IBRS

Dr. Joseph Sweeney

Future of Work

Teams Governance: Emerging Better Practices

Special Report

So you've got Teams... now what?

The use of Microsoft Teams (Teams) skyrocketed in 2020, largely due to the need to get staff working from home quickly and collaborating seamlessly. Microsoft reported a greater than 50% increase in Teams usage in the later half of 2020. Furthermore, IBRS clients report that the rapid uptake of Teams during lockdowns has not abated as people return to work. The value of collaborative working environments has been fully demonstrated, and there is no turning back.

In short, Teams is one of the platforms spearheading the introduction of deep collaboration.

Deep collaboration is where new collaborative working environments fundamentally alter not only how people work together, but the processes of how work gets done, who does it, where it's done, and most significantly for this guide, your organisation's information lifecycle.

> "Deep collaboration is disruptive."

This special report focuses on how to address the disruptive nature of Teams and the new risks: that is, what is urgently needed for Teams governance. However, IBRS recommends that better practices for Teams governance should be considered within the scope of a comprehensive Future of Work Strategy.

Following this report, you will be able to quickly identify the seven key Teams governance areas to address in 2021. These areas not only protect your organisation, but provide foundations for the highly collaborative landscape that will define the next decade.

What is a Future of Work Strategy?

A Future of Work Strategy takes into account the tectonic shifts in how people will work in the post-COVID era. This strategy is more than just an attempt to balance office and home work locations. It must explicitly address how collaboration, while delivering many benefits, also disrupts many aspects of the workplace, how organisations are run and introduces new risks.

From a business perspective, this strategy must consider how collaborative working platforms will:

- enable processes that extend beyond the organisation's traditional boundaries
- change where and how new staff are sourced
- change hiring practices and staff contract conditions
- introduce new workforce behaviours and habits
- alter how staff performance is measured, who has access to such measures, the impact to remuneration, and impact on workforce policies.

From a business ICT perspective, this strategy must consider how collaborative working platforms will:

- break traditional information management
- force a re-evaluation of compliance policies
- dramatically increase the risk of information leakage
- lead to new demands for electronic records and information management solutions
- force a re-imagining of identity management and access control
- create strong demand for zero-trust security
- accelerate the rise of citizen developers and analysts.

Beyond Teams: Impact of deep collaboration

With the rush to deploy Teams to enable remote work in 2020, the majority of organisations have not yet fully considered the highly disruptive nature of deep collaboration.

It is important to note that it is not actually Teams which is disruptive - it is the collaborative working practices it enables that cause the disruption. Any of the new collaboration platforms (Slack, Zoho, etc.) can introduce this disruption. Such tools were disruptive well before COVID-19. However, it is the rate at which staff have embraced these tools due to working from home that has caused collaborative working practices to become very disruptive, very quickly.

Flatter, leaner organisations

Disruptive collaboration changes how people communicate with each other, whom they communicate with, and how much empowerment they have to make decisions, either individually, or as a group. It also changes how those decisions are validated and checked. In short, the deep collaboration enabled by Teams encourages cross-departmental and even external-facing working practices, that quickly flattens organisational hierarchy.

Collaboration tools such as Teams are here to stay, whether staff are working in the office, remotely or from home. The result of the rapid uptake in Teams usage will be that organisational structures will start flattening over the next decade. So any decisions made about Teams governance need to consider the possibilities - and challenges - of a flatter, leaner organisation structure where staff have more decision-making power.

More performance metrics - but what for?

Along with changing organisational structure, the new collaborative tools allow far greater insights into what staff are actually doing. Tools such as Teams (and Office 365) are capturing metrics about staff activities at a rate never before considered.

An outcome of this is the ability to report on staff 'performance' at a much more granular level. Access to such metrics is a double-edged sword. On the plus side, it enables organisations to monitor collaborative activities and determine areas that may need additional coaching or direction. It also enables organisations to look at the differences in how various departments, or even individuals, engage with other staff. On the downside, it runs the risk of organisations overly focusing on activity, rather than outcomes.

