrastructure prior to Day 1. This timeframe complicated matters because they did not have an operational business partner with which to negotiate. To add further complexity, the infrastructure and data of the NOR business to be divested were thoroughly intermixed within Intel's IT environment. Expert advice from transitioning personnel was critical to the success of this phase of the divestiture project.

¹ "Prioritizing Information Security Risks with Threat Agent Risk Assessment." Intel Corporation, December 2009.

Data separation

We implemented both logical and physical data separation. First, we achieved logical separation by creating new UNIX* domains for each site and segregating the infrastructure behind a new network. Where possible, we also physically separated the networks.

Design engineering computing is responsible for UNIX disk space allocation and group permissions for each internal customer, and project disk space is created according to globally defined Intel IT standards. Consequently, design engineering computing could readily locate data that was to transfer to the new company. Furthermore, the access control process was already in place. To validate the logical segregation, we scrutinized and modified the project access permissions, looking for transitioning employees and special access cases, such as administrative accounts.

To validate the physical separation, we managed the space allocation based on which products were transferring to the new company. We also deployed dedicated licensing and build servers. We restricted access to transitioning personnel and a small support team, and replaced critical systems in our environment that transferred to the new company.

Physical facilities

A co-location period of 18 months was unusually long; however, the new company needed to prepare facilities to receive assets that were part of the transaction. In addition to the inherent delays of new construction, local regulations introduced additional delays.

Facility improvements included construction of data centers, offices, labs, and test floors in China and California; we experienced significant delays in China due to local laws.

Additionally, before construction could begin, the new company had to obtain licenses, hire a contracting firm, develop building plans, and receive funding approval from the management team.

Frequent candid conversations between Intel, the deal partner, and the new company helped all stakeholders understand delays and the associated impacts on the program schedule.

OFFICE COMPUTING

Network carve-out planning required extensive use of inter-company connections (ICCs) and the deployment of pocket networks—the primary design solution that enabled phased data network transition, shown in Figure 4. The pocket network design allowed us to capture the volume of network traffic that the new company required and to identify applications and services that needed to be

