STAR COMPLIANCE

compliance (r)isk concepts

THE CONTROL ROOM HANDBOOK

Who Needs One
How To Build One
Why The Future Is Now

AIR TRAFFIC CONTROL MEETS DEAL TRAFFIC CONTROL

Picture an air traffic controller, binoculars in hand, scanning a bustling airport. Planes taking off and landing. Radio communications blaring. Radar blips in constant motion. There's a ceaseless stream of information coming in from every angle, all of which must be quickly sorted through to eliminate risk.

Air traffic control is to aviation what control rooms are to financial firms—the fast-paced center of it all where a small team of professionals has to stay on top of everything. Deals pop up unexpectedly and must be handled immediately. Crisscrossing emails demand constant monitoring. There's a lot riding on how well either job is done, and both require a mix of technology and human analysis to do it right.

For years, control room officers have used a combination of spreadsheets and email chains to sort through potential conflicts and monitor deal team members. If they were lucky, they could access HR and CRM systems for further risk crosschecks. However, control room officers in many firms—including large ones—are using decades-old tech to do a job that has only gotten more complex. More regulation. Bigger firms doing bigger deals. More people working those deals. And with people in this day and age less likely to stay somewhere long term, there's less institutional memory to ensure conflicts are avoided.

This is where modern, automated tech comes in, designed from the ground up specifically for the control room. Tech that can corral all this data streaming back and forth, no matter where it originates from—giving control room teams a single, centralized location from which to monitor and manage it. Tech that reveals where a deal stands, where it's going, and how it relates to every other deal in the pipeline. Tech that integrates seamlessly with other firm systems, so a more complete and thoroughly holistic picture of all deal-related activity is possible—and high-flying enterprise financial firms stay flying high.

This guide will take you step-by-step through the design and development of a modern control room. It will help you get the most from all the resources at your disposal, including people and tech. It will put you on the path to the kind of control room that will operate with maximum efficiency and effectiveness, and offer maximum risk reduction for your firm.

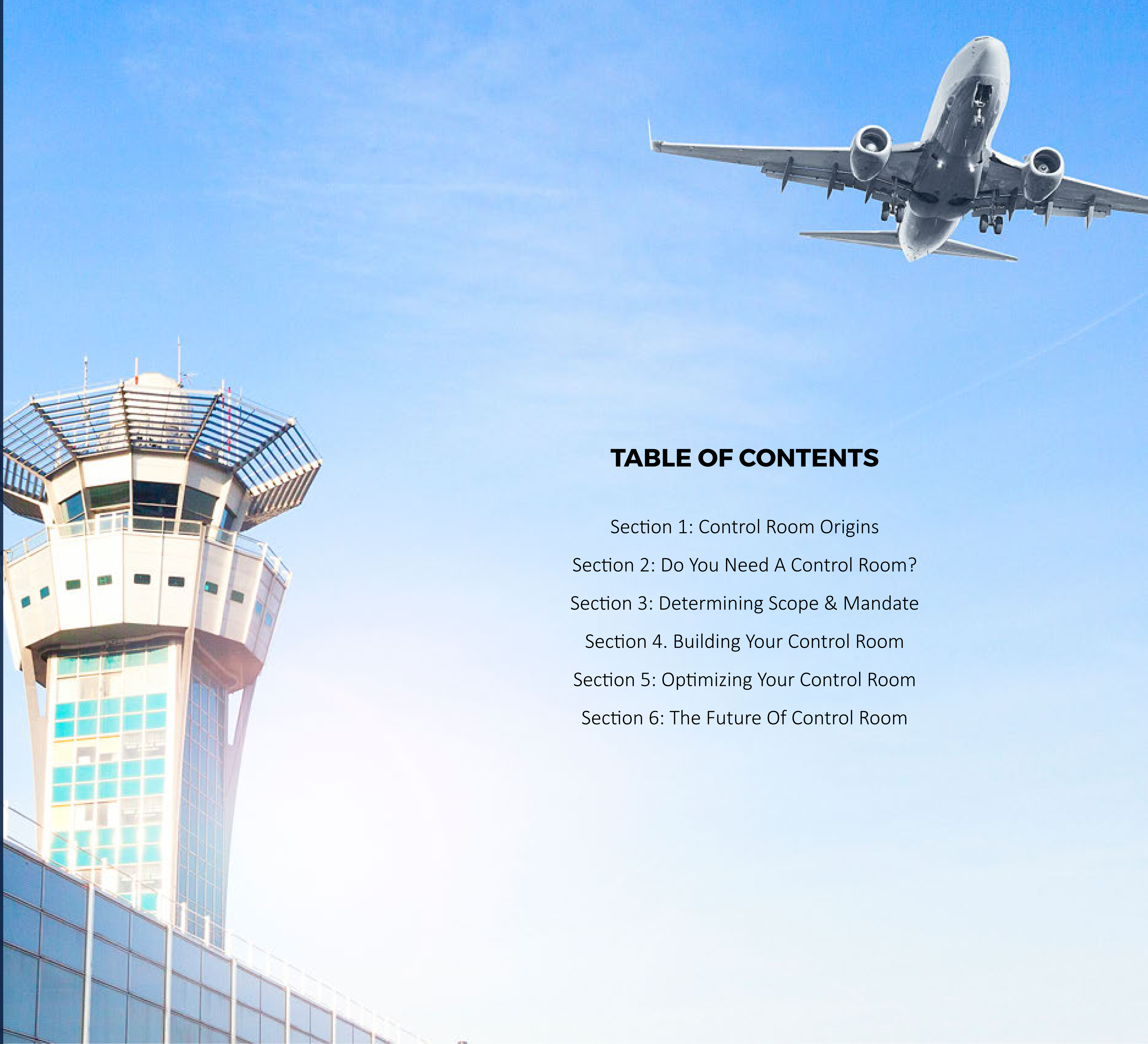


TABLE OF CONTENTS

SECTION 1:
CONTROL ROOM ORIGINS

If you're just getting started in the control room space, this section is for you. If you know the basics and you're ready for actionable advice, skip ahead to SECTION 3: DETERMINING SCOPE & MANDATE

In the beginning, there was Ivan Boesky and spreadsheets

"Control rooms evolved out of compliance departments in the early 1990s, after the passage of the Insider Trading & Securities Fraud Enforcement Act Of 1988," says Steve Brown, "better known simply as ITSFEA." Brown is Director Of Broker-Dealer Client Services at Compliance Risk Concepts, a compliance services consulting firm. He's also a veteran control room officer, and was there at the very beginning of the compliance control room function. "The 1980s saw a number of high-profile insider trading and securities fraud cases: Chiarella, Dirks, Boesky, Milken, to name a few. ITSFEA was meant to address what was seen as a real problem in the world of finance—that is, trading on inside information—thus the impetus to establish a dedicated control room function."

