

## FINANCE, AUDIT AND RISK COMMITTEE

3 AUGUST 2022

AGENDA ITEM D2

PUBLIC EXCLUDED

### RISKS TO COUNCIL IT SYSTEMS AND ARCHITECTURE

#### **Purpose of Report**

To inform the members of Finance Audit and Risk Committee of the current and emerging risks relating to Council's IT systems and architecture.

#### **Recommendations**

Officers recommend that the Council:

1. *Receive the Risks to Council IT Systems and Architecture Report.*
2. *That this report and associated minutes stay in public excluded until the Chief Executive determines there are no longer any reasons to withhold the information under the Local Government Official Information and Meetings Act.*

#### **1. Executive Summary**

The expectations on Council's (Information Technology) IT services are significant. Our current strategy of moving to a customer-focused culture while modernising and standardising our core services and processes is highly dependent on IT for success.

The desire for accurate and timely data and reporting that support decision-making, and for the removal of paper from processes and automation can only be fulfilled with investment in IT. Furthermore, the consumerisation of IT with readily available and continuously improving applications and services has raised the expectations staff have of the quality of the digital experience they receive.

The drive to consolidate and standardise IT architecture and applications to manage cost and reduce risk is ongoing. At the same time, new IT service delivery models such as 'cloud' services provide both opportunities and challenges for our IT services.

Moving forward requires a balanced approach between sustaining IT services and driving and supporting innovation. To achieve this, there is a need for stronger strategy, planning, and value management across our IT architecture.

At the same time, Council needs to address greater compliance, business continuity/disaster recovery, security, and privacy concerns and maintain or retire existing services.

Previous levels of investment in our IT architecture have not kept pace with the evolving needs of our organisation. Historically, there hasn't been the appetite for increasing our spend on our IT architecture and systems, instead adopting a patchwork approach. This has meant that our IT architecture is now not fit for purpose and presents an unnecessary risk to Council operations.

We must transform the function of IT to be responsive and agile, to support and enable new delivery options while maintaining the integrity of our services.

## **2. The impact of local government reform on our IT investment needs**

The local government sector is likely to face major challenges in managing future information technology requirements. Local authorities are complex organisations which manage multiple databases and information systems and engage with their communities online in numerous ways.

In coming years there will be considerable demand on the sector to align systems, digitise records, manage increasingly complex cybersecurity issues, and develop systems that provide customers and residents the best and most seamless online services. This can be expected to impose significant costs and demands on local authorities, including those which already face staffing and capacity constraints.

## **3. Past IT service provision**

Whilst our future plan will address the twin objectives of quality IT services that ensure we operate effectively, and digital transformation that enables us to enhance our services and effectiveness, this is currently not the case.

Until recently we have run an on-site IT administrator support model. This has meant that any issues that arose that required significant investment were often out of budget and required us to outsource the work as it was unrealistic to expect one moderately skilled IT resource to have expertise in all IT disciplines.

## **4. IT services and methodology – moving forward**

Our adopted investment focus is on freeing funds from “maintaining services” through a program of standardisation and consolidation so that we can invest in transformation programs that are aligned to Council’s strategic imperatives and bring the most value to us.

With the departure of our sole IT resource, the Executive took the decision to vary the existing agreement with our long-standing IT trusted specialist provider, Tech Planet. This move allowed us to maintain levels of service, whilst also having ‘on tap’ a vast array of additional expertise never before available. Our new service provider model

delivers services where cost effectiveness, scale and standardisation are the key drivers as well as delivering discrete solutions and local services. We now view our IT support in two ways:

#### **4.1 Quality IT Services**

- Focus on service quality and effectiveness through the provision of performing and resilient services that meet the broadest organisational need.
- Enhance integrated IT support using high-quality staff, knowledge sharing, and relationship building.

#### **4.2 Digital transformation**

- Build and maintain a resilient IT architecture.
- Support staff to utilise and exploit technology to seek our information and resource and innovate.
- Understand and improve the user (employee, elected members, public) experiences to enhance service outcomes. We will grow our understanding of the journey's that they follow, and use analytics and enhanced processes to improve service effectiveness.
- Improve organisational performance by optimising business processes across Council, removing paper forms and automating workflows.
- Enhance the quality and accessibility of key information for decision-makers.