As Office 365 and Teams continues to collect an increasing amount of activity data, organisations need to carefully consider what they wish to do with such information, the insights that may benefit the organisation, and what the impact of reporting such insights will be on staff. How much of that information should be shared? How to measure people's actual outcomes - not just activities - in this new world of deep collaboration?

Benefits of borderless organisations

Deep collaboration allows for a fundamental change in how organisations think about who does the work. In the past, when working with a client or a supplier, there was a very clear delineation between the stakeholders and the work being done. With deep collaboration and the ability to bring external guests (clients, suppliers, contractors, etc) into a Team, the clear delineation of work breaks down.

Organisations are discovering that having external and internal stakeholders jointly working on projects and documents in real-time provides far better outcomes than the traditional 'back and forth' work

patterns of the past.

IBRS research into the impact of collaboratively working with external stakeholders revealed some powerful benchmarks for the development of enterprise strategies, procurement documents and other complex, knowledge-rich reports:

- Projects finished faster: overall time to deliver reduced by 20-30%
- More efficient delivery: total hours spent reduced by 5-15%
- Sharper deliverables: document word count reduced in size by 25%
- Great quality: information density (the number of discrete points of consideration) increased by up to 40%
- Improved satisfaction: acceptance of deliverables on first draft date close to 100%
- More actionable: reports and strategies developed with collaborative practices saw close to 90% adoption at 6 months and 3 year review marks

Hiring changes

The lockdowns of 2020 proved that work from home, when empowered by appropriate collaboration tools, does not impact productivity for many roles. Human resource executives have now recognised that hiring remote workers is not only viable from a productivity and inclusivity perspective, but can significantly lower staff turnover and costs.

Organisations have reported to IBRS that hiring remote workers (that is, workers from outside of central city locations) can lower salaries by up to 20%. Obtaining a more diverse workforce is also demonstrably easier if remote working conditions are offered. Several organisations also report hiring remote workers dramatically increases staff retention, provided an appropriate collaborative work environment such as Teams is in place and managers are well versed in managing remote teams.

IBRS expects that as staff and management become increasingly

familiar with working in a deeply collaborative, collegial environment with a flatter organisation structure, there will be a significant shift to hiring more for talent and specific skills, than geographic location. At the very least, while competition for specialist skills will remain high, the ability to recruit staff from far afield can restrain salaries.

Security is not a wall

Deep collaboration means the traditional 'networked borders' of organisations will be rendered next to useless for information security. Attempting to 'wall off' an organisation's documents from external parties via controlling network access simply won't work when external stakeholders are collaborating with your staff.

Both technology and business executives need to fundamentally shift thinking about how information is secured. At the very least, a 'zero trust' approach must be considered for information assets.

Click here to book a complementary Whiteboard Session

The promise of Teams… and the risks

Staff take the lead

During 2020, Teams rapid uptake was driven by one key feature: its ability to host staff video sessions. However, users have quickly found that its deeper benefits lie in its ability to group work and all the conversations, ideation and documents into… well… *teams*.

Discussions with over 80 Australian organisations across both the public and private sector, confirm that once staff experience Teams's collaborative workplaces, they quickly adapt it into day-to-day operations, often in ways that were not previously considered by ICT groups or executives. Staff quickly 'make Teams their own'. As a result, Teams is being increasingly applied to work processes that have not previously been digitised, and to processes that previously required multiple back-and-forth approvals.

It is important to note it is the staff themselves, not ICT, that are applying Teams in this way. Teams is first and foremost a staff-led tool for solving the work issues that matter to them.

New ways of working means news risks

Unfortunately, most staff members do not consider the business risks associated with using Teams in new ways.

For example, creating a work group (a *team*) for evaluating new hires may dramatically improve the quality of human resources decisions, but it may also expose sensitive information to other parts of the organisation or even externally. A working group may use Teams to develop a new policy report collectively, yet not appreciate this approach may breach requirements for tracking submissions and document changes.