ITSFEA specifically required broker-dealers to develop adequate policies and procedures designed to prevent and detect the misuse of material nonpublic information, or MNPI. To further complement the ITSFEA regulation, Congress also directed the Securities and Exchange Commission to investigate the adequacy of federal securities laws surrounding insider trading. So in 1990, the SEC released *Broker-Dealer Policies and Procedures Designed to Segment the Flow and Prevent the Misuse of Material Nonpublic Information*. This report came out of a comprehensive review of broker-dealer policies and procedures, and included an assessment of how well self-regulatory organizations (SROs) oversaw member firms' information barrier activity. "A primary finding of this report was, no two compliance infrastructures to control the flow of MNPI were alike," says Brown. "Based on this, the SEC recommended that firms memorialize in greater detail their procedures, and similarly improve the documentation, communication, and recordkeeping associated with information barrier activities."

In 1991, the National Association Of Securities Dealers (now FINRA), the New York Stock Exchange, and the Securities Industry Association (now SIFMA) released a joint memo that laid out the minimum elements of adequate information barrier policies and procedures pursuant to ITSFEA requirements. Based on this guidance firms began to memorialize policies and procedures, surveil employee and proprietary trading, supervise interdepartmental communications, and conduct training. "By 1992 the bulge-bracket firms officially started to develop control rooms," says Brown. "They were likely staffed by compliance professionals that were previously generalists, trying their best to figure out how to control the flow of MNPI. These pioneering control room officers were tasked with determining how to deal with all the new regulations and guidance, without anyone else ever having done it before."

A swivel chair, a windowless office, and a key to lock up

"An early control room may have looked and operated something like this," says Brown, speaking from experience. "The CCO would give the newly minted control room officer his own office. This was a 'control room' in the most literal sense. He would get a key to lock up at night, or when he had to physically leave the space to ask someone about a potential conflict. Broker-dealer statements would pile up on his desk. There were no electronic broker feeds. This person would spend his days, and many weekends, locked in the room checking employee trading statements against a spreadsheet, which is where the watch and restricted lists lived. With any luck, at some point in this long, painful process, he might have an ah-ha moment."

From there—unlike in a modern, automated control room, where integrated firm systems funnel all deal-related data through a single, centralized platform—the control room officer would wheel from monitor to monitor in his swivel chair (a critical piece of tech back in the day) and try and corroborate his suspicions by checking different firm systems. He might also leave the control room space and double check where people were sitting, to determine if the bankers he was investigating perhaps sat near each other. Brown:

> *"I had an idea where the employees sat. So I'd review the deal-team list and think, now who sits next to whom exactly? I'd literally get up and go down several flights of stairs to look."*

With standards and policies in place, and control room officers figuring out best practices and procedures, the act of uncovering questionable activity gained some structure. But, as is apparent, it was still far from easy—the equivalent of looking for a needle in a haystack. "We were relying on passion, pure human-observation skills, and frankly dumb luck, to identify potential red flags and investigate them through," says Brown. But because the work was so arduous and time intensive, and because the process was nothing close to being a comprehensive look at all avenues of risk, control room teams had plenty of ammunition to go to senior management with to ask that processes be put into place to make reviews easier and more thorough. These included requiring employees to maintain accounts in house, requests to expand control room team size as the firm grew in size, and of course, requests for the latest tech. Anything that could make the job of control room officer easier and, in turn, reduce firm risk.

SECTION 2:
DO YOU NEED A CONTROL ROOM?

That depends. On a whole host of factors. From the type of activity and MNPI you're dealing with to what happens when someone does something they shouldn't have

Type of activity, breadth of activity, and MNPI

"The truth is, there aren't explicit rules or job descriptions that speak to what a control room does," says Brown. "The regulations simply state that firms need to have 'adequate policies and procedures in place to prevent and detect insider trading.' It's up to firms to assess the markets, products, and services they offer, determine which generate MNPI and which don't, and then develop the processes to monitor and control its flow."

Whether or not a firm needs a control room, then, is not a black-and-white call. Size has something to do with it, but not everything. It also comes down to breadth of activity, the amount of MNPI in play, and the kind of business activities the firm engages in. Does the firm have relationships with private equity? Does it assist them with M&A advisory or acquisition financing? Does the firm offer equity or fixed-income research to support sales and trading efforts? Does the firm offer wealth or asset management services? The list goes on. But it's when these types of business activities and resulting regulatory challenges start to appear—where existing controls need to be enhanced to manage the risk—that a real need emerges for a control room.

And occasionally, the business side may spot the need for a control room function before compliance. "Most times it's compliance identifying the need for compliance support," says Brown, "but other times it's the business saying: 'We're doing M&A, trading, sales, research, and leveraged finance. There's a lot of MNPI, and we need better controls to monitor the flow.' They'll demand the firm have proper processes, people, and tech in place. Individuals that understand the firm needs to avoid regulatory and reputation risk in order to succeed. *You know you're operating in a good environment when the business is demanding that compliance up its game and build a control room."*

Someone does something they shouldn't have

Sometimes, some unhappy event occurs that could become the impetus for automation or formalization of the control room function. Someone does something they shouldn't have and a regulator issues a fine or a cease-and-desist order. Perhaps a banker trades on inside information by accessing MNPI contained in deal files, or a trader trades ahead of a research report. Perhaps a banker fails to report a watch list item or notify the control room of a pending deal announcement. All of these instances lead to regulatory and/or policy violations. In these cases, regulators may also require firms to retain an independent consultant to address deficient areas.

Speaking of which, Brown is also clear about the distinction between regulatory violations and policy violations. "If someone doesn't pre-approve a trade, as long as they're not trading on inside information, it's a policy violation. Not to downplay policy violations, but focusing on the risk spectrum there's a big difference between policy violations and regulatory violations. Firms simply can't mess around with regulatory violations. No one should trade on inside information, fail to monitor research, or fail to report watch or restricted list items. These are all potential regulatory violations."

And if you think that perhaps regulations are at least one area that's black and white, where the lines are clear-cut and easy to follow, you're mistaken. "Like with most things regulatory," says Brown, "when it comes to insider trading, market manipulation, and fraud, you're often told what you're supposed to do, but not how to do it. That's up to each firm to figure out. With employee trading, the rules are clear. With sales, there are clear rules surrounding suitability and customer onboarding. But when it comes to information barriers, manipulation, insider trading, and MNPI, firms have to turn to case law, rule interpretations, and industry precedent in order to determine the best course. *It's good to have control room people on staff with industry contacts—colleagues they can reach out to—and the firm needs connections to consultants and legal counsel to tap for critical insights and best practices."*

SECTION 3: DETERMINING SCOPE & MANDATE

If you think your firm needs a control room, this is where you start to wrap your head around the concept on a practical level—how it should look and how to think about making the case for it

Your first step in setting up a control room is to figure out the business. At this point, you know enough about it to know you need a control room. But now you have to think about the specifics—precisely what activities the firm is already engaged in or will be engaged in—to determine the scope and coverage of your control room function. In short, you want to have a conversation with the business.