### **5. Investment analysis**

There are many forces at work that will influence IT expenditure and investment during the coming years. These include the adoption of cloud services, increased user mobility, rapidly improving digital literacy, an increasingly complex regulatory environment, and an ever-evolving cybersecurity threat-scape.

The ongoing maintenance of legacy systems and outmoded services can be expensive and can consume an ever-growing portion of the available resources if not actively managed.

To respond to these forces the Council must constantly review IT services and the value they provide and adapt accordingly.

#### **5.1 Stages of required IT transformation and change**

Council is at a critical stage of its development in terms of its IT investment. Much has yet to be done to get us to a place where we can trust in having the basics in place. For this reason, the roadmap will look as follows:

**Phase 1: Change Control** – we need to review how we provide access to our systems, cyber risks, management of privacy, access to files/folders, remote access, business continuity, security etc. This is all about getting the basics right and professionalising how we operate day to day. It is also about ensuring that any in progress projects are factored into our long terms IT plans (digitisation, Majiq moving to the cloud)

**Phase 2: Automation** - How we manage hardware updates, push software updates, logging and resolution of jobs by end users, systematising our IT processes to remove duplication of effort and reduce human error and interactions, operating dashboards etc.

**Phase 3: Proactive** – How we manage our IT assets, invest further in our architecture, complementary projects i.e., digitisation, upskilling staff on SharePoint, and thinking ahead in terms of how we enable better and more efficient ways of working, through the use of technology.

Quality IT services and architecture must be maintained and improved. The Council will need to continue to standardise, simplify, and automate core services with the goal of streamlining IT operations.

As with our recent move to 'Desktop as a Service' (DAAS) via Tech Planet, selective sourcing will be utilised for some core activities i.e., Helpdesk services, within the constraints of Council's Procurement Policy.

## **6. Statement of immediate Risks**

### **6.1 System architecture and software**

- a. Our servers are approaching 'end of life'. This means that Microsoft will not be actively maintaining or updating the server software from October 2022.

**Risk:** If two of four servers fail, there is a risk that any data stored will not be retrievable.

### **6.2 Disaster recovery, business continuity and backups**

- a. VMware is our 'cloud' computing software. The license must be renewed in July, but in due course will be packaged up with our wider disaster recovery approach.

**Risk:** Failure to renew would mean that we would be operate our cloud enabled platforms to operate.

- b. Our disaster recovery system consists of using older servers located at the Palmerston North centre.

**Risk:** The servers are coming to the end of their life.

- c. The current backup cycle to our disaster recovery server, is not live, but takes place at the end of each day only.

**Risk:** As a full backup process is not in place, we risk not having a useable copy of our data to work with in case of a disaster.

- d. One of our servers is backing up to itself, rather than to a backup server.

**Risk:** Backing up information to itself is pointless and would result in data loss in case of disaster.

- e. Our lessons learned from our operational response to the Covid pandemic showed that we faced several and varied IT issues.

**Risk:** Instances of Covid or similar risk, are likely to re-emerge, and our system architecture needs to be of a standard that allows us to operate efficiently and effectively.

### 6.3 IT transition

- a. Since transitioning to (Desktop as a Service) DAAS, there are certain services that we have not been able to migrate, due to the operational risks. How we migrate them, needs to be well considered and planned.

**Risk:** Not migrating them will result in duplication of effort and cost.

- b. The cost savings that we hoped would be realised at the start of the financial year, from these services, are now being carried over, and will continue until such a time that a detailed transition plan can be developed. The services in question are telephony, disaster recovery management, and the hosting of the disaster recovery servers in Palmerston North.

**Risk:** Without an expediting the previous points made, we will not be able to migrate these services, thus continuing to incur unnecessary costs.

## 7. Management of the risk

All risks have been captured in the Risk Register and are being appropriately managed by ELT. The risks outlined above are a list of the most pressing risks.