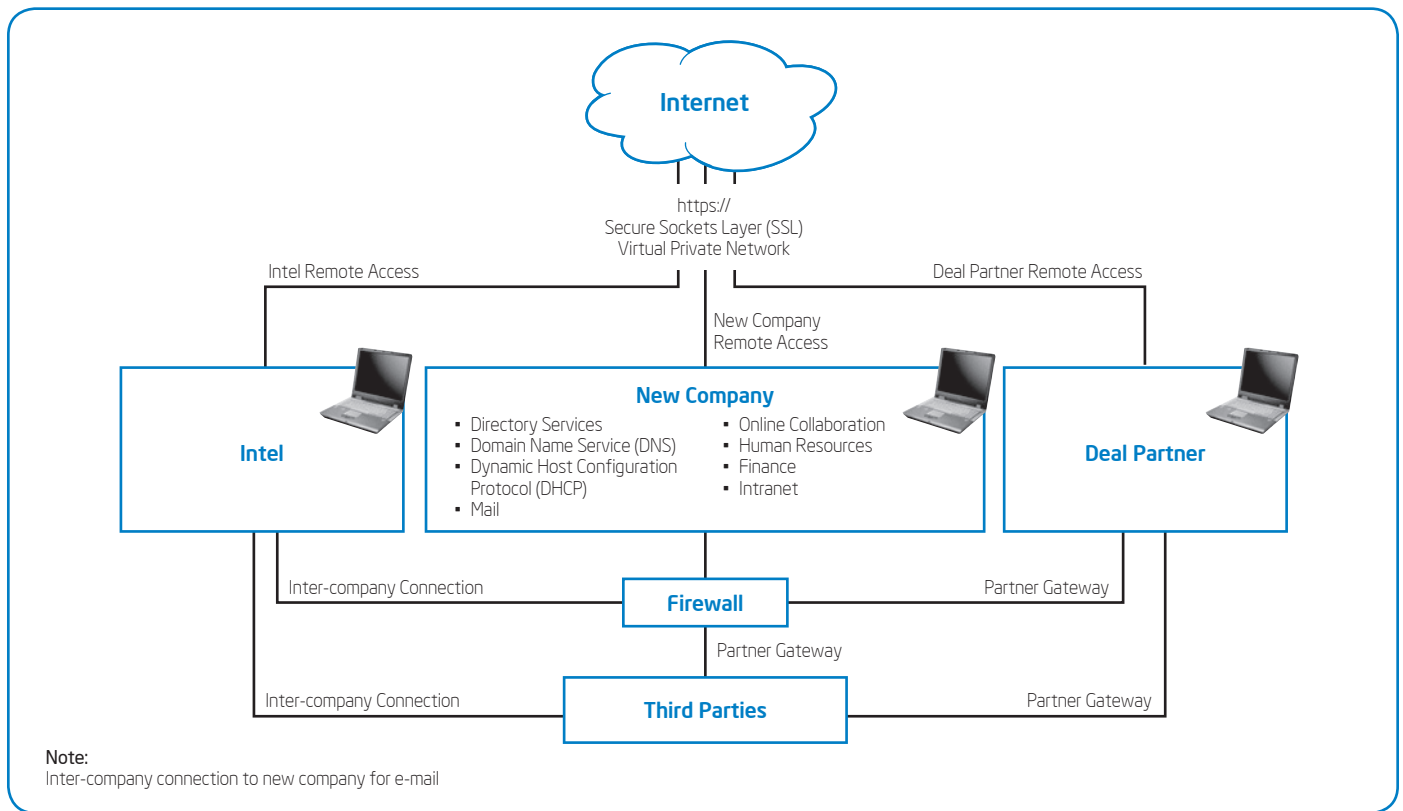


Figure 4. Extensive use of inter-company connections and pocket networks enabled us to keep the new business running on the Intel IT infrastructure during co-location.

dispositioned prior to carve-out. Because the new company's enterprise was not complete until after the physical transition of the network, we had to implement 191 separate ICCs to keep the new business running. We supported and maintained these connections for six months.

Directory services environment

We created and managed the new company's directory services, including the identities and relationships that comprise the network, by creating a local domain within the Intel pocket network. This pocket network featured one-way trusts established from the new company's local domain to the Intel corporate domain. New company employees still authenticated to the corporate domain, and Intel IT retained administrative access to new company's domain as operationally required.

Shared data

We transferred shared drive and enterprise content management data to existing new company servers residing on the Intel network prior to carve-out. This made data migration more efficient as we did not have to worry about external bandwidth constraints. We migrated online collaboration content using software designed specifically for that purpose. This helped the new company keep its business running because all permissions migrated along with the collaboration sites and data. A single owner with access rights to both the Intel and new company networks managed the migrations. Prior to transition, we took snapshots of the data.

End user data

End users managed client PC data migration using USB flash thumb drives. Using USB drives had multiple advantages, such as requiring that we only provide guidelines for transitioning appropriate data, simplifying the migration process, and reducing the data migration cost.

MANUFACTURING COMPUTING

The manufacturing environment was one of the most challenging areas to carve out.

It presented a high level of complexity to maintain the existing production and shipment of products while simultaneously separating multiple factories from the Intel network in different geographic regions without impacting safety, security, or data integrity.

To start the process, we mapped all manufacturing automation applications to factory tools, enterprise, and engineering applications. This helped us define the project's scope, streamline the migration plan, and prioritize the manufacturing carve-out activities. We could measure downtime in mere hours—not weeks or months as we initially anticipated.

Facility separation

To separate the manufacturing facilities, we used two strategies:

Create a new physical infrastructure and then transition applications and products at one time. The first separation occurred at the wafer fabrication facility. To separate this facility, the new company team accomplished the physical infrastructure carve-out prior to supply chain and enterprise application migration. Although the new company was able to run the factory on its own network, this strategy required more than 35 ICCs between Intel and the new company.

Several hundred new-company employees retained their legacy Intel accounts to access the supply chain and manufacturing applications required to perform their jobs. This access was possible because Intel and new company data was separate. Joint planning, open communication, and clear expectations were critical to minimizing risk and impact to operations. We called this strategy the "Big Bang," as all enterprise applications and products transitioned at the same time several months after the network carve-out was complete.