Assess who has access to MNPI

The starting point for determining the scope of the control room and developing a clear mandate is to assess what businesses and employees have access to MNPI and should therefore be monitored by the control room. A lot of deal-critical information zips around a firm at any given time, and MNPI can originate from the private as well as the public side of the information barrier. But no matter where it comes from, unaccounted for MNPI and breaches of the information barrier can endanger deals and reputations. At this point, you're undertaking a risk-assessment, and it will position your firm to be able to properly develop and implement policies and procedures. This risk assessment should include:

☑ All legal entities

☑ The rules, regulations, and market conventions applicable to each business

☑ Industry best practices for protecting client and customer information

Potential steps in the risk assessment may include:

□ Conducting interviews to assess each business unit

□ Assessing legal entities and regulatory requirements

□ Assessing the physical location of employees in all facilities

□ Taking inventory of the types of products offered by each business unit

□ Taking inventory of the types of MNPI obtained and generated by business units

□ Identifying types of material produced by business units

□ Assessing how the businesses interact with each other

□ Identifying the back-office support the front-office businesses rely upon

□ Assessing the licensing and supervisory universe, including who's licensed vs. who's required to be

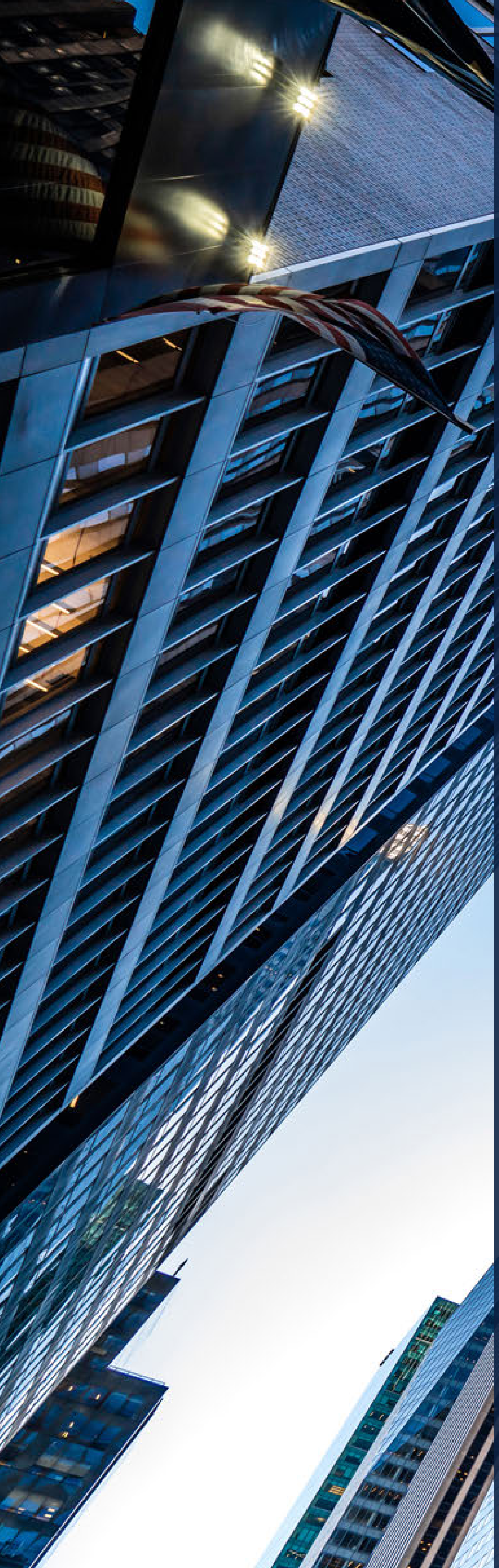
> *"Let's say a bank wants to start a broker-dealer business," says Brown. "It's going to have to go through a registration process and submit an application to FINRA. Part of the application will require the firm to define how it will address information barriers and insider trading. In the beginning, maybe the chief compliance officer builds a team of compliance officers, who are probably all generalists to start. And as the firm grows—and the complexity of products and services increases and the firm starts to accumulate MNPI—ideally the business or compliance will ask if what's currently in place needs to be enhanced."*

Here are specifics to think about as you begin to outline scope and mandate for your control room:

- What happens when there's too much information and too many employees to adequately monitor with the controls, policies, and procedures you have in place? What's at risk? How much risk is the firm willing to entertain?
- At some point your employees will become aware of MNPI. What are you going to do when this occurs? What are the controls that will be put in place? All firms must develop policies, procedures, and training to deal with instances when employees become aware of MNPI.
- Smaller firms reach an inflection point where they have too many employees, too much information in motion, and not enough compliance resources or automation. Are you at that point? If not, can you define what that inflection point would look like so you can be prepared?
- Ultimately, compliance leadership will need to balance staffing with automation. This may mean adding internal headcount, utilizing outsourcing or offshoring, and developing or purchasing automation tools. Make sure you have a line item in your scope for the cost of such people and tech.

Part of the process of considering scope and mandate is how deal teams will be staffed. You'll need to consider the products, services, and markets the firm serves. Some big picture questions to consider are:

- Will a relationship and/or product specialist be required to deliver the engagement?
- How will the firm staff the opportunity with qualified personnel while considering potential conflicts?
- When conflicts are identified, who will determine how to proceed?



Here's what goes into building a deal team for a complex transaction, like a merger-and-acquisition advisory or financing assignment:

- There's likely a finite set of senior and junior bankers available with the experience to work on a large, complex transaction like this, so the pool of possible deal-team members may be limited—which means you need a very clear understanding of who is assigned to what deal, the MNPI they have access to, and how you're going to manage potential assignment challenges.
- Industry-focused bankers, product specialists, and junior bankers are always needed to execute capital markets, M&A advisory, or financing transactions. These are groups of bankers who are used to working with each other, and perhaps work really well together: combinations that may give the firm the best chance of deal success.
- If potential deal team bankers or the firm have conflicts, then they may not be available for staffing on a particular deal. This may occur during M&A auction situations, and also where the firm may have multiple clients seeking advisory or financing services.
- This may also be the case if the firm is already working with a client involved in the transaction, has prior commitments to clients, has made non-compete promises to clients, or has knowledge of employee limitations.
- In these situations, multiple deal teams may need to be established and the firm must consider how to wall off and separate the teams. Sometimes this may be referred to as multiple deal teams, or as deal trees.
- Depending on the opportunity, advisory or financing will also play a role in the types of bankers required to staff an engagement. For a financing transaction, for example, deal teams will likely require bankers that specialize in credit products such as leveraged finance, asset-based lending, high yield, or investment grade bonds.
- These staffing decisions are complicated and will vary depending on the structure of the transaction and the products involved.