Training in risk management and cyber security awareness are important, and IBRS strongly recommends that any training in Teams usage explicitly includes these topics. But such training only goes so far. ICT groups will need to negotiate a Teams governance framework with the business, and then configure Teams to support this framework. It is also likely that additional technologies may be required to reduce risks - especially concerning information leakage.

Understanding Microsoft Teams

From an ICT perspective, Teams governance demands a consideration of four key areas, as shown in Figure 1.

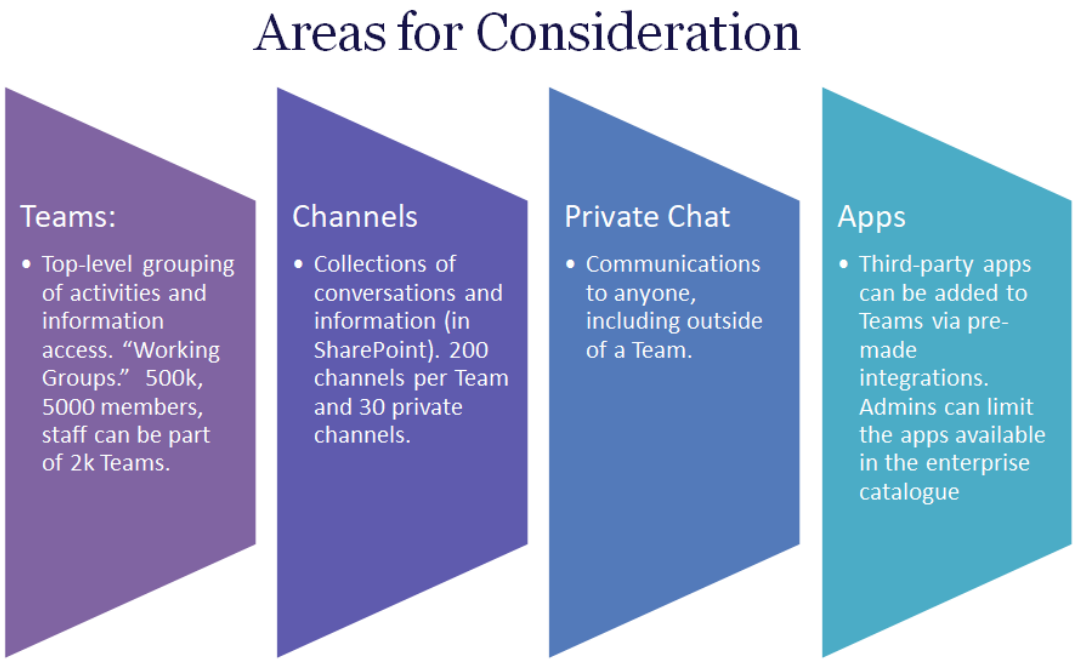

Figure 1: Microsoft Teams Areas for Governance Consideration

What are Teams teams?

Not the entire product itself, but the 'working group' feature called *teams* for which the product is named[1]. These *team* (work groups) are the way the product groups people around specific activities, processes and information. The product allows for half-a-million teams, each of which may have up to 5,000 members. Each user of the product may be assigned to up to 2,000 *teams* work groups.

Teams work groups are an important consideration because once a user is invited into a *team*, they can access the discussions and information held within that *team* work group. Note that a user may be an internal staff member or an external guest, such as a contractor or even a customer. Therefore, tight controls must be put in place to ensure that

[1] To help distinguish terms, IBRS differentiates the Microsoft Teams proc work group feature of the product by using italics for the feature.

only the right people are invited to participate. In addition, *teams* store information in various ways, which impacts information lifecycle management, retention and disposal policy, and e-discovery.

In addition, the structure of your *teams* effectively represents the new collaborative working structure of an organisation. Consideration is needed to define *teams* to best meet the organisation's current and future needs. Over time, IBRS predicts that the structure of *teams* (which teams are created for which traditionally cross-departmental activities) will replace the traditional department structure of organisations.