## 8. Conclusion and next steps

We are on a journey towards most of Council's IT services and resources being secure, safe, and automated. Services are expected to be delivered economically via cloud-based solutions that best fit the business need. Council networks, services, and applications will be resilient, proactively monitored, and protected. Analytics will be captured and utilised to drive service improvement and service strategy. With respect to cyber risks, we will modernise our cybersecurity by integrating advanced security technologies that protect the business and its data while also reducing total cost of ownership.

For us to achieve these objectives, our priority is to first address our immediate IT risks, and respond to IT failures, but have a plan in place to focus on longer term proactive maintenance.

In this initial report, our current and future state has been outlined, as well as a high-level roadmap for our IT transitional plans. With these plans, over the coming weeks and months, will come a need for additional budget to be assigned to addressing these critical business needs.

## **9. Appendices**

Appendix 1 – Council IT Systems and Architecture PowerPoint Presentation

Contact Officer: Paul Gardner, General Manager, HR and Corporate Services

Reviewed By: Harry Wilson, Chief Executive Officer

# **Appendix 1 – Council IT Systems and Architecture PowerPoint Presentation**



# COUNCIL IT SYSTEMS AND ARCHITECTURE

Paul Gardner

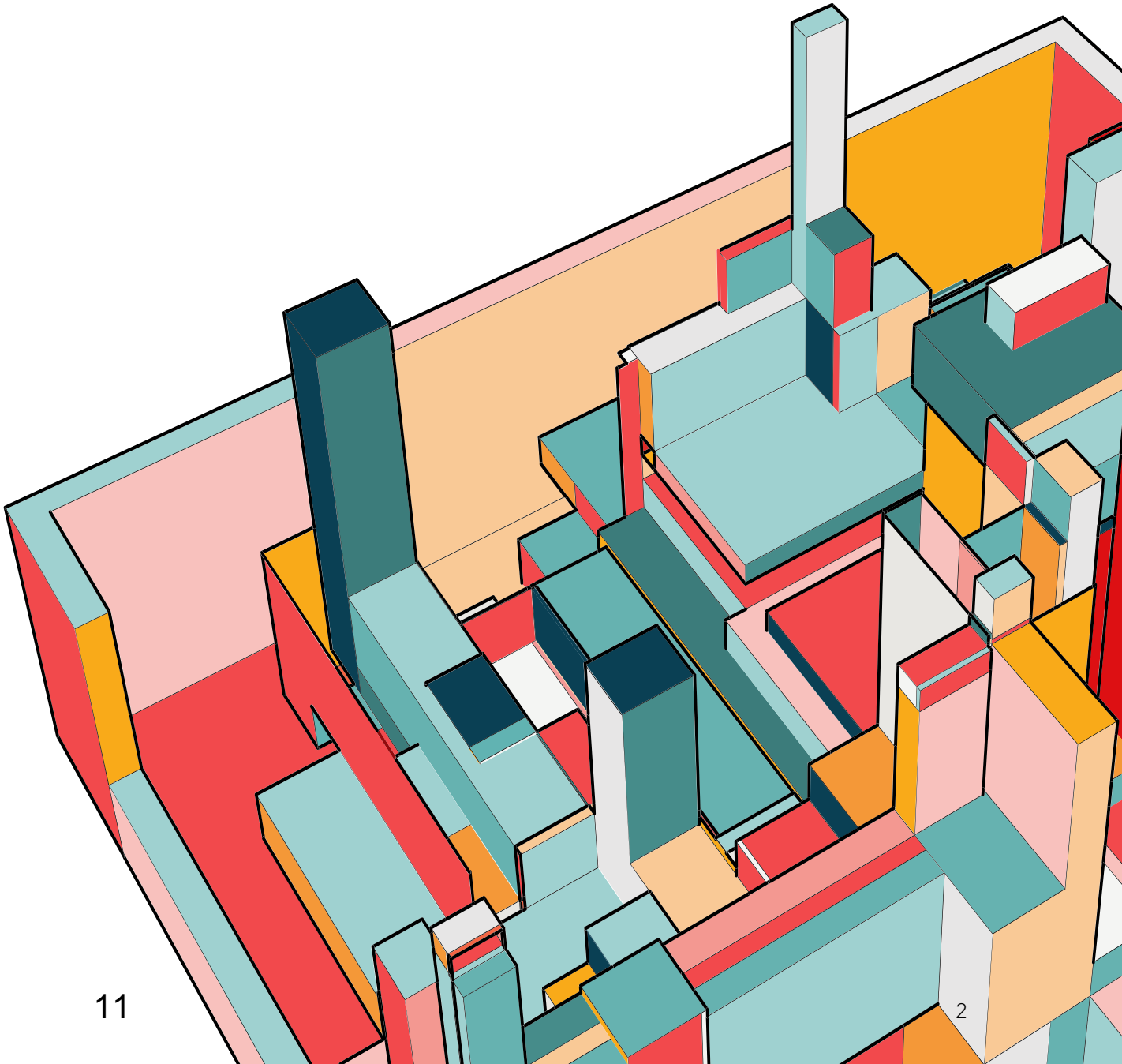
General Manager, HR & Corporate Services