Here are some things to think about as you seek buy-in for the formation of the control room department:

- Management buy-in can be a challenge, especially for firms that are just starting out in a space that typically requires a control room. How are you going to approach this potential challenge? What steps do you need to take to get that buy-in from the start?
- If leadership doesn't understand or doesn't have experience dealing with MNPI, then compliance management will need to educate leadership of the regulatory risks and reputational challenges. Be prepared to educate, and to share real life examples of firms who may have allowed risk to go unmonitored for too long.
- Make sure leadership understands the current state of affairs—inefficiencies or overloads the firm is facing that might indicate change is needed. Do you have more employees than ever at the firm? Has processing paper or PDF brokerage statements become unmanageable? Do you feel compliance is understaffed in terms of managing all the risk and manual processes you face? Take this evidence to firm leadership and back it up with tangible data.
- If people haven't come from more established firms—where they understand what is required and expected—employees are likely to complain about the rigorous processes the control room implements. While it's an overused phrase, tone from the top is important and can help curb complaints as the rest of the firm sees the level of support coming from leadership.
- And tone from the top demonstrates to the rest of the firm that the processes compliance is putting in place are critical to safeguard the firm. Without that tone from the top, it will be much harder to convince employees to adhere to the new control room policies and processes.
- Establishing the appropriate culture is key. Obviously, the message should come from senior management first and foremost, but middle management also has a responsibility to set the tone for relationship managers, bankers, traders, sales, research, and support personnel.
- Training is critical at every level of the organization so everyone understands the important role control room plays and why the oversight this department establishes is necessary.

SECTION 4: BUILDING OUT YOUR CONTROL ROOM

Once you've determined scope of coverage and mandate, the next step is designing the appropriate information barriers, policies, procedures, controls, and last but not least, staffing

> *"Steering a big ship like a bank onto a new financial course, like maybe setting up a capital markets program, is like steering an aircraft carrier," says Brown. "You can't just turn it on a dime. It takes time. It takes configuring. You have to tailor it. You need adequate policies and procedures in place. What does that mean for a regional bank versus a bulge-bracket firm? What's adequate for one firm might not be adequate for another. You have to have a lot of conversations to figure out what's going to work."*

Power to the people—control room people

Let's talk about people. That's right, people. For all the focus in the modern era on the capabilities of tech and automation—and those capabilities are significant—you still need good people in charge. Control room officers are the top guns of compliance, to return to our aviation metaphor. They are specialists who have to operate at the highest levels of risk mitigation. The firm's biggest deals offer the greatest potential reward but also the greatest potential risk. Missing an engagement or research report, or not properly vetting your deal team for conflicts, could mean not just loss of a profitable deal but also regulatory scrutiny and the consequent fines, sanctions, and/or cease-and-desist orders.

So where do they come from, these compliance hotshots? Some have made the climb from the bottom of the ladder, starting out as generalists who rotated around their firms and got a good handle on many different aspects of compliance. They're people who aren't afraid to walk out into the employee population and press the flesh: a very human skill, and an important one even in the age of automation. They're people who are passionate and naturally curious, people who aren't afraid to ask questions. They're investigators and puzzle solvers. People persistent enough to push for what they know is right and who are constantly thinking about ways to protect the firm. They're also team players.

> *"I think of the control room function as a team sport," says Brown. "I'm a cycling enthusiast, and thus a big fan of the Tour de France. That's a 2,100 mile bike race over 21 days. A marathon, not a sprint. And it's a team effort: the riders have to rely heavily on each other and support staff. It made me think of the control room function. The teams that make it successfully to the finish line of the control room marathon are those that work together closely and work together well. Without passion, team effort, and team spirit, control room teams will inevitably spin their wheels and deal-sinking conflicts will be missed—to the detriment of the firm overall and the employees at every level who work to make the company a success."*

What a typical day in the life of a control room officer looks like:

It's fair to say that no two days are alike. This is what keeps the job of a control room officer interesting. At the same time, control room officers have to be on their toes. Ready to react to difficult situations that suddenly pop up.

In the control room that may mean:

- Reacting to a potential insider trading alert.
- Reacting to an underwriting with a Reg M restriction, as trading is asking questions around what is permissible.
- Clearing a research report when you're uncertain whether there's a safe harbor to rely upon.

It also means keeping up with new opportunities, pitches, and engagements, as well as lost, announced, and closed transactions. Control room officers may attend and monitor origination and industry pipeline meetings, along with morning research, sales, and trading meetings to better stay aware of potential control room situations.

Control room officers also frequently work with fellow equity and debt compliance officers to participate in or monitor committee meetings. They also talk with fellow compliance officers to understand what they do and educate them on the control room.

The best control room officers reach out across the firm to learn about all the products and services offered by the firm and develop relationships with legal—both internal and external—counsel.

Finally, control room managers should constantly be thinking of what additional processes control room employees can do to keep up with internal clients—whether that's attending new employee training to learn what analysts and associates are being taught, or by attending industry roundtables.

Information Barriers, Policies, Procedures, Controls, And Training

Firms must clearly establish their information barriers to physically and electronically separate employees that deal with MNPI—deal-side employees like bankers—from those that recommend or execute security transactions, e.g., trading, sales, or research employees. This process includes defining and assigning public-side, private-side, and above-the-wall personnel, including committee personnel. Operations and support-side personnel—including those in compliance, legal, operations, finance (FinOp), information technology, credit, and risk management—must also be considered in this assignation process. Useful tools firms should consider leveraging are human resource applications—like Workday—which contain organizational hierarchies and structures. Control rooms should determine if there is a way to plug into these HR systems and assign designations to employees. HR systems may also be helpful when assigning and tracking personnel for deal-team purposes.

When designing firm information barriers, it's helpful to leverage an MNPI inventory in creating the information barrier, policies, procedures, and controls. By methodically reviewing the types of activities and information the firm has, the control room will be in a better position to create the appropriate infrastructure to support the businesses across legal entities, affiliates, and subsidiaries. This process will also be helpful in mapping out how information flows through the organization, which is important in identifying potential conflict areas. Out of this, firms may wish to create process maps or flow charts to visualize the flow of MNPI. These designation and assignation processes can also help identify any third parties, advisors, consultants, or temporary employees who need to be considered in light of the control room function.

Information Barrier Considerations

Public-Side Employees

- Sales & Trading
- Research
- Wealth Advisory
- Asset Management
- Rates
- IT
- Operations
- Other Support
- Portfolio Management

Above-The-Wall Employees

- Executive Management
- Senior Management
- Compliance
- Legal
- Credit

Private-Side Employees

- Corporate & Commercial Banking
- Capital Markets
- Leveraged Finance
- Specialty Finance
- Financial Sponsors Coverage
- Project Finance
- Credit Solutions
- Loan Syndication
- Private Equity

Managing The Flow And Sealing The Gaps

Action Items + Workbook

Conflicts Considerations

An important part of controlling the flow of MNPI is establishing a process to identify and manage conflicts. Firms should think about conflicts in four ways:

1. Firm versus client
2. Client versus client
3. Employee versus client
4. Remote employees versus onsite

Firms are most successful when they assemble cross-functional representatives from corporate and investment banking, capital markets, compliance, legal, and other risk-support functions to identify, discuss, and review:

- □ Potential areas of conflict.
- □ Where conflict-resolution gaps currently exist.
- □ The current business selection and conflicts-of-interest process in the relationship, pitch, origination, and approval process.
- □ The policy, process, and team tasked with researching potential conflicts, escalating, resolving, and documenting opportunities and engagements.
- □ Legal documents—including NDAs and engagement, commitment, and underwriting letters—which clarify scope of services provided and the ability to perform additional roles.
- □ Disclosures and consent, as regards notifying clients of existing or potential conflicts of interest.
- □ Fairness opinions regarding material relationships between the investment bank and involved firms (FINRA Rule 5150).
- □ Standards for frequent areas of conflict, i.e., the requirements firms adhere to when providing services like acquisition financing, fairness opinions, staple financing, research, and underwritings.