What are Teams channels?

Channels are collections of threaded discussion and information sharing within a *team*. They can be thought of as the 'topics of interest' within a working group. Each *team* may have up to 200 channel, plus 30 private channels.

Like *teams*, channels require consideration from an information management perspective. What conversational activities need to be captured? How will channels be structured to align with desired work practices and processes?

What is Teams private chat?

Teams allows for private chat between users, much like instant messaging with limited file sharing capabilities. It is possible for private chats to be with external people.

Private chat needs consideration of how to balance compliance of staff privacy, information security, trust and regulatory compliance for tracking conversations.

What are Teams apps?

Many popular software solutions can be integrated with Teams with minimal effort. For example: Zoom and Webex are common integrations for video conferencing, LucidChart and Cacoo for diagrams, Wrike and Microsoft Planner for project management, Service Now for workflow, and more. As Teams becomes the de facto 'work bench' for staff, the

demand to integrate apps into Teams will grow.

Consideration must be given to who decides which apps will be deployed into Teams, and how such decisions will be made. As information is added to these integrated apps through Teams, consideration of information management is also needed.

Where's data stored in Teams?

Given the pressing need to consider information management in all areas of Teams, it is important to understand where information resides. Figure 2 details where information from different Teams services are stored. From an information management lifecycle compliance perspective, the majority of these storage capabilities may need third-party products for backup and recovery, archival, compliance with data retention and disposal policies, privacy and e-discovery.

In short, information managers and enterprise architects need to work hand-in-hand to ensure that the information within Teams is robustly managed.

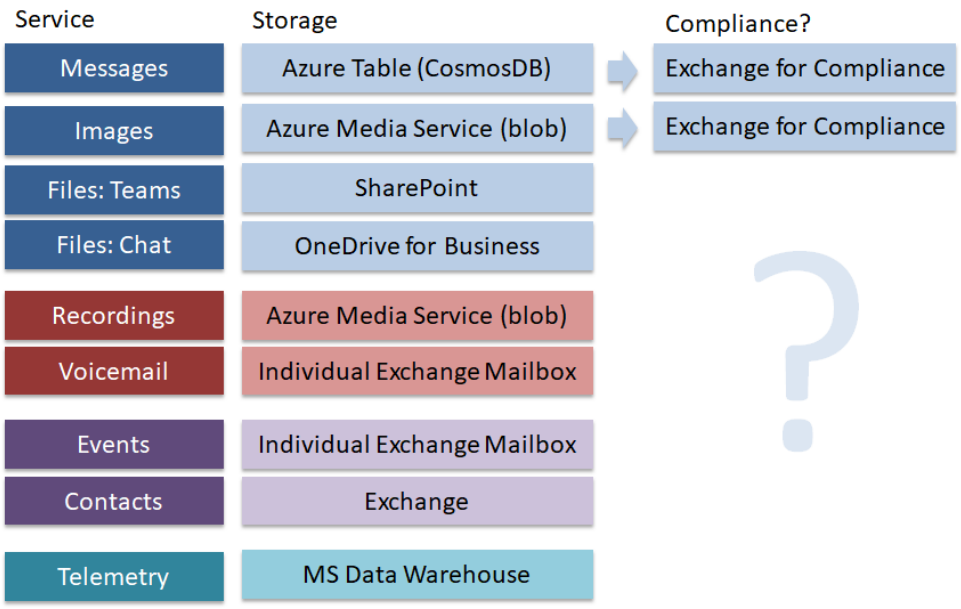

Figure 2: Where is Data Stored in Microsoft Teams?

Information management is the common problem

In all four areas, the need to know where information is stored, controlling who has access to it, and managing its lifecycle - including backup, archival and disposal - are common issues. Therefore, considering the impact of Teams on information management must be a priority for any business that has deployed the product.

Seven critical governance issues

Provisioning teams

It is one thing to provide Teams to the organisation. It is another to provision teams (working groups) to the organisation.