SOUTH WAIRARAPA  
DISTRICT COUNCIL  
*Kia Reretahi Tātau*



# THE PROBLEM





# STAGES OF REQUIRED IT TRANSFORMATION & CHANGE

## 1: Change Control

Getting the basics right and eliminating/reducing immediate Disaster Recovery (DR), security, aged assets and backup risks

## 2: Automation

How we manage hardware updates, push software updates, logging and resolution of jobs by end users, systematising our IT processes

## 3: Proactive

How we manage our IT assets, invest further in our architecture, complementary projects i.e., information management/digitisation, website, intranet

# NEW IT SERVICE DELIVERY MODEL

How we'll scale in the future

## Level 1

### Change Control

Desktop as a service (DaaS)

## Level 2

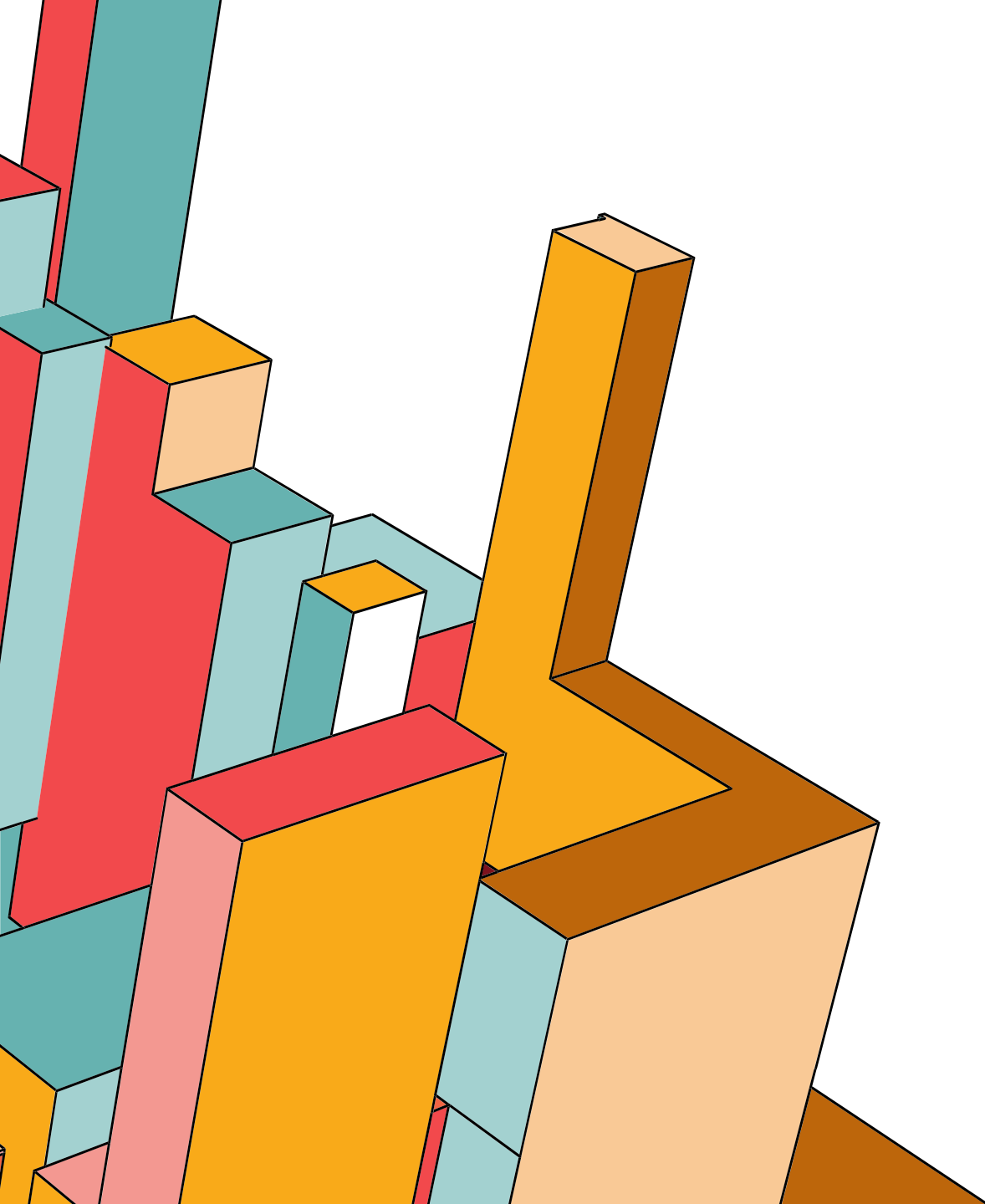
### Automation

Significant BAU  
Service improvement  
Transitioning to the Cloud  
Software as a Service (SaaS)

## Level 3

### Proactive

Projectised work i.e. Information  
Management with ringfenced  
budgets  
PMO / PM managed



# IMMEDIATE HIGH-LEVEL RISKS FOR FY 22/23

- System architecture, hardware and software
- Disaster recovery, security, business continuity and backups
- IT transition

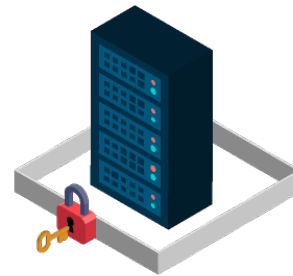
# RED TASKS: INDICATIVE FUNDING REQUIRED FY 22/23



VMWare, SERVER  
2016

\$80,000

Estimate costs only for  
replacement



SYSTEM  
HARDENING

\$28,000  
Plus \$6,000 annually

Estimated costs only  
for servers, operating  
systems, applications  
and databases



SECURITY

\$42,000  
annually

Estimated costs only for  
security/restrictions for  
working remotely/offsite -  
inc Identity Mngt