Watch & Restricted List Considerations

The primary tools control rooms rely on to manage the flow of MNPI are the watch and restricted lists. One of the biggest challenges control rooms face is the timely collection of information in order to determine if a situation should be added to the watch or restricted list. Once that determination is made, keeping track of the opportunity to determine the next step—updating the watchlist notes, updating the deal team, moving it to the restricted list, or removing it from one of the lists all together—is of critical importance.

While there are tools that can make a control room officer's job easier, what control rooms really need are bankers, traders, salespeople, and research analysts who understand the firm's processes and risks and will promptly inform the control room when a trigger occurs. It's up to each firm to determine when a trigger occurs. For bankers, it may be when a firm is likely to be engaged for a deal. For trading and sales, it may be when they learn material nonpublic portfolio information from a buy-side customer. For research, it may be when they learn price-movement information from the CFO of a company they cover.

"Whatever the trigger," says Brown, "it ultimately comes down to proper training of covered employees to immediately notify the control room of the event, so a determination may be made of what needs to be done. This is all part and parcel of the strict culture that needs to be ingrained in a firm if it wants to operate at the highest levels."

Above-The-Wall Versus Over-The-Wall Personnel

Inevitably, public and private-side employees must report to a manager. This group of senior managers is often referred to as "above-the-wall." This should not be confused with "over-the-wall" employees. Above-the-wall personnel have a unique obligation to manage the firm while maintaining the sanctity of the information barrier. Significant consideration should occur prior to designating someone as above-the-wall. Once these managers have been identified, they must be tracked, trained, and monitored.

Over-the-wall situations generally occur when a public-side employee's skills and knowledge are required to assist private-side bankers in executing a transaction. These situations must also be closely controlled and monitored. Identify. Document. Train. Monitor. These are the four processes to keep in mind when determining who is above-the-wall or over-the-wall, and how to manage both cohorts.

Need-To-Know Standard

One of the most important principles in building an effective information barrier is creating a "need-to-know" culture. Simply put, a "need-to-know" exists if access to the information is vital to providing the client with the products or services it has requested. Examples of this situation include:

- ☑ Executing the client strategy or business purpose
- ☑ Managing the client relationship
- ☑ Complying with credit, legal, or compliance requirements
- ☑ Protecting firm exposure

One of the keys to a successful firm business model is creating and enforcing an effective information-barrier policy and sharing MNPI only on a need-to-know basis. As a general rule, firm employees with MNPI or confidential information must not share that information with those that aren't on the client's deal team, do not have a need to know, or are public-side individuals. Finally, creating a need-to-know culture is critical for managing firm conflicts and reputation risks. Implementing training will help cement the cultural shift at the firm.

Practical considerations include:

- □ Assessing supervisory reporting lines to determine if public-side employees are reporting to private-side supervisors. If these reporting lines exist, firms should determine if there are information barriers, MNPI, or need-to-know standards concerns.
- □ Assessing walls between origination and execution, portfolio management, secondary loan trading, and any portfolio management hedging activities.
- □ Working with the business and IT to assess and assign system, application, and electronic folders access controls by client focus, job function, need-to-know, and organizational structure.
- □ Implementing CRM software controls, so only deal team and need-to-know users have access to client information.
- □ Plenty of need-to-know training.

Write any additional notes here

Surveillance Considerations

Many regulators require firms to prevent and detect potential misuse of MNPI. In addition, regulators are becoming more proficient with analyzing big data sets in order to bring fines and sanctions against firms. The ability to conduct surveillance is therefore critical, and should start with the basics: conflict, watch, and restricted list surveillance of firm, customer, and employee activities. It's obvious firms must ensure they're capturing activities and comparing them with names on the watch and restricted lists. But what do you do with this information? How do you record your analysis? What additional information should be added to support the surveillance?

Firms should develop a comprehensive and consistent employee and employee-related accounts policy that provides detailed requirements regarding permissible employee trading. Considerations may include:

- □ Requiring employees to maintain their accounts at a limited number of designated brokers in order to receive electronic feeds and eliminate paper statements.
- □ Requiring all employees and employee-related accounts to pre-approve all trades, not just trades in securities included on the restricted list.
- □ Implementing business unit and conflict restrictions defined by employee type.
- □ Implementing a securities-holding period to discourage speculative trading, which could be an indication of potential manipulative activity. Holding periods are a common industry practice and typically range from 7 to 30 days.
- □ Imposing additional limitations on employee investments, e.g., no trading in options or futures.
- □ Requiring employees to attest they've disclosed all their employee and employee-related accounts in accordance with firm policies and procedures.

Pre-Trade (Preventative) Reviews & Approvals

Firms may wish to implement controls to restrict trading activities through order management system (OMS) configuration rules. For example, a firm may require additional approvals for trading restricted-list securities. Firms may also simplify and streamline employee personal trading through the use of pre-clearance software that scans potential trades against: (1) watch and restricted lists; (2) fund-trading activity; (3) holding periods; (4) blackout windows; and (5) de minimis thresholds. Finally, firms may facilitate testing of trading activity through automated electronic feeds from brokerage firms.

Post-Trade (Detective) Surveillance

Firms may wish to identify trading in securities where MNPI may be known. They may also use automated rules or statistical algorithms to identify patterns of trading activity that could indicate the use of MNPI based on multiple risk factors. These risk factors could include timing, capital-at-risk, or performance. Firms may also enhance their existing data sets—and by extension their ability to monitor for insider trading—by incorporating third-party reference data such as market data and news feeds.

Electronic Communications (E-Comms) Surveillance

We all know that firms must monitor internal and external emails, instant messages (IMs) and chats. With the plethora of electronic communication applications available, identifying and capturing all vendors, services, and tools is a challenge. We also know that surveillance of internal and external electronic communications has become a standard part of compliance and supervision in the post-research, Libor, and FX scandals. Now the question is, what role should the control room play in monitoring e-comms? One solution is incorporating watch or restricted list names into the monitoring lexicon. Firms obviously need to restrict and/or supervise e-comms between banking and research. Firms may also wish to monitor and/or restrict e-comms between banking and the rest of the public side—like sales, trading, and wealth management—and restrict project emails to non-deal team members or clients.

Firms should include testing of communications to identify incoming or outgoing MNPI, customer communication patterns vs. sales and trading activity, and relationships of interest. Firms should include e-mail, messenger software, Bloomberg, BlackBerry IM, and other web-based mail and social networking sites as used on firm networks. As firms mature they should consider incorporating surveillance and analysis of telephone logs, calendar entries, and gifts-and-entertainment logs.