Since Teams allows half-a-million *teams* to be created, allowing all staff the unfettered ability to create a *team* can result in a sprawl of working groups, many of which have overlapping roles. Larger organisations have reported that such sprawls can lead to information and working groups becoming isolated from each other - the exact opposite of the goal of Teams. Furthermore, with deep collaboration, organisational structures will flatten over time, with the structure of the collaboration environments becoming as, if not more, important than traditional departmental roles for day-to-day work activities.

As such, how *teams* are organised within the Teams environment is vitally important.

For example, *teams* may be organised around business practices, customer-centric processes, existing divisional structures, and more.

The discussion regarding how to structure *teams* must be held at an executive-level. It requires the input of human resources, sales and customer services, admin and finance and more. The discussion is literally - how will our staff work together in the new era of deep collaboration? How will the organisation be working in 10 years time?

A governance principle that appears to be emerging is that *teams* should match the work to be done, not the hierarchy of the organisation.

ICT's role is to outline how that world could look and explain why setting the foundations with *teams* is so important to get right at an early stage.

Once a decision is made on the structure of Teams, the ICT groups role then becomes how to either enforce, or at least monitor, the structure.

Organisations that wish to strictly control the creation of teams to fit the defined structure, limit the creation of *teams* to a service desk request. Others are using tools such as the Microsoft PowerPlatform or ServiceNow to allow staff to fill in forms detailing the required *team*, then have the *team* created via automation.

Principle

- *Teams* match the work to be done

Questions

- How do staff currently work together
- How can they work together in a collaborative era
- How can staff, processes and information be connected to improve outcomes
- What 'ethical walls' are needed between teams of people
- Which external stakeholders (clients, suppliers, contractors, etc) to invite into our collaboration workspace, and why
- Who can create a *team*
- How are *teams* structured or templated
- Who will act as *team* 'owners' vs 'members'
- Will the organisation use *teams* templates

Better Practices

- Larger organisations: automate creation of *teams* based on staff requests and workflow tools
- Reduce number of *team* owners through automation or third-party tools. Consider treating owners as admin roles
- Small organisations with digital maturity: staff take control

Lifecycles for teams

Just as information lifecycles needs to be managed, so too do *teams* lifecycles. Depending on the structure of teams in an organisation, *teams* may be evergreen (such as department or process oriented *teams*) or temporary (such as case or project oriented *teams*). It is also not uncommon for *teams* to be created and then forgotten, or even orphaned when all people involved in the *team* leave.

Lifecycle management involves knowing when to retain and destroy specific *teams* based on the work activities being conducted and information held within those *teams*.

Teams lifecycles also need to be closely aligned to any information retention requirements needed to meet compliance or regulation. For example, if a *team* is set up to manage a large public-sector procurement effort, the documents created and shared within it may need to be archived and held for seven years for prosperity issues. By extension, the discussions and chats related to the procurement likewise need to be archived.

Principle

- *Teams* last only as long as the work

Questions

- How can existing information lifecycle policies be applied to *teams*
- How will the organisation define *teams* that are continuous vs temporary
- Who defines *teams* lifecycles
- What happens when a *team* comes to end-of-life

Better practices

- Automate the alerts for *teams* lifecycle
- Consider using Teams retention expiry policy to remove unused *teams*
- Ensure existing information management policies are applied to *teams* lifecycle

A note on Backup and Recovery

Existing tools (such as AvePoint, Veeam) or newer tools (such as ShareGate Apricot) can be applied to manage *team* lifecycles. However,

one area that is not well catered for is the recovery of the entire Teams environment from a backup. Most archival tools can result in only parts of Teams data, as it is spread over multiple environments. Therefore, consideration should be given to the likelihood of needing to recover Teams in the case of a catastrophic event (e.g. an insider attack), versus having backups of the critical information assets in their stores (SharePoint, Exchange) etc.

Teams archival

Closely related to *teams* lifecycle, discussed above, archival is a critical consideration. If the principle for lifecycle is that "*teams* last only as long as the work", the next question becomes "what happens to the *team* when the work is finished"?