BACKUP & DISASTER  
RECOVERY

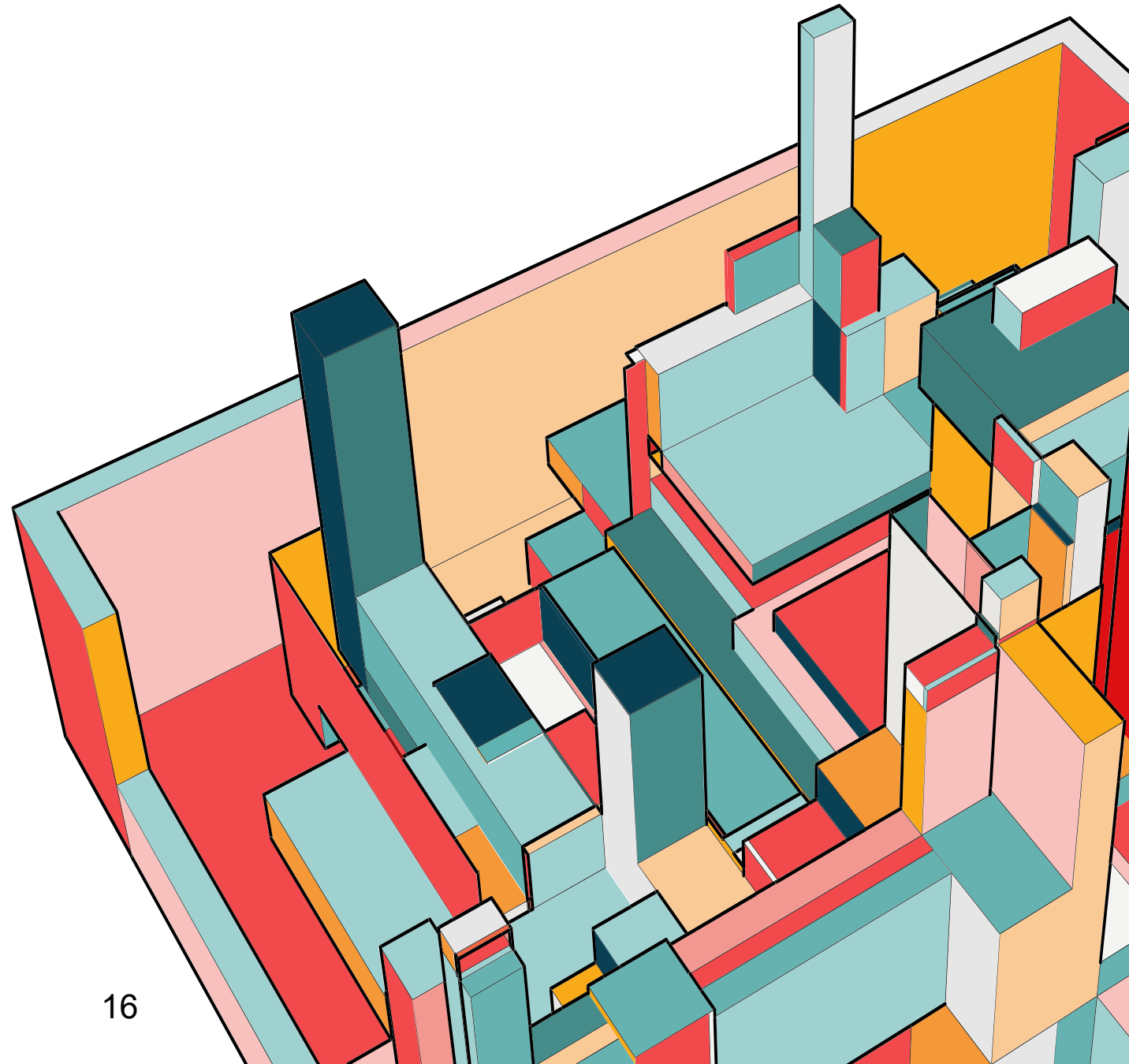
\$75,000  
annually

Access and  
functionality to IT  
infrastructure after  
natural disaster, cyber  
attack, or business  
disruptions

# SUMMARY UP FRONT COSTS **RED TASKS** FOR YEAR 1: FY 22/23

\$225,000 (estimated)

including year 1 of  
recurring annual costs



# AMBER TASKS: TASKS FY 23/24



## DEVICE ENROLEMENT

\$27,000  
Plus \$12,000  
annually

Estimate costs only



## DENIAL OF SERVICE

\$6,000 annually

Estimate costs only:  
Protection against  
ransomware attacks



## PENETRATION TESTING

\$9,500  
annually

Estimated costs only for A  
simulated cyberattack on  
our system, performed to  
evaluate the security of the  
system