Create a parallel physical infrastructure and transfer applications and products gradually. The second facility separation took place at an assembly and test factory. Because this separation occurred closer to the enterprise application migration, we

decided to create a parallel IT infrastructure, including a new data center. We instituted a joint change control review board to oversee technical details throughout the implementation.

Although this approach still required ICCs, it minimized risk as we were able to test operations and transition product lines gradually. As product flushed out of the Intel supply chain, it ran on Intel IT's infrastructure; as product transitioned to the new company, it ran on their infrastructure. Intel IT and the new company worked closely to successfully migrate applications. We provided training to individuals on Level 0 through Level 3 support to bridge any support gaps. The new company's former Intel employees aided the continuity of application support.

Building infrastructure together with the new company provided on-the-job training for new company employees and enabled us to immediately transfer maintenance responsibilities of the new infrastructure once it was complete. By transferring high-end servers and storage area networks from a closed Intel facility near the new company's manufacturing site, we avoided approximately USD 1 million in equipment costs, mutually benefiting both Intel and the new company.

SUPPLY CHAIN

When we decided to clone the deal partner's supply chain for the new company, it quickly became apparent that running the new company's business on the Intel network was a bigger task than we had anticipated. The supply chain touches every aspect of the business and posed significant challenges for the Intel IT team. These challenges included keeping the new company's business running for 18 months as well as transitioning it to its own enterprise and business processes.

Maintaining data segregation

Until the carve-out was complete, Intel ordered, planned, sourced, and delivered goods on behalf of the new company, using existing Intel business processes and

enterprise systems. Intel IT worked closely with Intel Legal to identify key areas of focus and created a business process to remove, restrict, and audit access to any system, data, or tool as necessary for either company.

In connection with the TSA, we also established boundary conditions that defined our relationship to the new company during the carve-out process:

- No change to Intel supply chain systems or legal entity flows would occur; Intel Finance captured activities and reported to the new company.
- Purchasing occurred under Intel terms and conditions; changes could be made only at the purchase-order level.
- Sales operated under Intel terms and conditions.

Transitioning supply chain data

Once we were operating on behalf of the new company, we began to focus on transitioning supply chain data to the new company. Product naming and setup initiated processes in multiple functional areas that required close coordination to address interdependencies. We encouraged each functional area to map its “as-is” Intel process to the new company’s “to-be” process. Our role was merely to migrate the data to the new company.

Transitioning the supply chain network

We considered migrating areas of the supply chain, such as order management, materials, planning, and warehouse management, independently of each other. But because it would have been difficult to automate cross-enterprise requirements, we decided to transition the supply network all at once. This required all manufacturing areas—including subcontractors—to develop a coordinated, interdependent schedule for the transition, which occurred over a six-week timeframe.

ASSET MANAGEMENT AND TRACKING

Typically, the term “asset” relates to hardware devices and other depreciable tangible items. In this project we expanded the definition to include hardware, data, intellectual property,

and software. Each of these areas had their own associated transition activities and the movement of every byte, cable, and application required documentation.

Hardware assets

Transferring hardware assets to the new company involved identifying which assets needed to be transferred, adhering to country and local laws concerning asset transfer, and cleaning data from the equipment.

Identifying assets. Intel extracted an asset list from its system to identify which assets would be transferred to the new company. This list was validated by our IT finance and operations groups. After the deal announcement, we performed a physical inventory at each site using the asset list as our guide, marking all assets to be transferred. By identifying each and every asset in advance, the actual transfer at closing was much easier.

Adhering to local law. Assets to be transferred to the new company were located throughout the world. Each jurisdiction has its own local laws and regulations regarding how different assets can be transferred in different situations. Coordination with local legal counsel, especially foreign counsel, in planning the asset transfers helped to define the scope, structure, and budgeting of this transfer process.

Cleaning the data. All transferred computing assets needed to meet Intel’s requirements for data destruction prior to transfer. We removed any data that wasn’t part of the divestiture deal from each asset and then conducted either a full disk sanitization or a free space wipe, depending on the asset. We documented what happened to each asset. Once the asset was cleaned, it was ready for transfer, and once all assets were transferred, we received delivery confirmation from the new company.