Other areas of concern and potential abuse firms should not ignore include:

- □ Loan trading
- □ Distress trading
- □ Over-the-wall activities
- □ Market-moving events and regulatory filings
- □ Front running, i.e., trading ahead of a client, research, M&A, and capital market events
- □ MNPI produced "outside the four walls" of the firm

Information Security & Employee Electronic Access

Does your information security protocols limit who can see client, project, and borrower specific information, especially for public companies? In order to bolster information barriers, firms should assess system controls—including pipelines, CRMs, confidential files, credit and loan portfolio files—to determine if access controls are sufficient. Firms have the best results when control rooms work with first-line businesses and IT to assess and assign system access across the board by client focus, job function, need to know, and organizational structure. Procedures should also be developed to limit deal team folder access to only members of the deal team, and controls developed to limit and monitor access and training on protecting client information. If unauthorized access is discovered, firms should investigate the situation and determine what actions should be taken.

Training & Reviews

After establishing comprehensive policies and procedures, firms must design compelling training programs that are more than just rote and one-size-fits-all. Firms should tailor training specific to the business unit and employee. Think of creating a bespoke training plan for each business and type of employee.

Insider Trading Training

Promote:	Training element:
Overall awareness and understanding	• Identify key terms related to insider trading. • Identify rules and regulations governing insider trading, including institution-specific guidelines, responsibilities, obligations, and prohibitions. • Train rigorously on information barriers, conflicts, and personal investment policy.
An understanding of what applies to each employee and why	• To illustrate real-life risks, use situations that your employees are likely to encounter.
An understanding of consequences of noncompliance	• Use actual enforcement cases to demonstrate consequences. • Always involve senior management in delivering key messages. • Use case law, news articles, real life examples, and frequent compliance bulletins to illustrate lessons learned.
An understanding of gray areas, and how to reach out when the employee has questions.	• Use scenario-based situations, based on client-specific examples.

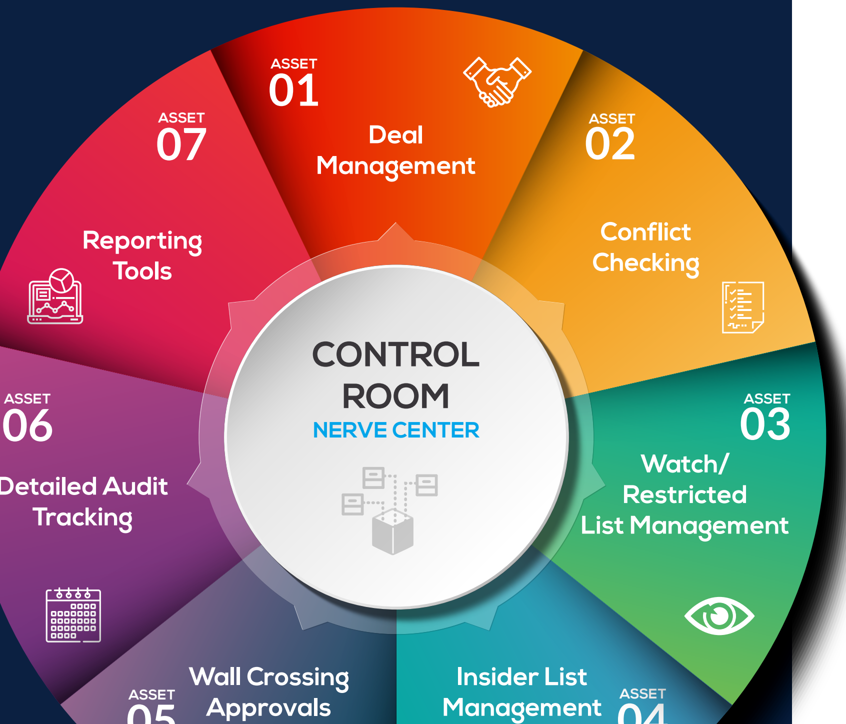
SECTION 5: OPTIMIZING YOUR CONTROL ROOM

In the modern age optimization means automation, and automation means software. Here's what a good control room software solution looks like

By this point, you've thought through a myriad of control room considerations. Policies. People. Controls. Training. On and on. Now, how are you going to manage it all? You might be surprised to learn that many of the largest financial firms still rely on a mix of spreadsheets, manual reviews, and institutional memory to do the job. Regardless of the size of the firm and the products offered, your firm could do the same. It would be an inexpensive way to get your control room up and running.

However, firms that are still employing manual or semi-manual processes can't keep doing it forever. Firms are only getting bigger, deals more complicated, and regulations more comprehensive and complex. And speaking of regulation, regulators are getting pretty tech savvy themselves. Regulators are now using Big Data to analyze trading; this wasn't the case even just a few years ago. It's fair to say that regulators now expect firms to implement technology to identify conflicts and suspicious trades.

Following are common concerns and challenges control room teams face and how technology can help.



MORE COMPREHENSIVE MONITORING OF MNPI

Policy violations—perhaps an employee not properly pre-clearing a trade—are unwelcome occurrences. But regulatory violations—like an employee trading on insider information, trading in violation of Reg M, or the firm issuing research during a distribution when there is no safe harbor—is an altogether different story. A regulatory violation will likely involve a prolonged investigation, fines and sanctions against the employee, and possibly against the firm and management. It will also likely lead to a cease-and-desist order against the firm. "Starting out," says Brown, "the biggest challenge I faced was we had so many different systems in the mix and none of them spoke to one another. There was no aggregator. Sure, we had access to all of them, but I had to constantly wheel from one monitor to another."

Today, software can be the aggregator. The deal-data centralizer. This is exactly what it sounds like: a system that gathers as much deal-related information as possible into one place, in particular through integrations. Good control room software means easy integrations with existing firm systems, including CRM, human resources, market data, and research. All of this adds up to simplified analysis of the deal data required to keep a close eye on activities, which translates into faster, safer decision making and less firm risk.

Now Let's Do The Math

Figure out the hourly salaries for those who spend their time aggregating data.

Multiply that number by the number of hours it takes

then multiply that by the number of days they spend doing the job.

You may be shocked at how much this actually costs. Now think about what your team could do if at least half of those hours were given back – what could you do with that time?

MORE COMPREHENSIVE COLLECTION OF MNPI

Modern control room software will integrate with your existing employee conflicts monitoring suite and CRM applications—giving your control room team the widest possible view of employee activity, and the clearest possible insights into potential deal-team conflicts and MNPI flow. On the employee side, good software offers users a portal through which they can self-report and update deal-projects and MNPI they've received. Thus, control room officers will immediately be made aware of any employee-surfaced deal-project or MNPI.

From a control room perspective, this process works similarly. **Control room software can provide deal team members an easy way to report and record any MNPI they've received**, giving control room officers the information required to advise on team formation or manage deals that are already in motion. Brown: "One thing that's too easy to forget is, just because a deal and deal-team members have been cleared initially doesn't necessarily mean everything is going to stay cleared through the end of the project. Deals and MNPI evolve and have to be monitored on an ongoing basis."