## MULTI FACTOR AUTHENTICATION

\$20,000

Self service

# ADDITIONAL FOR YEAR 2: FY 23/24

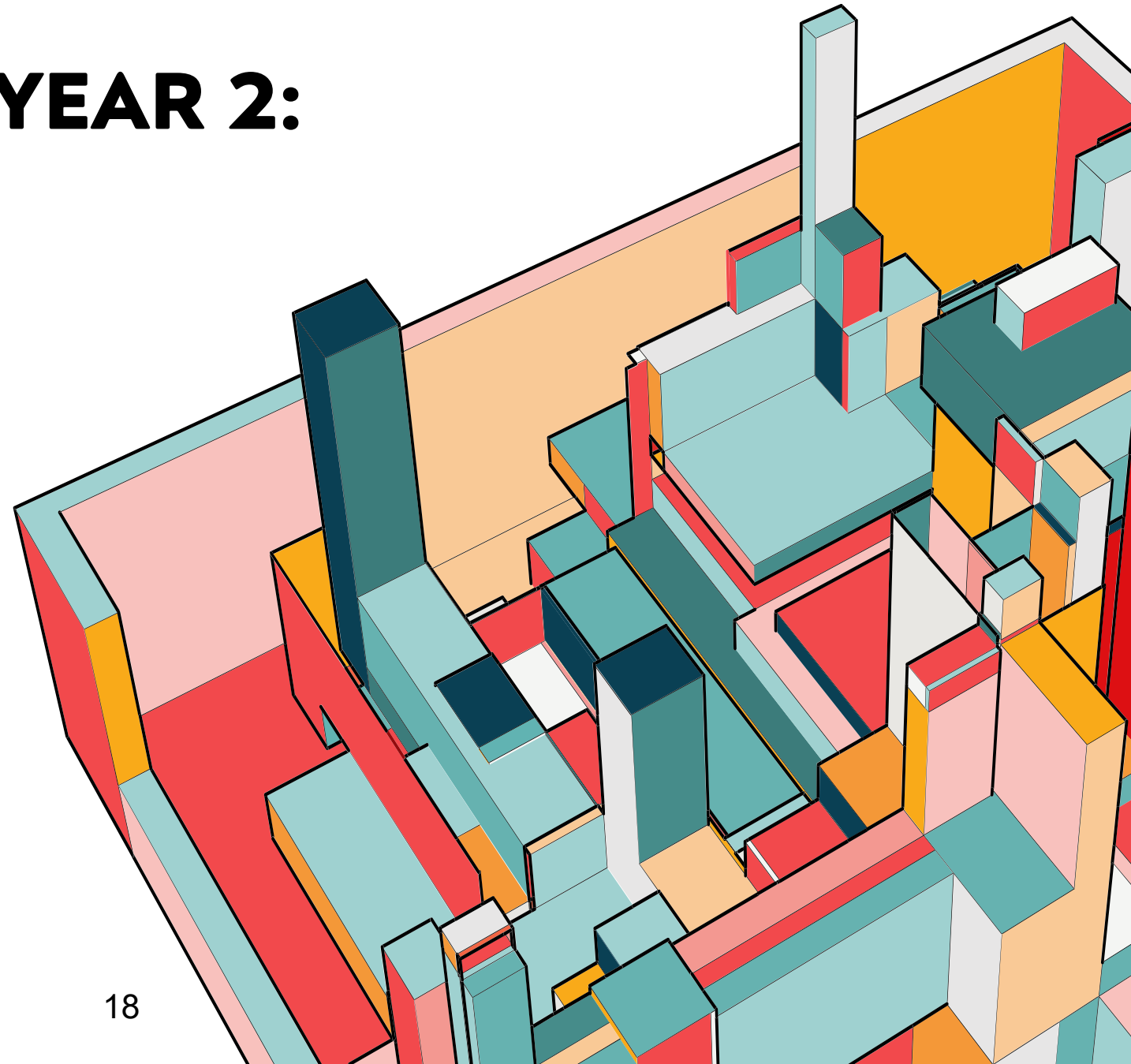
(BUILD INTO ANNUAL PLAN)