Data and intellectual property

During the carve-out, Intel transferred large amounts of data to the new company, requiring attention to protect Intel’s intellectual property. Intellectual property included design, engineering, and manufacturing data as well as enterprise-shared information. The

data transfer process required identifying, extracting, and then separating out any proprietary information, leaving only data intended for the new company. This activity was particularly challenging because the data was mixed throughout many data storage systems across Intel.

Moving intellectual property assets from Intel to the new company was successful throughout the entire process because we communicated the reasons behind the strict transition requirements. We did underestimate the time it would take to manage and track assets. Setting clear expectations with all stakeholders was crucial to understanding site requirements and planning for resources and timelines.

Controlled technology. Certain locations required special considerations regarding the transfer of intellectual property. We identified any controlled technology and worked closely with Intel Information Security and our export control teams to use established processes to handle this type of asset properly.

Data movement. The ability to track data was a key factor in the program’s success. We evolved a number of our policies including confidentiality, information security, internal audit, and other regulatory requirements. For example, our corporate data retention policies originally mandated that we save every document and file. This was not practical due to the size and scope of this project. The team developed risk mitigation policies to determine what to save or how and when to remove the data.

SOFTWARE

Transferring software required understanding the transferability provisions of various licensing agreements for both third-party and internally developed applications. A key consideration in migrating software applications to the new company was the ability to implement bridge licensing, which would provide Intel’s software licensing agreements to the new company for a specific time period until the new company acquired its own.

We inventoried software requirements, performing an electronic “pull.” In addition, each functional area documented their software applications. These two actions provided an initial master inventory list with over 9,000 applications. Using the electronic pull proved less than ideal, as it did not provide as much

detail as the data received from the functional areas. The team met weekly to review each line of the list, identify internal and external applications, remove any duplicates, and provide status updates.

Third-party applications

We identified more than 1,200 third-party applications, and Intel IT and purchasing groups had to work with more than 300 suppliers to create and extend bridge licensing agreements. These agreements helped the new company reduce costs and avoid business disruptions, as licenses were extended from between three to 12 months after Day 1. Bridge licensing gave the new company time to negotiate a contract and/or place a purchase order, enabling additional cost savings. We established controls and monitoring processes to enforce expiration dates. We also re-evaluated our own licensing requirements, leading to cost reductions for Intel as well.

Internally developed applications

Applications developed by Intel required a separate review process. Dedicated experts reviewed each application to determine if there was a risk of intellectual property exposure. Upon approval, we transferred approximately 1,000 internally developed applications to the new company.

IT QUICK CONNECT

During the carve-out, we needed to develop a connectivity solution that enabled employees of the new company to access Intel’s employee intranet. At the same time, we needed to reduce implementation time and integration cost, and mitigate risks to Intel due to data loss.

Our solution is called IT Quick Connect (IQC)—a secure external USB storage device that uses client virtualization and a virtual private network. IQC offers several benefits:

- Secure access to Intel’s employee intranet
- A fast and efficient means of rebuilding the new company’s client systems without exposing Intel to excessive risk

- Ability to access Intel IT’s client manageability tools and systems
- Enterprise application support managed by Intel’s global Service Desk
- Substantially reduced deployment times and costs for new laptops and for client integrations

LARGE-FILE TRANSFER CAPABILITY

Our team needed to transfer data securely to outside parties, including the new company. Some of these files were very large, and we also needed to track and report file sharing. We outlined a number of high-level requirements for large-file transfer (LFT) capability:

- Program managers should be able to set up project teams and allow members to share information.
- Project teams can consist of internal and external users.
- All access to project data should be available only to project teams and should be logged for audit purposes.
- Data transferred to and from the server may need to be archived externally for corporate data retention purposes.
- Access receipts may need to be archived for corporate data retention.
- External project participants may need to use digital certificates.
- Documents with Intel security classifications may need to be handled in different ways.

Our LFT tool, diagramed in Figure 5, is based on Intel® architecture and provides many benefits:

- Can transfer intellectual property with certified electronic receipt, which is important for auditing.
- Shares large files with simple drag-and-drop functionality.
- Is fast and secure.
- Provides a level of audit and reporting that did not exist previously.