BETTER DEAL TEAM BUILDING

On the subject of deal teams, here's how software can help you optimize the process of assembling them. As discussed earlier, there are many considerations that go into pulling together a group of people to work for what might be an extended period on a single deal, with the chance that many of these same people may end up working on other deals at the same time in different configurations. Perhaps there's a finite set of bankers—industry or product bankers—on tap who can work on a certain type of deal or transaction. Of those available, bandwidth for taking on another deal may be an issue. And some bankers may only work well with certain other bankers.

Staffing a deal team, then, can become a complex exercise in social engineering. But because a modern control room platform is a deal-data centralizer, you can far more easily sort through all these crisscrossing currents of potential deal-team conflicts. All the information you need to make an informed decision quickly and safely is right in front of you. **Spreadsheets and emails, and institutional memory, all quickly become relics of a past age you can barely believe you operated in.** "I once worked with a senior banker," says Brown, "and her responsibility was to know the employees and know who was available for what deal. She knew who was appropriate and who wasn't. Who worked well with whom. Deal-team staffing came down to a lot of institutional memory. But what happens when those bankers with 20+ years of experience leave or retire, and take all that information with them? How do we capture all that experience and intelligence? A control room software solution doesn't solve every problem, but can go a long way toward solving many."

EASIER INFORMATION BARRIER MANAGEMENT

Modern control room software makes management of the information barriers themselves radically easier. It means easier identification and tracking of employees by role, location, and whether they're public or private-side employees. It means an easier time granting and monitoring access to system and deal files. It means an easier time securely linking information to watch and restricted lists—on a global basis if necessary—and updating that information in real time.

With modern software you can associate entries with projects and associate entries with the type of required restrictions. You can maintain lists of employees and third-party contacts who hold MNPI and would be considered insiders against a project. You can associate entries down to the project level and type of required restriction, and eliminate duplicative data entry by publishing lists to downstream systems that your control room software has integrated with.

SECTION 6:
THE FUTURE OF CONTROL ROOM

Where is the control room function headed? How has COVID-19 affected the digitization and automation of control room processes that were already in progress?

Personal Investment Policy In The Time Of Coronavirus

For much of the developed world, everything changed in the first few months of 2020. Governments put their populations into various degrees of lockdown, economies nosedived, and markets went on a rollercoaster ride and took investors with them. Because of this market volatility, firms saw an increase in trading, including employee trading. A recent study by StarCompliance found that firms globally have experienced three, four, five, six, or even seven times the amount of employee stock trading as pre-COVID-19. Couple this increased-trading phenomenon with the other related effect—employees working remotely at unprecedented rates—and you have a recipe for significantly higher trading risks and possible regulatory risks.

"If it weren't for the pandemic," says Brown, "the future of the control room would be several years out. Based on conversations I've had with control room colleagues, no one really knows when employees are going to get back into a physical room. Maybe never, for some. COVID-19 has really accelerated the digitization and automation of processes for many different functions, including the control room. And if some control rooms aren't there yet, they need to quickly figure out how to deal with the paper deal files, posted notes, and paper statements that come with manual processes."

These next considerations offer a starting point to work coronavirus calculations into your control room plans:

□ Develop repeatable workflows.

□ Determine how to maintain the synergies you once had while in the office through alternative means of communication. These processes should be built into the workflows.

□ If you don't make it back into the actual control room, what are you going to do? Come up with a plan.

□ Work to digitize all necessary information in order to do the job, e.g., firm, customer, and employee trades.

□ Establish clear and easily repeatable pre-clearance processes. Compliance software platforms have gotten very good at this.

"The pandemic is making firms rethink many aspects of compliance," says Brown. "Take working from home, and how it might affect information leakage. Let's say three people work at the same firm. One's in trading, one's in research, and one's in banking. Previously, they all would have gone into the office and been in physically different locations. Now they're sharing an apartment in London and overhearing things they shouldn't, and in pre-COVID times wouldn't. People might also be more apt to let their guard down at home. There's no longer that clear separation between work and home."