As a starting point, organisations should review existing archival and information archival policies and overlay them to the *teams* structure.

However, this is complicated by the fact that a *team* contains a wide variety of information assets with different archival requirements. For example, documents and correspondence relating to financial transactions may need to be archived for the life of a contract plus seven years, though the conversations (chats) relating to those transactions may not be archived at all to meet privacy requirements.

Principle

- Adopt existing archive compliance

Questions

- What information native to Teams is to be archived
- What information outside of Teams is to be archived
- What information is already being archived, and how does Teams impact this process

Better practices

- Review existing archival approaches
- Consider third-party tools: e.g. Veeam, AvePoint

Access control for Teams

Like all collaboration tools, Teams is most useful when staff have the ability to bring people - including external stakeholders - into the work

environment to share information and communicate. By definition, when someone is invited into a *team*, they get to see all of the information and chat related to that *team*.

However, this also means there needs to be careful consideration as to who is given access to a *team*. It is not uncommon for a person to be invited into a *team* to review a specific document or to engage in a specific conversation, to then have access to sensitive information that perhaps they should not. It is easy to create an environment where oversharing of private or sensitive information occurs. In short, Teams is a significant new vector for information leakage, both internally and externally to the organisation.

Currently, many organisations are dealing with the above data leakage challenge by strictly controlling how people are added to *teams*. This is typically done by limiting who can invite others to access a *team*. The downside of this approach is that it hinders the ease of collaborative working.

The governance of Teams needs to consider who is the owner of each *team*, and to what extent they have control over granting access to the *team* and how they wish to manage the risks associated with information assets within the *team*.

One organisation IBRS interviewed allowed line-of-business managers to grant access to departmental *teams* (the ownership lay with the business managers), but not which documents should be uploaded into the Teams environment. Instead, all documents remained within the organisation's electronic document management solution (EDRMS), and only links to the EDRMS being shared in Teams. In this way, the ICT group enforced strict access control over the access to documents via the EDRMS, while allowing the business to take advantage of the collaborative environment of Teams.

However, most organisations IBRS have spoken with have approached the challenge of guest access by disabling guest access as a baseline defence, and strictly controlling who can grant access to each team via the ICT help desk.

Principle

- Access to *teams* is on a need to know basis

Questions

- What is the need for walled gardens (e.g. ethics)
- Who can grant access to a *team*
- What guardrails / tracking is needed for granting access
- Can external parties (guests) be given access? If so, who can grant guest access

Better practice

- If data leakage prevention technology is not implemented, disable guest access
- Limit the granting access rights
- Implement Microsoft's built-in security capabilities, and review frequently
- Share links to documents (held in EDRMS) rather than doc itself
- Link access to Identity Management lifecycle

Team member lifecycle

Just as important as granting access to teams is the need to monitor the lifecycle of people's *team* membership. Membership of *teams* should be audited regularly to ensure that only people that actively need access to the *team* retain such access, and all others are removed. Ideally, access to a *team* should be removed as soon as the person - especially an external stakeholder - no longer needs access.

Principle

- Remove *team* members immediately, but retain context

Questions

- How will people be added to and removed from *teams*
- Who decides
- When is membership reviewed
- What information must be retained after a member is removed

Better practice

- Leverage existing identity management (IDM) solutions for member management
- Ensure that when a staff member changes roles, their access to *teams* is also reviewed and updated accordingly - ideally via the IDM

- Automate archival of member information before removal

Organising & naming teams

Surprisingly, Teams has only the most rudimentary ability to apply tags to *teams*. This means it is difficult for administrators to quickly search for all *teams* that fit specific criteria, and perform governance or compliance related tasks. The lack of tagging also limited the potential to automate *teams* administration. In large organisations, it also means users are hindered in quickly locating the specific *teams* they may need for their job.