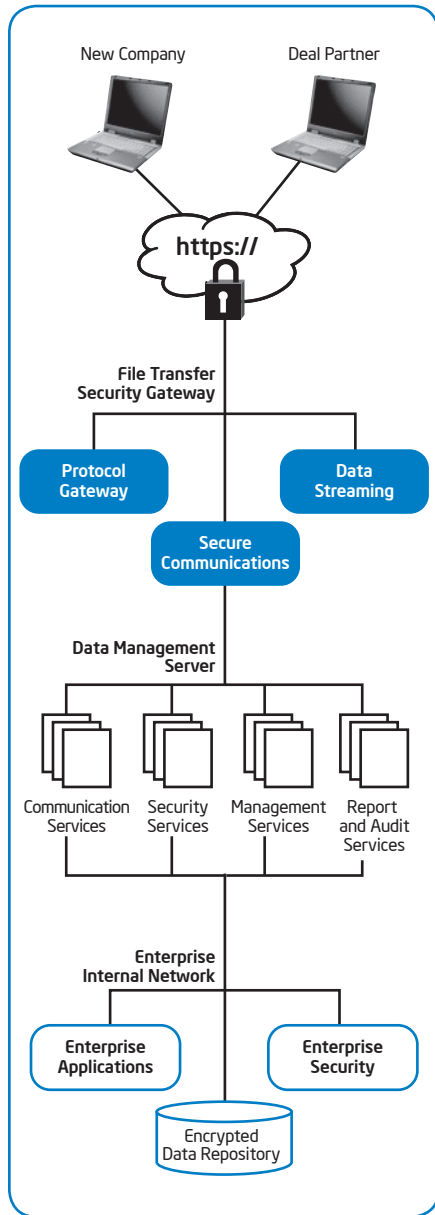


Figure 5. Our large-file transfer capability supports file sharing, access tracking, and archiving.

Summary of Results and Key Learnings

Intel successfully divested a previously unprofitable business area and, along with our deal partner, formed an independent new company. The new company's business used Intel IT's infrastructure and enterprise applications for more than 18 months, navigating complex legal requirements.

During the carve-out, Intel IT accomplished many significant achievements, summarized in Table 1. We also learned important lessons, summarized in Table 2, which we can use in future divestiture activities.

Some things we learned apply to the project as a whole:

- Inter-company connectivity allows for physical separation of the network prior to supply chain and enterprise application transition.
- Rely heavily on subject matter experts whenever possible to minimize the time and resources needed to complete specific items such software inventory and defining business processes.
- Large-scale programs such as this can impact hundreds of employees. Providing recognition to all team members involved in the program acknowledges their hard work and focus on corporate values. Recognition can be as simple as a commendation to the employee's manager or as significant as monetary recognition.
- Be open to evaluating corporate policies and procedures and adjusting when necessary if the proper risk mitigation can be implemented. This flexibility can prevent the team being overwhelmed with tactical issues, allowing them to focus on higher priority items.

Table 1. Intel IT Achievements

Intel IT Achievements
<ul style="list-style-type: none"> ▪ Avoided increased headcount by using Intel personnel to form the team. ▪ Provided agility, flexibility, and scalability with our innovative program management framework. ▪ Transferred 2,547 applications and managed the disposition of 1,384 applications. ▪ Transferred more than 16,000 assets while removing any inappropriate data, applications, and intellectual property. ▪ Separated and migrated 365 terabytes of data without any data integrity issues. ▪ Accurately removed thousands of assets from Intel's financials and tracked multiple budgets throughout the program. ▪ Separated three operational factories with minimal downtime and no impact to operations. ▪ Migrated 2,550 e-mail accounts within 24 hours with minimal disruption to business communications. ▪ Continued to support design engineering in multiple geographies while separating the environment and assets for transfer to new locations. ▪ Saved and/or avoided approximately USD 1 million in equipment costs by transferring equipment from a closed fabrication site to the new company's manufacturing computing site. ▪ Developed new tools that enabled secure connectivity to Intel's intranet by external parties and the ability to transfer, track, and share large files. ▪ Evolved and adjusted information security policies for all of Intel.