**Red tasks** (Recurring  
annual costs)

\$123,000

**Amber tasks**

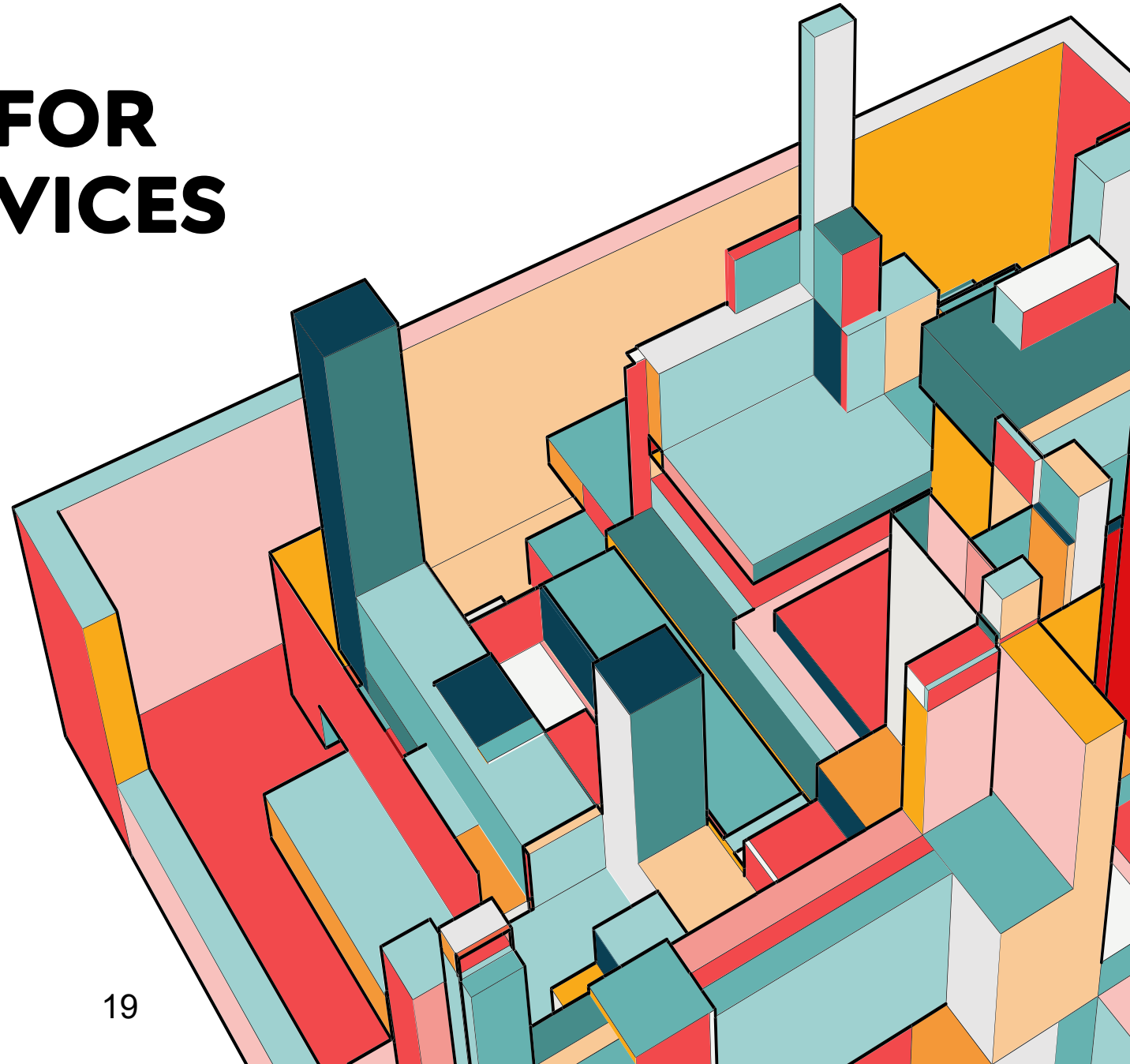
\$62,500





# SUMMARY COSTS FOR NEW ANNUAL SERVICES BEYOND YEAR 2

\$150,500  
(as part of annual  
planning)



# SIGNIFICANT POINTS TO NOTE

- Maintenance is crucial - investment is ongoing year to year, not one off
- **RED** tasks cannot be delayed
- Backup to the Cloud has already started at a cost of \$15,000
- These are high level costs only. As we turn over rocks, we may find more issues
- Work has started on what can be CAPEX versus OPEX
- These costs are in addition to our licensing, software and renewals of individual hardware