While IBRS believes Microsoft will add the ability for administrators to assign tags and possibly custom-fields to Teams in the future, currently organisations are being forced to adopt strict naming conventions - effectively using the *team* name to categorise or tag the *team*. Many organisations IBRS interviewed either add a prefix (or sometimes postfix) to the *team* name to classify each team.

Traditional information management skills must therefore be brought to bare on the naming of teams. The naming conventions must be matched to the structure of the business and the desired future state of the organisation, as discussed in Provisioning Teams, above.

IBRS notes that any naming conventions must be readily understandable by a typical staff member and possibly by external stakeholders.

The challenge with using prefixes in *teams* naming is that most staff are not consistent with how they apply such naming conventions. As a result some organisations have taken to only allowing the ICT help desk to not only setup, but also apply the name to each *team* request by the business stakeholders.

Principle

- Adhere to strict team naming conventions

Questions

- How will teams be named so they can be locally identified
- How will naming conventions be enforced
- What exceptions can exist to naming conventions

Better practice

- Build team naming codes into automated Teams provisioning if used
- Ensure naming codes are clear to all staff: prefix-suffix naming policies
- Watch for changes in Teams that may address the limitations of tags & plan to implement when available

Information Protection

Perhaps the most urgent governance issue to address with Teams is information protection. When staff and external parties work collaboratively, information will be overshared - it will leak.

While data leakage prevention (DLP) solutions can help reduce oversharing of information, it cannot address what happens once information is shared both internally or externally.

> In late 2020, Microsoft DLP solution moved into general availability. However, the Teams component of the DLP requires an O365 E5 or MS365 E5 license. Organisations with existing DLP solutions should consider the extent to which they may be applied to Teams, or look to the Microsoft solution, depending upon their current licensing level. Organisations without DLP should review the Microsoft solution, although using the availability of DLP as a case to move from an E3 to E5 license remains tenuous - the real need is Microsoft Information Protection, which is available in both E3 and E5 licensing, though with different levels of capability.

It is therefore vital that organisations look to adopt a new approach to protecting their information assets: one that assumes critical documents will eventually end up in the public domain.

The only viable approach is to adopt zero trust information protection: encrypting all information and only allowing reading (access to) the information via user authentication and contextual controls (where the document is being opened from, time, network, user behaviour, etc.).

Microsoft's solution for zero trust information project is a combination of its Access Control solution and its Microsoft Information Protection

(MIP, previously called Azure Information Protection). With MIP switched on, information originating within or added into the Office365 tenancy is encrypted, including information added into Teams. Accessing the information is defined by access rights rules, which can include personal identities, location, time, device, etc. Even when information is accessed from outside the organisations network, the access rights are still demanded.

However, for this zero trust environment to work, every information asset needs to be categorised in terms of its accessibility. This means that the organisation needs to first define the classification scheme it requires to protect information in the most appropriate and consistent way.

For example, categories may include information that is:

- only readable by board members,
- only readable by named human resources staff,
- be accessible by anyone in the business
- be viewed by external parties

Principle

- Everything is encrypted

Questions

- How are documents categorised in terms of risk
- What processes / technical guardrails are needed for each level of risk
- What architectural approach is used to secure information: DLP, third-party DLP, EDRMS, etc.

Better practice

- Assume that information will leak
- Adopt a DLP approach to minimise leakage and, more importantly, minimise the impact of leakage
- Embrace zero trust information management
- Explore Microsoft's approaches to information protections…but understand it comes with licensing uplifts

What's next

The seven critical areas of Microsoft Teams governance may look daunting. However, determining the resources you'll need and setting priorities to address each of these areas, plus any others that may be unique to your organisation, can be accomplished relatively quickly.

IBRS can assist you and your team by organising a Teams governance whiteboard session. In this session, our expert advisors will work with you and your team to set your organisations principles, identify the stakeholders needed to ensure the governance is sustainable, and establish working groups and objectives.

For more information on how IBRS can assist, please contact:

Nick Bowman
CEO, IBRS
Email: nbowman@ibrs.com.au