Table 2. Intel IT Key Learnings

Team construction is critical.
<ul style="list-style-type: none"> ▪ Early in the project, identify subject matter experts in each functional area who possess extensive knowledge of organization, business, and technical details. ▪ Empower these leads to make quick decisions in the dynamic process- and policy-building environment. ▪ Provide recognition to all team members involved in the program to acknowledge their hard work and embodiment of corporate values.
Policies and processes need to be flexible.
<ul style="list-style-type: none"> ▪ Evaluate policies and procedures, and adjust when necessary if the proper risk mitigation exists. This enables the team to focus on higher priority items. ▪ To allow the team to focus on the critical path, track key high-level milestones as well as lower-level milestones. ▪ When developing new processes, include preparation for an audit by documenting decisions, waivers, and procedures. ▪ Maintain a decision log by functional area and a corresponding log at the program level to capture new processes for future use and to help formalize IT best-known methods.
Don't forget finance support.
<ul style="list-style-type: none"> ▪ Establish agreed-upon processes for periodic review of the asset transfer agreement, and be prepared to add or remove asset line items. ▪ The transition services agreement (TSA) may require amendment. Establishing a formal review process for the TSA keeps all parties aligned on service, duration of service, and cost.
Establish techniques for efficient migration of supply chain, enterprise applications, and manufacturing.
<ul style="list-style-type: none"> ▪ When cloning the supply chain of one company and then migrating the other half of the business to the new supply chain, it is optimal to do the migration all at once. ▪ Inter-company connectivity allows for physical separation of the network prior to supply chain and enterprise application transition. ▪ Building a parallel infrastructure in partnership with a new company provides on-the-job training and a streamlined handover of maintenance responsibilities, and expedites independence from the parent company. ▪ When new construction of facilities is required, teams should account for any local laws or construction delays within the project schedule. Frequent and candid conversations between all stakeholders should occur to understand the impacts.

CONCLUSION

Intel has divested several businesses over the years—however divesting the NOR flash memory business was unprecedented in size, scope, complexity, and duration. Intel IT worked with a large, multi-faceted team to determine our overall strategy. We also developed new processes and tools that solved substantial challenges in the areas of intellectual property protection, legal compliance, asset transfer, and manufacturing carve-out.

Our team involved lead program managers from key groups from within IT, such as IT

operations, core system engineering, enterprise applications, and office automation. These experts contributed greatly to the success of the three-year project by sharing their detailed knowledge of each functional area. Despite 18 months of co-location, during which time the new company shared physical space with Intel and ran its business on Intel IT infrastructure, the new company operated independently. In addition, our strategy enabled three factories to continue to ship product throughout the carve-out process. The new company met its design and production objectives during the carve-out process, and our experiences enabled us to formalize best practices for future use.

For more straight talk on current topics from Intel's IT leaders, visit www.intel.com/it.

CONTRIBUTORS

Julia Alsberg, IT Business Operations
Shlomi Ben-porat, IT Program Manager
Craig Bolton, IT Program Manager
John Botkin, IT Program Manager
Dan Kolibaba, IT Program and Operations Manager
Ryan Ochsner, IT Finance
Rajiv Ojha, IT Program Manager
Jeff Pettitt, IT Program Manager
Matthew Rosenquist, IT Information Security
Chris Sellers, IT Executive Sponsor
Marjo M. Webster, IT Technical Solutions Manager
David R. Williams, IT Program Manager
Theresa Zawalski, IT Program Manager

ACRONYMS

ATA	asset transfer agreement
BKM	best-known method
CAD	computer-aided design
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DOME	Design engineering, Office, Manufacturing, and Enterprise
HR	human resources
ICC	inter-company connection
IQC	IT Quick Connect
LFT	large-file transfer
PMO	Intel IT Program Management Office
POR	plan of record
SSL	Secure Sockets Layer
TARA	Threat Agent Risk Assessment
TSA	transition services agreement
TSD	transitional Service Desk

This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

* Other names and brands may be claimed as the property of others.

Copyright © 2010 Intel Corporation. All rights reserved.

Printed in USA
0510/IPKA/KC/PDF

 Please Recycle
323005-001US