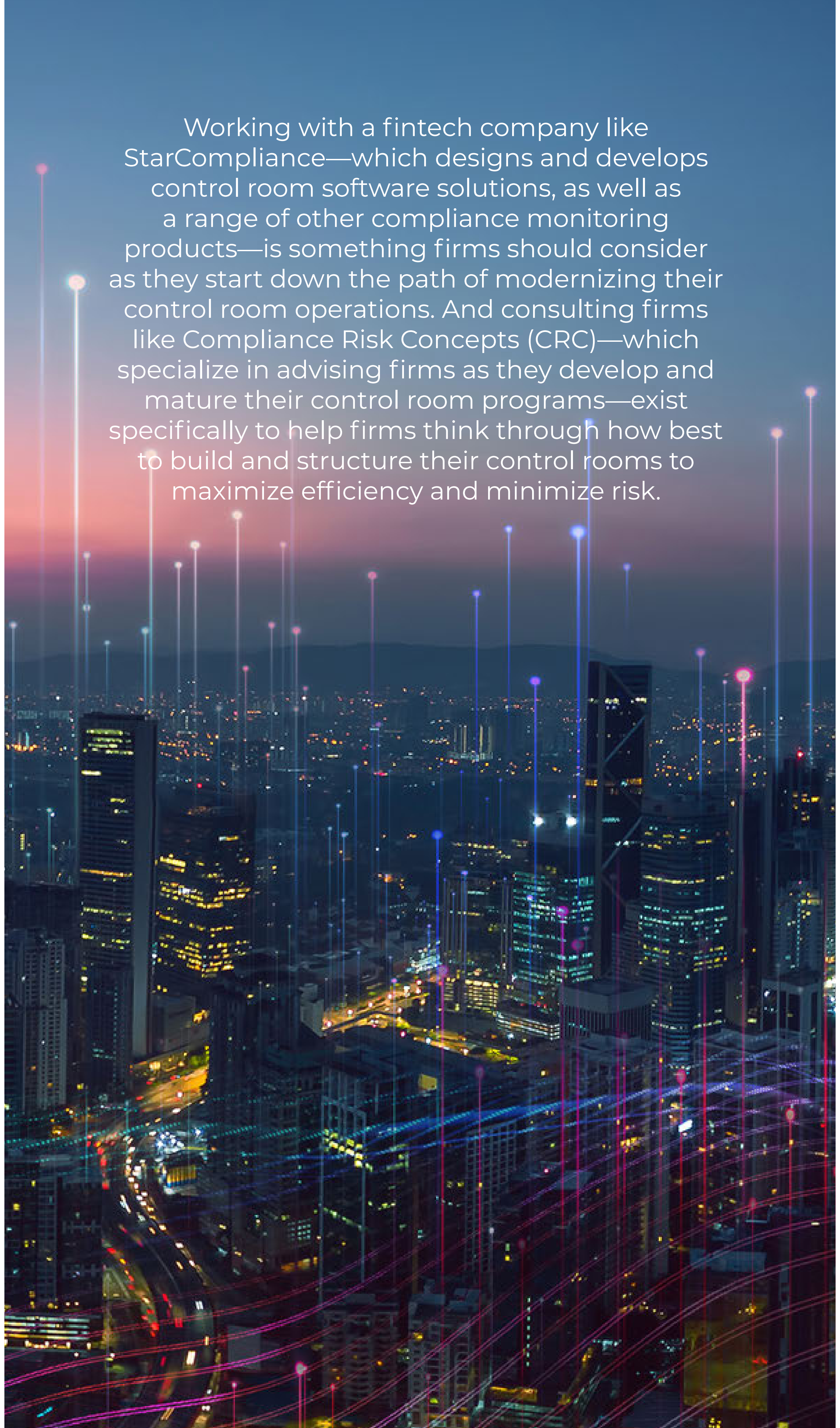
Reimagining line of sight

If people are no longer “at work,” at least not in the physical sense, what’s the next best thing? “From a supervisory perspective,” says Brown, “you always want line of sight. But line of sight as we know it, as a compliance control, may no longer exist. How can it be reimagined?” Monitoring communications will be part of that reimagining. Whether it’s email, chats, WebEx, WhatsApp, Zoom, Teams, etc., internal and external employee e-comms will have to be integrated into control room systems, so they can bump up against the watch and restricted lists and any potential conflicts can be identified. Perhaps even developing and monitoring employee behavior through metrics and profiling. Brown: “As futuristic and perhaps crazy as some of this sounds, firms will need to adapt, and keep an open mind and be forward thinking in the process.”

And what about roommates? Firms already keep an eye on spouses and significant others, but now it’s not just partners that are of concern. Someone in sales at one firm may be rooming with someone from research from another firm, and maybe someone from trading from yet another firm, all working around the same dining room table or in a similarly confined space. Brown: “You’re structuring the deal team and information barriers. You’re looking at relationships. But maybe firms need to understand who employees’ roommates are. The industry has been talking about significant others for a while anyway, but *the pandemic has taken this concern to the next level. Maybe it needs to go into future conflict assessments. Maybe innovative firms will create alternative, secure working spaces to solve this challenge.”*

And perhaps there will be more money in firms’ budgets now. As a result of COVID-19, more money can potentially be invested in the kinds of emerging technologies that can be instrumental in the reimagining of line of sight. Why might there suddenly be all this money lying around? Brown: “If most of the firm is working from home, and that trend continues beyond the end of the COVID-19 crisis, which I believe it will, there should be a considerable savings in real estate costs: the money previously poured into expensive urban workspaces. This could potentially be redirected into compliance for technology such as conflict and line-of-sight monitoring.”

And where might this line-of-sight tech come from? This leads directly to another observation by Brown: “It’s going to be more important than ever to know how to partner closely with fintech providers—third-party vendors—for solutions of all kinds. *Getting back to the acceleration of digitization and automation, tech was already becoming increasingly important for financial firms, which were increasingly turning toward vendor solutions for these needs.* The pandemic has meant an acceleration of the acceleration of these trends, and outside solutions of all kinds are coming into play. Vendor technology solutions are a way for the business world to keep up with this sudden shift.”



Working with a fintech company like StarCompliance—which designs and develops control room software solutions, as well as a range of other compliance monitoring products—is something firms should consider as they start down the path of modernizing their control room operations. And consulting firms like Compliance Risk Concepts (CRC)—which specialize in advising firms as they develop and mature their control room programs—exist specifically to help firms think through how best to build and structure their control rooms to maximize efficiency and minimize risk.

Hootin’ and hollerin’ from home

Traders and salespeople are a tightly knit bunch, accustomed to operating in close quarters with a lot of verbal banter and market commentary. Enabling this banter is something called the hoot-and-holler, often referred to simply as “the hoot.” It’s a squawk box system that keeps a circuit permanently open, so people—in this case traders and salespeople—can quickly and candidly communicate back and forth across an expansive trading floor. Firms had initially been reluctant to close their physical trading floors out of a fear that trading simply couldn’t be done from home: that the technology wasn’t sufficient to handle the volume and latency necessary to maintain an orderly market. And perhaps also out of a fear the in-person banter presumed necessary to do the job successfully couldn’t be replicated in a remote fashion.

What most firms found instead was that their business continuity plans worked well and the technology infrastructure was able to handle the load. In addition, firms started to get creative to make up for the lack of direct dialogue. Brown: “CRC recently hosted a virtual forum and one of the things people discussed was leaving Skype or Zoom open all day, to emulate office interaction.” At the time this e-guide went to press, UBS was considering issuing its trading staff virtual reality headsets with camera feeds in an attempt to recreate the in-person trading floor experience in traders’ homes. In the end, it would appear that firms have adjusted nicely to employees working remotely since the early days of the pandemic, at least from a revenue perspective. In the first half of 2020, investment banking and trading revenues for the world’s 12 largest investment banks hit an eight-year high, up 32% year-over-year.

“All that said,” says Brown,” there’s still an awful lot that comes from physically being in a room or on a trading floor with other people. Playing off one another. Hearing what’s going on. Interacting directly. Having that trading floor, bullpen, or control room banter. I don’t know exactly how you replace that, but the financial industry is doing a good job of it so far.”

“It’s about maintaining a balance. Taking the best of what existed pre-COVID and leveraging advances in technology to maintain line-of-sight supervision, track behavior, and monitor for the misuse of MNPI. Regardless of firm size or sophistication, that’s the critical thing. *Technology solutions and innovation can help control room officers assemble the data needed to identify patterns and conflicts.* But whatever path firms and control rooms take, we know that the control room function and control room officers will continue to play a vital role in the protection of the markets and firms.”

compliance risk concepts

CRC is a business-focused team of senior compliance consultants and executives providing top-tier compliance consulting services to clients on an as-needed, project or part-time basis. We provide our clients with the critical skills and expertise required to establish, maintain and enhance a balanced and effective compliance operational risk management program. We help organizations demonstrate a commitment to a strong risk management culture.

For companies with no in-house compliance implementation services, we handle ongoing, routine compliance matters at a fraction of the cost of traditional resources, including counsel and compliance consulting services.

For larger companies that have a CCO, General Counsel or in-house staff, we serve as overflow executives, acting as an extension of the in-house team to review and ensure compliance is working properly, manage spikes in workload or address underserved areas of the business.

For more information about Steve Brown & Compliance Risk Concepts, visit compliance-risk.com

Steve Brown - Director, Broker-Dealer Services
Compliance Risk Concepts

Steve is responsible for CRC's broker-dealer compliance practice. Steve has over 25 years of capital markets compliance experience and is an industry expert in control room, investment banking, and conflicts of interest issues.

Steve has successfully advised and completed over 100 projects for clients, including: assessing and creating control room and conflicts of interest programs; executing broker-dealer new business initiatives; assisting clients in developing governance, risk, and compliance strategies; assessing and implementing supervisory and compliance programs; creating and executing global compliance risk assessments; and assessing and developing global compliance programs.

STAR COMPLIANCE

www.starcompliance.com